Bundesamt für Sicherheit in der Informationstechnik

Federal Agency for Security in Information Technology

IT Baseline Protection Manual

October 2000

Bundesamt für Sicherheit in der Informationstechnik

IT Baseline Protection Manual

Standard Security Measures

Version: October 2000

Preface

The IT Baseline Protection Manual contains standard security safeguards, implementation advice and aids for numerous IT configurations which are typically found in IT systems today. This information is intended to assist with the rapid solution of common security problems, support endeavours aimed at raising the security level of IT systems and simplify the creation of IT security policies. The standard security safeguards collected together in the IT Baseline Protection Manual are aimed at a protection requirement which applies to most IT systems.

For the majority of IT systems, this considerably facilitates the task of drawing up a security policy, hitherto a labour-intensive process, by eliminating the need for extensive, and often complex, analyses of threats and probabilities of occurrence. If the manual is used, all that is required to identify security shortcomings and specify appropriate security measures is to compare the target safeguards presented here with the actual safeguards in operation.

The IT Baseline Protection Manual has been created so that it can be continuously updated and extended. It is revised every six months to incorporate suggestions for improvements, additional material and reflect the latest IT developments. I would like to thank those users of the IT Baseline Protection Manual who have contributed to this version.

Dr. Dirk Henze

What's new in the October 2000 version of the IT Baseline Protection Manual

Margin notes

On the replacement pages, margin notes have been inserted in the Comments column. These margin notes are intended as keyword pointers to the content of the material contained in each section of the document.

Footers

Pages which have been added to the manual for the first time or have had their content updated can be identified by the entry "October 2000" in the footer. Where the only change to have been made on a page is the change of spelling to comply with the new spelling rules or the addition of margin notes, the issue date shown in the footer has not been changed. In this way it is possible to tell directly from the footers which pages have had their content changed.

WWW pages on IT baseline protection

The Bundesamt für Sicherheit in der Informationstechnik (BSI, German Information Security Agency) can also be found on the Internet. You can read about the latest developments in IT baseline protection on the BSI's website at http://www.bsi.bund.de/gshb. This site contains a forum for presenting the latest information on the IT Baseline Protection Manual.

Updating and revision

No structural changes have been made in the new edition. The numbering of existing threats and safeguards has been retained so that a security policy prepared on the basis of last year's IT Baseline Protection Manual does not need to be revised. Nevertheless, we recommend that users read the selected safeguards in the revised version in full to enable them to take these new items into consideration and, if appropriate, brush up their knowledge of IT security issues. To identify accurately which parts of the documents have been changed, please refer to the Word version comparison which is contained on the CD in the ../VGL directory (currently German version only).

Development to meet users' needs

The manual has been developed further to meet the needs expressed by registered users during the year.

The following new modules have been prepared for the 2000 version:

- 3.0 IT Security Management
- 7.6 Remote Access
- 8.6 Mobile Telephones

Changes in the content

Chapters 1 and 2 have undergone substantial change of content. In this revised version the previous Chapter 1 "IT Security Management" has been integrated into the modules of the manual.

IT Baseline Protection Certificate

As the IT Baseline Protection Manual with its recommendations as to standard security safeguards has come to assume the role of an IT security standard, it is fitting that it should be used as a generally recognised set of IT security criteria. Having received frequent enquiries as to whether it is possible to

have the security level certified, the BSI has decided to develop a Baseline Protection Certificate. The relevant technical details are to be found in Section 2.7 "IT Baseline Protection Certificate".

CD-ROM

A revised electronic version will be available approx. six weeks after publication of the printed edition. Anyone wishing to receive this CD version should send a stamped (DM 3 if within Germany) addressed envelope (C5 format) to the following address:

Bundesamt für Sicherheit in der Informationstechnik (German Information Security Agency)

BSI IT Baseline Protection CD-ROM

Postfach 20 03 63

D-53133 Bonn

GERMANY

Management report

The last few pages of the manual contain a list of registered users of the IT Baseline Protection Manual. This list provides a summary of the industries, companies and official bodies in which IT baseline protection is used.

Table of Contents

Catalogues of Safeguards and Threats

Safeguards Catalogues

Threats Catalogues

Introduction

IT Baseline Protection - the Basis for IT Security

In our modern information and communication society, administrative tasks, both public and in industry, are increasingly routinely supported by the use of information technology (IT). Numerous work processes are electronically controlled and large amounts of information are stored in digital form, electronically processed and transferred on local and public networks. Many tasks performed within both the public and private sectors are simply not possible without IT, while others can only be partially performed without IT. Consequently many public or private sector organisations are totally reliant on the correct functioning of their IT assets. An organisation can only achieve its objectives if IT assets are used in a proper and secure manner.

There are many ways in which organisations depend on the correct functioning of IT resources. The financial success and competitiveness of companies is dependent on IT, so that ultimately jobs themselves depend directly on the functioning of IT assets. Whole industrial sectors such as banking and insurance, the car industry and logistics depend critically on IT today. At the same time, the well-being of every citizen also depends on IT, whether it is a matter of his job, satisfaction of his daily consumer needs or his digital identity in payment transactions, in communications and increasingly in e-commerce. As society becomes more dependent on IT, so the potential social damage which could be caused by the failure of IT resources increases. As IT resources of themselves are not without their weaknesses, there is justifiably great interest in protecting the data and information processed by IT assets and in planning, implementing and monitoring the security of these assets.

The potential damage which could result from malfunction or failure of IT assets can be assigned to several categories. The most obvious of these is loss of availability: if an IT system is out of service, no money transactions can be carried out, online orders are impossible and production processes grind to a halt. Another issue frequently discussed is loss of confidentiality of data: every citizen is aware of the necessity of maintaining the confidentiality of his person-related data, every company knows that company-confidential data about its sales, marketing, research and development would be of interest to competitors. Loss of integrity (the corruption or falsification of data) is another issue which can have major consequences: forged or corrupt data results in incorrect accounting entries, production processes stop if the wrong or faulty input materials are delivered, while errors in development and planning data lead to faulty products. For some years now, loss of authenticity, i.e. the attribution of data to the wrong person, has come to be regarded as another major aspect of the general concern regarding data integrity. For example, payment instructions or orders could be processed so that they are charged to a third party, digital declarations of intent that have not been properly protected could be attributed to the wrong persons, as "digital identities" are falsified or become corrupt.

This dependency on IT will only increase further in the future. Developments worthy of particular mention include the following:

- **IT penetration**. More and more areas are coming to be supported by information technology. For example, a shift in consumer behaviour towards e-commerce is taking place, car and traffic routing technology is being perfected with IT support, intelligent domestic appliances are looming on the horizon, and even waste disposal containers fitted with microprocessors are now in use.
- **Increasing degree of networking**. IT systems today no longer function in isolation but are becoming more and more heavily networked. Networking makes it possible to access shared data resources and to work closely with people in other parts of the world. This in turn leads not only to

dependence on the individual IT systems but increasingly also on the data networks. On the other hand, this means that security deficiencies in an IT system can rapidly spread across the world.

- **Propagation of IT resources**. More and more areas are supported by information technology. For example a shift in consumer behaviour towards e-commerce is taking place, car and traffic routing technology is being perfected with IT support, domestic appliances can now be programmed and networked.
- **Greater power**. The continuing trend towards miniaturisation is enabling an increase in the performance of hardware technology, so that ever more processor-intensive tasks can be shifted to decentralised computers or even to microprocessors. This is particularly evident in the area of smart card technology. Modern multi-function smart cards can be used to effect payment transactions, collect time-keeping information, enable access controls and perform highly complex mathematical encryption operations. The performance increase in the hardware also allows elaborate software algorithms, which a decade ago could only be performed on a mainframe computer, to be implemented in microcomputers. New ideas aimed at employing software as a kind of mobile code which, for example, could autonomously seek out competitively priced suppliers of certain goods on the Internet, are currently taking shape.

All this implies a disproportionate increase in the potential threats, due to the co-existence and interaction of multiple factors:

- Dependence on IT and hence vulnerability is increasing, as described above.
- Responsibility for implementing IT security measures is often spread over many individual persons. The complexity of the problems which can occur in the IT security area means that individuals with such responsibilities rapidly become out of their depth.
- Knowledge of threats and IT security safeguards is inadequate. Because of the short length of time it takes to develop IT innovations, it is difficult to be fully informed as to all the new or newly discovered threats and the countermeasures that are necessary. In many cases there is also uncertainty as to what security measures are appropriate to counter a given threat.
- Finally, the increasing functionality available actually broadens the front over which an IT system is vulnerable to attack. Security loopholes which could be exploited to perpetrate an attack are always being discovered in protocols and network services and also in local application software.
- IT systems are progressively becoming more open towards the outside world, e.g. as a result of networking, Internet access and maintaining a presence on the Internet. But this only means that the number of persons who could potentially attack an IT system is increased.

When considering the threat potential, a distinction should be made between loss or damage which is the result of wilful action and that which is caused by "chance events". This latter category includes problems which are the result of force majeure, technical failures, carelessness and negligence. Statistically, these "chance events" are the ones which, collectively, cause the most damage. By contrast, damage which is attributable to wilful action occurs more seldom, but when it does occur the consequences are often more serious. The perpetrators may be driven by the desire for revenge, envy or personal enrichment, or they may simply find it fun to wreak havoc on IT systems. Both in the deliberate and unintentional case, an additional distinction can be made as to whether the cause of the damage lies within or outside of the company or agency. It should be noted in this context that most IT damage which is the result of deliberate action can be attributed to "insiders".

In view of the potential threats outlined above and the increasing dependence on IT resources, every enterprise, whether a company or an official body, must ask itself several key questions regarding IT security:

- How secure are the IT assets of the organisation?
- What IT security measures need to be taken?
- How do these measures specifically need to be implemented?
- How can an organisation maintain and/or improve the level of security it has attained?
- How secure are the IT assets of other institutions with which the organisation works?

When seeking answers to these questions, it should be noted that IT security is not just a technical issue. Protection of an IT system to the level of security that is needed requires not only technical safeguards to be implemented but also measures covering organisational, personnel and building infrastructural aspects, and, in particular, it is necessary to establish IT security management roles which will be responsible for designing, co-ordinating and monitoring the IT security-related tasks.

If one now compares the IT assets of all institutions against the questions postulated above, a special group of IT assets emerges. The IT assets in this group may be characterised as follows:

- They are typically IT systems i.e. these systems are not individual solutions but are widely distributed.
- The protection requirements of the IT systems with regard to confidentiality, integrity and availability are nothing out of the ordinary.
- The secure operation of the IT systems requires standard security measures from the areas of infrastructure, organisation, personnel, technology and contingency planning.

If it were possible to identify a common set of security measures for this group of "typical" IT systems - a set of standard security measures - then this would significantly assist answering the above questions for those "typical" IT systems. Many of the protection requirements of IT systems which lie outside this group, possibly because the systems concerned are more unusual, customised systems or because they have very high protection requirements, can then be satisfied by implementing the standard security measures, although ultimately these systems need to be considered separately.

The IT Baseline Security Manual presents a detailed set of standard security measures which apply to virtually every IT system. It provides:

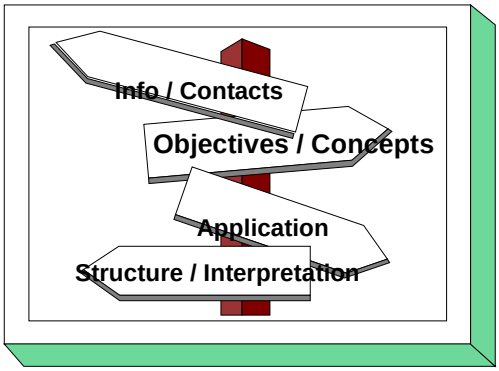
- standard security measures for typical IT systems with "normal" protection requirements,
- a description of the threat scenario that is globally assumed,
- detailed descriptions of safeguards to assist with their implementation,
- a description of the process involved in attaining and maintaining an appropriate level of IT security and
- a simple procedure for ascertaining the level of IT security attained in the form of a target versus actual comparison.

Because information technology is a highly innovative area and is constantly undergoing further development, the present manual is designed to be easily updated and expanded. The BSI continuously updates the manual and expands it to include new subjects on the basis of user surveys.

The response to this is very positive. In the Annex to the manual you will find a list of some of the organisations which use the IT Baseline Protection Manual. This list provides a summary of the industries, companies and official bodies in which IT baseline protection is applied.

As the manual is also held in high esteem internationally, an English-language version of it is also available in electronic form.

1 Finding Your Way Around the IT Baseline Protection Manual



1.1 IT Baseline Protection: the Aim, Concept and Central Idea

The IT Baseline Protection Manual presents a set of recommended standard security measures or "safeguards", as they are referred to in the manual, for typical IT systems. The aim of these IT baseline protection recommendations is to achieve a security level for IT systems that is reasonable and adequate to satisfy normal protection requirements and can also serve as the basis for IT systems and applications requiring a high degree of protection. This is achieved through the appropriate application of organisational, personnel, infrastructural and technical standard security safeguards.

To facilitate structuring and processing of the highly heterogeneous area of IT, including the operational environment, the IT Baseline Protection Manual is structured in a modular fashion. The individual modules reflect typical areas in which IT assets are employed, for example client/server networks, buildings, communications and application components Every module begins with a description of the typical threats which may be expected in the given area together with their assumed probability of occurrence. This "threat scenario" provides the basis for generating a specific package of measures from the areas of infrastructure, personnel, organisation, hardware, software, communications and contingency planning. The threat scenarios are presented in order to create awareness, and are not required any further for the creation of a security concept which affords IT baseline protection. It is not necessary for users to perform the analysis work mentioned above, which requires considerable effort, in order to attain the security level that is needed for an average protection requirement. On the contrary, it is sufficient to identify the modules which are relevant to the IT system or IT assets under consideration and to implement all the safeguards recommended in those modules in a consistent manner.

Using the IT Baseline Protection Manual, it is possible to implement IT security concepts simply and economically in terms of the resources required. Under the traditional risk analysis approach, first of all the threats are identified and assigned a likelihood of occurrence, and the results of this analysis are then used to select the appropriate IT security measures, following which the remaining residual risk can be assessed. The approach adopted in the IT Baseline Protection Manual on the other hand requires only that a target versus actual comparison is performed between the recommended measures and those already implemented. The security shortcomings which need to be eliminated through adoption of the recommended measures are defined in terms of those security measures identified which are lacking and not yet implemented. Only where the protection requirement is significantly higher is it necessary to also carry out a supplementary security analysis, weighing up the cost-effectiveness of implementing additional measures. However, it is generally sufficient here to supplement the recommendations made in the IT Baseline Protection Manual with appropriate tailored and more stringent measures.

The safeguards listed in the IT Baseline Protection Manual are standard security measures, i.e. measures which should be implemented for the modules concerned using the latest available technology in order to achieve a reasonable level of security. In some cases these safeguards also provide a higher level of protection than that required simply to implement a baseline level of protection; nevertheless, they are the minimum security precautions which it is reasonable to implement in the areas concerned.

Security concepts which are drawn up using the IT Baseline Protection Manual are compact, since all that is required within the concept is to reference the relevant safeguards in the manual. This makes them easier to understand and view in perspective. To facilitate implementation of the recommended measures, the safeguards are described in sufficient detail in the manual that they can serve as specific implementation instructions. With regard to the technical terminology used, care has been taken to ensure that the safeguard descriptions will be comprehensible to those who have to implement them. Accordingly, a distinction is made in the style and terminology used between safeguards which need to be implemented by an experienced administrator and those which a user is expected to implement.

To simplify implementation of the safeguards, the text of the manual is also available in its entirety in electronic form. In addition, implementation of the safeguards is also supported by aids and sample solutions, some of which have been provided by the BSI and some by users of the manual.

Bearing in mind the pace of innovation and version changes in the IT area, the IT Baseline Protection Manual has been designed so as to make it easy to expand and update. It therefore has a modular structure incorporating modules and catalogues and, as a collection of loose-leaf sheets, it is easy to expand. The BSI re-works and updates the existing modules at regular intervals in order to keep the recommendations made in the manual in line with the latest technological developments. In addition, new modules are regularly added to the existing body of documentation. In updating the IT Baseline Protection Manual, the BSI is guided by requests expressed by users which are obtained regularly from surveys. Only in this way can it be sure that in the long-term the document evolves in line with users' requirements. The BSI therefore offers all users the opportunity to register on a voluntary basis. Registration is free of charge. Registered users received information at regular intervals about topical subjects. Its pool of registered users also serves as the basis for its user surveys. It is only through a continuous exchange of experiences with users of the manual that the document can evolve in a manner which reflects users' needs. One of the aims of the BSI's efforts here is to be able to give up-to-date recommendations on the kinds of IT security problems currently actually experienced. Recommendations which are not continuously updated and expanded rapidly become out of date or else of necessity they become so generic that they fail to deliver the intended benefit of identifying security weaknesses and simplifying the specific task of implementing security measures.

1.2 Structure and Interpretation of the Manual

The IT Baseline Protection Manual is divided into five main areas. To facilitate understanding of the manual, a brief explanation is provided here of each of these areas.

Introduction and procedure

This first section comprises Chapters 1 and 2. These chapters introduce the concept of IT baseline protection, present guidance as to how to use the manual and how to move between topics in the manual, and discuss the procedure to be adopted in drawing up a security concept which affords IT baseline protection. To understand the manual, it is important to work through Chapter 2. This describes in detail what steps are necessary in order to achieve a "baseline protection" level of IT security. In particular, it explains how to map an existing IT infrastructure onto the various manual modules and how to perform and document a target versus actual comparison where the target state of affairs corresponds to IT baseline protection.

Modules

The second section of the manual comprises Chapters 3 to 9. These chapters contain the threat scenario and the safeguards that are recommended for various components, procedures and IT systems. In each case the relevant safeguards are gathered together in a single module. They are logically grouped into the following chapters:

Chapter 3: IT Baseline Protection of Generic Components
Chapter 4: Infrastructure
Chapter 5: Non-Networked Systems
Chapter 6: Networked Systems
Chapter 7: Data Transmission Systems
Chapter 8: Telecommunications
Chapter 9: Other IT Components

Threats Catalogues

This section of the manual contains detailed descriptions of the threats which are included in the threat scenarios for the individual modules. The threats are grouped into five catalogues:

T1: Force Majeure
T2: Organisational Shortcomings
T3: Human Error
T4: Technical Failure
T5: Deliberate Acts

Safeguards Catalogues

This section provides detailed descriptions of the IT security safeguards mentioned in the various modules of the manual. The measures are grouped into six catalogues of safeguards:

S 1: Infrastructural safeguards
S 2: Organisational safeguards
S 3: Personnel safeguards
S 4: Safeguards relating to hardware and software
S 5: Communications safeguards
S 6: Contingency planning safeguards

Annexes

The last section of the manual contains supplementary aids, forms, brief descriptions of tools covering all aspects of IT baseline protection and a list of registered users of the manual.

Interpretation of the manual

The modules, which all have the same structure, form the most important part of the IT Baseline Protection Manual. Each module starts with a brief description of the component, procedure or IT system under consideration.

This is followed by a description of the threat scenario. The threats here are divided into the aforementioned categories of Force Majeure, Organisational Shortcomings, Human Error, Technical Failure and Deliberate Acts.

To make it easier to see which modules are relevant and to avoid redundancies, in each case only a reference is provided to the text in which the threat is described in more detail. An example is provided below as to how a threat would be cited within a module:

- T 4.1 Disruption of power supply

In the code T x.y, the letter "T" stands for threat. The number x before the decimal point refers to the Threats Catalogue (in this case T 4 = Technical Failure) and the number y after the decimal point is the serial number of the threat within the catalogue concerned. This is followed by the name of the threat. It is recommended that the user then reads the text of the threat referenced for the sake of gaining awareness and understanding the safeguards which apply, but it is not absolutely essential to read this text in order to be able to draw up an IT security concept on the basis of the IT Baseline Protection Manual.

The recommended safeguards which are listed after the section on the threat scenario constitute the major part of a given module. Brief information is presented first of all on the safeguard package concerned. In some modules these statements contain, for example, information on the recommended sequence to follow in implementing the necessary safeguards.

As was done with the threats, the safeguards themselves are grouped according to the headings in the Safeguards Catalogues, i.e. in this case, under the headings Infrastructure, Organisation, Personnel, Hardware & Software, Communications and Contingency Planning. The same procedure is followed as in the handling of threats, i.e. in each case only a reference is provided to the relevant safeguard. An example is provided below as to how a recommended safeguard would be cited within a module:

- S 1.15 (1) Closed windows and doors

In the code S x.y, "S" refers to a safeguard, and the number x before the decimal point refers to the Safeguards Catalogue (in this case S 1 = Infrastructure). The number y after the decimal point is the serial number of the safeguard within the relevant catalogue.

The number in brackets - in this case (1) - assigns a priority to each safeguard. This is extremely important when drawing up a plan for the implementation of safeguards which have not previously been implemented or have only partially been implemented. In practice, it is during this phase that problems in finding sufficient financial or staff resources and/or with timescales frequently occur. If these would mean that full implementation of all the necessary safeguards would have to be delayed, then the starting point in determining the sequence to be followed in implementing any missing safeguards should be the priority assigned to each of the various safeguards in the modules. The following priority levels have been assigned:

1	These safeguards constitute the basis for security within the module concerned. Implementation of these safeguards should be given top priority.
2	These safeguards are important. If possible, they should be implemented speedily.
3	These safeguards are important in terms of rounding off the IT security. If bottlenecks prevent their being implemented immediately, they can be deferred until a later time.

Some of the safeguards are indicated as being *optional.* Example:

- S 2.18 (3) Inspection rounds (*optional*)

Safeguards can be designated optional for a variety of reasons, possibly because they are expensive to implement, because they are aimed at a higher protection requirement or because they replace other safeguards. As these safeguards cannot be viewed as reasonable for IT baseline protection in every case, a decision always needs to be made and justified as to whether it is reasonable and cost-effective to implement them. If the protection requirement is higher, implementation is generally advised.

In order to be able to draw up an IT security concept on the basis of the IT Baseline Protection Manual and perform the target versus actual comparison that is required, it is necessary to read the text on the safeguards in the modules identified in the relevant Safeguards Catalogue carefully. To illustrate the procedure, an excerpt from one of the safeguards is shown below as an example.

S 2.11Provisions Governing the Use of Passwords

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, users

[Text of the safeguard…]

Additional controls:

- Have the users been briefed on the correct handling of passwords?

[...]

Next to the actual recommendation as to how the various safeguards should be implemented various responsible persons are specified as a guide. *Initiation responsibility* refers to the persons or roles who/which should typically be responsible allocating resources and supervising the implementation of a safeguard. *Implementation responsibility* refers to the persons or roles who/which should be charged with implementing the safeguard.

At the end of the text some additional control questions are listed. These are intended to round off the subject covered and to motivate the reader to cast a critical eye over implementation of the safeguards. These additional control questions do not, however, claim to be complete.

The link between the threats assumed for IT baseline protection and the recommended safeguards is shown in the Safeguard-Threat Tables. These are not included in the printed version of the manual but will be found on the CD-ROM which goes with the IT Baseline Protection Manual (see Annex: Additional Aids). There is a Safeguard-Threat Table for every module.

As an example, an excerpt is provided below from the Safeguard-Threat Table for the module *Exchange of Data Media*:

	Priority	T 1. 7	T 1. 8	T 1. 9	T 2. 3	T 2. 10	T 2. 17	T 2. 18	T 2. 19	T 3. 1	T 3. 3	T 3. 12	T 3. 13	T 4. 7	T 5. 1	T 5. 2	T 5. 4	T 5. 9	T 5. 23	T 5. 29	T 5. 43
S 1.36	2*	X	X							X					X	X	X	X		X	
S 2.3	2				X	X	X							X	X	X	X	X	X	X	X
S 2.42	2							X		X											
S 2.43	1					X	X	X				X									
S 2.44	1	X	X	X								X		X	X	X		X		X	

All the tables are structured in the same way. The column headings show the threats listed in the associated modules together with their numbers. The column at the far left shows the numbers of the safeguards. Column 2 shows the priority assigned to a given safeguard in the module under consideration. If this column contains an asterisk, then the safeguard concerned should be viewed as "optional" in this module.

The other columns show the relationship between safeguards and threats. An "X" in a given cell means that the corresponding safeguard is effective against the relevant threat. The effect of the safeguard may be either of a preventive nature or else aimed at mitigating the loss or damage.

Where it is not possible to implement a recommended safeguard, it is possible to see from these tables which threats, if any, are not properly protected against. In such cases consideration should be given as to whether an alternative safeguard should be implemented. When using these tables, the number of "X" entries next to a given safeguard should not be interpreted as an indication of the relative importance of that safeguard. There are cases of safeguards which are only effective against a single threat but which are still absolutely essential.

Finally it should be pointed out that all the modules, threats, safeguards, tables and additional aids are contained on the CD-ROM which comes with the IT Baseline Protection Manual. The related text may be reused to assist in drawing up a security concept and/or implementing safeguards.

1.3 Using the IT Baseline Protection Manual

To successfully establish a continuous and effective IT security process, a whole series of actions must be performed. Here the IT Baseline Protection Manual offers advice on methodology and practical aids to implementation. It also contains possible solutions for different tasks relating to IT security, such as drawing up an IT security concept, security audits and certification. Depending on the task concerned, different ways of using the IT Baseline Protection Manual will be appropriate. This section is intended to facilitate getting up to speed with the various procedures. To this end it provides cross references to the relevant chapters of the IT Baseline Protection Manual.

IT security process and IT security management

In both the public and private sectors, organisations have become significantly more dependent over the last few years on the proper functioning of information technology. More and more business processes are either being automated or else redesigned in such a way that major components depend on information technology. There is no sign of this trend letting up in the foreseeable future. IT security must therefore be viewed as an integral element of the primary task. The following action plan contains all the essential steps which are necessary for a continuous IT security process, and should therefore be viewed as a reasoned approach as to how a reasonable level of IT security can be achieved and maintained. This should be systematically adopted.

- Develop an IT security policy
- Select and establish an appropriate organisational structure for IT security management
- Draw up an IT security concept
- Implement the IT security safeguards
- Arrange training and measures aimed at promoting security awareness
- Maintain IT security in ongoing operations

Chapter 3.0 presents an overview of the IT security process and provides a detailed explanation of the individual actions in the form of recommended standard safeguards.

IT structure analysis

"IT assets" refers to all the infrastructural, organisational, personnel and technical components which assist with the performance of tasks in a particular area in which information processing is performed. IT assets can refer to all the IT assets in an organisation or to individual areas defined in terms of organisational structures (e.g. departmental network) or shared IT applications (e.g. HR information system). To create an IT security concept and, in particular, to use the IT Baseline Protection Manual, it is necessary to analyse and document the structure of the existing IT assets. Given that IT systems today are commonly linked together in networks, it is recommended using a network topology plan as the starting point for the analysis. The following aspects must be considered:

- the existing infrastructure,
- the underlying organisational and personnel situation which forms a background to the use of the IT assets,
- the IT systems used, both networked and non-networked,
- the communication links between the IT systems and with the outside world,
- the IT applications run on the IT assets.

The various steps involved in the IT structure analysis are described in detail in Section 2.1 of this manual in the form of instructions on the actions to be taken.

Assessment of protection requirements

The aim of the assessment of protection requirements is to ascertain what protection is adequate and reasonable for the information and the IT assets used. For each application and the information processed within it the potential damage which could occur as a result of loss of confidentiality, integrity or availability is considered. A realistic assessment of the possible consequential damage is also important here. It has proved useful to distinguish three protection requirements categories, "basic to moderate", "high" and "very high". Explanations and practical advice on the assessment of protection requirements are to be found in Section 2.2.

Security concept

It is customary today in both the public and private sectors to network large numbers of IT assets. It is therefore generally expedient when performing an IT security analysis or drawing up an IT security concept to consider the IT assets as a whole rather than individual IT systems. To make this task manageable, it is useful to break down the IT assets into logically distinct parts and to consider each part separately. Before the IT Baseline Protection Manual can be applied to a set of IT assets, detailed documentation regarding its structure must be available. This can be obtained, for example, through performing the IT structure analysis mentioned above. The IT Baseline Protection Manual modules must then be mapped onto the various components which make up the IT assets in a modelling stage.

Section 2.3 of this manual describes how to model the IT assets using modules of the manual. Section 2.4 describes how to then gather information about existing IT protection using a basic security check.

Basic security check

The basic security check is an organisational tool which provides a rapid overview of the existing IT security level. Interviews are used to establish the status quo of an existing set of IT assets (assuming IT baseline protection) in relation to the extent to which the security safeguards contained in the IT Baseline Protection Manual have been implemented. The outcome of this check is a catalogue in which the implementation status of each of the relevant safeguards is classified "Unnecessary", "Yes", "Partially" or "No". By identifying safeguards which have not yet been implemented or have only been partially implemented it is possible to identify where there is scope for improving the security of the IT assets concerned. Section 2.4 describes an action plan for performing a basic security check. This takes into account both the organisational aspects and also the technical requirements during project implementation.

IT security audit

The security safeguards contained in the IT Baseline Protection Manual can also be used to carry out an audit of IT security. By way of example, checklists based on the modules

- 3.1 Organisation
- 3.2 Personnel
- 5.5 PC under Windows NT
- 5.6 PC with Windows 95

have been developed which are intended to support IT security management in reviewing the IT security implemented in the agency/company. Checklists are contained on the CD-ROM which comes with the IT Baseline Protection Manual (see Annex: Additional Aids). The current versions of the checklists should not be viewed as definitive; they merely serve as the basis for discussions and exchanges of experience with users of the IT Baseline Protection Manual. Comments and suggestions for improvement can be forwarded by e-mail to *itbpm@bsi.de.*

Supplementary security analysis

The standard security safeguards aimed at securing baseline protection will normally provide a reasonable and sufficient level of protection. However, if the protection requirement is high or very high it may be appropriate to check whether more stringent IT security safeguards are needed either in addition to or instead of the safeguards required to achieve IT baseline protection. To select a set of suitable IT security safeguards, a supplementary security analysis is performed. This can entail the use of a variety of methods, for example,

- risk analysis,
- penetration testing and
- differential security analysis.

An overview of these methods is presented in Section 2.5. The successful carrying out of the supplementary security analysis depends critically on the expertise of the project team. It may therefore be appropriate to employ the services of specialist external consultants.

Implementation of IT security concepts

A satisfactory level of IT security can only be established if existing weaknesses are ascertained in the security analysis, the status quo is determined in a security concept, the safeguards that are necessary are identified and, above all, these safeguards are also implemented systematically. Section 2.6 describes the factors which should be considered when planning the implementation of IT security safeguards.

IT Baseline Protection Certification

The IT Baseline Protection Manual is used today not only to assist in drawing up IT security concepts but also increasingly as a reference work in the sense of a security standard. By achieving IT Baseline Protection certification, an organisation can provide documentary evidence to the outside world that it has implemented IT baseline protection to the depth required. Section 2.7 introduces the idea of IT Baseline Protection Certification and defines the certification scheme that this entails. The certification level is assigned to one of three different classes which differ both in relation to quality (i.e. the degree of implementation of security safeguards that is necessary) and to assurance. The lowest level can be demonstrated by an employee of the agency/company, while the highest level requires testing by an independent third party.

1.4 Brief Outline of Existing Modules

The overview which follows provides a brief outline of the modules which currently exist in the IT Baseline Protection Manual. It gives a compact summary of the scope of the recommended safeguards contained in the IT Baseline Protection Manual.

3.0 IT Security Management

This chapter presents a systematic approach to establishing functional IT security management and adapting it over time in line with developments in business operations.

3.1 Organisation

This module lists the organisational procedures that are basically required for IT security. Examples are the determination of responsibilities, data media administration and procedures regarding the use of passwords. They apply to every IT system.

3.2 Personnel

The *Personnel* module describes staff-related safeguards to be observed for the achievement of IT security. Examples are arrangements during staff absences, training activities, and controlled procedures in the case of termination of employment. They apply regardless of the type of IT system employed.

3.3 Contingency Planning Concept

This module presents a procedure for drawing up a contingency planning concept and is especially important for larger IT systems.

3.4 Data Backup Policy

This module shows how a sound data backup policy can be systematically developed. It is especially intended for larger IT systems or IT systems on which a large amount of data is stored.

3.5 Data Privacy Protection

This module presents the basic conditions for realistic data privacy and shows the interrelationship of IT security and IT baseline protection. It was developed under the lead of the Federal Data Privacy Officer (BfD) in co-operation with the data privacy officers of the German state and the individual German *Länder*, and can be obtained from the BfD.

3.6 Computer Virus Protection Concept

The aim of the computer virus protection concept is to create a suitable package of safeguards which will enable penetration of an organisation's IT systems by computer viruses to be prevented or detected as early as possible so that countermeasures can be taken and possible damage can be minimised.

3.7 Crypto Concept

This module describes a procedure whereby in a heterogeneous environment both the data stored locally and the data to be transmitted can be protected effectively through cryptographic procedures and techniques.

3.8 Handling of Security Incidents

To maintain IT security in ongoing operations, it is necessary to have developed and practised a policy for the handling of security incidents. A security incident is an event whose impact could cause

significant loss or damage. To prevent or contain any loss or damage, security incidents should be dealt with swiftly and efficiently.

4.1 Buildings

This module specifies the safeguards which must be observed in every building in which data processing takes place. These include safeguards relating to the power supply, fire protection and building protection, as well as organisational safeguards such as key management.

4.2 Cabling

The *Cabling* module recommends safeguards which should be adopted when laying utility and communications lines in a building. Subjects covered include fire sealing of routes, selection of appropriate types of cables and documentation of cabling.

4.3.1 Offices

The *Office* module covers all the safeguards to be observed in connection with the use of IT in an office. Subjects covered include closed windows and doors and supervision of visitors and contractors.

4.3.2 Server rooms

This module lists the safeguards to be observed in the use of a room housing a server (for IT systems or PBXs). Subjects covered include avoidance of water pipes, air conditioning, local uninterruptible power supply (UPS) and smoking bans.

4.3.3 Storage Media Archives

If a room is used to accommodate data media archives, certain requirements for IT security must be adhered to. These are presented in the form of safeguards for IT baseline protection. Subjects covered include hand-held fire extinguishers, use of safety doors and smoking bans.

4.3.4 Technical Infrastructure Rooms

It is also necessary to take certain IT security measures in rooms where technical infrastructure is installed, for instance the PTT cable entry room, distributor room and low-voltage distribution room. These are specified in this section.

4.4 Protective Cabinets

Secure cabinets can be used to increase protection in rooms where data media or hardware are kept (e.g. server room, data media archive). If necessary, a special server cabinet can be used as an alternative to a server room. The necessary procedures for obtaining, siting and using a secure cabinet are described in this module.

4.5 Working Place At Home (Telecommuting)

This module describes the measures required to set up a telecommuting workstation with an appropriate security standard in such a way that it can be used for official tasks.

5.1 DOS PC (Single User)

This module specifies the safeguards to be observed when using a normal PC that is routinely used by a single user. Subjects covered include password protection, use of a virus detection program, regular backup.

5.2 UNIX System

This module considers IT systems which run under the UNIX or Linux operating systems and are operated either on a stand-alone basis or as a client in a network. Terminals or PCs which are run as terminals can be connected. Both organisational and UNIX-specific safeguards are listed.

5.3 Laptop PC

As compared with a normal PC, a portable PC (laptop) requires additional IT security safeguards because it is exposed to other threats due to its mobile nature. Examples of additional safeguards which apply to laptop PCs are suitable safe-keeping during mobile use and use of an encryption product.

5.4 PCs With a Non-Constant User Population

This module specifies the safeguards which must be adhered to when using a normal PC which is routinely used by several users. Subjects covered include PC security products, password protection, use of a virus detection program, regular backup.

5.5 PC under Windows NT

The safeguards needed for non-networked PCs which run under the Windows NT operating system (version 3.51 or 4.0) are described in this module. Security-specific aspects of individual Windows NT applications are only covered briefly.

5.6 PC with Windows 95

Non-networked PCs which run under Windows 95 can be configured as stand-alone systems or as clients in a network for one or more users. The necessary safeguards for both operating variations are described in this module.

5.99 Stand-Alone IT Systems Generally

For IT systems not yet considered in the IT Baseline Protection Manual the generic module 5.99 can be used.

6.1 Server-Supported Network

The necessary safeguards that must be taken into account when operating a server-supported network are explained in this module. These considerations are independent of the operating system used on the servers and clients. Safeguards pertaining to operating systems can be found in the specific modules of Chapters 5 and 6.

6.2 UNIX Server

IT systems which, as servers, provide services on a network and run under the UNIX or Linux operating system are considered here. Safeguards directed at providing IT security in this IT environment are described here. These safeguards are UNIX-specific and must be supplemented by Section 6.1.

6.3 Peer-to-Peer Network

This section describes how a peer-to-peer network can be securely operated for IT baseline protection. Topics include the design of such a network from the point of view of security, administrative options and functional limitations. The operating systems Windows for Workgroups 3.11, Windows 95 and Windows NT apply here.

6.4 Windows NT Network

The design and operation of a secure Windows NT network is described in this module. Windows NT-specific safeguards are predominantly dealt with here. They must be supplemented by the general safeguards contained in Section 6.1.

6.5 Novell Netware 3.x

This section covers a Novell 3.x network providing client/server functionality. As such, it serves as an operating system-specific supplement to Section 6.1 *Server-Supported Network*. The installation, configuration, operation and maintenance of Novell NetWare servers are dealt with.

6.6 Novell Netware 4.x

This section covers a Novell 4.x network providing client/server functionality. As such, it serves as an operating system-specific supplement to Section 6.1 *Server-Supported Network*. The necessary safeguards for installation, configuration and operation of a Novell 4.x network are described. The directory service NDS (NetWare Directory Services) is considered in detail.

6.7 Heterogeneous Networks

This module enables existing heterogeneous networks to be analysed and enhanced and new ones to be planned. It shows how to segment a heterogeneous network in a suitable way, how to plan and implement a network management system and how auditing and maintenance can be implemented, so as to ensure secure operation. Additional topics covered include redundant network components and backup of configuration data for contingency planning.

6.8 Network and System Management

A management system enables all the hardware and software components in a local network to be managed centrally. This module describes the steps necessary to successfully set up a network and system management system, starting with the design, then going on to procurement and finally use in service.

7.1 Exchange of Data Media

This module describes the safeguards which should be considered when exchanging data media. Technical measures, such as encryption, are described, as well as the correct choice of delivery method. These measures are addressed particularly at situations where data media are exchanged on a regular basis.

7.2 Modem

This module deals with measures to be adhered to when working with a modem, notably call-back mechanisms and encryption. Information is also given regarding remote maintenance over a modem.

7.3 Firewall

Networking of existing subnetworks with global networks such as the Internet requires that the internal network is effectively protected. In order that such protection can be provided by a firewall, the security objectives must be clearly formulated and then put into practice through the correct installation and administration of the firewall.

7.4 E-Mail

The safeguards required both on the mail server and the mail client for secure communication via e-mail are listed. The safeguards that have to be observed by the users are also presented.

7.5 WWW Server

A WWW server is an IT system which makes files from an information database available to WWW clients. A WWW client, also called a browser, displays the information from a WWW server on the user's computer. The security of the use of the WWW is based on the security of the WWW server, the WWW client and the communications link between the two. The *WWW Server* module describes the safeguards required for secure use of the WWW.

7.6 Remote Access

In order for a user to be able to access a remote computer network from his local computer, appropriate remote access services must be established. This module explains how to protect the individual RAS system components and draw up a corresponding RAS security concept.

8.1 Telecommunications System (Private Branch Exchange, PBX)

This module considers private branch exchanges (PBX) based on ISDN. A PBX is typically a complex IT system whose administration requires a number of safeguards if it is to operate securely.

8.2 Fax Machine

The transmission of information over a stand-alone fax machine opens up a new area of threats. The safeguards required to ensure IT baseline protection when using fax machines are described. These include the disposal of fax consumables, the appropriate positioning of the fax machine and, if appropriate, any communication between sender and receiver.

8.3 Answering Machine

Modern answering machines with remote access capabilities can be thought of as IT systems which store speech information. They are at risk from abuse of the remote replay facility. IT baseline protection measures for answering machines are described, also specifically in regard to this threat.

8.4 LAN connection of an IT system via ISDN

This module considers the integration of an IT system into a remote LAN by means of an ISDN adapter card with S_0-interface. It is assumed that this LAN contains a router which is connected to the public telephone network via an S_{2M}-interface.

8.5 Fax Servers

This module concentrates on fax transmissions using a fax server. A fax server in this sense is an application which is installed on an IT system and provides services on a network enabling other IT systems to send and/or receive faxes.

8.6 Mobile Telephones

This section presents a set of security safeguards for the components mobile phone, base station and fixed network and their mutual interaction, which are aimed at ensuring that use of digital mobile telephone systems based on the GSM standard (D and E networks) is secure.

9.1 Standard Software

A procedure is described as to how the life cycle of standard software can be structured, i.e. requirements catalogue, selection, testing, approval, installation and deinstallation. Aspects such as functionality tests and security characteristics, installation instructions and the approval process are described.

9.2 Databases

Safeguards relating to the selection, installation, configuration and ongoing operation of a database system are described. These include the development of a database concept, provisions for the creation of database users and user groups, and guidelines for database queries.

9.3 Telecommuting

The procedures for installing telecommuting workstations are described from an organisational and personnel point of view. The security-relevant requirements for telecommuting which need to be implemented through the use of suitable IT components are described.

1.5 Additional Aids

Through its recommendations for standard security safeguards the IT Baseline Protection Manual offers direct assistance with the implementation of IT security. In addition, several further aids are available for daily work with IT security. These aids fall into two broad categories, software and programs, and secondary documents.

Software tools

There are currently three software tools available for IT baseline protection. These are as follows (further information on these tools will be found in the annex):

- **BSI IT Baseline Protection Tool**. This tool, which was commissioned by the BSI, supports the entire process involved in drawing up a security concept aimed at achieving IT baseline protection, the target versus actual comparison, implementation of the safeguards and the subsequent security audit. In addition it is possible from the tool to access the text of the manual in electronic form. A reporting structure capable of being tailored to suit a given organisation provides support to the IT Security Officer as he goes about implementing IT baseline protection.
- **BSI USEIT tool**. This tool, which was commissioned by the BSI, enables a UNIX administrator to perform an automated check as to whether the technical settings of a UNIX system are consistent with IT baseline protection. The tool can be used for the common variants of UNIX including Linux. It can also be used to assist with security audits of UNIX networks, firewalls and WWW servers based on UNIX.
- **Chiasmus for Windows**. An encryption program which can be used under a Windows interface was developed by the BSI specially to meet administrative needs in Germany. It is also possible to physically delete files using this tool.

Secondary documents

To supplement the IT Baseline Protection Manual, a number of additional documents are available. Some of these were written by the BSI and some of them have been made available to the BSI for further distribution free of charge by users of the manual. A list of the aids available is provided in the annex.

At this point we would like to mention a few of these aids:

- example of an information security policy,
- example set of terms of reference for IT Security Officers,
- example of user rules for electronic communications services,
- example of a contract for the disposal of data media,
- example of an office agreement regarding e-mail and the Internet,
- set of viewfoils for making presentations on IT baseline protection to managers, those responsible for IT and employees, and
- record sheets when gathering information relevant to IT baseline protection.

Tools which have been developed by users of the IT Baseline Protection Manual and are made available here to other users can save the "IT security community" considerable work in that they obviate the need to continually reinvent the wheel. Tools can be forwarded to the BSI via the IT Baseline protection Hotline (0228/9582-316 or *itbpm@bsi.de*). Currently not all additional material is available in English.

1.6 Information Flow and Points of Contact

As well as regular updates and further development of the IT Baseline Protection Manual, the BSI publishes other topical information covering all aspects of IT baseline protection over various communications media.

BSI IT Baseline Protection CD-ROM

The CD-ROM enclosed with the manual contains all the text and auxiliary aids for the German IT Baseline Protection Manual both in Word and PDF format.

The BSI distributes special BSI CD-ROMs on the topic of IT baseline protection free of charge. These are normally available six weeks after a supplement to the manual has been issued. As well as the latest German version of the IT Baseline Protection Manual, the CDs also contain the English translation and the HTML version of the manual plus other information from the BSI.

These BSI CD-ROMs can be obtained by sending a stamped addressed envelope (size C5, with a DM 3 stamp if the return address is in Germany) to the BSI, IT-Grundschutz-Hotline, Postfach 20 03 63, 53133 Bonn.

IT baseline protection on the Intranet

The electronic versions of the IT Baseline Protection Manual can also be made available on Intranets. The best version to use for this purpose is the HTML version. Use of this version does not require any special permission from the BSI.

IT baseline protection on the Internet

The entire manual may also be accessed both in German and in English on the Internet at *http://www.bsi.bund.de/gshb*. Information on recent developments concerning the manual and the latest aids which are available can also be found there. In addition, the site contains links to mirror sites which similarly present the IT Baseline Protection Manual on the Internet. Provision of a mirror for IT baseline protection requires registration with BSI at *itbpm@bsi.de*, in order that the BSI can make the latest version of the manual available.

IT Baseline Protection Hotline

For topical questions relating to all aspects of the topic of IT baseline protection, the BSI provides a Hotline which is manned during normal office hours (8 a.m. to 4 p.m. Monday to Friday). The Hotline can be contacted as follows:

Phone: +49 (0)228/9582-316
Fax: +49 (0)228 / 9582-405
E-mail: *itbpm@bsi.de*

Suggestions for improvement, notification of inaccuracies and requests for new topics to be covered can also be passed to the IT Baseline Hotline.

Voluntary registration

To keep the manual up-to-date and in line with users' needs, the BSI needs to exchange experiences with users of the manual. At the same time it actively seeks channels by which it can inform users directly about topical aspects of the subject of IT baseline protection (advance notification of new modules and developments, invitations to the IT Baseline Protection Forum, questionnaire campaigns). To receive this information, users of the manual can voluntarily register themselves with the BSI. The data passed on by users is stored and only used for the purposes of exchanging information about IT security and IT baseline protection. Registration is free of charge. Due to the

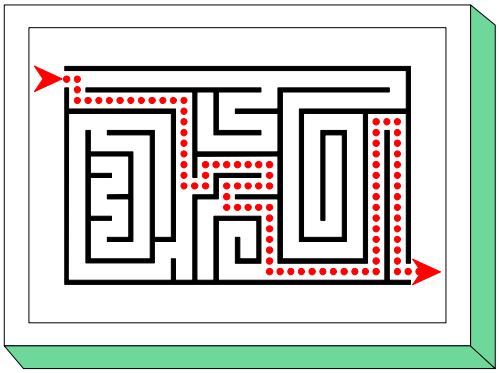
large number of voluntarily registered users, the BSI can only distribute such information by e-mail or fax. Postal services are only seldom used.

The form for voluntary registration will be found in the annex. It can be delivered to the BSI by writing to BSI, IT-Grundschutz-Hotline, Postfach 20 03 63, 53133 Bonn, Germany, by fax (+49 (0)228/9582-405) or by e-mail (itbpm@*bsi.de*).

To create transparency as to which sectors employ IT baseline protection, the BSI publishes the names of those registered institutions which agree to have their names published. The BSI regularly queries the registered users on this matter. The current status is available in the annex.

2 Using the IT Baseline Protection Manual

2 Using the IT Baseline Protection Manual



Implementation and maintenance of a reasonable level of IT security can only be ensured if all those involved proceed in a planned and organised fashion. The efficient implementation of IT security safeguards and review of their efficacy therefore necessitates a well thought out and controlled IT security process.

This IT security process begins with definition of the IT security objectives and the establishment of IT security management. The function of IT security management is to draw up and implement an IT security concept. As IT security is maintained in ongoing operations the IT security process regularly entails returning to the security concept so as to permit a continuous process. This approach is illustrated schematically in the diagram below.

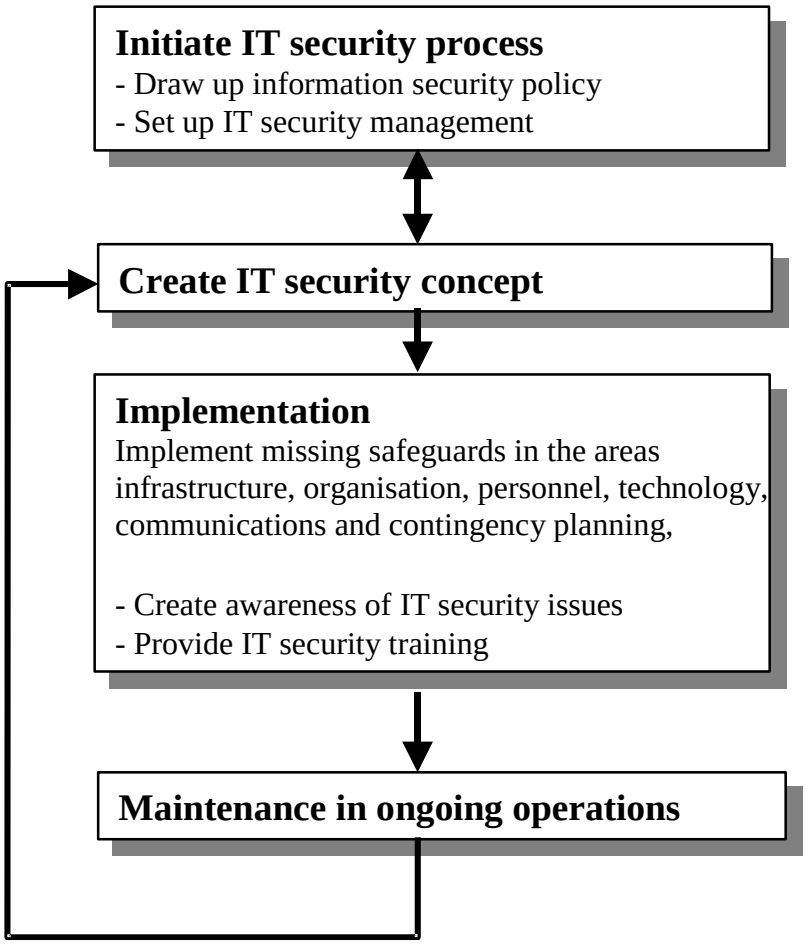


Figure: IT security process

Further information on the area of IT security management will be found in Chapter 3 of this manual.

The primary function of IT security management is to draw up the IT security concept, which is indispensable to the implementation of the necessary IT security safeguards. In the next few sections of this chapter a description will therefore be provided as to how an IT security concept can be created using the IT Baseline Protection Manual.

The general procedure to be followed is illustrated diagrammatically in the figure below:

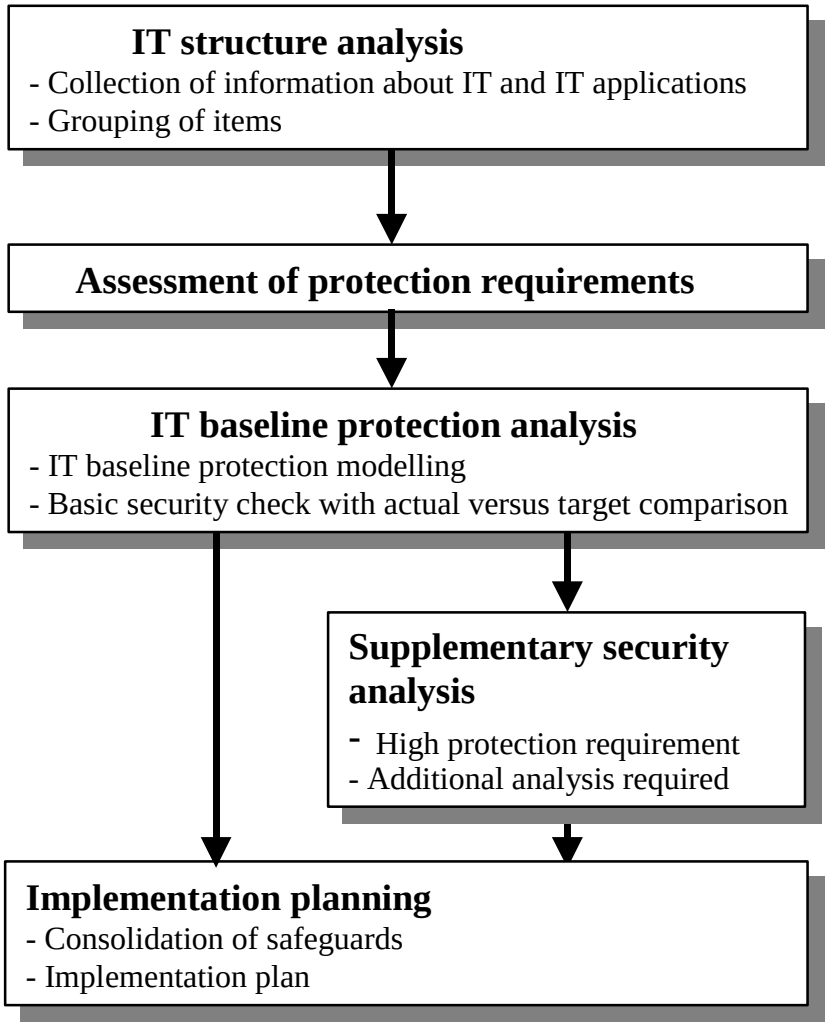
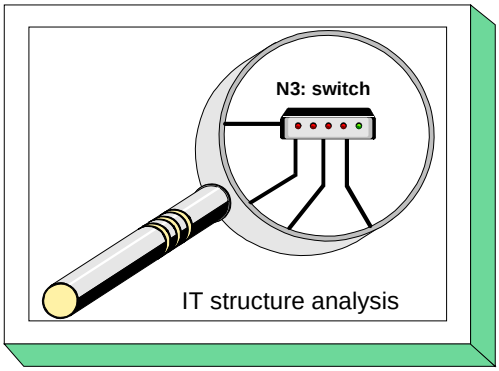


Figure: Creation of an IT security concept

Once information on the existing IT assets has been collected, the protection requirement is assessed. In the IT baseline protection analysis which follows, first of all the IT infrastructure under consideration is modelled using modules from the manual. A target versus actual comparison between the recommended standard security safeguards and the safeguards which have already been implemented is then carried out. If any components are identified during assessment of the protection requirement as having a high or very high protection requirement, then it is recommended that a supplementary IT security analysis is carried out after the IT baseline protection analysis. This can also be necessary in any instances where the IT Baseline Protection Manual does not contain any suitable modules. After the IT security concept has been drawn up using the IT Baseline Protection Manual, a plan is then prepared for implementation of the IT security safeguards identified and consolidated.

2.1 IT Structure Analysis



The IT structure analysis provides the means for performing a preliminary survey aimed at collecting information which will be needed later on when drawing up an IT baseline protection security concept. It is split into the following sub-tasks:

- Preparing a network plan
- Reducing complexity by identifying groups of similar assets
- Collecting information about the IT systems
- Capturing information about the IT applications and related information

These sub-tasks are described below and explained by means of an accompanying example. A detailed version of the example is included with the auxiliary aids contained on CD-ROM which comes with the IT Baseline Protection Manual.

Analysis of a network plan

A network plan (for example in the form of a network topology plan) can be a useful starting point for the IT structure analysis. A network plan is a graphical representation of the components used in the IT and communications area under consideration and of the manner in which they are networked together. The plan should represent the following objects:

- IT systems, i.e. clients and server computers, active network components (such as hubs, switches, routers), network printers etc.
- Network connections between these systems, i.e. LAN connections (e.g. ethernet, token ring), backbone technologies (e.g. FDDI, ATM), etc.
- Connections between the area under consideration and the outside world, i.e. dial-in access over ISDN or modem, Internet connections using ISDN, modem or routers, radio links or leased lines to remote buildings or sites.

Moreover, for each of the objects represented there should be a minimum set of information which can be obtained from an assigned catalogue. As a minimum, the following information should be noted down for each IT system:

- a unique name (for example the full host name or an identification number)
- type and function (for example, database server for application X)
- the underlying platform (i.e. hardware platform and operating system)
- location (e.g. building and room number)
- name of the responsible administrator
- type of network connection and network address.

Certain information is needed not only for the IT systems themselves but also for the network connections between the systems and for connections to the outside world, namely

- type of cabling (e.g. fibre optic cable),
- the maximum data transmission rate (e.g. 10 Mbps),

- the network protocols used on the lower layers (e.g. ethernet, TCP/IP),
- for external connections, details of the external network (e.g. Internet, name of provider).

If the IT assets in the company/agency have exceeded a certain scope, it is recommended that suitable support programs are used to help with data collection and maintenance of the network plan, as the documentation may be quite complex and require constant updates.

Updating of the network plan

As the IT structure is generally adapted to the specific requirements of the organisation and maintenance of the network plan ties up certain resources, the network plan will not always be up-to-date. In practice often only major changes in the IT structure of individual areas actually result in the plan being updated.

With regard to use of the network plan for the IT structure analysis, the next step entails comparing the existing network plan (or partial plans, if the overall plan has been divided into smaller sections to make it easier to read) with the actual existing IT structure and if necessary updating it to reflect the current situation. During this activity, those responsible for IT and any administrators of individual applications and networks should be consulted. If any programs are used for centralised network and system management, a check should be made in every case as to whether these programs offer any support in drawing up a network plan. However, it should be noted that functions for the automatic or semi-automatic detection of components temporarily generate additional network traffic. Steps must be taken to ensure that this network traffic does not impair IT operations.

Reducing complexity by identifying groups of similar assets

The next step is to remove from the network plan any information which is not necessary for the next set of tasks, in order to make it easier to use. Accordingly, any identical components should be combined into one group which is represented in the network plan by a single object. Components may then be assigned to one and the same group if all the components

- are of the same type,
- have identical or almost identical configurations,
- are attached to the network in the same or almost the same manner (e.g. on the same switch),
- are subject to the same administrative and infrastructural basic conditions and
- use the same applications.

If these conditions are adhered to in assigning individual assets to a single group, then for the purposes of IT security it may be assumed that a sample from one group will be representative of the IT security state of the group as a whole.

By far the most important instance where grouping of components in the network plan is appropriate is the grouping together of client computers. Usually there will be a large number of clients within a company/agency which, however, can be reduced to a manageable number of groups if the procedure outlined above is followed. If the number of IT assets is very large and for reasons of redundancy or throughput many servers perform the same task, servers too can be grouped together.

After the grouping process is complete, the components grouped together are shown on the network plan as a single object. The type and number of components represented in each group should be noted down.

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 1

In the discussion below a fictitious governmental department known as the BOV is used to illustrate how a simplified network plan can look. It should be noted that the IT structure of the BOV is by no means optimal as regards IT security. The example is simply used to illustrate the procedure of using the IT Baseline Protection Manual. (The complete example is included among the auxiliary aids on the CD-ROM.)

Let us assume that the BOV is an official body with a staff of 150, 130 of whom have their own workstations. The BOV is geographically split between its main office in Bonn and a branch office in Berlin where, amongst other things, tasks in the areas of policy, standards and co-ordination are performed. Of the 130 staff with IT-supported workstations, 90 work in Bonn and 40 in Berlin.

All the workstations are networked in order that staff can perform their tasks. The Berlin branch office is linked over a leased line. Every employee can call up the standards and regulations to which his work is subject, along with forms and document templates, at any time. All the relevant products of the work are placed in a central database. Draft documents are exclusively prepared, distributed and signed in electronic form. To implement and support all the necessary functionality, an IT department has been set up in Bonn.

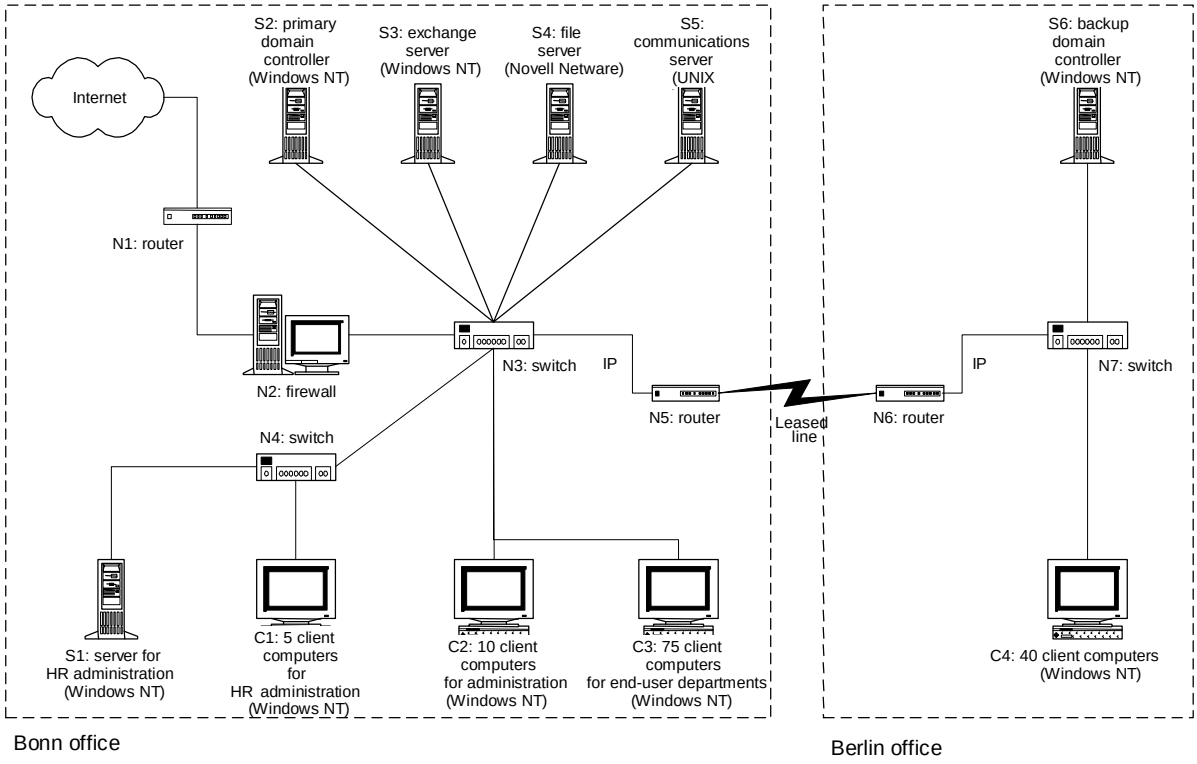


Figure: Example of a simplified network plan

In the network plan illustrated, each IT system (server, client or other active network component) is shown with an identifying number (Sn, Cn, Nn etc.), together with its function and, if appropriate, the operating system is indicated in brackets.

Both in Berlin and in Bonn the clients have been combined into appropriate groups. All 130 clients have virtually the same configuration but there are differences between them as regards the applications, integration into the network and the underlying infrastructure. Group C1 represents the 5

clients in the HR Department. They have access to server S1 in the HR Department in Bonn. C2 and C3 represent the 10 clients in the Administration Department and the 75 clients in the end-user departments in Bonn. The only differences here are in relation to the application programs used. Finally, group C4 represents the clients in end-user departments in Berlin. These differ from groups C1 to C3 in the environmental infrastructure and their integration into the overall network.

Collecting information about the IT systems

The next step relevant to the assessment of protection requirements and modelling of the IT assets to be subsequently performed is to prepare a list of the existing and planned IT systems in tabular form. The term "IT system" refers here not only to computers in the narrower sense, but also to other active network components such as network printers, private branch exchanges (PBX) etc. The focus here is on the technical implementation of an IT system, e.g. stand-alone PC, Windows NT server, PC client under Windows 95, UNIX server, PBX. At this point, only the system as such (e.g. UNIX server) should be recorded, rather than the individual elements which make up the IT system (i.e. CPU, keyboards, monitors etc. should be omitted).

Both networked and non-networked IT systems should be recorded, i.e. in particular, any IT systems which are not already included in the network plan previously considered. IT systems which have been grouped together as part of the exercise of simplifying the network plan can be viewed from now on as a single object. Again, the IT systems which are not included on the network plan should be checked to see whether it would be logical to group some of them together. For example, this might be possible if there is a large number of stand-alone PCs which satisfy the conditions stated as being necessary for grouping in the "Reducing complexity by identifying groups of similar assets" section above.

When collecting the data, the following information which will be needed at subsequent stages should be noted down:

- a unique name for the IT system,
- description (type and function),
- platform (e.g. hardware architecture/operating system),
- number of IT systems included in each group,
- installations site of the IT-system,
- status of the IT system (operational, in test stage, in planning stage)
- user/administrator of the IT system.

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 2

As an example, the table below shows an excerpt from the list of IT systems in the BOV. (The complete list is included in the auxiliary aids provided on the CD-ROM.)

No.	Description	Platform	Number	Installation site	Status	User(s) / Admin.
S1	Server for Human Resources	Windows NT Server	1	Bonn, R 1.01	Operat-ional	Human Resources
S2	Primary domain controller	Windows NT Server	1	Bonn, R 3.10	Operat-ional	All IT users
C1	Group of clients in HR data processing	Windows NT Workstation	5	Bonn, R 1.02 - R 1.06	Operat-ional	Human Resources
C2	Group of clients in the Administration Department	Windows NT Workstation	10	Bonn, R 1.07 - R 1.16	Operat-ional	Administration Department
C6	Group of laptops for the Berlin office	Laptop under Windows 95	2	Berlin, R 2.01	Operat-ional	All IT users in the Berlin office
N1	Router connecting to the Internet	Router	1	Bonn, R 3.09	Operat-ional	All IT users
N2	Firewall	Application gateway on UNIX	1	Bonn, R 3.09	Operat-ional	All IT users
N3	Switch	Switch	1	Bonn, R 3.09	Operat-ional	All IT users
T1	Private branch exchange for Bonn	ISDN PBX	1	Bonn, B.02	Operat-ional	All staff in the Bonn head office

IT systems/groups S1, S2, C1, C2, N1, N2 and N3 are taken directly from the network plan. In addition, the non-networked IT systems C6 (laptops) and T1 (PBXs) have been added.

Capturing information about the IT applications and related information

To reduce the amount of effort required, in each case only the most important IT applications already running or planned to be run on the IT systems under consideration have been included. It is not essential for the efficient performance of this task to record every application as long as all IT applications for a given IT system which fall within the following three categories are specified:

- applications in respect of which it is essential that their data/information and programs remain confidential (i.e. maximum requirement for confidentiality);
- applications in respect of which it is essential that their data/information and programs are correct and unaltered (integrity);
- applications for which only the minimum amount of down time can be tolerated (i.e. maximum requirements as regards availability).

To ensure that all the necessary data is collected, when recording information about IT applications the users and/or those responsible for a given IT application should be asked to provide an assessment.

The definition and gathering of information about IT applications is easier if the IT applications are compiled in a manner which is oriented to the IT systems. Due to their widespread impact, the servers should be the first items on which information is collected. To obtain as balanced a picture as possible, the survey can then be completed to include the clients and stand-alone systems. Which network switching elements support which IT applications must then be established.

It can be helpful here to assign a serial number to each application for reference purposes. As many IT Security Officers also perform the role of Data Privacy Officer responsible for the protection of person related data, we recommend making a note at this point as to whether any person related data is stored and/or processed on the described IT application.

The applications are then in each case assigned to the IT systems which are necessary to run them. This can be the IT systems on which the IT applications are processed, but it could also include IT systems which transfer data generated within the applications.

The result of this exercise is a summary of which major IT applications are processed on which IT systems, used by which IT systems and/or transferred by which IT systems. It is recommended that the results are documented in tabular form.

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 3

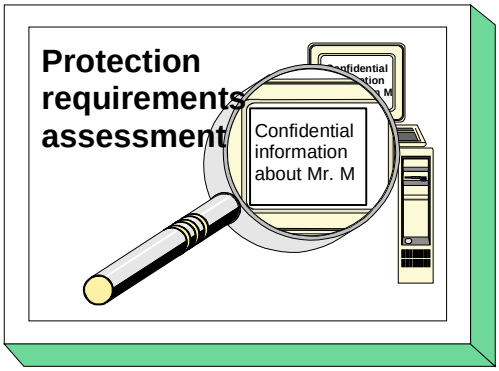
The table below shows an excerpt from the data collected on IT applications and their assignment to the IT systems concerned in the fictitious example of the BOV.

Description of the IT applications			IT-Systems						
Applicn no.	**IT application / information**	**Person related data**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**
A1	Processing of HR data	X	X						
A2	Benefits processing	X	X						
A3	Travel expense accounting	X	X						
A4	User authentication	X		X				X	
A5	System management			X					
A6	Exchange (e-mail, diary)	X			X				
A7	Central document administration					X			

Key: A_i X S_j = Execution of IT application A_i depends on IT system S_j.

Legende Kapitel 2.1

2.2 Assessment of Protection Requirements



Assessment of the protection requirement of the IT structure captured entails four separate steps. First of all the protection requirement categories are defined. Typical damage scenarios are then used to determine the protection requirements of the various IT applications. The protection requirements of the individual IT systems are then derived from the results. These in turn are then used to arrive at the protection requirements for the transmission routes and the premises in which the IT assets are located.

Assessment of protection requirements for IT applications

The aim of the assessment of protection requirements is to decide for every IT application, including the data held or used on it, what degree of protection is required in terms of confidentiality, integrity and availability. This protection requirement is geared towards the potential loss or damage which could occur in the event of degradation of the IT application concerned.

As the protection requirement is generally not quantifiable, the IT Baseline Protection Manual will confine itself below to a qualitative statement when assigning protection requirements to three categories.

Protection Requirement Categories	
Basic to moderate	The impact of any loss or damage is limited.
High	The impact of any loss or damage may be considerable.
Very high	The impact of any damage can attain catastrophic proportions which could threaten the very survival of the agency/company.

The steps outlined below explain how to determine the right protection requirement category for IT applications.

Step 1: define protection requirement categories

The loss or damage which could occur as a result of loss of confidentiality, integrity or availability of an IT application including its data can typically be assigned to the following damage scenarios:

- violation of laws, regulations or contracts,
- impairment of informational self-determination,
- physical injury,
- impaired performance of duties,
- negative effects on external relationships and
- financial consequences.

Often a single instance of loss or damage may involve several damage categories. Thus, for example, failure of an IT application could prevent essential work from being performed, resulting in direct financial loss and at the same time in a loss of image.

In order to be able to draw clear boundaries between the protection requirement categories "Basic to moderate", "High" and "Very high", upper and lower limits should be defined for the individual damage scenarios. To obtain a rough idea of what protection requirement is appropriate for a given level of potential damage and its impact, the following tables should be consulted.

Protection requirement category "Basic to moderate"	
1. Violation of laws, regulations or contracts	- Violations of regulations and laws with minor consequences - Minor breaches of contract which attract little in the way of contractual penalties
2. Impairment of the right to informational self-determination	- Impairment of the right to informational self- determination would be assessed as tolerable by the individual. - Possible misuse of person related data has minimal effects on the social or financial standing of those concerned.
3. Physical injury	- Does not appear possible.
4. Impaired performance of duties	- Impairment would be assessed as tolerable by those concerned. - The maximum acceptable down time is greater than 24 hours.
5. Negative effects on external relationships	- Minimal impairment of reputation / confidence, confined to within the agency/enterprise.
6. Financial consequences	- The financial loss is acceptable to the agency/company.

Protection requirement category "High"	
1. Violation of laws, regulations or contracts	- Violations of regulations and laws with major consequences - Major breaches of contract with high contractual penalties
2. Impairment of the right to informational self-determination	- Significant impairment of the individual's right to informational self-determination could be possible. - Possible misuse of person-related data would have considerable effects on the social or financial standing of those concerned.
3. Physical injury	- Physical injury to an individual cannot be absolutely ruled out.
4. Impaired performance of duties	- Impairment of the performance of duties would be assessed as intolerable by some of the individuals concerned. - The maximum acceptable down time is between one and 24 hours.

5. Negative effects on external relationships	- Considerable impairment of reputation / confidence can be expected.
6. Financial consequences	- The financial loss is considerable, but the agency/company can survive it.

Protection requirement category "Very high"	
1. Violation of laws, regulations or contracts	- Fundamental violation of regulations and laws - Breaches of contract with ruinous damage liabilities
2. Impairment of the right to informational self-determination	- A particularly significant impairment of an individual's right to informational self-determination could be possible. - Possible misuse of person-related data would mean social or financial ruin for those concerned.
3. Physical injury	- Serious injury to an individual is possible. - Danger to life and limb.
4. Impaired performance of duties	- Impairment of the performance of duties would be assessed as unacceptable by all individuals concerned. - The maximum acceptable down time is less than one hour.
5. Negative effects on external relationships	- A nation- or state-wide loss of reputation / confidence is conceivable, possibly even endangering the existence of the agencies/company.
6. Financial consequences	- The agency/company may not be able to survive the financial loss.

Customisation of the assignment table

It is possible that in an individual case there may be other damage scenarios which are not included in the six scenarios listed above, in which case the table should be extended accordingly. The borderline between "Basic to moderate", "High" and "Very high" must be decided for all instances of loss or damage which are not covered in the above table.

Moreover, the individual circumstances which apply to the agency/company should be taken into account. A loss of euro 200,000 could be relatively trivial as a proportion of turnover and IT budget in a large company, whereas for a small organisation even a loss of euro 10,000 could be difficult to survive. It may therefore be appropriate to express the boundaries as percentages of the total turnover, total profit or IT budget.

Similar considerations apply as regards the availability requirements. Thus, for example, in some organisations a down time of 24 hours could still be regarded as acceptable. However, if such incidents occur relatively frequently, e.g. more than once a week, the overall effect could be unacceptable.

When setting the boundary between "Moderate" and "High" it should be borne in mind that the standard security safeguards described in this manual should be sufficient for a moderate protection

requirement. The values decided on should be documented in the security concept in an appropriate manner.

Step 2: consider of damage scenarios

Starting from the assumption that a loss of confidentiality, integrity or availability of an IT application or the related information occurs, the maximum damage and consequential damage are considered. On the basis of the question

"What if ... ?"

realistic damage scenarios are developed *from the user's point of view* and the expected material or non-material damage is described. The extent of this possible damage ultimately determines the protection requirements of the IT application. The persons responsible for the IT applications under consideration and their users must be asked for their personal opinions. They will normally have a good idea of what damage could occur and should be able to provide a useful input into the data collected.

To simplify calculation of the possible damage, a set of questions is presented below for each of the damage scenarios mentioned, as a tool for drawing out the possible effects. These suggestions do not claim to be complete; they are merely intended as a guide. In every case it is necessary to consider the specific work and the situation of the agency/company, and the questions provided in this manual must be supplemented accordingly.

Working through the damage scenarios listed below, including the related questions, is recommended for each of the IT applications recorded. Once this has been done, the tables above should be used to determine the protection requirement with regard to confidentiality, integrity and availability by assigning each IT application to a protection requirement category.

Damage scenario „Violation of laws, regulations or contracts“

Such violations can result from the loss of confidentiality, integrity or availability. The severity of the ensuing damage will often depend on the specific legal implications for this agency/company.

Examples of relevant German legislation are:

The Constitution, the Civil Code, the German Penal Code, the Federal Data Privacy Act and the data privacy legislation of the individual *Länder*, the Social Security Code, the German Commercial Code, the Staff Representation Act, the Employees' Representation Act, the Copyright Act, the Patents Act, the Information and Communication Services Act (IuKDG), the Control and Transparency in Business Act (KonTraG).

Examples of relevant regulations are:

Administrative regulations, ordinances, and service regulations.

Examples of contracts:

Service contracts in the area of data processing, contracts for the safeguarding of business/industrial secrets.

Questions:

Loss of confidentiality

Is confidentiality of the data required by law?

Is disclosure of information likely to result in criminal prosecution or a claim for compensation?

Is the agency/company bound to observe any contracts which stipulate that certain information is to be treated as confidential?

Loss of integrity

Is data integrity required by law?

How severe would any violation of regulations/laws due to loss of integrity be?

Loss of availability

Would failure of the IT application result in infringement of any regulations or even of any laws? If so, to what extent?

Is certain information required to be available at all times by law?

Have any deadlines been set which it is imperative to observe when using the IT application?

Are there any contractual conditions for certain deadlines which have to be observed?

Damage scenario "Impairment of the right to informational self-determination"

When implementing and operating IT systems and IT applications, the danger exists of impairing the right to informational self-determination which can lead to abuse of person-related data.

Examples of impairment of the right to informational self-determination include:

- unauthorised collection of person-related data without legal cause or the consent of the individual;
- unauthorised acquisition of information during data processing or the transmission of person-related data;
- unauthorised disclosure of person-related data;
- use of person-related data for a purpose other than the permitted purpose for which it was collected;
- corruption of person-related data in IT systems or during the transmission of data.

The following questions can be used to assess the consequences and the extent of any damage:

Questions:

Loss of confidentiality

What harm could come to an individual if his person-related data were not kept confidential?

Is any person-related data processed for unauthorised purposes?

When carrying out authorised processing of person-related data, is it possible, for example, to determine the health or financial status of a person from this data?

What loss or damage could be caused by misuse of stored person-related data?

Loss of integrity

What harm could come to an individual if his person-related data were to be corrupted by accident or wilfully tampered with?

When would the loss of integrity of person-related data first be noticed?

Loss of availability

Is it possible in the event of an IT application crashing or of a fault occurring during the transmission of person-related data for any data to get lost or become corrupted so that the person concerned's social standing is harmed or he faces the risk of personal or financial detriment?

Damage scenario "Physical injury"

The malfunctioning of an IT system or an IT application can result directly in injury, disability or even death. The extent of the damage must be assessed on the basis of the direct personal damage.

Examples of such IT applications and systems are:

- medical monitoring computers,
- medical diagnosis systems,
- flight control computers, and
- traffic routing systems.

Questions:

Loss of confidentiality

Could a person be physically or psychologically injured through the disclosure of person-related data?

Loss of integrity

Could tampering with program sequences or data endanger people's health?

Loss of availability

Could the failure of an IT application or of the IT system result in physical injury?

Damage scenario "Impaired performance of duties"

Loss of availability of an IT application or loss of data integrity, in particular, can significantly impede or disrupt the performance of tasks within a company or agency. Here, the severity of any ensuing damage depends on the duration of the impairment and the extent to which the services offered are constrained.

Examples are:

- non-adherence to deadlines due to delays in the handling of administrative procedures,
- late delivery due to delayed processing of orders,
- faulty production due to incorrect control parameters,
- insufficient quality assurance due to the failure of a test system.

Questions:

Loss of confidentiality

Is there any data whose confidentiality is critical to task performance (e.g. criminal prosecution information, investigation findings)?

Loss of integrity

Could data alterations restrict the performance of tasks in such a way that the company/agency will be unable to act?

Would significant damage be caused if tasks were performed using corrupt data? When would unauthorised data alterations be detected at the earliest?

Could corrupted data in the IT application under consideration lead to errors in other IT applications?

If data were incorrectly attributed to a person who did not actually generate it, what would be the consequences?

Loss of availability

Could failure of an IT application impair performance of the tasks of the given agency/company to such an extent that the resulting wasted time was no longer acceptable to those concerned?

Would any other IT applications be affected by the failure of this IT application?

Is it important to the agency/company that access to IT applications, including programs and data, must be ensured at all times?

Damage scenario "Negative effects on external relationships"

Loss of one of the fundamental parameters of confidentiality, integrity or availability in an IT application can result in a number of negative effects on external relationships, for example,

- compromise of an agency's/company's image;
- loss of trust in an agency/company;
- impairment of commercial relations between partner companies;
- loss of confidence in the quality of an agency/company's work;
- loss of competitive position.

The extent of damage is defined on the basis of the severity of the loss of confidence, or on how far such external impact has actually spread.

Such damage can have a variety of causes:

- an agency/company's inability to act due to IT system failure;
- incorrect publications on account of manipulated data;
- wrong placing of orders due to faulty stock control programs;
- non-compliance with confidentiality agreements;
- passing on of "*wanted* list" data to interested third parties.
- leaking of confidential data to the press.

Questions:

Loss of confidentiality

What implications would the unauthorised publication of sensitive data stored in the IT application have for the agency/company?

Could the loss of confidentiality of the data stored in the IT application result in any impairment of the enterprise's competitive position?

Would the disclosure of confidential data held in the IT application raise doubts about the observation of official secrecy?

Could the publication of data lead to political or social insecurity?

Loss of integrity

What damage could result from the processing, dissemination or transmission of incorrect or incomplete data?

Would the data corruption become publicly known?

Could the publication of corrupted data lead to a loss of prestige?

Could the publication of corrupted data lead to political or social insecurity?

Could corrupted data lead to reduced product quality and thus to loss of prestige?

Loss of availability

Would the failure of the IT application restrict information services provided to external parties?

Would (temporary) failure of the IT application be noticed by outsiders?

Damage scenario "Financial consequences"

Direct or indirect financial damage can result from the loss of confidentiality of sensitive data, from alteration of data, or from the failure of an IT application. Examples include:

- unauthorised release of R&D results
- manipulation of financially-relevant data in an accounting system
- failure of an IT-controlled production system, resulting in a drop in sales
- obtaining knowledge of marketing strategy papers or of turnover figures
- failure of a booking system of a travel agency
- failure of an e-commerce server
- breakdown of a bank's payment transactions
- theft or destruction of hardware

The extent of the total damage caused is determined by the direct and indirect costs, e.g. damage to property, compensation, additional expenses (e.g. data recovery).

Questions:

Loss of confidentiality

Could the publication of confidential information result in claims for compensation?

Does the IT application contain any data which, if known to a third party (e.g. a competitor), could give it any financial advantage?

Is any research data of significant value stored using the IT application? What would happen if such data were copied and passed on without permission?

Could any damage be caused by premature publication of sensitive data?

Loss of integrity

Could any data relevant to accounting be altered by data manipulation in such a way as to cause financial loss?

Could the publication of incorrect information result in any claims to compensation?

Could any financial loss result from corrupted ordering data (e.g. just-in-time production)?

Could corrupted data lead to wrong business decisions?

Loss of availability

Would failure of the IT application impair production, inventory management or distribution?

Would failure of the IT application result in financial loss due to delayed payments or loss of interest?

How much would it cost to repair or restore the IT system if it were to fail, develop a fault, be destroyed or stolen?

Could failure of the IT application result in deficient solvency or in contractual penalties?

How many important customers would be affected by a failure of the IT application?

Step 3: documentation of the results

It is recommended that the protection requirements ascertained above for the various IT applications are documented in a table. Such a central document offers the advantage that it can be referenced during the subsequent assessment of the protection requirements of the IT systems.

Care should be taken here to ensure that not only the assessed protection requirements are documented, but also the underlying rationale for these conclusions. This rationale will ensure that the conclusions can be traced and reused subsequently.

Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 4

The table below shows the main IT applications, their protection requirements and the reasoning behind the assignment of protection requirements categories.

IT application			Assessment of protection requirements		
No.	**Name**	**Personal data**	**Basic parameter**	**Protection Requirement**	**Rationale**
A1	Processing of HR data	X	Confidentiality	High	HR data constitutes particularly sensitive personal details, disclosure of which could significantly harm the person concerned.
			Integrity	Moderate	The protection requirement is only "moderate" since errors can be detected quickly and data subsequently corrected.
			Availability	Moderate	Down times of up to a week can be handled by following manual procedures.
A2	Benefits processing	X	Confidentiality	High	Benefits data includes person-related data which has a particularly high protection requirement. Some of it may also refer to illnesses and the results of medical tests. Disclosure of this data could be very harmful to the persons concerned.
			Integrity	Moderate	The protection requirements is only "moderate" since errors can be detected quickly and data subsequently corrected.
			Availability	Moderate	Down times of up to a week can be handled by following manual procedures.

At this point it may be appropriate to look beyond this information and consider the protection requirements also from an overall view of the business processes or specialist tasks. To this end it is recommended describing the purpose of an IT application within a business process or in a specialist task and inferring its importance from this. This importance can be classified as follows:

The importance of the IT application to the business process or specialist task is

- **Basic to moderate:** the business process or specialist task can be performed by alternative means (e.g. manually) at a level of additional expense that is acceptable.
- **High:** the business process or specialist task can be performed by alternative means (e.g. manually) at significant additional expense.

- **Very high:** the business process or specialist task cannot be performed at all without the IT application.

The particular advantage of implementing such a standard assignment to predefined categories is that when it comes to the assessment of protection requirements, Management, which has the last say in determining the protection requirement of individual IT applications, can now act. For example, it might be that a person responsible for an IT application views its protection requirements as "basic", whereas a manager might assess it more highly, given his view of the application within the wider business process or specialist task.

This optional data should likewise be documented in a table.

Assessment of protection requirements for IT systems

In order to determine the protection requirement of an IT system, it is first of all necessary to consider the IT applications which have a direct association with the IT system. A summary of which IT applications are relevant was prepared under the previous step "Capturing information about the IT applications and related information".

In order to determine the protection requirement of the IT system, the potential damage to the relevant IT applications must be considered in its entirety. The protection requirement of an IT system is determined by the damage or the sum of the most serious instances of damage (**maximum principle**).

When studying the possible damage and its implications, it must also be born in mind that IT applications of an IT system may use the results of other IT applications as input. A seemingly less important IT application A can assume significantly greater importance if another, important IT application B depends on its results. In this case the protection requirement ascertained for IT application B must also be transferred to IT application A. If the IT applications in question are from different IT systems, the protection requirements of the first IT system must be transferred to the other **(dependency relationship)**.

If several IT applications or sets of information are processed on one IT system, it should be considered whether the cumulative effect of several cases of (e.g. minor) damage is greater. In this case, the protection requirement of the IT system increases accordingly **(cumulative effect)**.

Example: All the IT applications used by the typing department are held on one network server. The damage in the event of failure of this IT application was estimated as low, however, as there are sufficient alternatives. Should the server fail, however, (and thus also all the IT applications), the resulting damage is considerably higher. It may no longer be possible to perform the work required within the necessary time-frame. The protection requirement of these "central" components should thus also be considered higher.

The opposite effect can also occur. Thus it is possible for an IT application to have a high protection requirement, but for its protection requirement not to be passed on to an IT system under consideration because only insignificant parts of the IT application run on that IT system. In this case the protection requirement must be put in perspective (**distribution effect**).

Examples: The distribution effect is mainly relevant to the basic parameter of availability. Thus, for example, where IT systems have been designed in a redundant fashion, the protection requirement of the individual components may be lower than that for the entire application. Distribution effects are also possible in the area of confidentiality. For example, if there is no possibility of a client being able to retrieve critical data from a highly confidential database application, then the client, unlike the database server, may have only a low protection requirement.

Presentation of Results

The results of the assessment of the protection requirements of the IT systems should once again be recorded in a table. This should show the protection requirements of each IT system with regard to confidentiality, integrity and availability. Particular importance is to be attached to providing a rationale for the assessments made so that these **can also be understood** by third parties. Here reference may be made to the assessment of protection requirements for the IT application.

Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 5

Such a table might be structured as follows:

IT system		Assessment of protection requirements		
No.	**Description**	**Basic Parameter**	**Protec-tion Reqt.**	**Reasoning**
S1	Server for Human Resources	Confidentiality	High	Maximum principle
		Integrity	Moderat e	Maximum principle
		Availability	Moderat e	Maximum principle
S2	Primary domain controller	Confidentiality	Moderat e	Maximum principle
		Integrity	High	Maximum principle
		Availability	Moderat e	The protection requirement for application A4 has been assessed as high; therefore a high protection requirements for this parameter should be assumed. However, it should be borne in mind that this application is distributed over two computer systems. It is also possible for staff working in the Bonn office to be authenticated via the backup domain controller in Berlin. Unserviceability of the primary domain controller is acceptable for a period of up to 72 hours. Given this distribution effect, the protection requirement is therefore only "moderate".

Notes: If the majority of IT applications on an IT system require only moderate protection, and one or only a few require high protection, it may be appropriate to consider the option of transferring these few applications to a stand-alone IT system as a way of achieving possible savings. The case for such an alternative can be prepared for submission to Management for a decision.

Additional aids:

Some record sheets have been developed as an aid to the task of assessing protection requirements. These will be found on the CD-ROM which comes with the manual (see Annex: Auxiliary Aids).

Assessment of protection requirements for communications links

Once the protection requirements for the IT systems under consideration have been established in the previous step, the protection requirement regarding the networking structure must now be determined. The main source used here is the network plan prepared in Section 2.1 for the IT assets under investigation.

To prepare the way for decisions as to which communications routes require the use of cryptographic security safeguards, which parts of the network should have built-in redundancy and over which connections attacks by insiders and external adversaries are to be expected, as well as the IT systems

themselves, the various communications links must now be considered. In this analysis, the following communications links should be regarded as critical:

- Communication links to the outside world, i.e. which lead into or through uncontrolled areas (e.g. to the Internet or over land to which the public have access). These links are potentially exposed to the threat of attempts to penetrate the system to be protected from outside and the danger of computer viruses or Trojan horses being imported. Moreover, an internal perpetrator could pass confidential information to the outside world over such connection.
- Communications links over which information which has a high protection requirement is transmitted. The information concerned may have a high protection requirement as regards either one or more of the basic parameters of confidentiality, integrity and availability. These links could be targeted for wilful bugging or tampering. Moreover, failure of such a link could have a detrimental effect on the operational capability of significant numbers of IT assets.
- Communications links over which certain highly sensitive information may not be transmitted. Here the primary concern is the transmission of confidential information. If any network switching elements are configured inappropriately or incorrectly, it could be possible for precisely this information which should not be transmitted over such a connection to nevertheless be transmitted and as a result become vulnerable to attack.

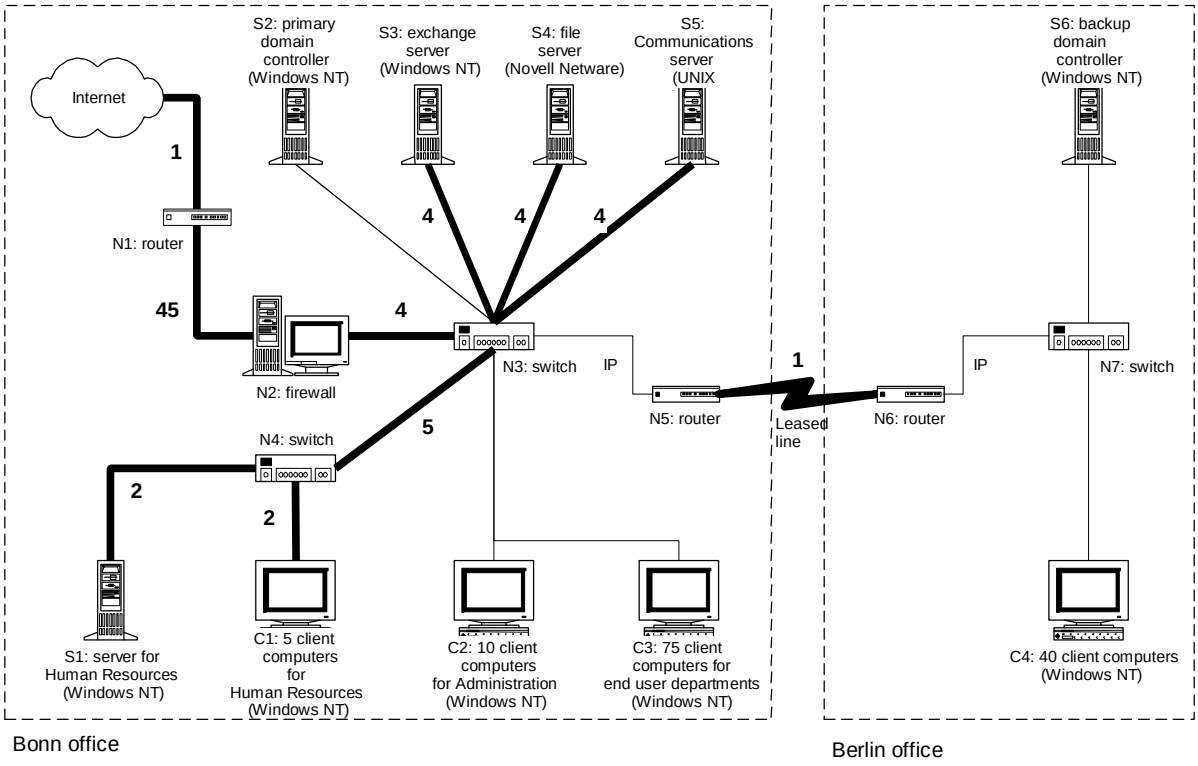
One approach to gathering information about critical communications links is as follows. Initially all "external connections" are identified and recorded as critical connections. All the connections which lead from an IT system with a high or very high protection requirement are then investigated. In this way the connections over which information having a high protection requirement is transmitted are identified. The connections over which this sensitive data is transmitted downstream are then investigated. Finally the communication links over which such information is not supposed to be transmitted must be identified. The information collected should include:

- the communications routes;
- whether the connection has an outside link;
- whether information having a high protection requirements is transmitted and whether this protection requirement is related to confidentiality, integrity or availability;
- whether information having a high protection requirement is not allowed to be transmitted over the line.

The data collected during this exercise can either be documented in tabular form or else highlighted graphically on the network plan.

Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 6

In our fictitious example of the BOC, there are the following critical connections:



In the diagram, the critical connections are indicated by "bold" lines. The numbers next to the lines indicate the reason (or reasons) why a particular connection is critical and are explained in the column headings of the next table.

	Reason for criticality				
Connection	**1 External connect-ion**	**2 High confiden-tiality**	**3 High integrity**	**4 High availability**	**5 Transmission not permitted**
N1 - Internet	X				
N5 - N6	X				
S1 - N4		X			
S3 - N3				X	
S4 - N3				X	
S5 - N3				X	
C1 - N4		X			
N1 - N2				X	X
N2 - N3				X	
N4 - N3					X

It is very important during this survey to make sure that the summary produced is complete. It only takes **one** critical connection to be omitted for the overall security to be compromised. Thus, for example, all the modems used must be recorded as potentially critical connections to the outside world could run from them. Often, however, these modem external connections are viewed as objects conferring prestige on their "owners" and their existence is denied in order to obtain personal advantage, or modems are purchased and classified as consumables without those responsible for IT being informed of the purpose for which they are to be used. However, if IT security is to be maximised, such critical devices and connections must not be overlooked.

Assessment of protection requirements for IT rooms

When it comes to IT baseline protection modelling and planning of the target versus actual comparison, it will be helpful if a summary has been drawn up of the rooms in which IT systems are installed or which are used for IT operations. These include both rooms which are used solely for IT operations (e.g. server rooms, data media archives) and rooms in which IT systems happen to be operated (e.g. offices). Where an IT system is housed in a protective cabinet instead of in a special technology room, the protective cabinet should be classified as a room.

Note: the installation locations should have already been recorded when information was being gathered about the IT systems.

The protection requirements for each room should then be derived from the results of the assessment of the protection requirements of the IT systems. This protection requirement is derived from the protection requirements of the IT systems or the data media stored in the room according to the maximum principle. During this assessment the possibility of a cumulative effect should be considered where a relatively large number of IT systems are located in a single room, such as is frequently the case in server rooms. In addition, the reasoning behind the assessed protection requirement should be documented.

Once again, it is helpful to draw up a table containing the necessary information.

Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 7

The table below shows an extract of the results obtained for the BOV:

Room			**IT assets**	**Protection requirement**		
Desig-nation	Type	Location	IT systems / data media	Confiden-tiality	Integrity	Availabilit y
R U.02	Data media archive	Bonn building	Backup data media (weekly backups of servers S1 to S5)	High	High	Modera te
R B.02	Technology room	Bonn building	Private Branch Exchange	Modera te	Modera te	High
R 1.01	Server room	Bonn building	S1, N4	High	High	Modera te
R 1.02 - R 1.06	Offices	Bonn building	C1	High	Modera te	Modera te
R 3.11	Protective cabinet in room R 3.11	Bonn building	Backup data media (daily backups of servers S1 to S5)	High	High	Modera te

R E.03	Server room	Bonn building	S6, N6, N7	Moderate	High	High
R 2.01 - R 2.40	Offices	Bonn building	C4, some with fax machines	Moderate	Moderate	Moderate

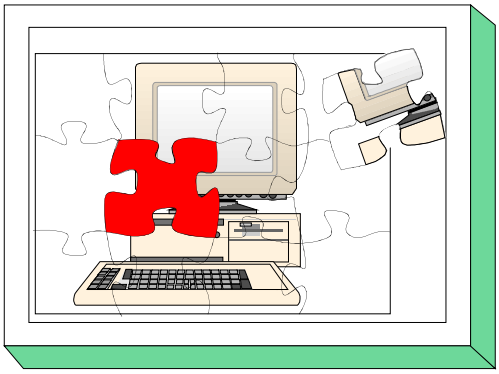
Interpreting the results of the protection requirement assessment

The results obtained from the protection requirements assessment serve as the starting point from which to proceed towards drawing up the IT security concept. The assumptions regarding protection requirements categories which are used to deduce the level of protection afforded by the standard security safeguards recommended in this manual are as follows:

Protective effect of standard security safeguards aimed at achieving IT baseline protection	
Protection requirement category "Basic to moderate"	Standard security safeguards aimed at IT baseline protection are generally adequate and reasonable.
Protection requirement category "High"	Standard security safeguards aimed at IT baseline protection afford a basic level of protection but may not be sufficient on their own. Additional safeguards can be ascertained by performing a supplementary security analysis.
Protection requirement category "Very high"	Standard security safeguards aimed at IT baseline protection afford a basic level of protection but generally are not sufficient on their own. The necessary additional security safeguards must be ascertained on a case-by-case basis on the basis of a supplementary security analysis.

If the protection requirement for an IT system is defined as "moderate", then it is sufficient to implement the standard safeguards aimed at IT baseline protection across the board. For IT systems, network connections and rooms where IT assets are used which have a "high", and especially if they have a "very high", protection requirement, a supplementary security analysis should be planned in. Again, the high protection requirement of these components should be borne in mind during the target versus actual comparison when working through safeguards identified in the manual as being "optional". Thus, for example, safeguard S 1.10 *Use of Safety Doors* may not be necessary in a server room which has a moderate protection requirement, yet where a high level of confidentiality is required it could be absolutely essential.

2.3 IT Baseline Protection Modelling



Once the required information is available from the IT structure analysis and the assessment of protection requirements, the next major task is to model the IT assets under consideration with the aid of the existing modules of the IT Baseline Protection Manual. The outcome of this exercise is an IT baseline protection model of the IT assets which is made up from different modules of the manual, in some cases with the same modules being used several times over, and maps the security-relevant aspects of the IT assets onto specific modules and vice versa.

It makes no difference to the IT baseline protection model created whether the IT assets consist of IT systems already in service or whether the IT assets in question are still at the planning stage. However, the model may be used differently depending on whether the assets are already in use or not.

- The IT baseline protection model for IT assets already in service identifies the standard security safeguards that are relevant through the modules used. It can be used in the form of a **test plan** for carrying out a target versus actual comparison.
- By contrast, the IT baseline protection module for a planned set of IT assets constitutes a **design concept**. It specifies via the selected modules which standard security safeguards must be implemented on entry into service of the IT assets.

The diagram below clarifies the role of the modelling and its possible outcomes:

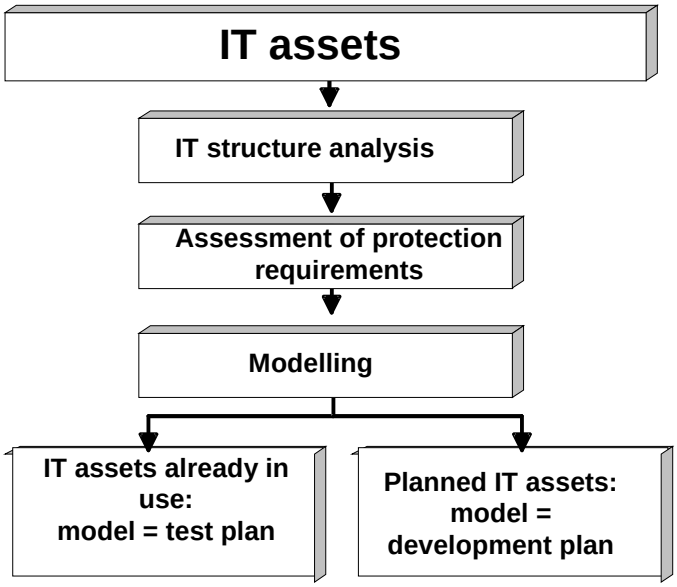


Figure: outcome of IT baseline protection modelling

Typically a set of IT assets currently in use will contain not only elements which have already been implemented but also elements which are still at the planning stage. The resulting IT baseline protection model then contains both a test plan and also elements of a design concept. The IT security concept will then be based on a combination of the IT security safeguards which are identified during

the target versus actual comparison as being inadequate or missing and those identified for IT assets which are still at the planning stage.

To map a generally complex set of IT assets to the modules in the manual it is recommended that the IT security aspects are considered as groups arranged according to particular topics.

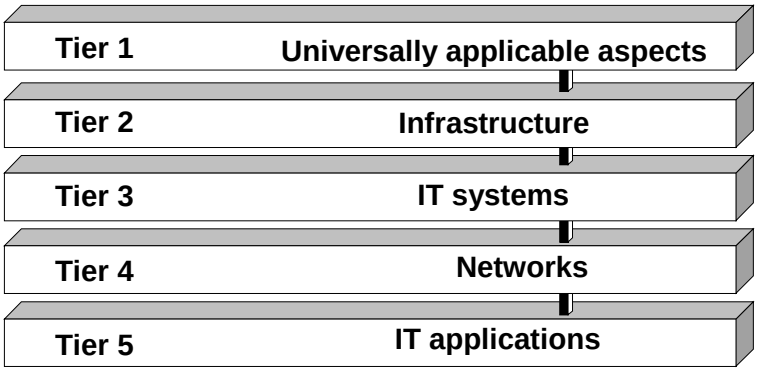


Figure: Tiers in the IT baseline protection model

The IT security aspects of a set of IT assets are assigned to the individual tiers as follows:

- Tier 1 covers all the general IT security aspects which apply equally to all or large numbers of the IT assets, particularly any universally applicable concepts and the procedures derived therefrom. Typical Tier 1 modules include *IT Security Management*, *Organisation*, *Data Backup Policy* and *Computer Virus Protection Concept*.
- Tier 2 is concerned with architectural and structural factors, in which aspects of the infrastructural security are brought together. This concerns especially the *Buildings*, *Rooms*, *Protective Cabinets* and *Working Place at Home (Telecommuting)* modules.
- Tier 3 concerns the individual IT systems in the set of IT assets which may be grouped together. The IT security aspects considered here relate not only to clients but also to servers and stand-alone systems. Thus, for example, the modules *UNIX System*, *Laptop PC*, *Windows NT Network* and *Telecommunications System (Private Branch Exchange)* fall within Tier 3.
- Tier 4 considers the networking aspects of the IT systems, which refer to the network connections and communications rather than to particular IT systems. The modules which are relevant here include, for example, *Heterogeneous Networks*, *Network and System Management* and *Firewalls*.
- Finally Tier 5 is concerned with the actual IT applications which are used on the IT assets. In this tier, the modules used for modelling purposes could include *E-Mail*, *WWW Server*, *Fax Servers* and *Databases*.

Using this tier approach has the following advantages.

- The complexity of the IT security is reduced because the individual aspects are divided up in a meaningful manner.
- As higher order aspects and common infrastructural issues are considered separately from the IT systems, duplication of effort is avoided as those aspects only need to be dealt with once and not repeated for every IT system.
- The various tiers have been defined so that responsibilities for the aspects under consideration are grouped. Tier 1 is concerned with fundamental issues relating to the use of IT, Tier 2 with site technical services, Tier 3 with matters that concern administrators and IT users, Tier 4 with matters

that concern the network and system administrators and finally Tier 5 with matters that concern those responsible for or who will run the IT applications.

- Breaking down the security aspects into tiers enables individual subject areas within the ensuing IT security concepts to be updated and expanded more easily, without having a significant effect on other tiers.

IT baseline protection modelling entails determining for the modules of a given tier whether and how they can be used to map the IT assets. Depending on the module considered, the objects which are mapped in this way may be of different kinds: individual components, groups of components, buildings, property, organisational units etc. If the target object is a group, then representative samples should be selected from it, and the relevant module should then be applied to those samples.

The IT baseline protection model, i.e. the assignment of modules to target objects, should be documented in the form of a table containing the following columns:

- *Number and title of the module*.
- *Target object or target group*. For example, this could be the identification number of a component or a group or the name of a building or organisational unit.
- *Sample*. If the target object is a group, then the number and names of the samples taken from this group should be noted.
- *Contact person*. This column serves initially only as a place holder. The contact person is not determined at the modelling stage, but only at the point when the target versus actual comparison in the basic security check is being planned.
- NB incidental information and the reasoning behind the modelling can be documented in this column.

The procedure for modelling a set of IT assets is described in detail in Section 2.3.1 below. Particular importance here is attached to any constraints which apply, when it is appropriate to use a given module and to which target objects it should be applied. Section 2.3.2 presents a shortened modelling procedure for the special case of a single IT system or a single group.

2.3.1 Modelling a Set of IT Assets

When modelling a set of IT assets it is recommended that the modules are assigned using the 5-tier model. This is then followed by a completeness check.

Tier 1: Higher order aspects of IT security

In this tier the generic aspects of the IT assets, which apply to each individual component, are modelled. The primary elements under consideration here are policies and procedures derived from those policies. These aspects should be controlled uniformly for the entire set of IT assets so that in most cases the corresponding modules then only have to be applied once to the entire set of IT assets.

- Module 3.0 **Security Management** is applied once to the entire set of IT assets.
- Module 3.1 **Organisation** must be used at least once for every set of IT assets. If some of the IT assets under consideration are assigned to another organisational unit and are therefore subject to different framework conditions, the module should be applied separately to each organisational unit. If some of the IT assets are outsourced, this should be viewed as an important special case.
- Module 3.2 **Personnel** must be used at least once for every set of IT assets. If some of the IT assets under consideration are assigned to a different organisation or organisational unit and are therefore subject to different framework conditions, the module should be applied separately to each organisation or organisational unit. If some of the IT assets are outsourced, this should be viewed as an important special case.
- Module 3.3 **Contingency Planning Concept** must as a minimum be used where any components have been identified during the protection requirements assessment as having a high or very high protection requirement as regards availability or where relatively large IT systems and/or extensive networks are operated. When working through the module, particular attention should be given to these components.
- Module 3.4 **Data Backup Policy** is applied once to the entire set of IT assets.
- Module 3.6 **Computer Virus Protection Concept** should be applied once to the entire set of IT assets if this includes any systems which could fall prey to computer viruses.
- Module 3.7 **Crypto concept** should as a minimum be used where any components have been identified in the protection requirements assessment as having a high or very high protection requirement as regards confidentiality or integrity or where cryptographic procedures are already in use.
- Module 3.8 **Handling of security incidents** should as a minimum be used where any components have been identified in the protection requirements assessment as having a high or very high protection requirements as regards one of three basic parameters, or where failure of the entire set of IT assets would result in damage in the categories "high" or "very high".
- Module 9.1 **Standard Software** should be applied at least once to the entire set of IT assets. If there are any sub-areas within the IT assets which have different requirements or procedures as regards the use of standard software, then module 9.1 should be applied to each of these sub-areas separately.

Tier 2: Security of the infrastructure

The structural conditions relevant to the existing IT assets are modelled with the aid of the modules contained in Chapter 4 *Infrastructure*. This entails assignment of the relevant module from the IT Baseline Protection Manual to every building, room or protective cabinet (or group of these components).

- Module 4.1 **Buildings** must be used once for every building or every sample taken from a group of buildings.
- Module 4.2 **Cabling** must generally be applied once per building or sample of buildings (in addition to module 4.1). However, it may be that certain areas, for example the server room or control room, have special cabling requirements, in which case it may be advisable to apply module 4.2 to those parts of the building separately.
- Module 4.3.1 **Office** must be applied to all rooms or samples of rooms in which information technology is used but to which none of modules 4.3.2, 4.3.3 or 4.3.4 is being applied.
- Module 4.3.2 **Server Room** must be applied to every room or sample of rooms in which servers or PBXs are operated. Servers are IT systems which make services available on the network.
- Module 4.3.3 **Data Media Archives** must be applied to every room or sample of rooms in which data media are stored or archived.
- Module 4.3.4 **Technical Infrastructure Room** must be applied to every room or sample of rooms in which technical devices which require little or no human intervention to run are operated (e.g. distribution cabinet or standby power supply system).
- Module 4.4 must be applied to every **protective cabinet** or sample of cabinets once. Protective cabinets can serve as an alternative to a dedicated server room.
- Module 4.5 must be applied once to every **working place at home** or sample of the same (if corresponding groups have been defined).

Tier 3: Security of the IT systems

This tier is concerned with security aspects relating to IT systems, i.e. to server and client computers, hosts, terminals etc. Tier 3 is covered by modules from Chapters 5 to 9 of the IT Baseline Protection Manual.

By analogy with the area "Security of the infrastructure", the modules relating to the area of "Security of the IT systems" may be applied either to individual IT systems or to samples from groups. This is assumed below although no further specific reference to it is made.

- Module 5.1 **DOS-PC (single user)** must be applied to every stand-alone computer or client on which the DOS operating system is installed.
- Module 5.2 **UNIX System** must be applied to every stand-alone computer or client which runs under the UNIX operating system.
- Module 5.3 **Laptop PC** must be applied to every mobile computer (laptop).
- Module 5.4 **PCs with a Non-Constant User Population** must be applied to every stand-alone computer or client on which different users work at different times.

  NB it may not be necessary to apply module 5.4 to IT systems which are being modelled using modules 5.5, 5.6 or 5.9. These modules specifically address security aspects of situations where IT assets are used at different times by different users.
- Module 5.5 **PC under Windows NT** must be applied to every stand-alone computer or client which runs under Windows NT.
- Module 5.6 **PC with Windows 95** must be applied to every stand-alone computer or client which runs under Windows 95.
- Module 5.99 **Stand-alone IT systems** must be applied to every IT system for which there is no operating system-specific module in the IT Baseline Protection Manual.

- Module 6.1 **Server-supported Network** must be applied to every IT system which offers services (e.g. file or print services) as a server in the network.
- Module 6.2 **UNIX Server** must be applied to every server which runs under the UNIX operating system.
- Module 6.3 **Peer-to-Peer Network** must be applied to every client which offers peer-to-peer services (for example shared directories) in the network.
- Module 6.4 **Windows NT Network** must be applied to every server which runs under Windows NT.
- Module 6.5 **Novell Netware 3.x** must be applied to every server which runs under this operating system.
- Module 6.6 **Novell Netware 4.x** must be applied to every server which runs under this operating system.

  NB in addition to the operating system-specific module, module 6.1 must be applied for every server as this module draws together all the platform-independent security aspects of servers.
- Module 8.1 must be applied to every **private branch exchange** or to every sample of the same from a corresponding group.
- Module 8.2 must be applied to every **fax machine** or to every sample of the same from a corresponding group.
- Module 8.3 must be applied to every **answering machine** or to every sample of the same from a corresponding group.
- Module 8.6 **Mobile Telephones** should be applied at least once if the use of mobile phones is not forbidden in the organisation or organisational unit under consideration. If there are several different mobile phone operational areas (for example several mobile phone pools) then module 8.6 should be applied separately to each one.
- Module 9.3 **Telecommuting** must also be applied to every IT system which is used for telework.

Tier 4: Security in the network

This tier is concerned with security aspects in the network which cannot be isolated to particular IT systems (e.g. servers) in the network. Rather, the concern here is those security aspects which relate to the network connections and communications between the IT systems.

To simplify matters, it may be appropriate to consider sections within the complete network rather than the whole network at once. The division of the full network into subnetworks should be performed in accordance with these two criteria:

- The assessment of protection requirements will have identified connections over which certain data must under no circumstances be transported. These connections should be viewed as "interfaces" between subnetworks, i.e. the two endpoints of such a connection should be in different subnetworks. Conversely, connections which transport data that has a high or very high protection requirement should if possible not pass over any subnetwork boundaries. If this principle is followed, the protection requirements of the resulting subnetworks will be uniform as far as possible.
- Components which are only connected to each other over a long-distance connection should not be assigned to the same subnetwork i.e. subnetworks should not extend over more than one location or property. This is desirable both in order to retain an overview and for the efficient conduct of the project.

If these two criteria do not lend themselves to a suitable division of the full network (for example because some of the resulting subnetworks are too large or too small), as an alternative the division into subnetworks may proceed at the organisational level. Under this approach, the subnetworks are defined so that they correspond to discreet areas of responsibility of the different administrators or teams of administrators.

It is not possible to make a definite recommendation as to how best to subdivide the complete network into subnetworks, as the requirements stated above might be incompatible with the existing IT assets. Instead, a decision should be made in the individual case as to what is the most practical way of splitting up the complete network, bearing in mind the modules of the IT Baseline Protection Manual which are to be used.

- Module 6.7 **Heterogeneous Networks** must generally be applied to every subnetwork. However, if the subnetworks are small and several subnetworks fall within the responsibility of the same team of administrators, it may be sufficient to apply module 6.7 only once to all of these subnetworks.
- Module 6.8 **Network and System Management** must be applied to every network or system management system used on the IT assets under consideration.
- Module 7.2 **Modem** must be applied to every IT system equipped with a modem or to each corresponding sample thereof.
- Module 7.3 **Firewall** must be applied to every external connection to third party IT systems or networks where IT systems in the internal network which have a high protection requirement can be accessed over this external connection. This applies also if no firewall system is in use there yet. Examples here are Internet connections, remote access facilities and links to networks owned by business partners.
- Module 7.6 **Remote Access** must be applied once wherever remote access to the internal network is possible by a route other than over a dedicated leased line (e.g. telework, linking of staff working out in the field over analogue dial-up lines, ISDN or mobile phone).
- Module 8.4 **LAN integration of an IT system via ISDN** must be applied to all external connections which are implemented over ISDN.

Tier 5: Security in applications

The lowest tier entails modelling of the applications. Modern applications are seldom limited to a single IT system. In particular, core applications used across an entire organisation are generally implemented as client/server applications. In many cases servers themselves access other servers downstream, e.g. database systems. The security of the applications must therefore be considered independently of the IT systems and networks.

- Module 7.1 **Exchange of Data Media** should be used once for every application which serves as a source of data for an exchange of data media or processes data received by this route.
- Module 7.4 **E-Mail** must be applied to every e-mail system (internal or external) of the IT assets under consideration.
- Module 7.5 **WWW Server** must be applied to every WWW service (e.g. Intranet or Internet) of the IT assets under consideration.
- Module 8.5 must be applied to every **fax server** or to every sample of the same from a corresponding group.
- Module 9.2 **Databases** should be used once for every database system or sample of the same.

Completeness check

In the final step a check should be performed as to whether the entire system has been modelled without any gaps. It is recommended that the network plan or a similar overview of the IT assets is used here and that the individual components are checked systematically. Every component should either be assigned to a group or else be modelled separately. If the complete network has been divided into subnetworks in connection with Tier 4, a check should be performed as to whether

- every subnetwork has been completely represented and
- the sum of all the subnetworks completely describes the whole system.

It is important that not only all hardware and software components are represented from a technical perspective, but that the related organisational, personnel and infrastructural aspects are fully covered also. This can be checked using the tables provided in Section 2.3.2, in which for a few typical components those modules of the IT Baseline Protection Manual which should be included in the modelling in every case are specified.

If, when performing these checks, any gaps are revealed in the modelling, the relevant missing components must be added. Otherwise there is a risk that important elements of the complete system or important security aspects will be overlooked when using the IT Baseline Protection Manual.

If it is not possible to perform all the modelling because some modules which are needed are missing from the IT Baseline Protection Manual, we would ask you to notify your requirements to the BSI's IT Baseline Protection Hotline.

Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 8

The table below is an excerpt from the modelling performed for the fictitious BOV Department.

No.	Name of module	Target object / target group	Sample	Contact person	Notes
3.1	Organisation	Bonn site			The Organisation module must be worked through separately for the Bonn and Berlin sites, as Berlin has its own organisational procedures.
3.1	Organisation	Berlin site			
3.2	Personnel	Entire BOV			The BOV's Human Resources Department is located centrally in Bonn.
4.3.3	Storage Media Archives	R U.02 (Bonn)			The backup data media are kept in this room.
5.3	Laptop PC	C5	1 in R 1.06 (Bonn)		A sample will be selected from all the laptops, both in Bonn and Berlin.
5.3	Laptop PC	C6	1 in R 2.01 (Berlin)		
7.5	WWW Server	S5			S5 functions as the server for the Intranet.
9.2	Databases	S5			A database is used on server S5.

2.3.2 Modelling of an Individual IT System

Depending on the object(s) under examination, the tables below serve different functions. If the IT assets under consideration consists only of a single IT system or a single group of IT systems which have the same configuration, same framework conditions and same applications, then as a minimum the modules required for modelling can be read directly out of these tables. Modules with no entry in the relevant column should be used as well if they are relevant to the individual IT system under consideration.

If on the other hand the IT assets are composed out of different components, then the tables provided below will help in checking whether modelling as described in Section 2.3.1 is complete. If, for example, the present IT assets contains Windows NT clients, then all the modules which have an "X" in the relevant table should be considered during modelling. Modules identified with "(X)" only need to be used when certain conditions apply. These conditions are listed in Section 2.3.1.

Key:

X: The module must be applied to this IT system.

(X): The module must be applied to this IT system if the conditions specified in Sectio 2.3.1 apply.

X1: A server room can be replaced by a server cabinet.

	IT Systems	**Stand-Alone Systems / Clients**					
	Module	DOS-PC (Single User)	UNIX System	Laptop PC	PC (Multi-user)	Windows NT PC	Windows 95 PC
3.0	IT Security Management	X	X	X	X	X	X
3.1	Organisation	X	X	X	X	X	X
3.2	Personnel	X	X	X	X	X	X
3.3	Contingency Planning Concept	(X)	(X)	(X)	(X)	(X)	(X)
3.4	Data Backup Policy	X	X	X	X	X	X
3.6	Computer Virus Protection Concept	X	X	X	X	X	X
3.7	Crypto Concept	(X)	(X)	(X)	(X)	(X)	(X)
3.8	Handling of Security Incidents	(X)	(X)	(X)	(X)	(X)	(X)
4.1	Buildings	X	X		X	X	X
4.2	Cabling	X	X		X	X	X
4.3.1	Offices	X	X		X	X	X
4.3.2	Server rooms						
4.3.3	Storage Media Archives						
4.3.4	Technical Infrastructure Rooms						
4.4	Protective Cabinets						

4.5	Working Place At Home (Telecommuting)						
5.1	DOS PC (Single User)	X		(X)	(X)		
5.2	UNIX System		X	(X)	(X)		
5.3	Laptop PC			X	(X)		
5.4	PCs With a Non-Constant User Population	(X)	(X)	(X)	X		
5.5	PC under Windows NT			(X)		X	
5.6	PC with Windows 95			(X)			X
5.99	Stand-Alone IT Systems Generally						
6.1	Server-Supported Network						
6.2	UNIX Server						
6.3	Peer-to-Peer Network						
6.4	Windows NT Network						
6.5	Novell Netware 3.x						
6.6	Novell Netware 4.x						
6.7	Heterogeneous Networks						
6.8	Network and System Management						
7.1	Exchange of Data Media	(X)	(X)	(X)	(X)	(X)	(X)
7.2	Modem						
7.3	Firewall						
7.4	E-Mail						
7.5	WWW Server						
7.6	Remote Access						
8.1	Telecommunications System (Private Branch Exchange, PBX)						
8.2	Fax Machine						
8.3	Answering Machine						
8.4	LAN connection over ISDN						
8.5	Fax Servers						
8.6	Mobile Telephones						
9.1	Standard Software	X	X	X	X	X	X
9.2	Databases						
9.3	Telecommuting						

	IT Systems	**Stand-Alone Systems / Clients**	**Stand-Alone Systems / Clients**
	Module	Telecommuting	Stand-Alone IT Systems Generally
3.0	IT Security Management	X	X
3.1	Organisation	X	X
3.2	Personnel	X	X
3.3	Contingency Planning Concept	(X)	(X)
3.4	Data Backup Policy	X	X
3.6	Computer Virus Protection Concept	X	X
3.7	Crypto Concept	(X)	(X)
3.8	Handling of Security Incidents	(X)	(X)
4.1	Buildings		X
4.2	Cabling		X
4.3.1	Offices		X
4.3.2	Server Rooms		
4.3.3	Storage Media Archives		
4.3.4	Technical Infrastructure Rooms		
4.4	Protective Cabinets		
4.5	Working Place At Home (Telecommuting)	X	
5.1	DOS PC (Single User)	(X)	
5.2	UNIX System	(X)	
5.3	Laptop PC		
5.4	PCs With a Non-Constant User Population		
5.5	PC under Windows NT	(X)	
5.6	PC with Windows 95	(X)	
5.99	Stand-Alone IT Systems Generally	(X)	X
6.1	Server-Supported Network		
6.2	UNIX Server		
6.3	Peer-to-Peer Network		
6.4	Windows NT Network		
6.5	Novell Netware 3.x		
6.6	Novell Netware 4.x		
6.7	Heterogeneous Networks		
6.8	Network and System Management		

7.1	Exchange of Data Media	(X)	(X)
7.2	Modem	(X)	
7.3	Firewall		
7.4	E-Mail		
7.5	WWW Server		
7.6	Remote Access		
8.1	Telecommunications System (Private Branch Exchange, PBX)		
8.2	Fax Machine	(X)	
8.3	Answering Machine	(X)	
8.4	LAN connection over ISDN	(X)	
8.5	Fax Servers		
8.6	Mobile Telephones		
9.1	Standard Software	X	X
9.2	Databases		
9.3	Telecommuting	X	

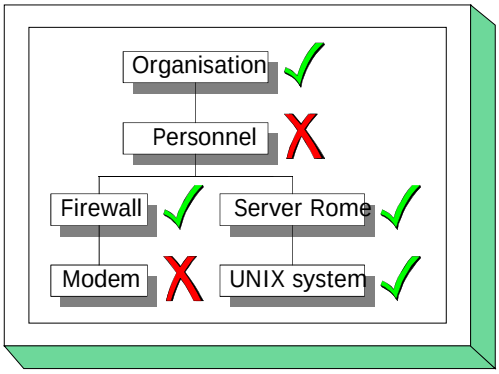
	IT System	**Server / Network**				
	Module	UNIX Network	Peer-to-Peer Network	Windows NT Network	Novell 3.x Network	Novell 4.x Network
3.0	IT Security Management	X	X	X	X	X
3.1	Organisation	X	X	X	X	X
3.2	Personnel	X	X	X	X	X
3.3	Contingency Planning Concept	(X)	(X)	(X)	(X)	(X)
3.4	Data Backup Policy	X	X	X	X	X
3.6	Computer Virus Protection Concept	X	X	X	X	X
3.7	Crypto Concept	(X)	(X)	(X)	(X)	(X)
3.8	Handling of Security Incidents	(X)	(X)	(X)	(X)	(X)
4.1	Buildings	X	X	X	X	X
4.2	Cabling	X	X	X	X	X
4.3.1	Offices		X			
4.3.2	Server Rooms	X		X	X	X
4.3.3	Storage Media Archives					
4.3.4	Technical Infrastructure Rooms					
4.4	Protective Cabinets	X1	X1	X1	X1	X1
4.5	Working Place At Home (Telecommuting)					

5.1	DOS PC (Single User)		(X)			
5.2	UNIX System		(X)			
5.3	Laptop PC		(X)			
5.4	PCs With a Non-Constant User Population		(X)			
5.5	PC under Windows NT		(X)			
5.6	PC with Windows 95		(X)			
5.99	Stand-Alone IT Systems Generally		(X)			
6.1	Server-Supported Network	X		X	X	X
6.2	UNIX Server	X				
6.3	Peer-to-Peer Network		X			
6.4	Windows NT Network			X		
6.5	Novell Netware 3.x				X	
6.6	Novell Netware 4.x					X
6.7	Heterogeneous Networks	X	X	X	X	X
6.8	Network and System Management					
7.1	Exchange of Data Media					
7.2	Modem					
7.3	Firewall					
7.4	E-Mail					
7.5	WWW Server	(X)		(X)	(X)	(X)
7.6	Remote Access					
8.1	Telecommunications System (Private Branch Exchange, PBX)					
8.2	Fax Machine					
8.3	Answering Machine					
8.4	LAN connection over ISDN					
8.5	Fax Servers	(X)		(X)	(X)	(X)
8.6	Mobile Telephones					
9.1	Standard Software	X	X	X	X	X
9.2	Databases	(X)		(X)	(X)	(X)
9.3	Telecommuting					

	IT System	**Communication System**				
	Module	Firewall	Private Branch Exchange	Fax Machine	Answer-phone	Fax Servers
3.0	IT Security Management	X	X	X	X	X
3.1	Organisation	X	X	X	X	X
3.2	Personnel	X	X	X	X	X
3.3	Contingency Planning Concept	(X)	(X)	(X)	(X)	(X)
3.4	Data Backup Policy	X	X	X	X	X
3.6	Computer Virus Protection Concept	X	X	X	X	X
3.7	Crypto Concept	(X)	(X)	(X)	(X)	(X)
3.8	Handling of Security Incidents	(X)	(X)	(X)	(X)	(X)
4.1	Buildings	X	X	X	X	X
4.2	Cabling	X	X	X	X	X
4.3.1	Offices			X	X	
4.3.2	Server Rooms	X	X			X
4.3.3	Storage Media Archives					
4.3.4	Technical Infrastructure Rooms					
4.4	Protective Cabinets	X1	X1			X1
4.5	Working Place At Home (Telecommuting)					
5.1	DOS PC (Single User)					
5.2	UNIX System					
5.3	Laptop PC					
5.4	PCs With a Non-Constant User Population					
5.5	PC under Windows NT					
5.6	PC with Windows 95					
5.99	Stand-Alone IT Systems Generally					
6.1	Server-Supported Network	X				X
6.2	UNIX Server	(X)				(X)
6.3	Peer-to-Peer Network					
6.4	Windows NT Network	(X)				(X)
6.5	Novell Netware 3.x	(X)				(X)
6.6	Novell Netware 4.x	(X)				(X)
6.7	Heterogeneous Networks	X				X
6.8	Network and System Management					
7.1	Exchange of Data Media					

7.2	Modem					
7.3	Firewall	X				
7.4	E-Mail					
7.5	WWW Server					
7.6	Remote Access					
8.1	Telecommunications System (Private Branch Exchange, PBX)		X			
8.2	Fax Machine			X		
8.3	Answering Machine				X	
8.4	LAN connection over ISDN					
8.5	Fax Servers					X
8.6	Mobile Telephones					
9.1	Standard Software	X				X
9.2	Databases					
9.3	Telecommuting					

2.4 Basic Security Check



In the discussion below it is assumed that for a given set of IT assets a summary was prepared of the existing assets, their installation locations and the IT applications supported, based on the IT structure analysis of the IT assets. Building on this, the protection requirements were then assessed, resulting in an overview of the protection requirements of the IT applications, the IT systems, the rooms in which IT assets are used and the communication links. This information was then used to perform IT baseline protection modelling of the IT assets, in the course of which the IT assets under consideration were mapped to modules in the manual.

This IT baseline protection module is now used as a test plan to establish, using a target versus actual comparison, which standard security safeguards have been adequately implemented and which have not been satisfactorily implemented.

This section describes how to perform the basic security check in the context of the central task of drawing up an IT security concept which affords IT baseline protection. This basic security check consists of three different steps. The first step entails making the organisational preparations and in particular selecting the relevant contact persons for the target versus actual comparison. In step 2 the target versus actual comparison is performed using interviews and sampling checks. In the final step, the results of the target versus actual comparison are documented, together with the reasoning behind it.

These three stages of the basic security check are described in detail below.

2.4.1 Organisational Preliminary Work

To ensure that the target versus actual comparison proceeds smoothly, a certain amount of preliminary work is required. It is necessary first to inspect all the in-house documentation which controls IT security-relevant processes, e.g. organisational instructions, work instructions, security instructions, manuals and "informal" procedures. These documents can be helpful in ascertaining the degree of implementation, especially for questions about existing organisational procedures. It is further necessary to clarify who is currently responsible for their content, in order to be able subsequently to determine the correct contact person.

It must then be established whether and to what extent any external parties need to be involved in ascertaining the implementation status. For example, this might be necessary if there are any external computer centres, external parent organisations, companies to which parts of the IT operations have been outsourced or building authorities which are responsible for infrastructural measures.

Another step which needs to be performed before the target versus actual comparison can be carried out is to ascertain who are the right people to interview. Here one should start by establishing a primary point of contact for every individual module which has been used in modelling the existing IT assets.

- For the modules in Tier 1 "Higher order aspects of IT security" a suitable contact person will generally be found from the subject matter dealt with in the module. For example, for module 3.2 *Personnel* someone who works in the relevant Human Resources Department should be selected as point of contact. For the design modules, e.g. module 3.4 *Data Backup Policy*, ideally the person who is responsible for updating the relevant document should be made available. Otherwise the person whose terms of reference include the updating of procedures in the area under consideration should be interviewed.
- For Tier 2 " Infrastructure" the selection of suitable contact persons should be agreed with the general services and/or site technical services sections. Depending on the size of the agency/company being examined, different contact persons could be responsible, for example, for the two infrastructural areas *Cabling* and *Protective Cabinets*. In small organisations the caretaker will often be able to provide information. It should be noted that in the infrastructural area it may be necessary to involve external parties. This applies especially to larger companies and agencies.
- In the modules of Tier 3 "IT systems" and Tier 4 "Networks" there is a heavy emphasis on technical aspects in the security safeguards to be checked. This means that generally the main point of contact will be the administrator for the component or group of components to which the module in question has been assigned during modelling.
- For the modules in Tier 5 "IT applications" persons who support or are responsible for the individual IT applications should be selected as the main points of contact.

In many cases the main point of contact will not be able to provide information on every aspect of the relevant module. In such cases it is useful to include one or more additional persons in the interview. Guidance as to which persons should be involved is provided in the entries "Initiation responsibility" and "Implementation responsibility" which are to be found at the beginning of every safeguard description.

A schedule, possibly including alternative dates, should be prepared to cover the interviews with the system administrators, administrators and other contact persons. Special attention should be given here to co-ordinating appointments with persons from other organisational units or other agencies/companies.

Depending on the size of the project team, tasks should be allocated between different teams of interviewers. Experience shows that working in two-man teams works very well. Here one person writes down the answers and comments on them while the other is asking the necessary questions.

2.4.2 Performing the Target Versus Actual Comparison

Once all the necessary preliminary work has been completed, the actual survey can begin on the previously agreed dates. This entails working through the safeguards contained in the module for which the person being interviewed is responsible in sequence.

The answers regarding implementation status for the individual safeguards may be classified into the following categories:

„Unnecessary“ - Implementation of the recommended safeguards is not necessary in the form suggested as other measures (e.g. safeguards which are not contained in the IT Baseline Protection Manual but achieve the same effect) already provide sufficient protection against the relevant threats, or else the measures recommended are not relevant (e.g. because certain services have not been implemented).

"Yes" - All the recommendations in the safeguard have been implemented effectively and in their entirety.

"Partially" - Some of the recommendations have been implemented, while others have not yet been implemented or only partially implemented.

"No" - Most of the recommendations contained in the safeguard have not yet been implemented.

Reading out the text of the recommendations contained in a given safeguard during the interview is not recommended as the manual was not designed for this purpose. Hence, the interviewer needs to be familiar with the contents of the module. If necessary, handy checklists containing keywords should be prepared in advance of the interviews. In order to be able to clarify any disagreements in case of doubt, it is nevertheless useful to have the full text of the safeguards at hand. Direct entry of the answers into a PC during the interview is likewise not recommended as it would be distracting to those involved and cause unwanted interruption to communication.

If the interview begins with a few introductory words and the purpose of the basic security check is briefly introduced, this can help to create a relaxed, open and productive atmosphere. It is recommended continuing by naming and briefly explaining the safeguard. Rather than conducting a monologue, it is better to give the interviewee(s) the opportunity to go into those parts of the safeguard which have already been implemented and then discuss any items still at issue.

The questions asked should always be directed at the level of standard security safeguards, and only after the basic security check has been completed should any more far-reaching aspects of highly sensitive applications be considered. If there is a requirement to verify the statements made in the interviews, this could be achieved, for example, by examining samples of the relevant procedures and concepts, in the case of the area of infrastructure by visiting the objects under investigation on-site with the contact person, and/or by checking client and/or server settings in selected IT systems.

To conclude each safeguard, the interviewee should be informed of the assessment result (i.e. safeguard implementation status = Unnecessary/Yes/ Partially/No) and this decision should be explained.

2.4.3 Documentation of Results

When it comes to documenting the results of the basic security check, some forms are provided on the CD-ROM which comes with the IT Baseline Protection Manual (see Annex: Additional Aids). The directory contains a file in Word format for every module of the IT Baseline Protection Manual, in which the results of the target versus actual comparison can be entered in tabular form for every safeguard in the given module.

First of all at the beginning of the form the following information should be entered in the fields provided:

- the number and name of the component or group of components to which this module was assigned during modelling;
- the location of the assigned component or group of components;
- the date on which the information was recorded and the name of the author;
- the name of the person interviewed.

The actual results of the target versus actual comparison are entered in the table contained on the form. For each safeguard in the relevant module, the fields should be completed as follows:

- Degree of implementation (Unnecessary/Yes/Partially/No)
  In this field the implementation status which has been established during the interview for the relevant safeguard is entered.
- Implement by
  This field is generally not completed during the basic security check. It serves as a place holder which will be used during implementation planning to document the date by which the safeguard concerned should have been fully implemented.
- Person responsible
  If during carrying out of the target versus actual comparison it is clear which member of staff will be responsible for implementing fully a safeguard that is not currently in place, the name of this person can be documented in this field. If it is not clear who will be responsible for implementation, this field should be left blank. It will be completed later during implementation planning with the name of the person to whom responsibility is then assigned.
- Notes / reason(s) for non-implementation
  In the case of safeguards whose implementation appears unnecessary, the rationale for this should be stated and/or any alternative measure taken which achieves the same end should be specified. In the case of safeguards which have not yet been implemented or only partially implemented, it should be documented in this field which recommendations of the safeguard still have to be implemented. Any other notes which will assist in rectifying security shortcomings or which need to be considered in the context of the safeguard should also be entered here.
- Cost estimate
  In the case of measures which have not yet been implemented or only partially implemented, an estimate can be entered in this field of the financial and staffing resources which will be needed to eliminate the deficits.

An example of a completed survey form is provided at the end of this section.

The results can also be documented using a tool, for example the IT Baseline Protection Tool which was specially developed for the BSI. This tool serves as a convenient way of analysing and auditing

the results, for example, it is possible to search for particular entries, generate user-defined reports, perform various statistical analyses etc.

IT Baseline Protection Survey: Form for Module 6.1, "Server-Supported Network"

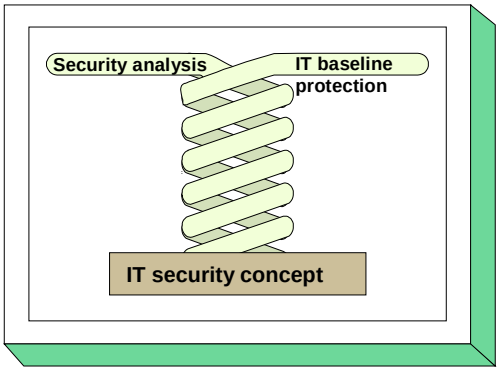
Nu S5 — 24 May 2000

Communications server for Intranet — N. Meyer

Bonn, Room 3.10

Safeguard	Module: Server-supported Ne					Imp	Pers	
S 1.28 (2)	Local Uninterruptible Power Supply (UPS)			X		31/12/01	A. Müller	There is a UPS capacity.
S 1.29 (3)	Adequate Siting of an IT System (optional)		X					
S 1.32 (1)	Adequate siting of the Consoles, Devices with Exchangeable Data Media, and Printers		X					
S 2.03 (2)	Data Media Control		X					
S 2.04 (2)	Maintenance/Repair Regulations	X						This safeguard maintenance a
S 2.09 (2)	Ban on Using Non-Approved Software				X	31/12/00	N. Meyer	
S 2.10 (3)	Survey of the Software Held				X	30/6/00	C. Schulz	
S 2.13 (2)	Correct Disposal of Resources Requiring Protection		X					
S 2.22 (2)	Escrow of Passwords			X		31/12/00	A. Müller	Depositing of p consistently pe systematic proc
S 2.25 (1)	Documentation of the System Configuration		X					

2.5 Supplementary Security Analysis



As explained in Section 2.2 "Assessment of Protection Requirements", the standard security measures aimed at securing baseline protection will normally provide a reasonable and sufficient level of protection. However, if in the course of assessing protection requirements it has transpired that an IT application together with its data has a high or very high protection requirement, it may be appropriate to check whether the standard security safeguards need to be supplemented or replaced by more stringent IT security safeguards, which will generally also be more expensive. The additional measures which are appropriate can be determined after the basic IT baseline protection security check has been performed using a supplementary security analysis.

To limit the amount of effort devoted to a supplementary security analysis to what is strictly necessary, it may be appropriate to concentrate on the sensitive areas rather than analysing all the IT assets. For this purpose the areas which possess a high or very high protection requirements or are classified as sensitive should be extracted from the results of the protection requirements assessment. These might be as follows:

- IT systems which have a high protection requirement,
- communications links to the outside world,
- communications links over which highly sensitive data is passed,
- communications links which should not be used to transport particular data,
- IT rooms which have a high protection requirement.

A supplementary security analysis is then performed on this subset of the IT assets, comprising only the sensitive items. Various methods can be used here. These include

- risk analysis,
- penetration testing and
- differential security analysis.

It should be mentioned in advance that the success of the supplementary security analysis depends critically on the expertise of the project team. It is essential that the team members have in-depth specialist knowledge in the areas of information technology and IT security, ideally supplemented by broad background experience. Otherwise there is a danger that significant weaknesses or safeguards could be overlooked and that the results could convey an unwarranted impression of security. It may therefore be appropriate to have the supplementary security analysis performed by specialist external consultants.

Risk analysis

In a risk analysis, an attempt is made to identify the threats to which an IT system is exposed due to existing security weaknesses. The probability of each of these threats occurring is then estimated and combined with the protection requirements to rate the existing risks. For any risks which are unacceptable a set of IT security measures is then selected so as to reduce the probability of occurrence and/or the extent of the potential damage.

Estimation of probabilities is particularly difficult and prone to error. Usually no statistical information is available. It is especially difficult to make these estimates for threats which entail wilful action by

perpetrators. The estimates only needs to be a little on the low side to produce a risk which appears to be acceptable so that no additional measures are taken even though these are in fact necessary.

A description of how to perform a risk analysis is provided in the IT Security Manual (see References).

Penetration testing

Penetration testing is used to estimate in advance the prospects of a deliberate attack on a set of IT assets succeeding and to deduce from this what additional measures are necessary. It entails simulating the aggressive behaviour of a wilful insider or external aggressor and ascertaining what existing security weaknesses could be used and what potential damage could be caused. The following are some of the approaches commonly used:

- attacks involving the guessing of passwords or dictionary attacks,
- attacks involving recording of and tampering with network traffic,
- attacks involving the import of false data packets,
- attacks involving exploitation of known software weaknesses (macro languages, operating system errors, remote access services etc.).

A distinction should be made here between two different forms of penetration testing:

- Black box approach: the aggressor does not have any information about the IT assets in advance. This approach is used to simulate an external aggressor.
- White box approach: the aggressor is in possession of information about the internal structure, applications and services used. Typically this would be information available to an insider.

A further distinction is whether penetration testing is only co-ordinated with Management or whether the staff concerned are given advance warning. Penetration testing requires in-depth knowledge and experience to perform effectively, as otherwise the possibility that the "attacks" implemented during testing may cause unintended damage cannot be excluded.

Differential security analysis

One approach to identifying the more stringent IT security measures that are necessary for those IT assets which are particularly sensitive is to perform a differential security analysis. The first step here is to investigate which IT security safeguards go beyond baseline protection or which IT baseline protection safeguards that have been implemented are classified as optional. A comparison is then performed as to whether the more stringent safeguards taken correspond to the standard solutions which have been established in practice for highly sensitive IT areas. It should be noted here that the relevant basic parameters (confidentiality, integrity and availability) are critical in determining whether the more stringent safeguards are appropriate. Thus, for example, cryptographic measures will assist in raising confidentiality and integrity aspects of security but generally they will have little effect on availability or they may even have a negative impact on achieving this objective of protection. It is also important to ensure that any products needed are suitable and that the more stringent safeguards are correctly implemented so that they can achieve their full effect.

Typical more stringent measures in the area of IT systems include the use of certified operating systems or special security versions of operating systems, the use of authentication tokens or even isolation of IT systems. Examples of more stringent measures which might be used in the area of communications links are: capping of external connections, line encryption or end-to-end encryption, armoured cable runs or pressure-monitored cables, redundant communications lines or redundant cable routing and the use of multi-level firewalls combined with intrusion detection tools. In the area of

infrastructural security, the possibilities include isolating filters, fire extinguishing technology, video monitoring, access control systems and intruder detection devices through to backup computer centres.

The BSI publishes "protection class models" in which sets of more stringent safeguards suitable for IT assets with high and very high protection requirements are collected together for particular subject areas (e.g. private branch exchanges).

2.6 Implementation of IT Security Safeguards

This section presents a number of aspects which have to be considered when implementing IT security safeguards. It describes how the implementation of IT security safeguards identified as being missing or inadequately implemented can be planned, carried out, overseen and monitored.

Before work can commence on implementing IT security safeguards, the IT structure analysis, baseline protection assessment and modelling described in Sections 2.1 to 2.3 must have already been performed for the IT system or IT assets under examination. The results of the basic security check, and in particular of the target versus actual comparison which is the outcome of the basic security check, must also be available. If any supplementary security analysis has been performed for selected areas due to their higher protection requirements, then the suggestions which have been put forward as a result as to additional measures to be taken should also be available and taken into account in the process.

If there are a number of safeguards to be implemented but only limited financial and staffing resources are available to implement them, then implementation of the IT security safeguards can proceed as described below. An example to explain the procedure will be found at the end of this section.

If only a few missing safeguards have been identified whose implementation will tie up only small amounts of financial or staffing resources, it is often possible to decide on an ad hoc basis who should implement these measures and by when. This can be documented simply and without complication in the tables used to document the target versus actual comparison. In this case, steps 1, 3 and 4 may be omitted.

Step 1: Examine results of investigation

As a first step, the missing or only partially implemented IT baseline protection safeguards should be evaluated in an overall view. To do this, it is recommended that all the safeguards which have either not been implemented or only partially been implemented, including their priorities, are extracted from the results of the basic security check and put in a table.

Any additional safeguards requiring implementation can be identified through supplementary security analyses. These too should be drawn up in the form of a table. These additional measures should be arranged by subject in line with the objects examined during modelling and the corresponding IT baseline protection modules.

Step 2: Consolidate the safeguards

The first action here is to consolidate the IT security safeguards still requiring implementation. If any additional security analyses have been performed, these could have identified additional IT security safeguards which supplement or even replace safeguards contained in the IT Baseline Protection Manual. A check should be performed here as to which IT baseline protection safeguards do not need to be implemented as they are to be replaced by more stringent IT security safeguards.

As recommendations are made in the IT Baseline Protection Manual for a variety of different types of organisation and technical configurations, the safeguards that are selected may need to be made more specific and adapted so as to reflect the organisational and technical circumstances in the agency/company concerned. Moreover, all the IT security safeguards should be reviewed once more to ensure that they are suitable: they must provide effective protection against the possible threats but at the same time it must in practice be feasible to implement them. For example, they must not hinder the

organisational processes or undermine other security measures. In such cases it could be necessary to replace certain IT baseline protection safeguards by adequate alternative IT security safeguards.

In order subsequently to be able to trace the procedure followed in drawing up and refining the list of specific measures, this should be suitably documented.

Examples:

- It was established during a supplementary security analysis that in addition to the IT baseline protection safeguards it is also necessary to implement smart card-supported authentication and local encryption of hard disks on NT clients used for processing HR data. These additional measures would replace safeguard S 4.48 *Password Protection under Windows NT.*
- It has been established in the basic security check that safeguard S 1.24 *Avoidance of Water Pipes* has not been implemented and due to structural considerations would not be cost-effective to implement. As an alternative, metal sheets allowing water to be deflected are to be installed under the water-bearing pipes, and these will also be monitored by a water alarming device. An alarm will be sent to the porter so that in case of damage any leakage of water can be detected and contained quickly.

Step 3: Prepare an estimate of the costs and effort required

As the budget for implementing IT security measures is in practice always limited, it is necessary for every measure to be implemented to identify how much will need to be invested and how much labour this will entail. A distinction should be made here between one-off and recurring investment/labour costs. At this point it should be mentioned that experience shows that savings on technology often result in high ongoing labour costs.

In this connection it is necessary to ascertain whether all the measures identified can be afforded. If there are any safeguards which cannot be funded, consideration should be given as to what alternative measures could be taken instead or whether the residual risk resulting from failure to implement a given measure is acceptable. This decision must likewise be documented.

If the financial and staffing resources estimated as being necessary are available, then one can proceed to the next step. However, in many cases it is necessary to take a further decision as to the extent of the resources to be used to implement the IT security measures. It is recommended here that a presentation on the results of the security study should be given to the person(s) responsible for making such decisions (Management, IT Manager, IT Security Officer etc.). To make those responsible aware of the security issues involved, the security weaknesses identified (i.e. missing or only partially implemented IT security safeguards) should be presented by protection requirement. It is also recommended that the cost and effort associated with implementing the missing priority 1, 2 and 3 safeguards should be presented. A decision regarding the budget should then be made following this presentation.

If it proves to be not possible to make available a sufficient budget to cover implementation of all the missing safeguards, then the residual risk resulting from failure to implement or delay in implementing certain measures should be pointed out. To assist with this, the Safeguard-Threat Tables (see CD-ROM: word20\tabellen) can be used to ascertain which threats are no longer adequately covered. The residual risk relating to any chance or wilful threats should be described clearly and presented to Management for decision. The remaining steps can only take place after Management has decided that the residual risk is acceptable, as Management must bear the responsibility for the consequences.

Step 4: Determine implementation sequence

If the existing budget or staffing resources are not sufficient to be able to implement all the missing safeguards immediately, the sequence in which these measures will be implemented must be determined. When determining the sequence, the following aspects should be considered:

- The priority of a safeguard should be viewed as a guide to the order in which it should be implemented. Safeguards which have been assigned a priority 1 should be implemented first.
- With some safeguards a time sequence is suggested naturally by the logical inter-relationship of the measures concerned. Thus, for example, safeguards S 2.25 *Documentation of the System Configuration* and S 2.26 *Appointment of an Administrator and his Deputy* are both important, but without an Administrator it is not practical to implement S 2.25.
- Many of the safeguards have a significant effect in broad areas, whereas others have only a limited, local effect. Often it is advisable to start with the safeguards which have a broad effect.
- Some modules have a bigger impact on the aspired-to security level than others. Safeguards contained in such modules should be given preference, especially where their implementation will result in the elimination of weaknesses in areas having a high protection requirement. Thus, for example, the server should always be protected first (e.g. through implementation of module 6.2 *UNIX Server*) and only then the clients that are connected to it.
- Modules in respect of which there is a particularly large number of missing safeguards represent areas in which security is particularly weak. Preference should likewise be given to these.

Step 5: Assign responsibilities

Once the sequence in which the safeguards will be implemented has been determined, it is then necessary to specify who is responsible for implementing which safeguards and by when. Unless this is done, experience indicates that implementation of safeguards tends to be delayed and in some cases never takes place. Care must be taken here to ensure that the person to whom responsibility is assigned possesses the skills and authority necessary to implement the safeguards and that the resources he needs are made available to him.

Similarly, someone must be allocated responsibility for overseeing implementation. This person must also be notified when implementation of individual safeguards has been completed. Typically it is the IT Security Officer who is notified. Progress in the matter of implementation should be checked at regular intervals to ensure that the implementation work does not drag on.

The implementation plan which should now be complete should contain the following information as a minimum:

- description of the target operational environment
- number of module to be considered
- names and description of the safeguards
- implementation schedule
- budgetary framework
- person responsible for implementation
- person responsible for overseeing implementation

Step 6: Measures to accompany implementation

It is also important to specify any measures which need to take place in parallel to implementation and to plan them into the implementation. In particular, such measures include measures designed to inform members of staff who will be affected by the new IT security measures of their necessity and consequences and to make them aware of the importance of IT security.

The staff concerned must also receive training as to how to implement and apply the new IT security safeguards correctly. If this training is left out, it is possible that the safeguards might not be implemented and/or that they might fail to achieve the desired effect. Another consequence would be that staff would feel inadequately informed, and this in turn often results in a negative attitude towards IT security.

After the new IT security measures have been implemented, the IT Security Officer should check to ensure that staff have fully accepted them. Should it turn out that the new measures have not gained acceptance, they are doomed to failure. The causes of the lack of acceptance should be investigated and, if necessary, those concerned should be given an additional briefing.

Example:

Excerpts from a fictitious example are provided below in order to illustrate the steps listed above in more detail. The table below shows the consolidated list of safeguards to be implemented, together with estimates of the associated costs, which is generated as a result of steps 1 to 3.

Target object	Module	Safeguard	Priority			Costs	Notes
			1	2	3		
Entire organisation	3.1	S 2.11 Provisions Governing the Use of Passwords	P			a) euro 0 b) 2 working days c) euro 0 p.a. d) 0 working days p.a.	
Server room R 3.10	4.3.2	S 1.24 Avoidance of Water Pipes			X	a) euro 20,000 b) 12 working days c) euro 0 p.a. d) 0 working days p.a.	This safeguard is not cost-effective to implement. Instead, safeguard A1 will be implemented.
Server room R 3.10	4.3.2	A1 Installation of metal sheets to take water away, with monitoring via a water alarming device which alerts the porter.				a) euro 4,000 b) 3 working days c) euro 0 p.a. d) 0 working days p.a.	Replaces safeguard S 1.24.
Server S4	6.5	S 1.28 Local Uninterruptible Power Supply	X			a) euro 1,000 b) 1 working day c) euro 0 p.a. d) 0 working days p.a.	
C1 group of clients	5.5	A2 Smart card-supported authentication plus local encryption of hard disks				a) euro 1,400 b) 2 working days c) euro 0 p.a. d) 2 working days p.a.	This additional measure replaces safeguard S 4.1.
...							

Key:

- Safeguard
  A1 = additional measure 1 (additional to the IT baseline protection safeguards)
- Priorities
  P = partially implemented, X = missing, has not been implemented
- Costs:
  a) = one-off investment cost

b) = one-off personnel expense
c) = recurring investment cost
d) = recurring personnel expense

The implementation plan resulting from Management's decisions regarding the above table is now drawn up in tabular form.

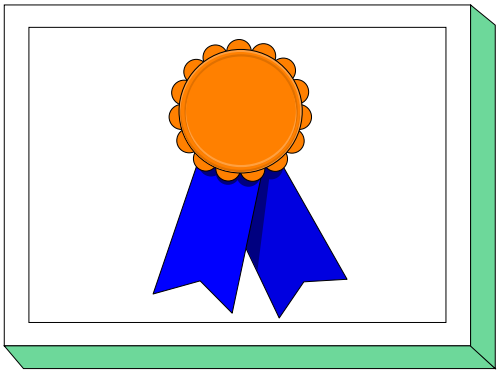
Implementation plan (as of 30 September 2000)

Target object	Module	Safeguard	Implement by	Person responsible	Budgetary framework	Notes
Entire organisation	3.1	S 2.11 Provisions Governing the Use of Passwords	31/12/00	a) A. Müller b) P. Meier	a) euro 0 b) 2 working days c) euro 0 p.a. d) 0 working days p.a.	
Server room R 3.10	4.3.2	A1 Installation of metal sheets to take water away, with monitoring via a water alarming device which alerts the porter.	30.04.2001	a) C. Schmitz b) F. Hofmann	a) euro 1,000 b) 1 working day c) euro 0 p.a. d) 0 working days p.a.	Metal sheets only to be installed under pipes carrying fresh and wastewater.
Server S4	6.5	S 1.28 Local Uninterruptible Power Supply	31.10.2000	a) C. Schulz b) P. Meier	a) euro 500 b) 1 working days c) euro 0 p.a. d) 0 working days p.a.	
C1 group of clients	5.5	A2 Smart card-supported authentication plus local encryption of hard disks	31.12.2000	a) C. Schulz b) P. Meier	a) euro 1,400 b) 2 working days c) euro 0 p.a. d) 2 working days p.a.	
...						

Key:

- Responsibilities:
  a) = Responsible for implementation of the safeguard
  b) = Responsible for overseeing implementation
- Budgetary framework: available for implementation of the safeguard
  a) = one-off investment cost
  b) = one-off personnel expense
  c) = recurring investment cost
  d) = recurring personnel expense

2.7 IT Baseline Protection Certificate



As a result of having received frequent queries as to whether a certificate can be issued for a set of IT assets in which IT baseline protection standards security safeguards have been implemented, the BSI has decided to take positive action. The motivation behind interest in an IT baseline protection certificates is diverse:

- IT service providers see in such a certificate a reliable way of demonstrating that they have implemented the safeguards specified in the IT Baseline Protection Manual.
- Partner companies are interested in knowing what degree of IT security their business partners are able to assure.
- Institutions which are linking up to a network for the first time are asked to provide evidence that IT security in their organisations is sufficient to rule out the possibility of any unacceptable risks resulting from these institutions being connected to the network.
- Companies and agencies are interested in providing evidence to customers/the public of the effort they put into achieving an adequate level of IT security.

As the IT Baseline Protection Manual with its recommendations as to standard security safeguards has come to assume the role of an IT security standard, it is fitting that it should be used as a generally recognised set of criteria for IT security.

In future it will be possible for an institution to obtain the IT Baseline Protection Certificate for a selected set of IT assets when an independent, accredited body can demonstrate from a basic security check that the required IT baseline protection standards security safeguards have been implemented. The procedure to be followed is that outlined in Sections 2.1 to 2.4. Since an IT baseline protection security concept is produced as a by-product of the basic security check, it is possible to reuse the documents generated in the certification process.

Naturally no guarantee can be given that the results of the basic security check will allow a certificate to be granted. For such cases BSI is considering granting the institution the opportunity to announce publicly its efforts in the IT security process aimed at obtaining an IT Baseline Protection Certificate. It is envisaged that an institution will be able to issue a self-generated declaration that it has achieved a certain entry level (a still to be defined minimum level) or an additional, higher level (still less than IT baseline protection level) and hopes to obtain the IT Baseline Protection Certificate after the missing safeguards have been implemented.

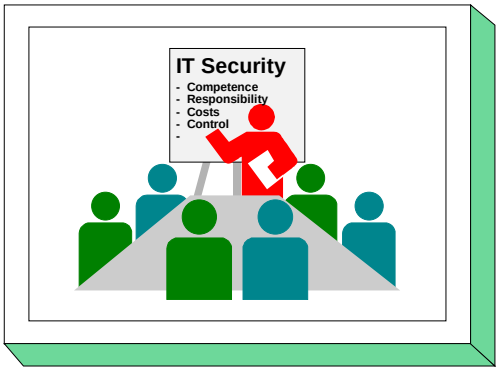
Further information regarding the discussion status of the "IT Baseline Protection Certificate" may be obtained from the BSI server at *http://www.bsi.bund.de*/gshb.

3 IT Baseline Protection of Generic Components

This chapter deals with generic or fundamental IT baseline safeguards on the following subjects:

3.0 IT Security Management
3.1 Organisation
3.2 Personnel
3.3 Contingency Planning Concept
3.4 Data Backup Policy
3.5 Data Privacy Protection
3.6 Computer Virus Protection Concept
3.7 Crypto Concept
3.8 Handling of Security Incidents

3.0 IT Security Management



Description

As the requirement for information technology grows, the complexity of people's requirements has grown continuously. Increasingly, implementation and maintenance of a reasonable level of IT security is requiring planned and organised action on the part of all those involved. The efficient implementation of IT security measures and review of their efficacy therefore necessitates a well thought out, controlled IT security process. This planning and control task is referred to as *IT security management*. It is imperative that functional IT security management is established at the start of the IT security process.

However, functional IT security management must be integrated into the existing management structures of a given organisation. It is therefore virtually impossible to specify a **single** IT security management structure will be directly usable within every organisation. Instead, modifications to organisation-specific circumstances will frequently be necessary.

This chapter is intended to present a systematic approach to establishing functional IT security management and improving it over time in line with developments in business operations. The approach presented is therefore intended to be viewed as a framework which can be modified in line with specific characteristics of a given organisation.

Note: In some other sections of this manual the term *IT security management* is also used to refer to the IT Security Management Team, i.e. to that group of persons which is responsible for the IT security process within an organisation.

Threat Scenario

Threats in the environment of IT security management can be of a varied nature. The threat listed below is covered in this chapter and may be viewed as typical:

Organisational Shortcomings:

- T 1.1 Lack of or inadequate IT Security Management

Recommended Countermeasures

Safeguard S 2.191 *Establishment of the IT security process* should be worked through at the outset in every case. This safeguard describes a procedure for initiating and implementing a complete IT security process. The steps and activities which are necessary for this are described, and these in turn are covered in detail in the safeguards which follow.

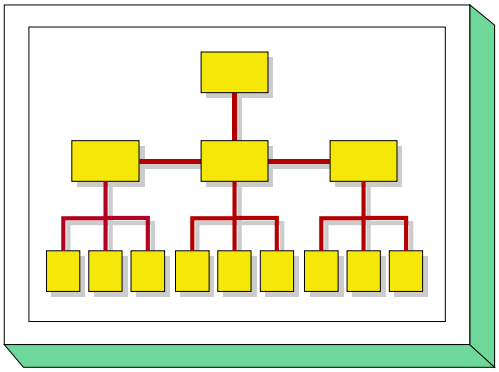
The safeguards package for the area "IT security management" is summarised below.

Organisation:

- S 2.191 (1) Establishment of the IT security process
- S 2.192 (1) Drawing up an Information Security Policy
- S 2.193 (1) Establishment of a suitable organisational structure for IT security
- S 2.194 (1) Drawing up a schedule of existing IT systems
- S 2.195 (1) Drawing up an IT security concept
- S 2.196 (1) Implementation of the IT security concept in accordance with an implementation plan
- S 2.197 (2) Drawing up a training concept for IT security
- S 2.198 (2) Making staff aware of IT security issues
- S 2.199 (1) Maintenance of IT security
- S 2.200 (1) Preparation of management reports on IT security
- S 2.201 (2) Documentation of the IT security process
- S 2.202 (2) Preparation of an IT Security Organisational Manual (optional)
- S 2.203 (3) Establishment of a pool of information on IT security (optional)

❒

3.1 Organisation



Description

This Chapter lists general and generic measures in the organisational field which, as standard organisational measures, are required to achieve a minimum protection standard. Specific measures of an organisational nature which directly relate to other measures (e.g. LAN administration) are listed in the relevant chapters.

Threat Scenario

In this Chapter, the following typical threats (T) are considered as regards IT baseline protection:

Organisational Shortcomings

- T 2.1 Lack of, or insufficient, rules
- T 2.2 Insufficient knowledge of requirements documents
- T 2.3 A lack of compatible, or unsuitable, resources
- T 2.4 Insufficient monitoring of IT security measures
- T 2.5 Lack of, or inadequate, maintenance
- T 2.6 Unauthorised admission to rooms requiring protection
- T 2.7 Unauthorised use of rights
- T 2.8 Uncontrolled use of resources
- T 2.9 Poor adjustment to changes in the use of IT
- T 2.10 Data media are not available when required

Human Failure

- T 3.1 Loss of data confidentiality/integrity as a result of IT user error

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended.

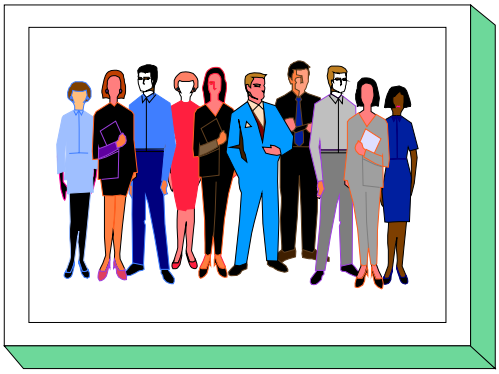
In the following, the countermeasure group "Organisation" is set out:

Organisation

- S 2.1 (2) Specification of responsibilities and of requirements documents for IT uses
- S 2.2 (2) Resource management
- S 2.3 (2) Data media control
- S 2.4 (2) Maintenance/repair regulations
- S 2.5 (1) Division of responsibilities and separation of functions
- S 2.6 (1) Granting of site access authorisations
- S 2.7 (1) Granting of (system/network) access rights
- S 2.8 (1) Granting of access rights
- S 2.9 (2) Ban on the use of non-approved software
- S 2.10 (2) Survey of the software held
- S 2.11 (1) Provisions governing the use of passwords
- S 2.12 (3) Services and counselling for IT users (*optional*)
- S 2.13 (2) Correct disposal of resources requiring protection
- S 2.14 (2) Key management
- S 2.37 (2) Clean desk policy
- S 2.39 (2) Response to violations of security policies
- S 2.40 (2) Timely involvement of the staff/factory council
- S 2.62 (2) Software acceptance and approval Procedure
- S 2.69 (2) Establishing standard workstations
- S 2.110 (2) Data privacy guidelines for logging procedures
- S 2.167 (2) Secure deletion of data media
- S 2.177 (2) Security during relocation
- S 2.182 (2) Regular revision of IT security measures

❒

3.2 Personnel



Description

This Chapter states the generic IT baseline protection safeguards which, on a standard basis, should be implemented with regard to personnel matters. A wide variety of safeguards are required, commencing with the taking on of new staff until the termination of their employment. Personnel-related safeguards linked to a specific function, e.g. the appointment of a system administrator of a LAN, are listed in the IT-specific chapters.

Threat Scenario

In this Chapter, the following typical threats (T) are considered as regards IT baseline protection:

Force Majeure
- T 1.1 Loss of personnel

Organisation deficiencies
- T 2.2 Insufficient knowledge of requirements documents

Human Failure:
- T 3.1 Loss of data confidentiality/integrity as a result of IT user error
- T 3.2 Negligent destroying of equipment or data
- T 3.3 Non-compliance with IT security measures
- T 3.8 Improper use of the IT system

Deliberate Acts:
- T 5.1 Manipulation/destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.42 Social engineering

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

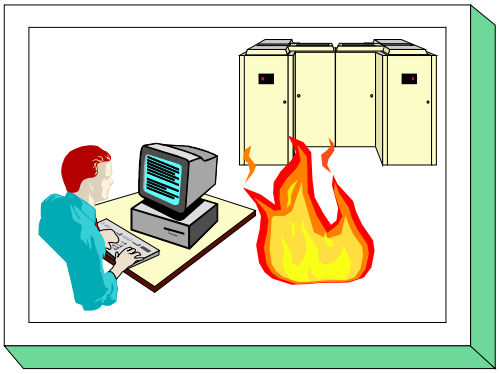
In the following, the safeguard package for "Personnel" is set out:

Personnel:

- S 3.1 (1) Well-regulated familiarisation/training of new staff with their work
- S 3.2 (2) Commitment of staff members to compliance with relevant laws, regulations and provisions
- S 3.3 (1) Arrangements for substitution
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.6 (2) Regulated procedure as regards termination of employment
- S 3.7 (3) Point of contact in case of personal problems (*optional*)
- S 3.8 (3) Avoidance of factors impairing the organisation climate (*optional*)

❒

3.3 Contingency Planning



Description

Contingency planning comprises safeguards which, in case of failure (due to technical reasons, caused intentionally or as a result of negligence) of an IT system, are designed to restore its operating state. Depending on the time of implementation of these measures, contingency planning safeguards can be grouped into four stages:

Stage 1: Contingency planning

In this stage, the measures suitable and economically viable for a particular IT system are identified. It is determined which measures can be taken during operation of an IT system (e.g. smoking ban, uninterruptible power supply, service, data backup) so that an emergency situation is prevented and that damage resulting from an emergency situation is reduced. Furthermore, contingency plans, which are part of a contingency manual, stipulate which measures must be taken in case of an emergency.

Stage 2: Implementing the contingency measures accompanying IT operation

In stage 2, the contingency measures are implemented and maintained. These must be carried out prior to an emergency situation in order to reduce the probability of an emergency or to allow swift and cost-effective restoration of the operating state.

Stage 3: Emergency preparedness exercises

Emergency drills are particularly important in connection with stage 2 in order to train the implementation of the measures listed in the Emergency Manual and to increase efficiency.

Stage 4: Implementing planned measures after an emergency situation arises

After it has been officially decided that an emergency situation is present, the measures set out in the Emergency Manual for this case must be implemented without delay.

In order to be able to make contingency planning cost-effective, the costs incurred must be compared to the potential damage (costs due to a lack of availability in the event of an emergency) and assessed. The following costs should be considered:

- Costs for compiling contingency planning
- Costs for the implementation and maintenance of the safeguards accompanying IT operation
- Costs for emergency drills
- Costs for the restoration of the operating state

This chapter offers a systematic approach as to how an Emergency Manual can be compiled and trained. This covers stage 1 and stages 3 and 4. The Implementation of stage 2 requires an assessment of the individual IT system. These measures are described in the relevant modules of this manual.

The compilation of an Emergency Manual and the safeguards required involve considerable expense. It is thus particularly recommended to use this chapter for

- IT systems requiring a high degree of availability
- large IT systems (mainframe computers, large UNIX systems, extensive networks)
- a large number of IT systems concentrated in one area.

Threat Scenario

In this Chapter, the threat

- T 1.2 Failure of the IT system

is considered as representative for all threats which could cause failure as regards IT baseline protection.

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

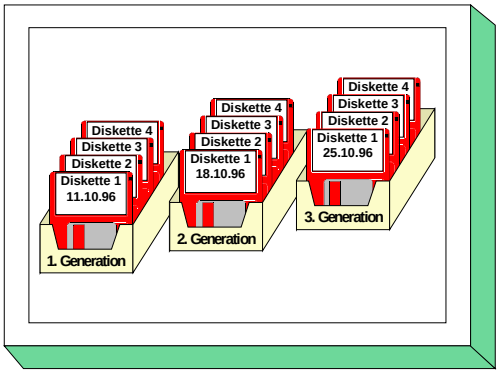
The safeguards should be treated in the order stated so as to ensure that the Emergency Manual is compiled systematically.

Contingency Planning:

- S 6.1 (2) Development of a survey of availability requirements
- S 6.2 (2) Definition of "emergency", person-in-charge in an "emergency"
- S 6.3 (2) Development of an Emergency Procedure Manual
- S 6.4 (2) Documentation on the capacity requirements of IT applications
- S 6.5 (2) Definition of "restricted IT operation"
- S 6.6 (2) Study of internally and externally available alternatives
- S 6.7 (2) Responsibilities in an emergency
- S 6.8 (1) Alert plan
- S 6.9 (1) Contingency plans for selected incidents
- S 6.10 (2) Contingency plans for breakdown of data transmission
- S 6.11 (2) Development of a post-incident recovery plan
- S 6.13 (2) Development of a data backup plan
- S 6.14 (3) Replacement procurement plan
- S 6.15 (3) Agreements with suppliers (*optional*)
- S 6.16 (2) Taking out insurance (optional)
- S 6.12 (1) Emergency preparedness exercises

❒

3.4 Data Backup Policy



Description

As a result of technical failure, inadvertent deletion or manipulation, data can be rendered useless or lost. The creation of back-ups thus ensures that any redundant data of the IT operation can be restored quickly in the event that parts of the operative data are lost.

Due to the complexities involved, however, such a back-up must be conceived systematically. This chapter describes how to prepare a data backup policy for an IT system.

Threat Scenario

The following typical threat is assumed for a data backup policy as part of IT baseline protection:

Technical Failure:
- T 4.13 Loss of stored data

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

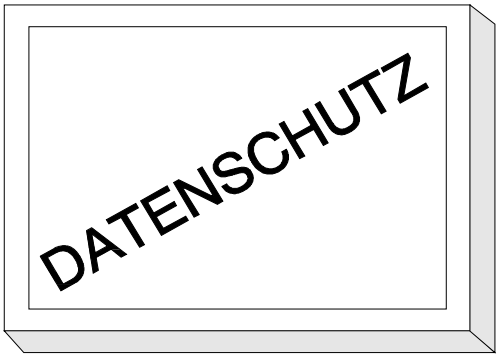
The safeguard group "Data Backup" is presented in the following. These safeguards are particularly useful for large IT systems and those handling large volumes of data. The safeguards should be treated in the order stated so as to ensure that the data backup policy is compiled systematically.

Contingency Planning:
- S 6.36 (1) Stipulating a minimal data backup policy
- S 6.37 (2) Documenting data backup procedures
- S 6.33 (2) Development of a data backup policy (optional)
- S 6.34 (2) Determining the factors influencing data backup (optional)
- S 6.35 (2) Stipulating data backup procedures
- S 6.41 (1) Training data reconstruction

Organisation:
- S 2.41 (2) Employees' commitment to data backup
- S 2.137 (2) Procurement of a suitable data backup system

❒

3.5 Data Privacy Protection



Description

The goal of data privacy protection is to protect individuals from impairment of informational self-determination due to abuse of person-related data.

Due to the close interconnection between data privacy protection and IT security, the aim of an IT baseline protection chapter on the topic of data privacy protection should both present the conditions for data privacy protection in a way that is suitable for practical implementation and show the connection between IT security and IT baseline protection.

The draft for such a chapter was developed by the federal data privacy officer in co-operation with the data privacy officers of the individual federal states. It is concerned with the national and state offices, the private suppliers of telecommunications services and postal services.

This draft can be requested by e-mail from the federal data privacy officer under the address:

heinz.biermann@bfd.bund400.de

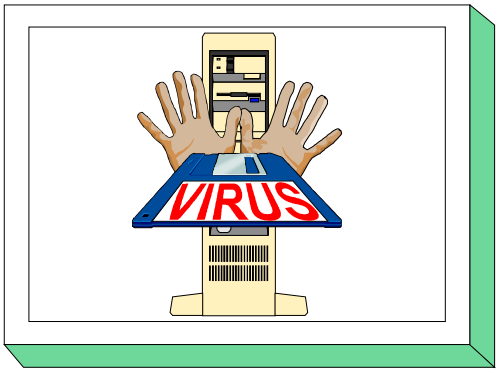
or

X.400: C=de, A=bund; P=bfd; S=biermann; G=heinz

The draft can also be found on the Internet server of the federal data privacy officer under the address *www.bfb.bund.de*. In addition, a version of this chapter that can be downloaded, which is formatted for the loose-leaf edition of the IT Baseline Protection Manual, is currently under preparation.

❒

3.6 Concept of computer virus protection



Description

The aim of the concept of computer virus protection is to create suitable safeguards with which the occurrence of computer viruses in the IT systems of an organisation can be prevented or detected as early as possible. In this way, countermeasures can be taken and possible damage can be minimised. In the protection against computer viruses it is essential that the safeguards are consistently adhered to and that technical countermeasures are constantly updated. This requirement is due to the continual occurrence of new computer viruses or variants of viruses. The development of operating systems, programming languages and application software may also provide opportunities for computer viruses to attack. This should therefore be taken into account and suitable countermeasures should be taken.

Since computers in government agencies or companies are increasingly integrated in local networks or connected to public communication networks, passing on data via means other than floppy disks can create additional infection paths for computer viruses. This often makes it necessary to continually check for viruses in the computers used.

In order to protect an entire organisation effectively against computer viruses, this chapter describes the steps that have to be taken to create and implement a concept of computer virus protection. Recommended safeguards for protection against computer viruses can be found in the corresponding chapters 5 and 6.

Threat Scenario

For IT baseline protection concerning computer viruses, the following typical threats will be considered.

Organisational shortcomings:
- T 2.1 Lack of, or insufficient, rules
- T 2.2 Insufficient knowledge of requirements documents
- T 2.3 A lack of compatible, or unsuitable, resources
- T 2.4 Insufficient monitoring of IT security measures
- T 2.8 Uncontrolled use of resources
- T 2.9 Poor adjustment to changes in the use of IT
- T 2.26 Lack of, or inadequate, test and release procedures

Human Failure:
- T 3.3 Non-compliance with IT security measures

Deliberate Acts:
- T 5.2 Manipulation of data or software
- T 5.21 Trojan Horses
- T 5.23 Computer viruses
- T 5.43 Macro viruses
- T 5.80 Hoaxes

Recommended Countermeasures (S)

When a computer virus protection concept is created (see S 2.154 *Creation of a computer virus protection concept*), it must first be determined which of the available or planned IT systems are to be included in the computer virus protection concept (see S 2.155 *Identification of IT systems potentially threatened by computer viruses*). For these IT systems, the factors that influence the implementation of security measures must be taken into account. Based on this, the technical and organisational measures can then be selected. In this context, it is particularly important to select suitable technical countermeasures such as virus scanning programs (see S 2.156 *Selection of a suitable computer virus protection strategy* and S 2.157 *Selection of a suitable computer virus scanning program*). In addition to setting up a report body (see S 2.158 *Reporting computer virus infections*) and coordinating the updating of protection products used (see S 2.159 *Updating the computer virus scanning programs used*), a series of regulations for implementing the concept are to be agreed (see S 2.11 *Regulations on computer virus protection*) in which additional safeguards required for virus protection are specified.

One of the most important safeguards for protecting computers against damage from viruses is regular data backup (see S 6.32 *Regular data backup*).

For the implementation of IT baseline protection, we recommend selecting the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4. Additional recommended literature is volume 2 the German Information Security Agency's series of scripts on IT security "Information on computer viruses".

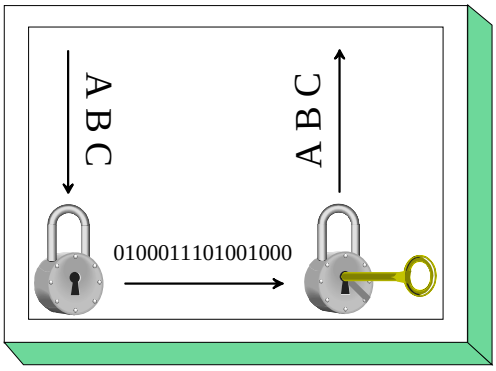
Organisation:
- S 2.154 (1) Creation of a computer virus protection concept
- S 2.155 (2) Identification of IT systems potentially threatened by computer viruses
- S 2.156 (2) Selection of a suitable computer virus protection strategy
- S 2.157 (2) Selection of a suitable computer virus scanning program
- S 2.158 (2) Reporting computer virus infections
- S 2.159 (2) Updating the computer virus scanning programs used
- S 2.160 (2) Regulations on computer virus protection
- S 2.9 (3) Ban on using non-approved software
- S 2.10 (3) Survey of the software held
- S 2.34 (2) Documentation on changes made to an existing IT system
- S 2.35 (2) Obtaining information on security weaknesses of the system

Personnel:
- S 3.4 (2) Training before actual use of a program
- S 3.5 (2) Education on IT security measures

Hardware & Software:
- S 4.3 (2) Periodic runs of a virus detection program
- S 4.33 (2) Use of a virus scanning program when exchanging of data media and data transmission
- S 4.44 (2) Checking of incoming data for macro viruses
- S 4.84 (2) Use of BIOS security mechanisms

Contingency Planning:
- S 6.23 (2) Procedure in case of computer virus infection
- S 6.24 (2) PC emergency floppy disk
- S 6.32 (1) Regular data backup

3.7 Crypto-concept



Description

This module describes a process with which, in a heterogeneous environment, both the data stored locally and the data to be transmitted can be protected effectively through cryptographic procedures and techniques. For this purpose, the module explains how and where in a heterogeneous environment cryptographic procedures and the corresponding components can be used. As a large number of influencing factors should be taken into account when using cryptographic procedures, a crypto-concept should be created.

This module describes how to create a crypto-concept. It starts by determining the requirements and influencing factors, then goes on to the selection of suitable cryptographic solutions and products, and ends with raising the awareness of and training the users as well as crypto contingency planning.

This module can also be consulted when only a cryptographic product is to be selected for one of the possible areas of use. In this case, it is possible to leave out several of the steps described in the following and only perform those that are relevant for the particular area of use.

In order to implement this module, it is necessary to have a basic understanding of the fundamental cryptographic mechanisms. An overview of basic cryptographic terms can be found in S 3.23 *Introduction to basic cryptographic terms*.

Threat Scenario

Cryptographic procedures are used to guarantee

- confidentiality,
- integrity,
- authenticity and
- non-repudiation.

Therefore, the following threats to cryptographic procedures are primarily taken into account for IT baseline protection:

- T 4.33 Poor-quality or missing authentication
- T 5.85 Loss of integrity of information that should be protected
- T 5.27 Repudiation of a message
- T 5.71 Loss of confidentiality of classified information

If cryptographic procedures are used, the following threats should also be taken into account for IT baseline protection:

Organisational shortcomings:
- T 2.1 Lack of, or insufficient, rules
- T 2.2 Insufficient knowledge of requirements documents
- T 2.4 Insufficient monitoring of IT security measures
- T 2.19 Inadequate key management for encryption

Human Failure:
- T 3.1 Loss of data confidentiality/integrity as a result of IT user error
- T 3.32 Violation of basic legal conditions for the use of cryptographic procedures
- T 3.33 Improper use of cryptomodules

Technical Failure:
- T 4.22 Software vulnerabilities or errors (here: poor encryption methods)
- T 4.34 Failure of a cryptomodule
- T 4.35 Insecure cryptographic algorithms
- T 4.36 Mistakes in encoded data

Deliberate Acts:
- T 5.81 Unauthorised use of a cryptomodule
- T 5.82 Manipulation of a cryptomodule
- T 5.83 Compromising cryptographic codes
- T 5.84 Forged certificates

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules"), as described in chapters 2.3 and 2.4, is recommended.

For cryptographic procedures essentially the following additional steps have to be taken:

1. Develop a crypto-concept (see S 2.161)

   The use of cryptographic procedures is determined by a large number of influencing factors. These factors include the IT system, the volume of data, the desired level of protectionn and the demands on availability. For this reason, a concept should first be developed which takes into account all influencing factors and criteria which determine the choice of a particular cryptographic procedure and the corresponding products. At the same time, this concept should be economically feasible.

2. Determine the requirements that the cryptographic procedure has to meet

   A requirement catalogue must be created which describes the influencing variables and the decision criteria on which the use of cryptographic procedures are based (see S 2.162 *Determining the need to use cryptographic procedures and products* and S 2.163 *Determining the factors influencing cryptographic procedures and products*). Cryptographic procedures can be used on the various layers of the ISO/OSI model. According to the specified demands or threats, it is recommended to use the procedure on particular layers (see also S 4.90 *Use of cryptographic procedures on the various layers of the ISO/OSI reference model*).

3. Select a suitable cryptographic procedure (S 2.164 *Selection of a suitable cryptographic procedure*)

   When selecting cryptographic procedures, it is first necessary to ascertain whether symmetric, asymmetric or hybrid algorithms are suitable then determine the required strength of the mechanism. Finally, suitable products should be determined.

4. Select a suitable cryptographic product (S 2.165 *Selection of a suitable cryptographic product*)

   After all the conditions have been determined, a product must be selected which provides the level of security laid down in the crypto-concept. Such a product, called crypto module for short, can consist of hardware, software, firmware or a combination of these, and of the components such as memory, processors, busses, electricity supply, etc. which are necessary to perform cryptographic processes. A crypto module can be used to protect sensitive data or information in various computer or telecommunications systems.

5. Use the crypto module appropriately (S 2.166 *Provisions governing the use of crypto modules*)

   Even while a crypto module is in operation, it must satisfy a number of security requirements. In addition to ensuring the security of the data that the crypto module is to protect, it is also important to protect the crypto module against direct perpetration and unauthorised interference.

6. The security demands on the IT systems in which the cryptographic procedures are used are to be found in the corresponding system-specific components. For example, the components for clients (including laptops) are to be found in chapter 5 and those for servers in chapter 6.

7. Contingency planning includes

   - backing up data when using cryptographic procedures (see S 6.56), that is to say backing up the keys, the configuration data of the products used and the encrypted data
   - obtaining information about and reacting to security breaches.

The following describes the safeguards for the area "crypto-concept". Safeguards from other chapters will not be repeated here.

Organisation:
- S 2.161 (1) Development of a cryptographic concept
- S 2.162 (1) Determining the need to use cryptographic procedures and products
- S 2.163 (1) Determining the factors influencing cryptographic procedures and products
- S 2.164 (1) Selection of a suitable cryptographic procedure
- S 2.165 (1) Selection of a suitable cryptographic product
- S 2.166 (1) Provisions governing the use of crypto modules
- S 2.35 (1) Obtaining information on security weaknesses of the system
- S 2.39 (2) Response to violations of security policies
- S 2.46 (2) Appropriate key management

Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.23 (1) Introduction to basic cryptographic terms

Hardware & Software:
- S 4.85 (3) Design of suitable interfaces for crypto modules (optional)
- S 4.86 (2) Secure separation of roles and configuration with crypto modules
- S 4.87 (2) Physical security of crypto modules (optional)
- S 4.88 (2) Operating system security requirements when using crypto modules
- S 4.89 (3) Emission security (optional)
- S 4.90 (3) Use of cryptographic procedures on the various layers of the ISO/OSI reference model

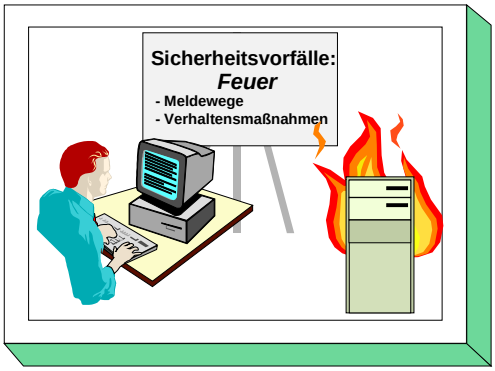
Contingency Planning:
- S 6.56 (2) Data backup when using cryptographic procedures

Many other components contain safeguards which touch upon the topic of cryptographic procedures and can be considered as implementation examples. For example, these include:

- S 4.29 Use of an encryption product for laptop PCs
- S 4.30 Utilisation of the security functions offered in application programs
- S 4.34 Using encryption, checksums or digital signatures
- S 4.41 Use of a suitable PC security product
- S 4.72 Database encryption
- S 5.33 Secure remote maintenance via modem
- S 5.34 Use of one-time passwords
- S 5.36 Encryption under UNIX and Windows NT
- S 5.50 Authentication via PAP/CHAP

- S 5.52 Security-related requirements for communications computers
- S 5.63 Use of PGP
- S 5.64 Secure Shell
- S 5.65 Use of S-HTTP
- S 5.66 Use of SSL

3.8 Handling of security incidents



Description

To maintain IT security in ongoing operations, it is necessary to have developed and practised a policy for the handling of security incidents. A security incident refers to an event whose impact could cause significant loss or damage. To prevent or contain any loss or damage, security incidents should be dealt with swiftly and efficiently. If there is a predefined procedure available to be invoked, then reaction times can be minimised. The possible loss or damage which could occur in a security incident can affect both the confidentiality and integrity of data and also its availability.

A special part of security incident handling is the contingency planning concept (see Section 3.3). In a contingency planning concept, the effects of failure of critical components in particular IT systems are analysed in advance and a procedure for ensuring that availability is maintained or can be restored is specified.

Security incidents can, for example, be triggered by

- user errors which result in loss of data or alteration of sensitive system parameters,
- the appearance of security loopholes in hardware or software components,
- large-scale infection by computer viruses,
- hacking of Internet servers,
- disclosure of confidential data,
- loss of personnel resources or
- criminal action (break-in, theft or blackmail relating to IT equipment).

All types of security incident must be tackled in an appropriate manner. This applies both to security incidents against which it is possible to take specific protective measures, e.g. computer viruses, and also to security incidents which affect the organisation unexpectedly.

This chapter presents a systematic approach as to how to draw up a policy for the handling of security incidents and how to ensure that this is implemented and integrated within an organisation. The effort involved in preparing and implementing such a policy is not trivial. Therefore this chapter should be considered mainly where relatively large IT systems are used and/or for systems on which the organisation is especially reliant.

Threat Scenario

Security incidents can be triggered by a number of threats. The catalogue of threats contains a large collection of threats which can cause major or minor security incidents.

A great deal of damage can be triggered by these threats if no suitable procedures have been developed as to how to handle them. This chapter therefore considers the following threat as representative of all the threats which can occur in the field of security incidents:

- T 2.62 Inappropriate handling of security incidents

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended.

To establish an effective system for handling security incidents, a number of steps must be taken. These steps are described in safeguard S 6.58 *Establishment of a management system for handling security incidents* and are explained in the safeguards which follow it. Hence it is best to start with implementation of safeguard S 6.58.

The safeguards relating to the area of "Handling of security incidents" are listed below.

Contingency Planning

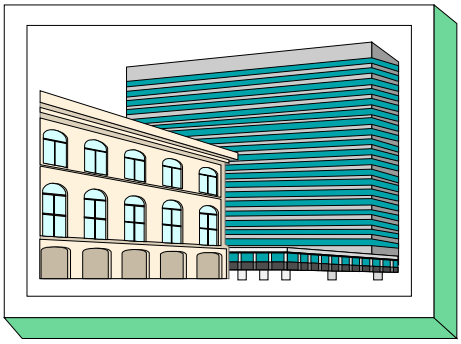
- S 6.58 (1) Establishment of a management system for handling security incidents
- S 6.59 (1) Specification of responsibilities for dealing with security incidents
- S 6.60 (1) Procedural rules and reporting channels for security incidents
- S 6.61 (1) Escalation strategy for security incidents
- S 6.62 (1) Specifying priorities for handling security incidents
- S 6.63 (1) Investigation and assessment of a security incident
- S 6.64 (1) Remedial action in connection with security incidents
- S 6.65 (1) Notification of parties affected
- S 6.66 (2) Evaluation of security incidents
- S 6.67 (2) Use of detection measures for security incidents (optional)
- S 6.68 (2) Testing the effectiveness of the management system for the handling of security incidents

❒

4 IT Baseline Protection in the Area of Infrastructure

This chapter defines IT baseline protection in the following modules:

4.1 Buildings



Description

The building surrounds the IT and thus guarantees external protection. Furthermore, infrastructure installations of the building allow IT operation in the first place. These are, for example, the building itself, i.e. walls, ceilings, floors, roof, windows and doors, but also utilities throughout the building, such as electricity, water, gas, heating, pneumatic dispatch, etc. The cabling within a building and PBX facilities are dealt with separately in Chapter 4.2, and in Part I, Chapter 8, respectively.

Threat Scenario

The following typical threats (T) are assumed as regards IT baseline protection for a building:

Force Majeure
- T 1.3 Lightning
- T 1.4 Fire
- T 1.5 Water

Organisational shortcomings:
- T 2.1 Lack of, or insufficient, rules
- T 2.6 Unauthorised admission to rooms requiring protection

Technical Failure:
- T 4.1 Disruption of power supply
- T 4.2 Failure of internal supply networks
- T 4.3 Inoperability of existing safeguards

Deliberate Acts:
- T 5.3 Unauthorised entry into a building
- T 5.4 Theft
- T 5.5 Vandalism
- T 5.6 Attack

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

In the following, the countermeasure package for "Buildings" is set out:

Infrastructure:

Power Supply

- S 1.1 (2) Compliance with relevant DIN standards/VDE specifications
- S 1.2 (2) Regulations governing access to distributors
- S 1.3 (1) Adapted segmentation of circuits
- S 1.4 (3) Lightning protection devices (*optional*)
- S 1.5 (3) Galvanic separation of external lines (*optional*)

Fire Protection

- S 1.6 (2) Compliance with fire-protection regulations and requirements imposed by the local fire department
- S 1.7 (2) Hand-held fire extinguishers
- S 1.8 (2) Room allocation, with due regard to fire loads
- S 1.9 (1) Fire sealing of trays
- S 1.10 (2) Use of safety doors (*optional*)

Building Protection

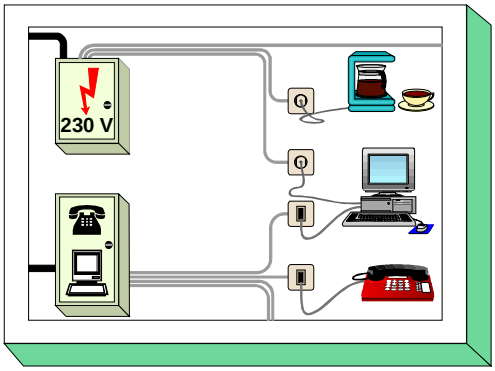
- S 1.11 (2) Plans detailing the location of supply lines
- S 1.12 (2) Avoidance of references to the location of building parts requiring protection
- S 1.13 (3) Layout of building parts requiring protection
- S 1.14 (2) Automatic drainage
- S 1.15 (1) Closed windows and doors
- S 1.16 (3) Selection of a suitable site (*optional, if and where alternatives exist*)
- S 1.17 (3) Entrance control service (*optional*)
- S 1.18 (2) Intruder and fire detection devices (*optional*)
- S 1.19 (2) Protection against entering and breaking (optional)

Organisation:
- S 2.14 (2) Key management
- S 2.15 (2) Fire safety inspection
- S 2.16 (2) Supervising or escorting outside staff/visitors (*optional*)
- S 2.17 (2) Entry regulations and controls
- S 3.18 (3) Inspection rounds (*optional*)

Contingency Planning:
- S 6.17 (1) Alert plan and fire drills

❒

4.2 Cabling



Description

Cabling of IT systems covers all cables and passive components (jumper distributors/splice distributors) of networks, from any existing delivery point of an extraneous network (telephone, ISDN) to the terminal points of network subscribers. Active network components (repeater, star coupler, bridge, etc.) are not dealt with in this Chapter.

Threat Scenario

The following threats (T) are assumed as regards IT baseline protection with regard to cabling:

Force Majeure
- T 1.6 Burning cables

Organisational shortcomings:
- T 2.11 Insufficient bandwidth planning
- T 2.12 Insufficient documentation on cabling
- T 2.13 Inadequately protected distributors
- T 2.32 Inadequate line bandwidth

Human Failure:
- T 3.4 Inadmissible connection of cables
- T 3.5 Inadvertent damaging of cables

Technical Failure:
- T 4.4 Impairment of lines due to environmental factors
- T 4.5 Cross-talk
- T 4.21 Transient currents on shielding

Deliberate Acts:
- T 5.7 Interception of lines
- T 5.8 Manipulation of lines

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

In the following, the countermeasure package for "Cabling" is set out:

Infrastructure:
- S 1.9 (1) Fire sealing of trays
- S 1.20 (3) Selection of cable types suited in terms of their physical/mechanical properties (*when providing new networks with cables*)
- S 1.21 (2) Sufficient dimensioning of lines (*when providing new networks with cables*)
- S 1.22 (3) Physical protection of lines and distributors (*optional*)
- S 1.39 (3) Prevention of transient currents on shielding

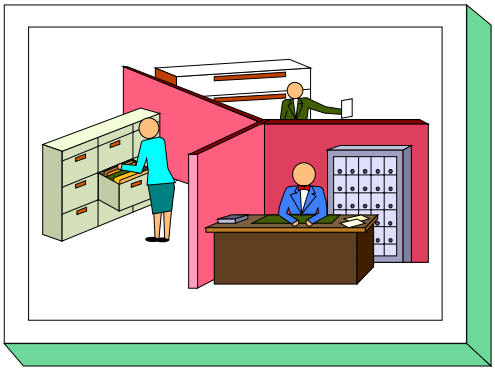
Organisation:
- S 2.19 (2) Neutral documentation in distributors
- S 2.20 (3) Monitoring of existing lines (*optional*)

Communications:
- S 5.1 (3) Removal, or short-circuiting and grounding, of unneeded lines
- S 5.2 (2) Selection of an appropriate network topography (*when providing new networks with cables*)
- S 5.3 (2) Selection of cables types suited in terms of communication technology (*when providing new networks with cables*)
- S 5.4 (2) Documentation on, and marking of, cabling
- S 5.5 (2) Damage-minimising routing of cables (*when providing new networks with cables*)

Contingency Planning:
- S 6.18 (3) Provision of redundant lines (*optional*)

❒

4.3.1 Offices



Description

An office is a room where one or several staff members are present in order to fulfil their duties, possibly including IT-supported tasks. Such duties may cover a wide variety of tasks: production of documents, processing of files and lists, conferences and telephone calls, reading of records and other documents, etc.

However, if an office is used primarily for keeping archives of data media, reference is also to be made to Chapter 4.3.3, "Data Media Archives". If a server (LAN; PBX, or the like) is installed in an office, the safeguards in Chapter 4.3.2 (server room) should also be observed.

Threat Scenario

The following typical threats (T) are assumed as regards IT baseline protection of an office:

Organisational Shortcomings:

- T 2.1 Lack of, or insufficient, rules
- T 2.6 Unauthorised admission to rooms requiring protection
- T 2.14 Impairment of IT usage on account of adverse working conditions

Human Error:

- T 3.6 Hazards posed by cleaning staff or outside staff

Deliberate Acts:

- T 5.1 Manipulation or destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.4 Theft
- T 5.5 Vandalism

Recommended Countermeasures (S)

To implement IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended.

In the following, the safeguard package for "Office" is set out:

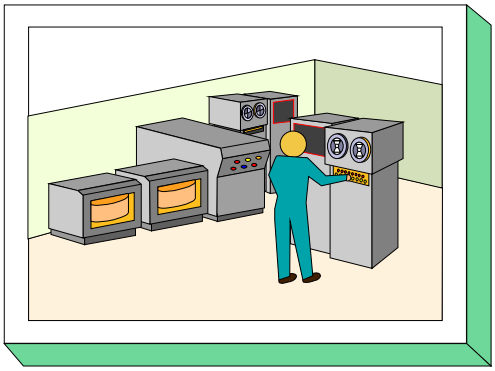
Infrastructure:
- S 1.15 (1) Closed windows and doors
- S 1.23 (1) Locked doors
- S 1.46 (3) Use of anti-theft devices (optional)

Organisation:
- S 2.14 (2) Key management
- S 2.16 (2) Supervising or escorting outside staff/visitors
- S 2.17 (2) Entry regulations and controls
- S 3.18 (3) Inspection rounds (*optional*)

Personnel:
- S 3.9 (3) Ergonomic workplace (optional)

❒

4.3.2 Server Room



Description

The server room primarily serves to accommodate a server, e.g. a LAN server, a UNIX host computer or a server for a PBX facility. In addition, server-specific documentation, small numbers of data media, additional hardware (star coupler, logging printer, air conditioning system) may be kept in that room.

A server room is not occupied by regular staff; it is used only sporadically and for short-term assignments. However, it must be borne in mind that, on account of the accumulation of IT devices and data, significantly greater damage may be caused in a server room than, for instance, in an office room.

Threat Scenario

The following threats (T) are assumed as regards IT baseline protection of a server room:

Force Majeure

- T 1.4 Fire
- T 1.5 Water
- T 1.7 Inadmissible temperature and humidity

Organisational shortcomings:

- T 2.1 Lack of, or insufficient, rules
- T 2.6 Unauthorised admission to rooms requiring protection

Technical Failure:

- T 4.1 Disruption of power supply
- T 4.2 Failure of internal supply networks
- T 4.6 Voltage variations / overvoltage / undervoltage

Deliberate Acts:

- T 5.1 Manipulation/destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.3 Unauthorised entry into a building
- T 5.4 Theft
- T 5.5 Vandalism

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

In the following, the safeguard package for "Server Room" is set out:

Infrastructure:

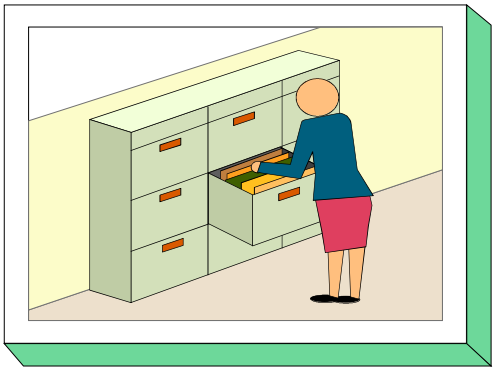
- S 1.3 (1) Adapted segmentation of circuits
- S 1.7 (2) Hand-held fire extinguishers
- S 1.8 (2) Room allocation, with due regard to fire loads
- S 1.10 (2) Use of safety doors (*optional*)
- S 1.15 (1) Closed windows and doors
- S 1.18 (2) Intruder and fire detection devices (*optional*)
- S 1.23 (1) Locked doors
- S 1.24 (3) Avoidance of water pipes (*optional*)
- S 1.25 (2) Overvoltage protection (*optional*)
- S 1.26 (2) Emergency circuit-breakers (*optional*)
- S 1.27 (2) Air conditioning (*optional*)
- S 1.28 (1) Local uninterruptible power supply [UPS] (*optional*)
- S 1.31 (3) Remote indication of malfunctions (*optional*)

Organisation:

- S 2.14 (2) Key management
- S 2.16 (2) Supervising or escorting outside staff/visitors
- S 2.17 (2) Entry regulations and controls
- S 3.18 (3) Inspection rounds (*optional*)
- S 2.21 (2) Ban on smoking

❑

4.3.3 Data Media Archives



Description

Data media archives serve keep all types of data media. Within the framework to of IT baseline protection, no additional fire protection requirements are laid down for an archives room. Fire protection can, according to the needs of the IT operator, be ensured by means of the containers housing the data media.

When using central data media archives and data backup archives it is advisable to install protective cabinets (c.f. Chapter 4.4) to increase the protection against fire and unauthorised access.

Threat Scenario

The following threats (T) are assumed as regards IT baseline protection of data media archives:

Force Majeure

- T 1.4 Fire
- T 1.5 Water
- T 1.7 Inadmissible temperature and humidity
- T 1.8 Dust, soiling

Organisational shortcomings:

- T 2.1 Lack of, or insufficient, rules
- T 2.6 Unauthorised admission to rooms requiring protection

Deliberate Acts:

- T 5.3 Unauthorised entry into a building
- T 5.4 Theft
- T 5.5 Vandalism

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

In the following, the safeguard group "Data Media Archives" is set out:

Infrastructure:

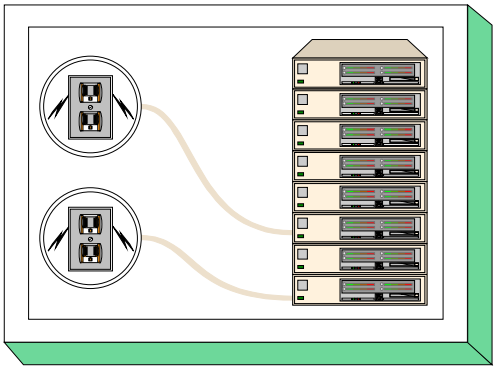
- S 1.6 (2) Compliance with fire-protection regulations and requirements imposed by the local fire department
- S 1.7 (2) Hand-held fire extinguishers
- S 1.8 (2) Room allocation, with due regard to fire loads
- S 1.10 (2) Use of safety doors (*optional*)
- S 1.15 (1) Closed windows and doors
- S 1.18 (2) Intruder and fire detection devices (*optional*)
- S 1.23 (1) Locked doors
- S 1.24 (3) Avoidance of water pipes (*optional*)
- S 1.27 (2) Air conditioning (*optional*)

Organisation:

- S 2.14 (2) Key management
- S 2.16 (2) Supervising or escorting outside staff/visitors
- S 2.17 (2) Entry regulations and controls
- S 3.18 (3) Inspection rounds (*optional*)
- S 2.21 (2) Ban on smoking

❒

4.3.4 Technical Infrastructure Room



Description

As a rule, technical infrastructure rooms house those equipment items and facilities which require no, or infrequent, human attendance. Usually, these will be distributors of internal supplies (e.g. PTT cable transfer room, high-tension lead-in room, medium-voltage lead-in room, low-voltage main distributor). In instances, these rooms may also house the fuses for power supply. Installation of other devices/equipment (uninterruptible power supply, star coupler, etc.) is also conceivable. Even a network server might be accommodated here if a specific room (Chapter **4.3.2,** Server Room) is not available.

Threat Scenario

The following typical threats (T) are assumed as regards IT baseline protection of a technical infrastructure room:

Force Majeure
- T 1.4 Fire
- T 1.5 Water
- T 1.7 Inadmissible temperature and humidity

Organisational shortcomings:
- T 2.1 Lack of, or insufficient, rules
- T 2.6 Unauthorised admission to rooms requiring protection

Technical Failure:
- T 4.1 Disruption of power supply
- T 4.2 Failure of internal supply networks
- T 4.6 Voltage variations / overvoltage / undervoltage

Deliberate Acts:
- T 5.1 Manipulation/destruction of IT equipment or accessories
- T 5.3 Unauthorised entry into a building
- T 5.4 Theft
- T 5.5 Vandalism

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

In the following, the safeguard package for "Technical Infrastructure Room" is set out:

Infrastructure:

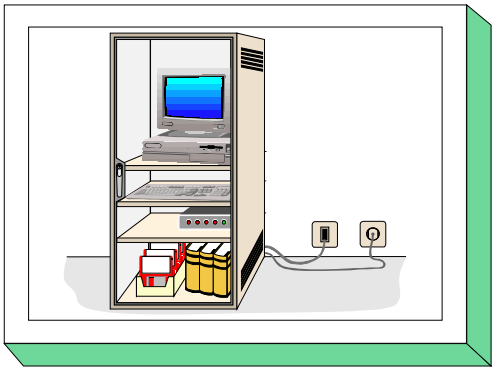
- S 1.3 (1) Adapted wiring of circuits
- S 1.6 (2) Compliance with fire-protection regulations and requirements imposed by the local fire department
- S 1.7 (2) Hand-held fire extinguishers
- S 1.8 (2) Room allocation, with due regard to fire loads
- S 1.10 (2) Use of safety doors (*optional*)
- S 1.15 (1) Closed windows and doors
- S 1.18 (2) Intruder and fire detection devices (*optional*)
- S 1.23 (1) Locked doors
- S 1.24 (2) Avoidance of water pipes (*optional*)
- S 1.25 (2) Overvoltage protection (*optional*)
- S 1.26 (2) Emergency circuit-breakers (*optional*)
- S 1.27 (2) Air conditioning (*optional*)
- S 1.31 (3) Remote indication of malfunctions (*optional*)

Organisation:

- S 2.14 (2) Key management
- S 2.16 (2) Supervising or escorting outside staff/visitors
- S 2.17 (2) Entry regulations and controls
- S 3.18 (3) Inspection rounds (*optional*)
- S 2.21 (2) Ban on smoking

❒

4.4 Protective cabinets



Description

Protective cabinets serve as depository for data-media of all types or as a place for IT devices (server cabinet). These cabinets should protect their contents against unauthorised access and/or the effects of fire or harmful substances (e.g. dust). They can substitute for a server room or a data media archive (see chapter 4.3.2 and 4.3.3), if the available space or organisational conditions do not allow the use of complete rooms.

Furthermore, protective cabinets can be implemented in server rooms or data media archives to increase the protective effect of the room. They are also recommended for a situation whereby servers from various organisational units are situated in one server room and only the appropriate administrators may have access to the respective servers.

As the costs of protective cabinets are not insignificant, a cost comparison is highly recommended. The comparison must be made between the cost of obtaining and maintaining a protective cabinet, and the cost of setting up and maintaining a server room or data media archive.

In order to achieve protection with a protective cabinet comparable to that obtained with rooms dedicated to this purpose, the safeguards ranging from the choice of cabinet to the siting and usage regulations are outlined in the following chapter.

Threat Scenario

The following typical threats are assumed for protective cabinets as part of IT baseline protection:

Force Majeure
- T 1.4 Fire
- T 1.5 Water
- T 1.7 Inadmissible temperature and humidity (only server cabinets)
- T 1.8 Dust, soiling

Organisational shortcomings:
- T 2.4 Insufficient monitoring of IT security measures

Human Failure:
- T 3.21 Improper use of code keys

Technical Failure:
- T 4.1 Disruption of power supply (only server cabinet)
- T 4.2 Failure of internal supplies (only server cabinet)
- T 4.3 Inoperability of existing safeguards
- T 4.4 Impairment of lines due to environmental factors

Deliberate Acts:
- T 5.1 Manipulation/destruction of IT equipment or accessories
- T 5.4 Theft
- T 5.5 Vandalism
- T 5.16 Threat posed by internal staff during maintenance/administration work
- T 5.17 Threat posed by external staff during maintenance work
- T 5.53 Deliberate misuse of protective cabinets for reasons of convenience

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

The following describes the safeguards for the area "protective cabinets". It is grouped according to the safeguards which must be implemented for the room where the cabinet is sited, the cabinet in general and for server cabinets.

For the room in which the protective cabinet is to be sited, the following safeguards must be observed:

Infrastructure:
- S 1.7 (2) Hand-held fire extinguishers
- S 1.8 (2) Room allocation, with due regard to fire loads
- S 1.15 (2) Closed windows and doors
- S 1.18 (2) Intruder and fire detection devices (*optional*)
- S 1.24 (3) Avoidance of water pipes (*optional*)

Organisation:
- S 2.6 (1) Granting of site access authorisations
- S 2.14 (2) Key management
- S 2.16 (2) Supervising or escorting outside staff/visitors
- S 2.17 (2) Entry regulations and controls
- S 3.18 (3) Inspection rounds (*optional*)
- S 2.21 (2) Ban on smoking (*optional*)

When obtaining and installing a **protective cabinet**, the following safeguards must be implemented:

Infrastructure:
- S 1.1 (2) Compliance with relevant DIN standards/VDE specifications
- S 1.18 (2) Intruder and fire detection devices (for the cabinet) (*optional*)
- S 1.40 (1) Appropriate siting of protective cabinets

Organisation:
- S 2.6 (1) Granting of site access authorisations
- S 2.14 (2) Key management
- S 2.95 (1) Obtaining suitable protective cabinets
- S 2.96 (1) Locking of protective cabinets
- S 2.97 (1) Correct procedure for code locks (if available)

Personnel:
- S 3.3 (1) Arrangements for substitution
- S 3.5 (2) Education on IT security measures
- S 3.20 (1) Instructions concerning the operation of protective cabinets

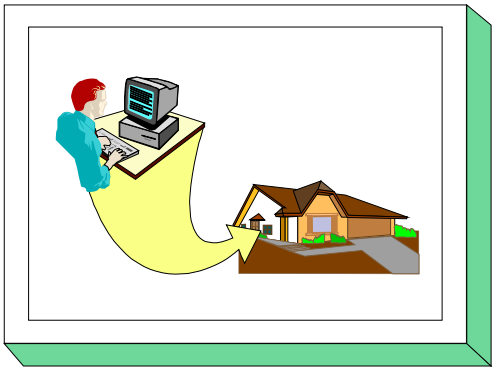
If the protective cabinet is to be used as a **server cabinet**, the following safeguards must be implemented in addition to those mentioned above.

Infrastructure:
- S 1.25 (2) Overvoltage protection (*optional*)
- S 1.26 (2) Emergency circuit-breakers
- S 1.27 (2) Air conditioning (*optional*)
- S 1.28 (2) Local uninterruptible power supply [UPS] (*optional*)
- S 1.31 (2) Remote indication of malfunctions (*optional*)
- S 1.41 (2) Protection against electromagnetic irradiation (*optional*)

Organisation:
- S 2.4 (2) Maintenance/repair regulations

❒

4.5 Working place at home (Telecommuting)



Description

If professional tasks are performed at home instead of a company or institute, appropriate measures must be taken to achieve a degree of security comparable with that prevailing on office premises. A home environment does not normally provide the security infrastructure present on the premises of a company or institute. Visitors and family members often have access to a home workstation. This chapter describes the threats and safeguards pertaining typically to home workstations. Such a workstation can be used, for example, by regular employees for the purpose of telecommuting, as well as by freelancers and self-employed people.

Threat Scenario

The following typical threats are assumed as regards IT baseline protection of a working place at home:

Force Majeure

- T 1.4 Fire
- T 1.5 Water

Organisational shortcomings:

- T 2.1 Lack of, or insufficient, rules
- T 2.6 Unauthorised admission to rooms requiring protection
- T 2.14 Impairment of IT usage on account of adverse working conditions
- T 2.47 Insecure transport of files and data media
- T 2.48 Inadequate disposal of data media and documents at the home work place

Human Failure:

- T 3.6 Hazards posed by cleaning staff or outside staff

Deliberate Acts:

- T 5.1 Manipulation/destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.3 Unauthorised entry into a building
- T 5.69 Higher risk of theft from a working place at home
- T 5.70 Manipulation by family members or visitors
- T 5.71 Loss of confidentiality of classified information

Recommended safeguards:

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

The safeguard package for "Workstations at Home" is specified in the following.

Infrastructure:

- S 1.1 (2) Compliance with relevant DIN standards/VDE specifications
- S 1.7 (3) Hand-held fire extinguishers (optional)
- S 1.15 (1) Closed windows and doors
- S 1.19 (2) Protection against entering and breaking (optional)
- S 1.23 (1) Locked doors
- S 1.44 (2) Suitable configuration of a home workplace
- S 1.45 (1) Suitable storage of business-related documents and data media

Organisation:

- S 2.13 (1) Correct disposal of resources requiring protection
- S 2.16 (2) Supervising or escorting outside staff/visitors
- S 2.37 (2) Clean desk policy
- S 2.112 (2) Regulation of the transport of files and data media between home workstations and institutions
- S 2.136 (2) Observance of rules concerning workstations and working environments

Personnel:

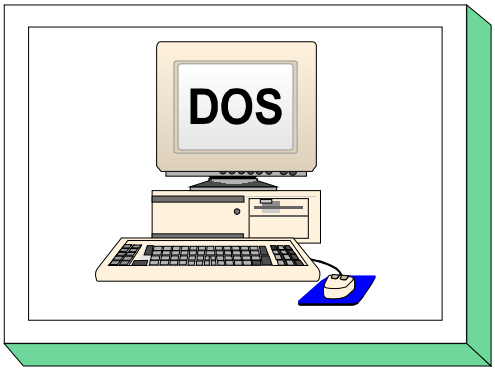
- S 3.9 (3) Ergonomic workplace (optional)

❒

5 Non-Networked Systems and Clients

This chapter defines IT baseline protection for the following non-networked systems and systems used as clients in networks. For IT systems not yet considered in the IT Baseline Protection Manual the generic module 5.99 can be used.

5.1 DOS PC (single user)



Description

The subject here is a commercially available IBM-compatible PC run with DOS or a comparable operating system. Such a PC must not be connected to a local area network. It is equipped with a floppy disk drive, a hard disk and, optionally, a mouse. If available, a printer is to be directly connected to the PC. A graphic user interface can also be employed here. The following is based on the assumption that such a PC will be operated by a **single** user.

Threat Scenario

The following threats (T) are assumed for IT baseline protection of a DOS PC (Single User):

Force Majeure

- T 1.1 Loss of personnel
- T 1.2 Failure of the IT system
- T 1.4 Fire
- T 1.5 Water
- T 1.8 Dust, soiling

Human Failure:

- T 3.2 Negligent destroying of equipment or data
- T 3.3 Non-compliance with IT security measures
- T 3.6 Hazards posed by cleaning staff or outside staff
- T 3.8 Improper use of the IT system

Technical Failure:

- T 4.1 Disruption of power supply
- T 4.7 Defective data media

Deliberate Acts:

- T 5.1 Manipulation/destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.4 Theft
- T 5.9 Unauthorised use of IT systems
- T 5.23 Computer viruses
- T 5.43 Macro viruses

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

The safeguard package for "DOS PC (Single User)" is presented in the following:

Infrastructure:
- S 1.29 (3) Adequate siting of an IT system (*optional*)

Organisation:
- S 2.3 (2) Data media control
- S 2.4 (2) Maintenance/repair regulations
- S 2.9 (3) Ban on using non-approved software
- S 2.10 (3) Survey of the software held
- S 2.13 (2) Correct disposal of resources requiring protection
- S 2.22 (2) Escrow of passwords
- S 2.23 (3) Issue of PC Use guidelines (*optional*)
- S 2.24 (3) Introduction of a PC Checklist booklet (*optional*)

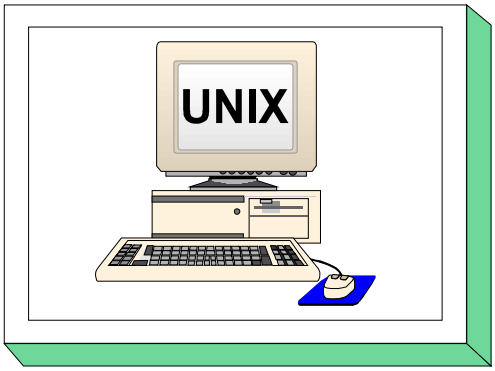
Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures

Hardware & Software:
- S 4.1 (1) Password protection for IT systems
- S 4.2 (1) Screen lock
- S 4.3 (2) Periodic runs of a virus detection program
- S 4.4 (3) Locking of floppy-disk drive slots (*optional*)
- S 4.30 (2) Utilisation of the security functions offered in application programs (optional)
- S 4.44 (2) Checking of incoming data for macro viruses
- S 4.84 (1) Use of BIOS security mechanisms

Contingency Planning:
- S 6.20 (2) Appropriate storage of backup data media
- S 6.21 (3) Backup copy of the software used
- S 6.22 (2) Sporadic checks of the restorability of backups
- S 6.23 (2) Procedure in case of computer virus infection
- S 6.24 (3) PC emergency floppy disk
- S 6.27 (3) Backup of the CMOS RAM
- S 6.32 (1) Regular data backup

❒

5.2 UNIX system



Description

Here we deal with a UNIX system, used as a stand-alone system or as a client in a network. Terminals, drives, printers and other devices may be connected. Also, a graphic shell (user interface) such as *X Windows* may be available. Accordingly, X terminals and graphic input devices may be connected in such cases. The following is based on the assumption that a UNIX system will usually be a multi-user system.

Threat Scenario

The following typical threats (T) are assumed as regards IT baseline protection of a UNIX system:

Force Majeure
- T 1.1 Loss of personnel
- T 1.2 Failure of the IT system
- T 1.4 Fire
- T 1.5 Water
- T 1.8 Dust, soiling

Organisational shortcomings
- T 2.7 Unauthorised use of rights
- T 2.9 Poor adjustment to changes in the use of IT
- T 2.15 Loss of confidentiality of sensitive data in the UNIX system

Human Failure
- T 3.2 Negligent destruction of equipment or data
- T 3.3 Non-compliance with IT security measures
- T 3.5 Inadvertent damaging of cables
- T 3.6 Hazards posed by cleaning staff or outside staff
- T 3.8 Improper use of the IT system
- T 3.9 Improper IT system administration

Technical Failure
- T 4.1 Disruption of power supply
- T 4.6 Voltage variations / overvoltage / undervoltage
- T 4.7 Defective data media
- T 4.8 Discovery of software vulnerabilities
- T 4.11 Lack of authentication possibilities between NIS Server and NIS Client
- T 4.12 Lack of authentication possibilities between X Server and X Client

Deliberate Acts
- T 5.1 Manipulation or destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.4 Theft
- T 5.7 Line tapping
- T 5.8 Manipulation of lines
- T 5.9 Unauthorised use of IT systems
- T 5.18 Systematic trying-out of passwords
- T 5.19 Abuse of user rights
- T 5.20 Abuse of Administrator rights
- T 5.21 Trojan horses

- T 5.23 Computer viruses
- T 5.40 Monitoring rooms using computers equipped with microphones
- T 5.41 Misuse of a UNIX system with the help of *uucp*
- T 5.43 Macro viruses
- T 5.89 Hijacking of network connections

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended.

In the following, the safeguard package for "UNIX system" is set out.

For any connected DOS PCs, the measures described in Chapter 5.1, are to be implemented.

In addition, the following measures will have to be taken:

Infrastructure
- S 1.29 (3) Adequate siting of an IT system (optional)

Organisation
- S 2.3 (2) Data media control
- S 2.4 (2) Maintenance/repair regulations
- S 2.9 (2) Ban on the use of non-approved software
- S 2.10 (3) Survey of the software held
- S 2.13 (2) Correct disposal of resources requiring protection
- S 2.22 (2) Escrow of passwords
- S 2.25 (1) Documentation of the system configuration
- S 2.26 (1) Appointment of an administrator and his deputy
- S 2.30 (1) Provisions governing the configuration of users and of user groups
- S 2.31 (1) Documentation on authorised users and on rights profiles
- S 2.32 (2) Establishment of a restricted user environment
- S 2.33 (2) Division of Administrator roles under UNIX
- S 2.34 (1) Documentation of changes made to an existing IT system
- S 2.35 (1) Obtaining information on security weaknesses of the system

Personnel
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.10 (1) Selection of a trustworthy administrator and his substitute
- S 3.11 (1) Training of maintenance and administration staff

Hardware & Software

Access to the UNIX system
- S 4.2 (2) Screen lock
- S 4.7 (1) Change of preset passwords
- S 4.13 (1) Careful allocation of identifiers
- S 4.14 (1) Mandatory password protection under UNIX
- S 4.15 (2) Secure log-in
- S 4.16 (3) Restrictions on access to accounts and/or terminals
- S 4.17 (2) Blocking and deletion of unnecessary accounts and terminals
- S 4.18 (1) Administrative and technical means to control access to the system-monitor and single-user mode
- S 4.105 (1) Initial measures after a Unix standard installation

Allocation of attributes / Working with the UNIX system

- S 4.9 (1) Use of the security mechanisms of X Windows
- S 4.19 (1) Restrictive allocation of attributes for UNIX system files and directories
- S 4.20 (2) Restrictive allocation of attributes for UNIX user files and directories
- S 4.21 (1) Preventing unauthorised acquisition of administrator rights
- S 4.22 (3) Prevention of loss of confidentiality of sensitive data in the UNIX system
- S 4.23 (3) Secure invocation of executable files

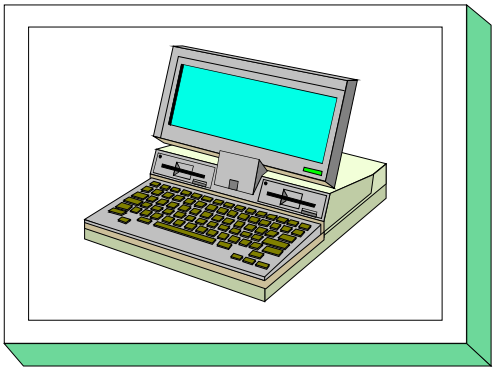
Logging / Security checks
- S 4.25 (1) Use of logging in UNIX systems
- S 4.26 (2) Regular security checks of the UNIX system
- S 4.40 (2) Preventing unauthorised use of computer microphones
- S 4.106 (2) Activation of system logging

Communication
- S 5.17 (1) Use of NFS security mechanisms
- S 5.18 (1) Use of NIS security mechanisms
- S 5.19 (1) Use of the sendmail security mechanisms
- S 5.20 (1) Use of the security mechanisms of *rlogin, rsh* and *rcp*
- S 5.21 (1) Secure use of *telnet, ftp, tftp* and *rexec*
- S 5.34 (2) Use of one-time passwords (*optional*)
- S 5.35 (1) Use of UUCP security mechanisms
- S 5.36 (2) Encryption under UNIX and Windows NT (*optional*)
- S 5.64 (2) Secure Shell
- S 5.72 (1) Deactivation of unnecessary network services

Contingency Planning
- S 6.20 (2) Appropriate storage of backup data media
- S 6.21 (2) Backup copy of the software used
- S 6.22 (2) Sporadic checks of the restorability of backups
- S 6.31 (2) Procedural patterns following a loss of system integrity
- S 6.32 (1) Regular data backup

❒

5.3 Laptop PC



Description

A portable Personal Computer (Laptop, Notebook) is understood to be a commercially available IBM-compatible PC run with DOS or a comparable operating system. It is equipped with a floppy disk drive and a hard disk. Data transmission devices (modem) are not dealt with here (c.f. Chapter 7.2.). The outstanding design features of this PC are its mobile operational capabilities, including the internal power supply. It is assumed here that the portable PC will be operated by only one user at any time. Any subsequent change of users is also considered.

Threat Scenario

The following typical threats (T) are assumed as regards IT baseline protection of a laptop PC:

Force Majeure
- T 1.1 Loss of personnel
- T 1.2 Failure of the IT system
- T 1.4 Fire
- T 1.5 Water
- T 1.8 Dust, soiling

Organisational shortcomings:
- T 2.7 Unauthorised use of rights
- T 2.8 Uncontrolled use of resources
- T 2.16 Non-regulated change of users in the case of laptop PCs

Human Failure:
- T 3.2 Negligent destroying of equipment or data
- T 3.3 Non-compliance with IT security measures
- T 3.6 Hazards posed by cleaning staff or outside staff
- T 3.8 Improper use of the IT system

Technical Failure:
- T 4.7 Defective data media
- T 4.9 Disruption of the internal power supply

Deliberate Acts:
- T 5.1 Manipulation/destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.4 Theft
- T 5.9 Unauthorised use of IT systems
- T 5.22 Theft in the case of mobile uses of IT systems
- T 5.23 Computer viruses
- T 5.43 Macro viruses

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

In the following, the safeguard group "Laptop PC" is set out:

Infrastructure:
- S 1.33 (1) Safe keeping of laptop PCs during mobile use
- S 1.34 (2) Safe keeping of laptop PCs during stationary use
- S 1.35 (3) Pooled storage of a number of laptop PCs (*optional*)

Organisation:
- S 2.3 (2) Data media control
- S 2.4 (2) Maintenance/repair regulations
- S 2.9 (2) Ban on using non-approved software
- S 2.10 (3) Survey of the software held
- S 2.13 (2) Correct disposal of resources requiring protection
- S 2.22 (3) Escrow of passwords
- S 2.23 (3) Issue of PC Use guidelines (*optional*)
- S 2.24 (3) Introduction of a PC Checklist booklet (*optional*)
- S 2.36 (2) Orderly issue and retrieval of a portable (laptop) PC

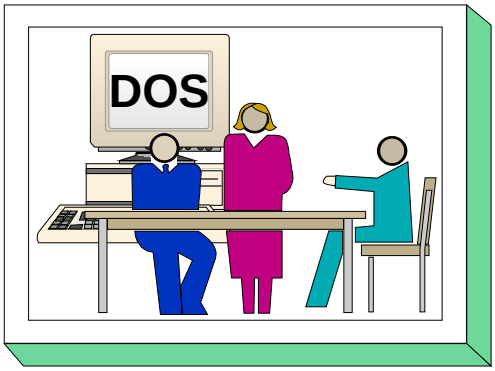
Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures

Hardware & Software:
- S 4.2 (1) Screen lock
- S 4.3 (2) Periodic runs of a virus detection program
- S 4.4 (2) Locking of floppy-disk drive slots (*optional*)
- S 4.27 (1) Password protection in laptop PCs
- S 4.28 (3) Software re-installation in the case of change of laptop PC user (*optional*)
- S 4.29 (1) Use of an encryption product for laptop PCs (*optional*)
- S 4.30 (2) Utilisation of the security functions offered in application programs (optional)
- S 4.31 (2) Ensuring power supply during mobile use
- S 4.44 (2) Checking of incoming data for macro viruses

Contingency Planning:
- S 6.20 (2) Appropriate storage of backup data media
- S 6.21 (3) Backup copy of the software used
- S 6.22 (2) Sporadic checks of the restorability of backups
- S 6.23 (2) Procedure in case of computer virus infection
- S 6.24 (3) PC emergency floppy disk
- S 6.27 (3) Backup of the CMOS RAM
- S 6.32 (1) Regular data backup

❒

5.4 PCs with a non-constant user population



Description

This module should be considered where PCs are used with a non-constant user population. The PCs in question here are commercially available IBM-compatible PCs which run under DOS or a comparable operating system. For PCs which run under other operating systems, the safeguards should be adapted as appropriate.

If the PC is connected to a local network, the relevant modules from Chapter 6 must be implemented.

The PC can possess floppy disks and CD drives, a hard disk, a mouse and other peripheral components. There may be a printer directly connected to it. A graphical user interface can also be employed here. It is assumed that several persons with access rights to the stored data use this PC.

PCs with a non-constant population of users can be used, for example, in PC pools, for training purposes or to meet specific organisational requirements.

Threat Scenario

For IT baseline protection of a PC used by a non-constant set of users, the following typical threats are assumed:

Force Majeure
- T 1.1 Loss of personnel
- T 1.2 Failure of the IT system
- T 1.4 Fire
- T 1.5 Water
- T 1.8 Dust, soiling

Organisational shortcomings
- T 2.1 Lack of, or insufficient, rules
- T 2.7 Unauthorised use of rights
- T 2.9 Poor adjustment to changes in the use of IT
- T 2.21 Inadequate organisation of the exchange of users
- T 2.21 Lack of evaluation of auditing data

Human Failure
- T 3.2 Negligent destruction of equipment or data
- T 3.3 Non-compliance with IT security measures
- T 3.6 Hazards posed by cleaning staff or outside staff
- T 3.8 Improper use of the IT system
- T 3.16 Incorrect administration of site and data access rights
- T 3.17 Incorrect change of PC users

Technical Failure
- T 4.1 Disruption of power supply
- T 4.7 Defective data media

Deliberate Acts
- T 5.1 Manipulation or destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.4 Theft
- T 5.9 Unauthorised use of IT systems
- T 5.18 Systematic trying-out of passwords
- T 5.21 Trojan horses
- T 5.23 Computer viruses
- T 5.43 Macro viruses

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended.

Every user is responsible himself for backing up his own data. Special attention should be given to the problem of viruses on computers with a changing user population. A resident virus scanning program should be on the computer. Otherwise, steps must be taken to ensure that a check is performed for computer viruses both **before** and **after** every change of user.

The safeguards which apply to the area "PCs with a non-constant user population" are listed below.

Infrastructure
- S 1.29 (3) Adequate siting of an IT system (optional)

Organisation
- S 2.3 (2) Data media control
- S 2.4 (2) Maintenance/repair regulations
- S 2.5 (2) Division of responsibilities and separation of functions
- S 2.7 (2) Granting of (system/network) access rights
- S 2.8 (2) Granting of access rights
- S 2.9 (2) Ban on the use of non-approved software
- S 2.10 (3) Survey of the software held
- S 2.13 (2) Correct disposal of resources requiring protection
- S 2.22 (3) Escrow of passwords
- S 2.23 (3) Issue of PC use guidelines (optional)
- S 2.24 (3) Introduction of a PC checklist booklet (optional)
- S 2.26 (1) Appointment of an administrator and his deputy
- S 2.37 (2) Clean desk policy
- S 2.63 (1) Establishing access rights
- S 2.64 (2) Checking the log files
- S 2.65 (1) Checking the efficiency of user separation on an IT System
- S 2.66 (2) The importance of certification for procurement

Personnel
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.10 (1) Selection of a trustworthy administrator and his substitute
- S 3.11 (1) Training of maintenance and administration staff
- S 3.18 (1) Log-out obligation for users

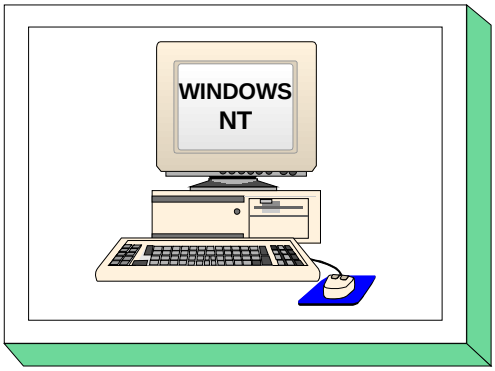
Hardware & Software
- S 4.3 (2) Periodic runs of a virus detection program
- S 4.4 (3) Locking of floppy-disk drive slots (optional)
- S 4.30 (2) Utilisation of the security functions offered in application programs (optional)
- S 4.41 (1) Use of a suitable PC security product
- S 4.42 (2) Implementation of security functions in the IT application (optional)
- S 4.44 (2) Checking of incoming data for macro viruses
- S 4.109 (2) Software reinstallation on workstations

Contingency Planning

- S 6.20 (2) Appropriate storage of backup data media
- S 6.21 (3) Backup copy of the software used
- S 6.22 (2) Sporadic checks of the restorability of backups
- S 6.23 (2) Procedure in case of computer virus infection
- S 6.24 (3) PC emergency floppy disk
- S 6.27 (3) Backup of CMOS RAM
- S 6.32 (2) Regular data backup

❒

5.5 Non-networked Windows NT computer



Description

Single, non-networked PCs with a hard disk (as described in chapter 5.1) and with the operating system Windows NT (version 3.51 or 4.0) are considered. The PCs can be equipped with a floppy disk drive. Security-specific aspects of single Windows NT applications are only covered briefly.

Threat Scenario

The following typical threats are assumed as regards IT baseline protection of single PCs with the operating system Windows NT.

Force Majeure
- T 1.1 Loss of personnel
- T 1.2 Failure of the IT system
- T 1.4 Fire
- T 1.5 Water
- T 1.8 Dust, soiling

Organisational shortcomings:
- T 2.7 Unauthorised use of rights
- T 2.9 Poor adjustment to changes in the use of IT
- T 2.31 Inadequate protection of the Windows NT system

Human Failure:
- T 3.2 Negligent destroying of equipment or data
- T 3.3 Non-compliance with IT security measures
- T 3.6 Hazards posed by cleaning staff or outside staff
- T 3.8 Improper use of the IT system
- T 3.9 Improper IT system administration

Technical Failure:
- T 4.1 Disruption of power supply
- T 4.7 Defective data media
- T 4.8 Discovery of software vulnerabilities
- T 4.23 Automatic CD-ROM-recognition

Deliberate Acts:
- T 5.1 Manipulation/destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.4 Theft
- T 5.9 Unauthorised use of IT systems
- T 5.18 Systematic trying-out of passwords
- T 5.21 Trojan Horses
- T 5.23 Computer viruses
- T 5.43 Macro viruses
- T 5.52 Misuse of administrator rights in Windows NT systems
- T 5.79 Unauthorised acquisition of administrator rights under Windows NT

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

Safeguards listed as "optional" in the following lists go at least partly beyond baseline protection, or refer to special environments. The safeguards are to be implemented if these conditions are fulfilled, especially if many users are working with the same system and need to be protected from one another, or, if the control of critical security functions does not lie with the user himself but must be administrated centrally.

In the following the safeguard group for "Non-networked Windows NT computer" is presented.

Infrastructure:
- S 1.29 (3) Adequate siting of an IT system (*optional*)

Organisation:
- S 2.3 (2) Data media control
- S 2.4 (2) Maintenance/repair regulations
- S 2.9 (2) Ban on using non-approved software
- S 2.10 (2) Survey of the software held
- S 2.13 (2) Correct disposal of resources requiring protection
- S 2.22 (2) Escrow of passwords
- S 2.23 (3) Issue of PC Use guidelines (*optional*)
- S 2.24 (3) Introduction of a PC Checklist booklet (*optional*)
- S 2.25 (1) Documentation on the system configuration
- S 2.26 (1) Designation of an Administrator and his deputy (*optional*)
- S 2.30 (2) Provisions governing the configuration of users and user groups (*optional*)
- S 2.31 (2) Documentation on authorised users and on rights profiles (*optional*)
- S 2.32 (2) Establishment of a restricted user environment (*optional*)
- S 2.34 (2) Documentation on changes made to an existing IT system (*optional*)
- S 2.35 (2) Obtaining information on security weaknesses of the system

Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.10 (1) Selection of a trustworthy administrator and a substitute (*optional*)
- S 3.11 (1) Training of maintenance and administration staff (*optional*)

Hardware & Software:
- S 4.1 (1) Password protection for IT systems
- S 4.2 (1) Screen lock
- S 4.3 (2) Periodic runs of a virus detection program
- S 4.4 (3) Locking of floppy-disk drive slots (*optional*)
- S 4.15 (2) Secure log-in
- S 4.17 (2) Blocking and erasure of unneeded accounts and terminals
- S 4.30 (2) Utilisation of the security functions offered in application programs (optional)
- S 4.44 (2) Checking of incoming data for macro viruses
- S 4.48 (1) Password protection under Windows NT
- S 4.49 (1) Safeguarding the boot-up procedure for a Windows NT system
- S 4.50 (2) Structured system administration under Windows NT (*optional*)

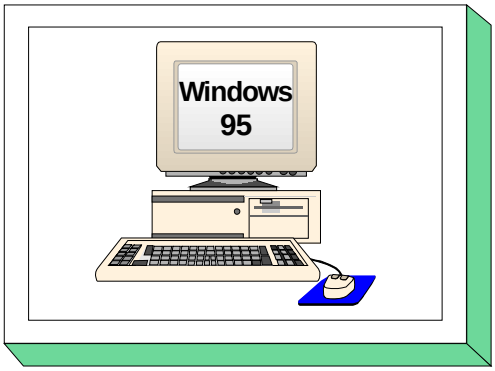
- S 4.51 (3) User profiles to restrict the usage possibilities of Windows NT (*optional*)
- S 4.52 (2) Protection of devices under Windows NT
- S 4.53 (2) Restrictive allocation of access rights to files and directories underWindows NT
- S 4.54 (2) Logging under Windows NT (*optional*)
- S 4.55 (2) Secure installation of Windows NT
- S 4.56 (3) Secure deletion under Windows NT and Windows 95
- S 4.57 (2) Deactivating automatic CD-ROM recognition
- S 4.75 (1) Protection of the registry under Windows NT
- S 4.76 (3) Secure system version of Windows NT
- S 4.77 (1) Protection of administrator accounts under Windows NT
- S 4.84 (1) Use of BIOS security mechanisms
- S 4.93 (1) Regular integrity checking

Contingency Planning:

- S 6.20 (2) Appropriate storage of backup data media
- S 6.21 (3) Backup copy of the software used
- S 6.22 (2) Sporadic checks of the restorability of backups
- S 6.23 (2) Procedure in case of computer virus infection
- S 6.27 (3) Backup of the CMOS RAM
- S 6.32 (1) Regular data backup
- S 6.42 (1) Creating start-up disks for Windows NT
- S 6.44 (1) Data back-up under Windows NT

❒

5.6 PC with Windows 95



Description

A typical PC with the operating system Windows 95 is considered. This PC should not be networked. The PC has a floppy disk drive, a removable or hard disk, a CD-ROM and possibly a mouse. If available, a printer is to be directly connected to the PC. The basis for further considerations is that multiple users will be using this PC.

The following fundamental considerations should also be taken into account:

Essential security properties of Windows 95 can be put into effect only in a server-supported network. If a non-networked Windows 95 computer is operated locally, multi-user operation should be avoided as long as important functions such as control of rights or protocols can still be carried out without the aid of PC security products. The same considerations must be taken even with a single user if this user is to be restricted by an administrator via the system guidelines, as this would actually result in multi-user operation.

Conclusion: A non-networked Windows 95 computer should only have one user who should not be restricted. Restriction of a user is only wise if this eases navigation of the system or if faulty operation can thereby be ruled out. If multi-user operation must nonetheless be implemented, then, for reasons of security, this is only wise in combination with a PC security product.

Threat Scenario

For IT-baseline protection of a PC with Windows 95, the following typical threats will be considered:

Force Majeure
- T 1.1 Loss of personnel
- T 1.2 Failure of the IT system
- T 1.4 Fire
- T 1.5 Water
- T 1.8 Dust, soiling

Organisational shortcomings:
- T 2.1 Lack of, or insufficient, rules
- T 2.7 Unauthorised use of rights
- T 2.9 Poor adjustment to changes in the use of IT
- T 2.21 Inadequate organisation of the exchange of users
- T 2.22 Lack of evaluation of auditing data
- T 2.36 Inappropriate restriction of user environment

Human Failure:
- T 3.2 Negligent destroying of equipment or data
- T 3.3 Non-compliance with IT security measures
- T 3.6 Hazards posed by cleaning staff or outside staff
- T 3.8 Improper use of the IT system
- T 3.16 Incorrect administration of site and data access rights
- T 3.22 Improper modification of the registry

Technical Failure:
- T 4.1 Disruption of power supply
- T 4.7 Defective data media
- T 4.23 Automatic CD-ROM-recognition
- T 4.24 File name conversion when backing up data under Windows 95

Deliberate Acts:
- T 5.1 Manipulation/destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.4 Theft
- T 5.9 Unauthorised use of IT systems
- T 5.21 Trojan Horses
- T 5.23 Computer viruses
- T 5.43 Macro viruses
- T 5.60 By-passing system guidelines

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

In the following the safeguard group "PC with Windows 95" is presented. The fundamental considerations at the beginning of the chapter (see above) should be observed. The safeguards are divided into the following categories:

- Basic safeguards (essentially, these are the same as for chapter 5.1 DOS-PC),
- Safeguards for multi-user operation,
- Restrictions and
- usage in the network

The following basic safeguards need to be implemented:

Infrastructure:
- S 1.29 (3) Adequate siting of an IT system (*optional*)

Organisation:
- S 2.3 (2) Data media control
- S 2.4 (2) Maintenance/repair regulations
- S 2.9 (2) Ban on using non-approved software
- S 2.10 (2) Survey of the software held
- S 2.13 (2) Correct disposal of resources requiring protection
- S 2.22 (2) Escrow of passwords
- S 2.23 (3) Issue of PC Use guidelines (*optional*)
- S 2.24 (3) Introduction of a PC Checklist booklet (*optional*)

Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures

Hardware & Software:
- S 4.1 (1) Password protection for IT systems
- S 4.2 (1) Screen lock
- S 4.3 (2) Periodic runs of a virus detection program
- S 4.4 (2) Locking of floppy-disk drive slots (*optional*)
- S 4.30 (2) Utilisation of the security functions offered in application programs (optional)
- S 4.44 (2) Checking of incoming data for macro viruses
- S 4.56 (1) Secure deletion under Windows NT and Windows 95
- S 4.57 (2) Deactivating automatic CD-ROM recognition
- S 4.84 (1) Use of BIOS security mechanisms

Contingency Planning:
- S 6.20 (2) Appropriate storage of backup data media
- S 6.21 (3) Backup copy of the software used
- S 6.22 (2) Sporadic checks of the restorability of backups
- S 6.23 (2) Procedure in case of computer virus infection
- S 6.27 (3) Backup of the CMOS RAM
- S 6.32 (1) Regular data backup
- S 6.45 (1) Data backup under Windows 95
- S 6.46 (1) Creating a start-up disk for Windows 95

If many users work on the Windows 95 computer, administration of the computer and division of users is essential. In this case, the following safeguards for multi-user operation must additionally be implemented:

Organisation:
- S 2.26 (1) Designation of an administrator and his deputy
- S 2.63 (2) Establishing Access Rights
- S 2.103 (1) Setting up user profiles under Windows 95

Personnel:
- S 3.10 (1) Selection of a trustworthy administrator and his substitute
- S 3.11 (1) Training of maintenance and administration staff
- S 3.18 (1) Log-out obligation for PC users

If particular user-specific restrictions are to be provided in the user environment, the following safeguards must be deployed (Safeguards S 2.64 and S 2.65 are only effective in connection with S 4.41 or S 4.42):

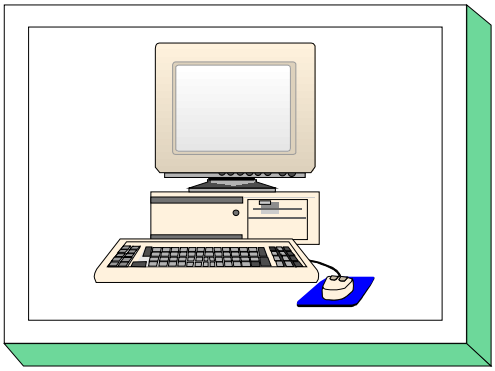
Organisation:
- S 2.64 (2) Checking the log files
- S 2.65 (1) Checking the efficiency of User separation on an IT System
- S 2.66 (2) The importance of certification for procurement
- S 2.104 (1) System guidelines for restricting usage of Windows 95

Hardware & Software:
- S 4.41 (1) Use of a suitable PC security product
- S 4.42 (2) Implementation of security functions in the IT application (optional)

If the PC with Windows 95 is merged in a network, then, additionally, the following measure is necessary:

Hardware & Software:
- S 4.74 (1) Networked Windows 95 computers ❒

5.99 Stand-alone IT systems



Description

Here, an IT system is considered which is not linked with any other IT system. It can be based on any operating system, run on any platform, and consist of a PC with or without a hard disk, Unix workstation or Apple Macintosh. The IT system can possess floppy disks and CD drives, a hard disk, a mouse and other peripheral components. If a printer is required, it is connected directly to the system. A graphic user interface can also be employed here.

This chapter provides an overview of the threats and IT security measures typical of stand-alone IT systems. The overview applies, in general, to all operating systems. For more detailed information, refer to additional chapters of the IT Baseline Protection Manual (e.g. Chapter 5.2 *Stand-alone Unix system*).

Threat Scenario

The following typical threats are assumed as regards IT baseline protection of a stand-alone IT system:

Force Majeure
- T 1.1 Loss of personnel
- T 1.2 Failure of the IT system
- T 1.4 Fire
- T 1.5 Water
- T 1.8 Dust, soiling

Organisational shortcomings:
- T 2.1 Lack of, or insufficient, rules
- T 2.7 Unauthorised use of rights
- T 2.9 Poor adjustment to changes in the use of IT

Human Failure:
- T 3.2 Negligent destroying of equipment or data
- T 3.3 Non-compliance with IT security measures
- T 3.6 Hazards posed by cleaning staff or outside staff
- T 3.8 Improper use of the IT system
- T 3.9 Improper IT system administration
- T 3.16 Incorrect administration of site and data access rights

Technical Failure:
- T 4.1 Disruption of power supply
- T 4.7 Defective data media

Deliberate Acts:
- T 5.1 Manipulation/destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.4 Theft
- T 5.9 Unauthorised use of IT systems
- T 5.23 Computer viruses
- T 5.43 Macro viruses

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

The safeguard package for "Stand-alone IT systems" is described in the following. The safeguards can be subdivided as

- Basic safeguards
- Safeguards for multi-user operation

Depending on the operating system in use, this module might need to be supplemented with additional safeguards.

The following basic safeguards need to be implemented:

Infrastructure:
- S 1.29 (3) Adequate siting of an IT system (*optional*)

Organisation:
- S 2.3 (2) Data media control
- S 2.4 (2) Maintenance/repair regulations
- S 2.9 (3) Ban on using non-approved software
- S 2.10 (2) Survey of the software held
- S 2.13 (2) Correct disposal of resources requiring protection
- S 2.22 (2) Escrow of passwords
- S 2.23 (3) Issue of PC Use guidelines (*optional*)
- S 2.24 (3) Introduction of a PC Checklist booklet (*optional*)

Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures

Hardware & Software:
- S 4.1 (1) Password protection for IT systems
- S 4.2 (1) Screen lock
- S 4.3 (2) Periodic runs of a virus detection program
- S 4.4 (2) Locking of floppy-disk drive slots (*optional*)
- S 4.30 (2) Utilisation of the security functions offered in application programs (optional)
- S 4.44 (2) Checking of incoming data for macro viruses
- S 4.84 (1) Use of BIOS security mechanisms

Contingency Planning:
- S 6.20 (2) Appropriate storage of backup data media
- S 6.21 (3) Backup copy of the software used
- S 6.22 (2) Sporadic checks of the restorability of backups
- S 6.23 (2) Procedure in case of computer virus infection
- S 6.24 (3) PC emergency floppy disk
- S 6.27 (3) Backup of the CMOS RAM (in the case of PCs)
- S 6.32 (1) Regular data backup

If an IT system is to be used by several persons, then administration of the computer and distinction between users are absolutely necessary. In this case, the following safeguards and threats are to be considered additionally for multi-user operation:

Threat Scenario

Organisational shortcomings:
- T 2.21 Inadequate organisation of the exchange of users
- T 2.22 Lack of evaluation of auditing data

Human Failure:
- T 3.17 Incorrect change of PC users

Deliberate Acts:
- T 5.18 Systematic trying-out of passwords
- T 5.19 Abuse of user rights
- T 5.20 Misuse of administrator rights
- T 5.21 Trojan Horses

Recommended Countermeasures (S)

Organisation:
- S 2.5 (2) Division of responsibilities and separation of functions
- S 2.7 (2) Granting of (system/network) access rights
- S 2.8 (2) Granting of (application/data) access permissions
- S 2.63 (1) Establishing Access Rights
- S 2.64 (2) Checking the log files
- S 2.65 (1) Checking the efficiency of User separation on an IT System

Personnel:
- S 3.10 (1) Selection of a trustworthy administrator and his substitute
- S 3.11 (1) Training of maintenance and administration staff
- S 3.18 (1) Log-out obligation for PC users

Hardware & Software:
- S 4.7 (1) Change of preset passwords

If the operating system underlying the IT system does not allow a division between users, the following safeguard should also be observed:
- S 4.41 (1) Use of a suitable PC security product

❒

6 Networked Systems

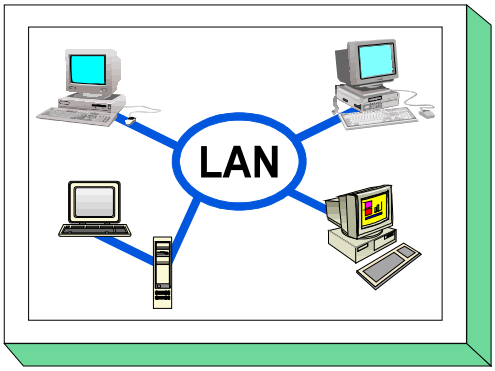
This chapter defines IT baseline protection for networked systems. As a basis, chapter 6.1 lists necessary safeguards independent of the operating system. Chapters 6.2, 6.4, 6.5 and 6.6 are supplementary and operating-system-specific. If Peer-to-Peer functionality is also used, please refer to chapter 6.3.

Chapter 6.7 is to be observed if heterogeneous networks are to be linked together.

Safeguards pertaining to connected clients can be found in chapter 5.

The following chapters are available:

6.1 Server-Supported Network



Description

Here, we deal with a local network with at least one server. The clients can be PCs with or without a hard disk (as described in chapter 5.1), also UNIX-workstations or terminals. This chapter offers an overview of the typical threats and IT security safeguards for a local network. However, the overview does not take the network operating system or the client's operating system into account. In this context, please refer to the supplementary chapters of the IT-baseline protection manual (e.g. chapter 6.2 UNIX servers).

Threat Scenario

The following typical threats (T) are assumed as regards IT baseline protection of a server-supported network:

Force Majeure

- T 1.1 Loss of personnel
- T 1.2 Failure of the IT system
- T 1.4 Fire
- T 1.5 Water
- T 1.8 Dust, soiling

Organisational Shortcomings:

- T 2.7 Unauthorised use of rights
- T 2.9 Poor adjustment to changes in the use of IT
- T 2.32 Inadequate line bandwidth

Human Error:

- T 3.2 Negligent destruction of equipment or data
- T 3.3 Non-compliance with IT security measures
- T 3.5 Inadvertent damaging of cables
- T 3.6 Hazards posed by cleaning staff or outside staff
- T 3.8 Improper use of the IT system
- T 3.9 Improper IT system administration
- T 3.31 Unstructured data organisation

Technical Failure:

- T 4.1 Disruption of power supply
- T 4.6 Voltage variations / overvoltage / undervoltage
- T 4.7 Defective data media
- T 4.8 Discovery of software vulnerabilities
- T 4.10 Complexity of access possibilities to networked IT systems

Deliberate Acts:

- T 5.1 Manipulation or destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software

  T 5.4 Theft

- T 5.7 Line tapping
- T 5.8 Manipulation of lines
- T 5.9 Unauthorised use of IT systems
- T 5.18 Systematic trying-out of passwords
- T 5.19 Abuse of user rights
- T 5.20 Abuse of Administrator rights
- T 5.21 Trojan horses

- T 5.23 Computer viruses
- T 5.24 Replay of messages
- T 5.25 Masquerading
- T 5.26 Analysis of the message flow
- T 5.27 Repudiation of a message
- T 5.28 Denial of services
- T 5.43 Macro viruses

Recommended Countermeasures (S)

To implement IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended.

In the following, the safeguard group "Server-supported Network" is presented.

It is required that the server be located in either a server room (see chapter 4.3.2) or a protective cabinet (see chapter 4.4). The safeguards to be implemented for the network operating system are contained in the supplementary chapters of the manual. This also applies to connected clients.

In addition, the following measures will have to be taken:

Infrastructure:
- S 1.28 (2) Local Uninterruptible Power Supply (UPS)
- S 1.29 (3) Adequate Siting of an IT System (optional)
- S 1.32 (1) Adequate siting of the Consoles, Devices with Exchangeable Data Media, and Printers

Organisation:
- S 2.3 (2) Data Media Control
- S 2.4 (2) Maintenance/Repair Regulations
- S 2.9 (2) Ban on Using Non-Approved Software
- S 2.10 (3) Survey of the Software Held
- S 2.13 (2) Correct disposal of resources requiring protection
- S 2.22 (2) Escrow of Passwords
- S 2.25 (1) Documentation of the System Configuration
- S 2.26 (1) Appointment of an administrator and his deputy
- S 2.30 (2) Provisions governing the configuration of users and of user groups
- S 2.31 (2) Documentation on authorised users and on rights profiles
- S 2.32 (3) Establishment of a restricted user environment (*optional*)
- S 2.34 (2) Documentation of changes made to an existing IT system
- S 2.35 (2) Obtaining information on security weaknesses of the system
- S 2.38 (2) Division of administrator roles in PC networks
- S 2.138 (2) Structured data storage
- S 2.204 (1) Prevention of insecure network access

Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.10 (1) Selection of a trustworthy administrator and his substitute
- S 3.11 (1) Training of maintenance and administration staff

Hardware and software:
- S 4.1 (1) Password protection for IT systems
- S 4.2 (1) Screen lock
- S 4.3 (2) Periodic runs of a virus detection program
- S 4.7 (1) Change of preset passwords
- S 4.15 (2) Secure log-in
- S 4.16 (2) Restrictions on access to accounts and/or terminals
- S 4.17 (2) Blocking and deletion of unnecessary accounts and terminals
- S 2.138 (2) Ensuring consistent system management

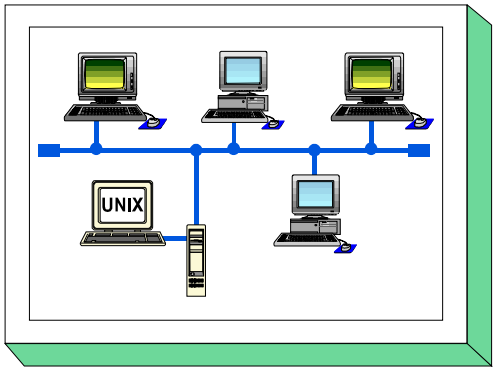
- S 4.44 (2) Checking of incoming files for macro viruses
- S 4.65 (2) Testing of new hardware and software

Communications:
- S 5.6 (1) Mandatory use of a network password
- S 5.7 (1) Network management
- S 5.8 (1) Monthly security checks of the network
- S 5.9 (2) Logging at the server
- S 5.10 (1) Restrictive granting of access rights
- S 5.13 (1) Appropriate use of equipment for network coupling

Contingency Planning:
- S 6.20 (2) Appropriate storage of backup data media
- S 6.21 (3) Backup copy of the software used
- S 6.22 (2) Sporadic checks of the restorability of backups
- S 6.25 (1) Regular data backup
- S 6.31 (2) Procedural patterns following a loss of system integrity
- S 6.32 (1) Regular data backup

❒

6.2 UNIX Server



Description

UNIX server consist of computers running on the UNIX operating system and offering services (as servers) for other IT systems within a network.

In this chapter, the threats and safeguards described are specifically for UNIX servers. Additional threats and safeguards applying to server-supported networks can be found in chapter 6.1.

Threat Scenario

The following typical threats (T) are assumed as regards IT baseline protection of a UNIX server:

Organisational Shortcomings:
- T 2.15 Loss of confidentiality of sensitive data in the UNIX system
- T 2.23 Security flaws involved in integrating DOS PCs into a server-based network
- T 2.65 Complexity of the SAMBA configuration

Human Error:
- T 3.10 Incorrect export of file systems under UNIX
- T 3.11 Improper configuration of *sendmail*

Technical Failure:
- T 4.11 Lack of authentication possibilities between NIS Server and NIS Client
- T 4.12 Lack of authentication possibilities between X Server and X Client

Deliberate Acts:
- T 5.40 Monitoring rooms using computers equipped with microphones
- T 5.41 Misuse of a UNIX system with the help of uucp
- T 5.89 Hijacking of network connections

Recommended Countermeasures (S)

To implement IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended.

In the following, the safeguard package for "UNIX servers" is set out.

Some measures refer to the configuration of the various servers; other measures will have to be implemented by servers and clients in order to become effective. For any clients connected, the safeguards outlined in chapter 5 must be implemented.

It is advisable to install the server in a separate server room. The appropriate measures are described in Chapter 4.3.2. If no server room is a available, a server cabinet should be used (c.f. Chapter 4.4).

In addition, the following measures will have to be taken:

Infrastructure:
- S 1.28 (1) Local Uninterruptible Power Supply (UPS)

Organisation:
- S 2.33 (2) Division of Administrator roles under UNIX

Hardware and software:

Access to the UNIX system
- S 4.13 (1) Careful allocation of identifiers
- S 4.14 (1) Mandatory password protection under UNIX
- S 4.18 (1) Administrative and technical means to control access to the system-monitor and single-user mode
- S 4.105 (1) Initial measures after a Unix standard installation

Allocation of attributes / Working with the UNIX system
- S 4.9 (1) Use of the security mechanisms of X Windows
- S 4.19 (1) Restrictive allocation of attributes for UNIX system files and directories
- S 4.20 (2) Restrictive allocation of attributes for UNIX user files and directories
- S 4.21 (1) Preventing unauthorised acquisition of administrator rights
- S 4.22 (3) Prevention of loss of confidentiality of sensitive data in the UNIX system
- S 4.23 (3) Secure invocation of executable files

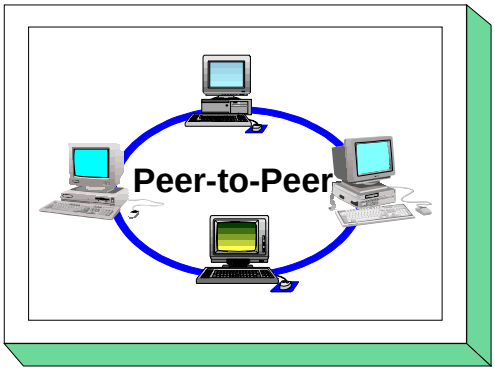
Logging / Security checks

- S 4.25 (1) Use of logging in UNIX systems
- S 4.26 (2) Regular security checks of the UNIX system
- S 4.40 (2) Preventing unauthorised use of computer microphones
- S 4.93 (1) Regular integrity checking
- S 4.106 (1) Aktivation of system logging
- S 4.107 (2) Use of vendor resources

Communications:
- S 5.16 (2) Survey of network services
- S 5.17 (1) Use of the NFS security mechanisms
- S 5.18 (1) Use of the NIS security mechanisms
- S 5.19 (1) Use of the sendmail security mechanisms
- S 5.20 (1) Use of the security mechanisms of *rlogin, rsh* and *rcp*
- S 5.21 (1) Secure use of *telnet, ftp, tftp* and *rexec*
- S 5.34 (2) Use of one-time passwords (*optional*)
- S 5.35 (1) Use of UUCP security mechanisms
- S 5.36 (2) Encryption under UNIX and Windows NT (*optional*)
- S 5.38 (2) Secure integration of DOS PC's into a UNIX network
- S 5.64 (2) Secure Shell
- S 5.72 (1) Deactivation of unnecessary network services
- S 5.82 (1) Secure use of SAMBA
- S 5.83 (2) Secure Connection of an External Network with Linux FreeS/WAN (optional)

Contingency Planning:
- S 6.31 (2) Procedural patterns following a loss of system integrity
- S 6.32 (1) Regular data backup

6.3 Peer-to-Peer network



Description

Here, networked PCs are considered which are operated with Windows for Workgroups (WfW), Windows 95 or Windows NT. Only the pure Peer-to-Peer functions of these operating systems are taken into consideration on the basis of resource-sharing (printer, hard disk). Only brief attention is paid to security-specific aspects of single applications when using Peer-to-Peer functions, e.g. *Mail Exchange*, *Schedule+*, *Direct Data Exchange (DDE)* or *Remote Access Service (RAS)*.

Since Peer-to-Peer networks offer considerably less security functions than server-supported networks, the use of Peer-to-Peer functions within a server-supported network should be avoided. Peer-to-Peer networks with a connection via WfW to another computer with WfW, Windows 95 or Windows NT should only be considered as a transitional solution until WfW has been replaced.

This chapter deals solely with the threats and safeguards specific to a Peer-to-Peer network. The threats and safeguards contained in the PC-specific units of Chapter 5 should thus also be observed.

Threat Scenario

The following typical threats (T) are assumed as regards Peer-to-Peer functions under Windows for Workgroups, Windows 95 or Windows NT:

Organisational shortcomings:

- T 2.25 Reduction of transmission or execution speed caused by Peer-to-Peer functions

Human Failure:

- T 3.9 Improper IT system administration
- T 3.18 Sharing of directories, printers or of the clipboard
- T 3.19 Storing of passwords for WfW and Windows 95
- T 3.20 Unintentional granting of read access for Schedule+

Deliberate Acts:

- T 5.45 Trying Out Passwords under WfW and Windows 95
- T 5.46 Masquerading under WfW
- T 5.47 Deleting the Post Office

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

When processing the original Peer-to-Peer safeguards, a strategy should be drawn up using S 2.67 *Determining a Security Strategy for the Peer-to-Peer Network*, as this is the basis for the subsequent measures.

In the following, the safeguard group for the area "Peer-to-Peer network" is presented:

Organisation:
- S 2.67 (1) Defining a security strategy for peer-to-peer networks
- S 2.68 (2) Implementation of security checks by the peer-to-peer network users
- S 2.94 (2) Sharing of directories under Windows NT

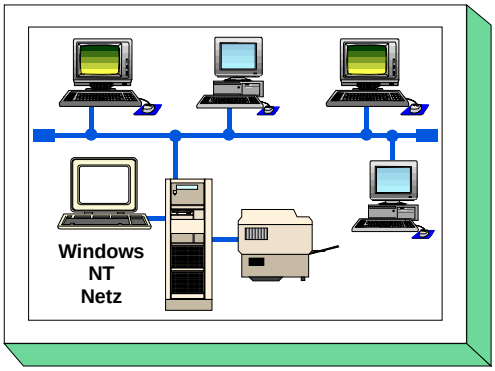
Personnel:
- S 3.19 (1) Instructions concerning the correct use of the security functions in Peer-to-Peer networks

Hardware & Software:
- S 4.1 (1) Password protection for IT systems
- S 4.2 (2) Screen lock
- S 4.7 (1) Change of preset passwords
- S 4.45 (1) Setting up a secure Peer-to-Peer environment
- S 4.46 (1) Use of the log-on password under WfW and Windows 95
- S 4.58 (2) Sharing of directories under Windows 95

Communications:
- S 5.37 (2) Restricting Peer-to-Peer functions when using WfW, Windows 95 or Windows NT in a server-supported network (optional)

Contingency Planning:
- S 6.32 (2) Regular data backup

6.4 Windows NT network



Description

This chapter concerns a Windows NT network functioning as a client-server system under the Windows NT operating system (version 3.51 or 4.0). The security aspects of a Windows NT server are dealt with.

The client-specific safeguards are covered in chapter 5. There are only marginal references to aspects of Windows NT applications specific to security, for example in relation to *Mail*, *Schedule+*, *Direct-Data-Exchange (DDE)* or *Remote Access Service (RAS)*. In addition to the dangers and protection safeguards detailed here, the safeguards specified in Section 6.1 for a general server-supported network still apply. If the Peer-to-Peer functionality of Windows NT is used in the Windows NT network, the contents of Section 6.3 should also be taken into account.

Threat Scenario

The following typical threats are assumed for IT baseline protection of a server-supported network under the Windows NT operating system:

Organisational shortcomings:

- T 2.23 Security flaws involved in integrating DOS PCs into a server-based network
- T 2.25 Reduction of transmission or execution speed caused by Peer-to-Peer functions
- T 2.30 Inadequate domain planning
- T 2.31 Inadequate protection of the Windows NT system

Technical Failure:

- T 4.10 Complexity of access possibilities to networked IT systems
- T 4.23 Automatic CD-ROM-recognition

Deliberate Acts:

- T 5.23 Computer viruses
- T 5.40 Monitoring rooms using computers equipped with microphones
- T 5.43 Macro viruses
- T 5.52 Misuse of administrator rights in Windows NT systems
- T 5.79 Unauthorised acquisition of administrator rights under Windows NT

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

When processing the specific Windows NT safeguards, a safety strategy should first be drawn up using safeguard S 2.91 *Determining a security strategy for the Windows NT client-server network.* In

addition, given that Peer-to-Peer functionality is used, safeguard S 2.67 *Determining a security strategy for the Peer-to-Peer network*, as this is the basis for the further safeguards.

The actual planning of the Windows NT network should then be carried out as described in safeguard S 2.93 *Planning of the Windows NT network*. In accordance with the specifications drawn up during this process, a server should first be installed and tested out with a small number of clients in order to be able to optimise and adapt the fixed structures, before they are deployed in detail.

For the systems networked under Windows NT the safeguards specified here must be implemented in addition to the safeguards outlined in Chapter 6.1. It seems sensible to install the file server in a separate server room. The appropriate measures are described in Chapter 4.3.2. As an alternative, server cabinets can be used (c.f. Chapter 4.4).

For any clients connected, the safeguards outlined in chapter 5 must be implemented. Given that the Peer-to-Peer functionality of Windows NT is also being used, the safeguards specified in Section 6.3 must also be implemented.

Safeguards marked with the suffix "optional" exceed, at least partially, the requirements of IT baseline protection, or they refer to special usage environments. They should be implemented if the usage conditions concerned exist and/or specific threats warded off by these safeguards can be expected.

The safeguard measures regarding a Windows NT network are presented in the following:

Organisation:

- S 2.91 (1) Determining a security strategy for the Windows NT client-server network
- S 2.92 (2) Performing security checks in the Windows NT client-server network
- S 2.93 (1) Planning of a Windows NT network
- S 2.94 (3) Sharing of directories under Windows NT

Hardware & Software:

- S 4.40 (3) Preventing unauthorised use of computer microphones
- S 4.48 (1) Password protection under Windows NT
- S 4.49 (1) Safeguarding the boot-up procedure for a Windows NT system
- S 4.50 (2) Structured system administration under Windows NT (*optional*)
- S 4.51 (3) User profiles to restrict the usage possibilities of Windows NT (*optional*)
- S 4.52 (2) Protection of devices under Windows NT
- S 4.53 (2) Restrictive allocation of access rights to files and directories underWindows NT
- S 4.54 (2) Logging under Windows NT
- S 4.55 (2) Secure installation of Windows NT
- S 4.56 (3) Secure deletion under Windows NT and Windows 95
- S 4.57 (2) Deactivating automatic CD-ROM recognition
- S 4.75 (1) Protection of the registry under Windows NT
- S 4.76 (2) Secure system version of Windows NT
- S 4.77 (1) Protection of administrator accounts under Windows NT
- S 4.93 (1) Regular integrity checking

Communications:

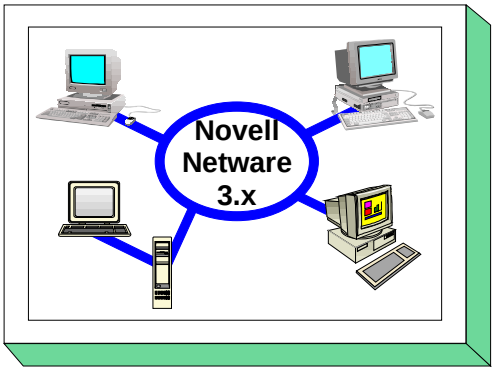
- S 5.36 (3) Encryption under UNIX and Windows NT (optional)
- S 5.37 (3) Restricting Peer-to-Peer functions when using WfW, Windows 95 or Windows NT in a server-supported network
- S 5.40 (1) Secure integration of DOS-PCs to a Windows NT network
- S 5.41 (2) Secure configuration of remote access under Windows NT
- S 5.42 (2) Secure configuration of TCP/IP network administration under Windows NT
- S 5.43 (2) Secure configuration of TCP/IP network services under Windows NT

Contingency Planning:

- S 6.32 (1) Regular data backup
- S 6.42 (2) Creating start-up disks for Windows NT
- S 6.43 (3) Use of redundant Windows NT servers (*optional*)
- S 6.44 (1) Data back-up under Windows NT

❒

6.5 Novell Netware 3.x



Description

A LAN with PCs that are networked with the network operating system Novell Netware 3.x is considered. The PCs can be equipped with hard disks, CD-ROMs and floppy disk drives. One, or possibly more printers, can be connected as waiting loop printers. The subject of this chapter is the Novell 3.x network in a client-server function. Thus, this chapter is a supplement to chapter 6.1 and is operating-system specific.

The functions of so-called Accounting will not be considered.

Note: File and program names will always be written in capital letters and italics (e.g. *SYS:PUBLIC\SYSCON.EXE*).

Threats and the necessary measures that arise have been put together on the basis of Novell versions 3.11 and 3.12. Due to the presence of various patch levels in the network operating-system, not all threats might apply to every variant of Novell Netware 3.x.

Threat Scenario

For IT baseline protection, the following typical threats will be considered.

Force Majeure

- T 1.2 Failure of the IT system

Organisational shortcomings:

- T 2.33 Siting of Novell Netware Servers in an insecure environment
- T 2.34 Absence of or inadequate activation of Novell Netware safeguards
- T 2.58 Novell Netware and date conversion to the year 2000

Technical Failure:

- T 4.1 Disruption of power supply

Deliberate Acts:

- T 5.23 Computer viruses
- T 5.43 Macro viruses
- T 5.54 Deliberately causing an Abnormal End
- T 5.55 Login Bypass
- T 5.56 Temporary free-access accounts
- T 5.57 Network analysis tools
- T 5.58 Hacking Novell Netware
- T 5.59 Misuse of administrator rights in the Novell Netware network

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

For networked PCs, the safeguards described in chapter 5 should be implemented. Bear in mind that these safeguards only concern the properties of Novell Netware 3.x. and that these, and the general network security safeguards described in chapter 6.1 "Server-supported network", complement one another.

The safeguards for Novell Netware 3.x are as follows:

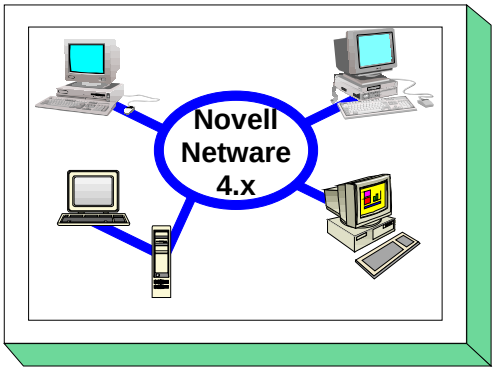
Infrastructure:
- S 1.28 (1) Local uninterruptable power supply (ups)
- S 1.42 (1) Secure siting of Novell Netware servers

Organisation:
- S 2.98 (2) Secure installation of Novell Netware servers
- S 2.99 (1) Secure set-up of Novell Netware servers
- S 2.100 (1) Secure operation of Novell Netware servers
- S 2.101 (2) Revision of Novell Netware servers
- S 2.102 (3) Relinquishing activation of the remote console (optional)

Hardware & Software:
- S 4.66 (1) Novell Netware - safe transition to the year 200

❒

6.6 Novell Netware 4.x



Description

The object under consideration is a Novell Netware 4.x network operating system (with a focus on Netware 4.11). Novell Netware is operated on PC servers and essentially provides the following infrastructure services in a network: authentication, directory service, file service, printing and logging. The subject of this chapter is the Novell 4.x network in a client-server function. Thus, this chapter is a supplement to chapter 6.1 and is operating-system specific.

A central aspect of the Novell Netware 4.x operating system is the distribution of the central database of the NDS (Novell Directory Services) - irrespective of any specific server systems - across the network, and an object-oriented approach towards the management of all elements in a homogeneous operating-system environment.

The functionality of Novell Netware add-on products such as DHCP, WEB Server and WAN Connectivity are also considered.

Remarks:

- Names of files and programs are always presented in italics (e.g. *SYS:PUBLIC\NWADMIN.EXE*).
- Threats and corresponding safeguards have been specified using Novell version 4.11 as a basis. Due to the presence of various patch levels in the network operating-system and/or due to different developments betwee Netware 4.10 and Netware 4.11, not all threats might apply to every variant of Novell Netware 4.x. If necessary this will be explicitely pointed out or marked in the text.

Threat Scenario

The following typical threats are assumed as regards IT baseline protection of Novell Netware Version 4.x:

Force Majeure
- T 1.2 Failure of the IT system

Organisational shortcomings
- T 2.33 Siting of Novell Netware Servers in an insecure environment
- T 2.34 Absence of or inadequate activation of Novell Netware safeguards
- T 2.42 Complexity of the NDS
- T 2.43 Migration of Novell Netware 3.x to Novell Netware Version 4
- T 2.58 Novell Netware and date conversion to the year 2000

Human Failure
- T 3.8 Improper use of the IT system
- T 3.25 Negligent deletion of objects
- T 3.26 Inadvertent sharing of the file system
- T 3.27 Improper time synchronisation
- T 3.38 Errors in configuration and operation

Technical Failure
- T 4.1 Disruption of power supply

Deliberate Acts
- T 5.23 Computer viruses
- T 5.43 Macro viruses
- T 5.55 Login Bypass
- T 5.56 Temporary free-access accounts
- T 5.57 Network analysis tools
- T 5.58 Hacking Novell Netware
- T 5.59 Misuse of administrator rights in the Novell Netware network

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended.

For networked PCs, the safeguards described in chapter 5 should be implemented. Bear in mind that these safeguards only concern the properties of Novell Netware 4.x. and that these, and the general network security safeguards described in chapter 6.1 "Server-supported network", complement one another.

The following measures are recommended in addition:

Infrastructure
- S 1.28 (1) Local uninterruptable power supply (ups)
- S 1.42 (1) Secure siting of Novell Netware servers

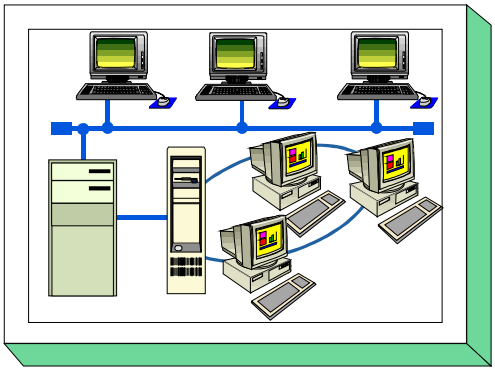
Organisation
- S 2,102 (2) Relinquishing activation of the remote console (optional)
- S 2.147 (1) Secure migration of Novell Netware 3.x servers to Novell Netware 4.x networks
- S 2.148 (1) Secure configuration of Novell Netware 4.x networks
- S 2.149 (2) Secure operation of Novell Netware 4.x networks
- S 2.150 (1) Auditing of Novell Netware 4.x networks
- S 2.151 (1) Design of an NDS concept
- S 2.152 (2) Design of a time synchronisation concept
- S 2.153 (1) Documentation of Novell Netware 4.x networks

Hardware & Software
- S 4.66 (1) Novell Netware - safe transition to the year 200
- S 4.102 (2) C2 security under Novell 4.11 (optional)
- S 4.103 (1) DHCP server under Novell Netware 4.x (optional)
- S 4.104 (2) LDAP Services for NDS (optional)
- S 4.108 (2) Simplified and secure network management with DNS services under Novell NetWare 4.11 (optional)

Contingency Planning
- S 6.55 (2) Reduction of restart times for Novell Netware servers

❒

6.7 Heterogeneous Networks



Description

A local network is composed of wiring (i.e. cables and connecting elements, which are passive network components) as well as active network coupling components. Generally, various types of cable and active network components can be integrated into a LAN. Active network components require a separate power supply. Such components include repeaters, bridges, switches, routers, gateways etc. Passive network components do not require a separate power supply. Such components include cables, distributor cabinets, patch fields and plug connectors.

Cabling is discussed in detail in Chapter 4.2, while Chapters 5 and 6 deal with application-related periphery. Consequently, this module focuses on the active network components, the topology underlying them, their configuration, criteria for choosing suitable components, the selection of communication protocols and the related network management.

Only LAN technologies, e.g. Ethernet, Token Ring and FDDI network protocols and the related network components such as bridges, switches and routers are considered here. These technologies can also be used in MANs. However, integration into WANs is not discussed here; this information is provided in Chapter 7.3 "Firewalls".

If a LAN is to be protected adequately from the perspective of IT baseline protection, a reference to this chapter alone is not sufficient. In addition to the active network components and network management software, a treatment of the physical wiring and of the server systems present in the network is also required. For this reason, it is absolutely necessary to refer to the above-mentioned chapters as well.

This chapter provides guidelines on how to analyse a heterogeneous network and use this analysis as a basis for realising and operating such a network from the perspective of IT security. Consequently, this chapter is intended for organisational departments responsible for operating networks and in possession of the corresponding technical know-how.

Threat Scenario

The following typical threats are assumed as regards IT baseline protection of a heterogeneous network:

Force Majeure

- T 1.1 Loss of personnel
- T 1.2 Failure of the IT system
- T 1.3 Lightning
- T 1.4 Fire
- T 1.5 Water
- T 1.7 Inadmissible temperature and humidity
- T 1.8 Dust, soiling

Organisational Shortcomings:

- T 2.7 Unauthorised use of rights
- T 2.9 Poor adjustment to changes in the use of IT
- T 2.22 Lack of evaluation of auditing data
- T 2.27 Lack of, or inadequate, documentation
- T 2.32 Inadequate line bandwidth
- T 2.44 Incompatible active and passive network components
- T 2.45 Conceptual deficiencies of a network
- T 2.46 Exceeding the maximum allowed cable/bus length or ring size

Human Error:

- T 3.2 Negligent destruction of equipment or data
- T 3.3 Non-compliance with IT security measures
- T 3.5 Inadvertent damaging of cables
- T 3.6 Hazards posed by cleaning staff or outside staff
- T 3.8 Improper use of the IT system
- T 3.9 Improper IT system administration
- T 3.28 Inadequate configuration of active network components
- T 3.29 Lack of, or unsuitable segmentation

Technical Failure:

- T 4.1 Disruption of power supply
- T 4.6 Voltage variations / overvoltage / undervoltage
- T 4.8 Discovery of software vulnerabilities
- T 4.31 Failure or malfunction of a network component

Deliberate Acts:

- T 5.1 Manipulation or destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.4 Theft

- T 5.5 Vandalism
- T 5.6 Attack
- T 5.7 Line tapping
- T 5.8 Manipulation of lines
- T 5.9 Unauthorised use of IT systems
- T 5.18 Systematic trying-out of passwords
- T 5.28 Denial of services
- T 5.66 Unauthorised connection of IT systems to a network
- T 5.67 Unauthorised execution of network management functions
- T 5.68 Unauthorised access to active network components

Recommended Countermeasures (S)

To implement IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended.

Here, it must be pointed out once again that adequate protection of a LAN from the perspective of IT baseline protection can only be ensured if the packages of safeguards described in Chapter 4.2 *Cabling*, Chapter 6.1 *Server-based networks* and, if applicable, additional measures related to the operating-system in use and Chapter 6.8 *Network and system management* are also implemented.

Furthermore, the active network components should be installed in rooms intended to accommodate technical infrastructure (e.g. distributor rooms), this means that the safeguards described in Chapter 4.3.4 *Technical infrastructure rooms* also need to be taken into account.

The network administrator's workstation also requires special protection. In addition to the safeguards described in Chapter 4.3.1 *Offices*, rules pertaining to the operating system in use must also be specified here (refer to Chapter 6).

Secure operation of a heterogeneous network requires the implementation of a number of measures, beginning with an analysis of the existing network environment, followed by the development of a network management concept, and leading to the actual operation of a heterogeneous network. The steps and measures involved are described below:

1. Analysis of the existing network environment (refer to S 2.139 *Survey of the existing network environment* and S 2.140 *Analysis of the existing network environment*)
   - Survey of load factors and analysis of traffic flow
   - Determination of network bottlenecks
   - Identification of critical areas
2. Conception
   - Conception of a network (refer to S 2.141 *Development of a network concept*, S 2.142 *Development of a network realisation plan* and S 5.60 *Selection of a suitable backbone technology*)
   - Conception of a network management (refer to S 2.143 *Development of a network management concept* and S 2.144 *Selection of a suitable network management protocol*)

3. Reliable operation of a network
   - Segmentation of a network (refer to S 5.61 *Suitable physical segmentation* and S 5.62 *Suitable logical segmentation*)
   - Use of a network management software package (refer to S 2.145 *Requirements for a network management tool* and S 2.146 *Reliable operation of a network management system*)
   - Auditing of a network (refer to S 4.81 *Auditing and logging of activities in a network* and S 2.64 *Checking the log files*)
4. Contingency planning
   - Redundant arrangement of network components (refer to S 6.53 *Redundant arrangement of network components*)
   - Backup of configuration files (refer to S 6.52 *Regular backup of configuration data of active network components* and S 6.22 *Sporadic checks of the restorability of backups*)

The complete package of safeguards for the area of heterogeneous networks is presented in the following; this package includes measures of a fundamental nature which need to be noted in addition to the measures described above.

Infrastructure:
- S 1.25 (1) Overvoltage protection
- S 1.27 (2) Air conditioning
- S 1.28 (1) Local Uninterruptible Power Supply (UPS)
- S 1.29 (3) Adequate Siting of an IT System (optional)
- S 1.32 (1) Adequate siting of the Consoles, Devices with Exchangeable Data Media, and Printers

Organisation:
- S 2.4 (2) Maintenance/Repair Regulations
- S 2.22 (2) Escrow of Passwords
- S 2.25 (1) Documentation of the System Configuration
- S 2.26 (1) Appointment of an administrator and his deputy
- S 2.34 (1) Documentation of changes made to an existing IT system
- S 2.35 (1) Obtaining information on security weaknesses of the system
- S 2.38 (2) Division of administrator roles in PC networks
- S 2.64 (2) Checking the log files
- S 2.139 (1) Survey of the existing network environment
- S 2.140 (1) Analysis of the existing network environment (*optional*)
- S 2.141 (1) Development of a network concept
- S 2.142 (1) Development of a network realisation plan
- S 2.143 (1) Development of a network management concept
- S 2.144 (1) Selection of a suitable network management protocol
- S 2.145 (2) Requirements for a network management tool
- S 2.146 (1) Secure operation of a network management system

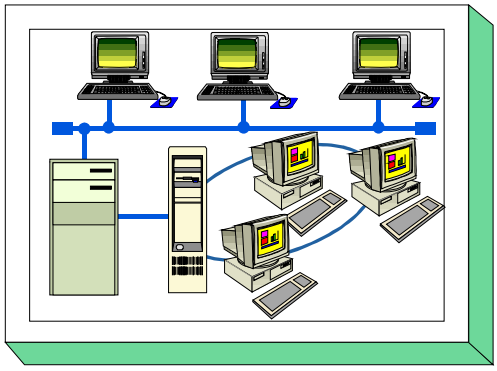
Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.10 (1) Selection of a trustworthy administrator and his substitute
- S 3.11 (1) Training of maintenance and administration staff

Hardware and software:
- S 4.7 (1) Change of preset passwords
- S 4.15 (2) Secure log-in
- S 4.24 (1) Ensuring consistent system management
- S 4.79 (1) Secure access mechanisms for local administration
- S 4.80 (1) Secure access mechanisms for remote administration
- S 4.81 (2) Auditing and logging of activities in a network

- S 4.82 (1) Secure configuration of active network components
- S 4.83 (3) Updating / upgrading of software and hardware in network components

Communications:
- S 5.2 (1) Chosing a suitable network topography
- S 5.7 (1) Network management
- S 5.12 (2) Setting up an additional network administrator
- S 5.13 (1) Appropriate use of equipment for network coupling
- S 5.60 (1) Selection of a suitable backbone technology
- S 5.61 (1) Suitable physical segmentation
- S 5.62 (1) Suitable logical segmentation (*optional*)
- S 5.77 (1) Establishment of Subnetworks (*optional*)

Contingency Planning:
- S 6.22 (2) Sporadic checks of the restorability of backups
- S 6.52 (1) Regular backup of configuration data of active network components
- S 6.53 (1) Redundant arrangement of network components
- S 6.54 (3) Procedures in case of a loss of network integrity



6.8 Network and System Management

Description

A management system for a local computer network is normally used to control all the hardware and software components located in the local network. Such systems should support the system administrators as much as possible in their daily work. There is a basic distinction between network management and system management. The differences are due to the components that are controlled.

Network management includes all the precautions and activities for securing the effective use of a network. For example, this includes checking that the network components are functioning correctly, monitoring the network performance and centrally configuring of the network components. Network management is primarily an organisational problem which can only be supported by technical means, a network management system.

System management is primarily concerned with the management of distributed IT systems. This includes, for example, the central administration of the users, the distribution of software, the management of the applications, etc. In several areas, such as configuration management (the monitoring and consolidation of configurations of a system or a network component), it is impossible to clearly distinguish between network management and system management.

In the following, the (software) system used to manage a network and its components is always referred to as "management system". The components that it manages are called "managed system". These terms are used particularly in the area of network management.

A network and system management framework is defined in ISO/IEC standard 7498-4 and in X.700 of ITU-T. The tasks of a management systems are:

1. configuration management,
2. performance management,
3. error management
4. invoice management
5. security management.

A specific system management product does not only have to offer support in each of these areas. The suppliers usually offer ranges of products designed in such a way that special functionalities can be obtained as a module or an associated individual product.

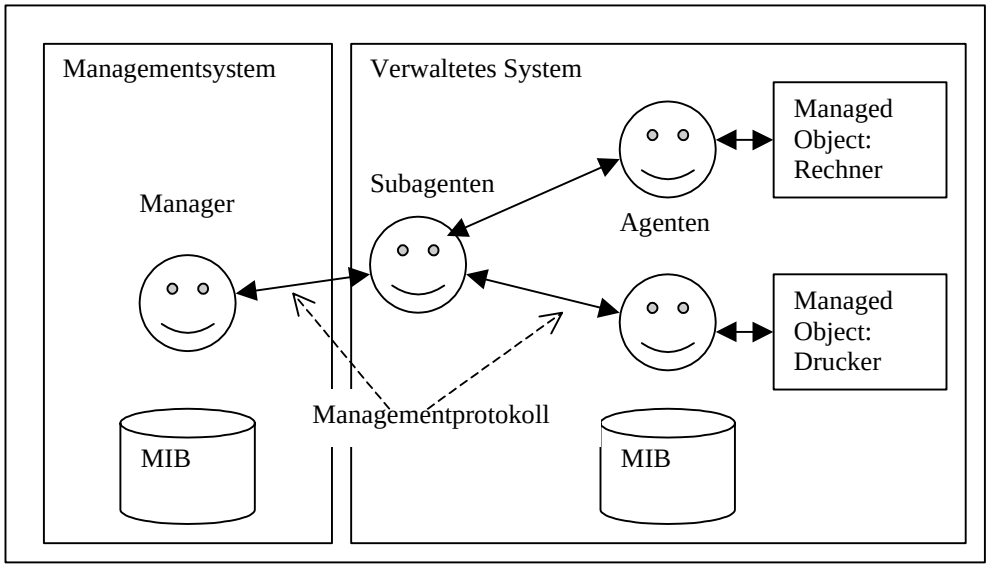
Network management is the older and more mature management discipline. In comparison, system management is a relatively new discipline, but is requested more and more due to the rapidly-increasing networking in enterprises and authorities and the resulting increase in heterogeneity and complexity. The goal here must be to integrate the two disciplines. The management products available at the moment are designed in such a way that they can primarily be used either for network management or for system management. Products which combine the two functionalities are still under development. As a rule, products that are designed for system management also allow access to information concerning network management.

Due to the heterogeneity of the hardware and software of current networks, system management is an extremely complex task. System management is made even more difficult through the fact that management software and the software to be managed have to work together. As a rule, the software

available today is not designed to work together with a management system. This is partly due to a lack of standards which, for example, guarantee sufficient security and partly due to the fact that large software packages are fitted with their own management, because restricted information necessary for managing the software should not be revealed. For example, the Microsoft Internet Explorer has management software, the "Internet Explorer Administration Kit (IEAK)", which allows the administrator to select security settings which cannot be changed by the user or can only be changed to certain values. The functions of this tool are proprietary and are not subject to any standards.

The architecture of management software generally has a centralist structure. There is a central management station or control panel from which the system administrators can manage the network for which they are responsible together with the hardware and software it contains. Particularly the systems for network management are based on this. As a result of the lack of standards in the area of system management, the available products often have centralist architecture, yet the details are proprietary and no general statement can be made about the architecture.

A *network management system* is usually based on a model which distinguishes between "manager", "agent" (also "management agent") and "managed objects". Other components are the protocol used for communication between the manager and the agents, as well as an information database, the so-called "MIB" (Management Information Base). The MIB must be available to both the manager and each management agent. The idea is that management agents and their MIB are seen to be part of the managed system.



An agent is responsible for one or more of the objects which are to be managed. It is possible to organise the agents hierarchically. Agents are then responsible for the subagents assigned to them. There is always an object to be managed at the end of each command chain formed in this way. An object to be managed is either an existing physical object (device) such as a computer, a printer or a router, or a software object such as a background process for the administration of print jobs. In the case of devices that can be managed with a management system, the management agent is usually "permanently" integrated in the device by the manufacturer. If the agent does not understand the communication protocol used by the manager, a software management agent is required which can convert the protocol. In a similar way, software components may already contain the management agent or a particular management agent is required which is designed for the administration of this software component.

In order to address the individual components of the system to be managed, the manager exchanges information with the agents. The type of protocol used for the communication has a considerable impact on the capabilities and, in particular, the security of the management system.

Management systems can basically be divided into three categories according to the communication protocol used (see also S 2.144 *Selection of a suitable network management protocol*):

1. SNMP (Simple Network Management Protocol), the widespread standard protocol of the TCP/IP-based system management, is used.
2. CMIP (Common Management Information Protocol), the less-common standard protocol of the ISO/OSI-based system management, is used.
3. A manufacturer-specific protocol is used. It is normally possible to use what are known as adapters to integrate the standard protocols, whereby there is usually only a SNMP connection.

The SNMP protocol is used most often. SNMP is an extremely simple protocol which only recognises five types of messages and is therefore easy to implement. CMIP is mainly used to manage telecommunications networks and is irrelevant in management based on the Internet or Intranet, as it uses the OSI protocol stack rather than the TCP/IP stack.

Although *system management systems* usually have a centralist structure to allow the system to be managed from a management station, the exact architecture depends on the possible size of the systems which can be managed and on the range of functions offered. These systems range from simple collections of management tools which can be used next to each other in small networks without being integrated to management platforms which can manage a world-wide company network containing thousands of computers.

Certain management platforms use proprietary protocols for communication between the components. These systems usually have a higher performance range and are not only used for network and system management but also offer resource management for entire organisations. Through the insufficiently-specified security mechanisms in the few existing standards, the manufacturers' own solutions provide security-relevant mechanisms such as cryptographic techniques.

Threat Scenario

The following typical threats are assumed for the IT baseline protection of a management system:

Force majeure
- T 1.1 Loss of personnel
- T 1.2 Failure of the IT system

Organisational shortcomings:
- T 2.59 Opertion of non-registered components
- T 2.60 Strategy for the network system and management system is not laid down or insufficient
- T 2.61 Unauthorised collection of personal data

Human Failure:
- T 3.34 Unsuitable configuration of the management system
- T 3.35 Disabling the server while in operation
- T 3.36 Misinterpretation of events

Technical Failure:
- T 4.38 Failure of components of a network management system or system management system

Deliberate Acts:
- T 5.86 Manipulation of management parameters

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

The system to be managed consists of individual computers, gateways and the physical network. Each of these components presents a potential security risk for the whole system. These risks cannot be eliminated entirely through the implementation of management software. This is due to the fact that it is not usually possible to include all systems in a management system to the same extent. The basic requirements for the security of the system are the definition and implementation of a security policy for the whole enterprise. In the case at question, this policy must be expressed particularly in the configuration of hardware and software. For this reason, particular attention should be paid to the safeguards of the modules listed in chapter 6. Module 6.7 can be used as a starting point.

As management systems are designed with a centralist structure, the management station is of particular importance for security considerations, and a particular effort must therefore be made to protect it. Thus, important components of a management system should be set up in rooms which correspond to the requirements for a server room (see chapter 4.3.2). If no server room is available, they can alternatively be set up in a server cabinet (see chapter 4.4 Protective Cabinets).

In order to successfully set up a network and system management system, a series of measures should be taken, starting with the design, then going on to the purchase and operation. The steps and measures involved are described below:

1. Creation of a management concept based on the requirements which result from the existing IT system.

   1.1 Requirement analysis (see S 2.168 *IT system analysis before the introduction of a system management system*)

1.2 Definition of the concept (see S 2.169 *Developing a system management strategy*)

2. Before purchasing the management system, it is first necessary

   2.1 to formulate the requirements for the management product resulting from the management concept (see S 2.170 *Requirements to be met by a system management system*) and, based on this,

   2.2 to select a suitable management product (see S 2.171 *Selection of a suitable system management product*)

3. The security-relevant safeguards for the operation of the management system are divided into the areas:

   3.1 Installation with the implementation of the management concept (see S 4.9 *Secure installation of a system management system*) and

   3.2 the current operation of the management system (see S 4.92 *Secure operation of a system management system*). Of course, the previous safeguards for

   3.3 the current operation of the managed system should also be observed (see chapters 4 to 9).

The following section presents the range of safeguards for the module *Network and system management*.

Infrastructure:
- S 1.29 (1) Adequate siting of an IT system

Organisation:
- S 2.2 (2) Resource management
- S 2.25 (1) Documentation on the system configuration
- S 2.40 (2) Timely involvement of the staff/factory council
- S 2.143 (1) Development of a network management concept
- S 2.144 (1) Selection of a suitable network management protocol
- S 2.168 (1) IT system analysis before the introduction of a system management system
- S 2.169 (1) Developing a system management strategy
- S 2.170 (1) Requirements to be met by a system management system
- S 2.171 (1) Selection of a suitable system management product

Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.10 (1) Selection of a trustworthy administrator and his substitute
- S 3.11 (1) Training of maintenance and administration staff

Hardware & Software:
- S 4.91 (1) Secure installation of a system management system
- S 4.92 (1) Secure operation of a system management system

Communications:
- S 5.68 (2) Use of encryption for network communications

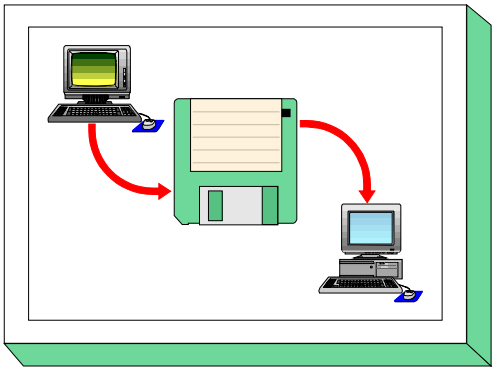
Contingency Planning:
- S 6.57 (2) Creation of an emergency plan for the failure of the management system

❒

7 Data Transmission Systems

This chapter describes IT baseline protection for data transmission systems:

7.1 Exchange of Data Media



Description

The exchange of data media for data transfer between non-networked IT systems is considered here. The data media dealt with include floppy disks, removable hard disks (magnetic, magneto-optical), CDs, magnetic tape and cassettes. Furthermore, the storage of data on the transmission and reception system is taken into account. Handling of the data media before and after dispatch is also described.

Threat Scenario

The following typical threats are assumed for the exchange of data media as part of IT baseline protection:

Force Majeure
- T 1.7 Inadmissible temperature and humidity
- T 1.8 Dust, soiling
- T 1.9 Loss of data due to intensive magnetic fields

Organisational shortcomings:
- T 2.3 A lack of compatible, or unsuitable, resources
- T 2.10 Data media are not available when required
- T 2.17 Inadequate labelling of data media
- T 2.18 Improper delivery of data media
- T 2.19 Inadequate key management for encryption

Human Failure:
- T 3.1 Loss of data confidentiality/integrity as a result of IT user error
- T 3.3 Non-compliance with IT security measures
- T 3.12 Loss of data media during transfer
- T 3.13 Transfer of incorrect or undesired data records

Technical Failure:
- T 4.7 Defective data media

Deliberate Acts:
- T 5.1 Manipulation/destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.4 Theft
- T 5.9 Unauthorised use of IT systems
- T 5.23 Computer viruses
- T 5.29 Unauthorised copying of data media
- T 5.43 Macro viruses

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

The safeguards package for the "Exchange of Data media" is presented in the following.

Infrastructure:
- S 1.36 (2) Safekeeping of data media before and after dispatch (*optional*)

Organisation:
- S 2.3 (2) Data media control
- S 2.42 (2) Determination of potential communications partners
- S 2.43 (1) Adequate labelling of data media for dispatch
- S 2.44 (1) Secure packaging of data media
- S 2.45 (1) Controlling the exchange of data media
- S 2.46 (2) Appropriate key management (optional)

Personnel:
- S 3.14 (2) Briefing personnel on correct procedures of exchanging data media (*optional*)

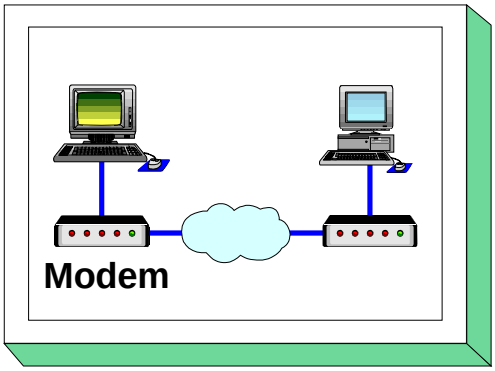
Hardware & Software:
- S 4.32 (2) Physical deletion of data media before and after usage
- S 4.33 (1) Use of a virus scanning program when exchanging of data media and data transmission
  (for IT systems generally prone to computer viruses)
- S 4.34 (1) Using encryption, checksums or digital signatures (*optional*)
- S 4.35 (3) Pre-dispatch verification of the data to be transferred (*optional*)
- S 4.44 (2) Checking of incoming data for macro viruses

Communications:
- S 5.22 (2) Compatibility check of transmission and reception systems (optional)
- S 5.23 (2) Selecting suitable types of dispatch for data media

Contingency Planning:
- S 6.38 (2) Backup copies of transferred data (optional)

❒

7.2 Modem



Description

A modem is used to link a data terminal, e.g. a PC with other data terminals via the public telephone network to allow the exchange of information. A modem converts digital signals from the data terminal into analogue electric signals which can be transmitted by the telephone network. For two IT systems to be able to communicate, they must be equipped with the required communication software.

A distinction is made between external, internal and PCMCIA modems. An external modem is an independent unit with a separate power supply, usually connected to the IT system via a serial interface. An internal modem consists of a plug-in modem board without a separate power supply. A PCMCIA modem is a credit-card sized plug-in board normally connected to laptops via a PCMCIA interface.

This chapter does not deal with data transmission via ISDN (c.f. Chapter 8, PBX System)

Threat Scenario

The following typical threats are assumed for modem operation as part of IT baseline protection:

Force Majeure
- T 1.2 Failure of the IT system

Human Error:
- T 3.2 Negligent destruction of equipment or data
- T 3.3 Non-compliance with IT security measures
- T 3.5 Inadvertent damaging of cables

Technical Failure:
- T 4.6 Voltage variations / overvoltage / undervoltage

Deliberate Acts:
- T 5.2 Manipulation of data or software
- T 5.7 Line tapping
- T 5.8 Manipulation of lines
- T 5.9 Unauthorised use of IT systems
- T 5.10 Abuse of remote maintenance ports
- T 5.12 Interception of telephone calls and data transmissions
- T 5.18 Systematic trying-out of passwords
- T 5.23 Computer viruses
- T 5.25 Masquerading
- T 5.39 Infiltrating computer systems via communication cards
- T 5.43 Macro viruses

Recommended Countermeasures (S)

To implement IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended.

The safeguards package for "Modem" is presented in the following.

Infrastructure:
- S 1.25 (3) Overvoltage protection (*optional*)
- S 1.38 (1) Suitable siting of a modem

Organisation:
- S 2.25 (2) Documentation of the System Configuration
- S 2.42 (2) Determination of potential communications partners
- S 2.46 (2) Appropriate key management (optional)
- S 2.59 (1) Procurement of a suitable modem
- S 2.60 (1) Secure administration of a modem
- S 2.61 (2) Requirements document for modem usage
- S 2.204 (1) Prevention of insecure network access

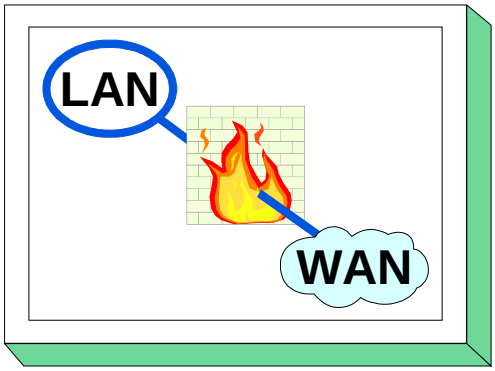
Personnel:
- S 3.17 (1) Briefing personnel on modem usage

Hardware and software:
- S 4.7 (1) Change of preset passwords
- S 4.30 (2) Utilisation of the security functions offered in application programs
- S 4.33 (1) Use of a virus scanning program when exchanging of data media and data transmission
  (for IT systems generally prone to computer viruses)
- S 4.34 (2) Using encryption, checksums or digital signatures (*optional*)
- S 4.44 (2) Checking of incoming files for macro viruses

Communications:
- S 5.30 (1) Activating an existing call-back option
- S 5.31 (1) Suitable modem configuration
- S 5.32 (1) Secure use of communications software
- S 5.33 (1) Secure remote maintenance via modem
- S 5.44 (2) One-way connection setup (optional)

❒

7.3 Firewall



Description

Firewalls are used to control communication between two networks. Usually a firewall protects a network against attacks originating from networks requiring a lower degree of protection, e.g. when a sub-network requiring protection is connected to an institution-wide network or when a company network is connected to the Internet.

In this chapter, a **firewall** is a combination of hardware and software which acts as the **sole** junction between two separate TCP/IP networks, one of which requires a higher degree of protection. As a firewall of this kind is often used to protect the internal network from attacks through the Internet, it is also called an Internet firewall.

In this chapter, only the threats and safeguards specific to a firewall are described. Furthermore, the threats and safeguards specific to the IT system with which the fire wall is implemented are also to be considered. It is assumed that a firewall is implemented on a UNIX system, i.e. the threats and safeguards described in Chapter 6.2 should be observed in addition to those contained below.

Threat Scenario

The following typical threats are assumed for a firewall as part of IT baseline protection:

Organisational shortcomings:
- T 2.24 Loss of confidentiality of sensitive data of the network to be protected

Human Failure:
- T 3.3 Non-compliance with IT security measures
- T 3.9 Improper IT system administration
- T 3.38 Errors in configuration and operation

Technical Failure:
- T 4.8 Discovery of software vulnerabilities
- T 4.10 Complexity of access possibilities to networked IT systems
- T 4.11 Lack of authentication possibilities between NIS Server and NIS Client
- T 4.12 Lack of authentication possibilities between X Server and X Client
- T 4.20 Data loss due to exhausting storage medium
- T 4.22 Vulnerabilities or errors in standard software
- T 4.39 Software conception errors

Deliberate Acts:
- T 5.2 Manipulation of data or software
- T 5.9 Unauthorised use of IT systems
- T 5.18 Systematic trying-out of passwords
- T 5.24 Replay of messages
- T 5.25 Masquerade
- T 5.28 Denial of services
- T 5.39 Infiltrating computer systems via communication cards
- T 5.48 IP spoofing
- T 5.49 Abuse of Source Routing
- T 5.50 Abuse of the ICMP Protocol
- T 5.51 Abuse of Routing Protocols
- T 5.78 DNS spoofing

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

A firewall protects the internal network against attacks from outside. In order to protect the internal network against attacks from inside, all necessary safeguards should also be taken even when a firewall is in place. If the internal network is a UNIX or a PC network, for example, the safeguards described in Chapter 6.1 and 6.2 should also be implemented.

The firewall should be sited in a separate server room. The appropriate measures are described in Chapter 4.3.2. If no server room is available, the firewall can alternatively be set up in a server cabinet (see chapter 4.4 Protective Cabinets).

In order to successfully set up a firewall, a series of measures should be taken, including the conception, purchase and operation of a firewall. The steps and measures involved are described below:

1. Concept of the network coupling using a firewall: (c.f. S 2.70 *Developing a Firewall Concept)*
   -
   - Determining the security objectives
   - Adapting the network structure
   - Basic requirements
2. Security policy of the firewall: (c.f. S 2.71 *Determining a Security Policy for a Firewall*)
   - Selecting the communications requirements
   - Selection of Services

     (Prior to the selection of services, the chapter S 5.39 *Safe use of protocols and services* should be consulted)
   - Organisational regulations
3. Procuring the firewall:
   - Selecting the type of firewall

     (c.f. S 2.72 *Demands on a Firewall* and S 2.73 *Selecting a Suitable Firewall*)
   - Procurement criteria

     (c.f. S 2.74 *Selection of a Suitable Packet Filter* and S 2.75 *Selection of a Suitable Application Gateway).*
4. Implementation of the firewall:
   - Establishing and implementation of filter rules (c.f. S 2.76 *Selection* and Implementation of Suitable Filter Rules)
   - Implementation of the IT baseline protection safeguards for firewall computers (see Chapter 6.2)
   - Check implementation of the IT baseline protection safeguards for the IT systems of the internal network (c.f. Chapter 6.1 6.2 and 6.3, for example)
   - Observe the conditions for the correct use of the various protocols and services (c.f. S 5.39 *Safe use of protocols and services*)
   - Inclusion of other components (see S 2.77 *Correct Configuration of Other Components*)
5. Operating the firewall: (see S 2.78 *Correct Operation of a Firewall*)
   - Regular checks
   - Adaptation to changes and tests
   - Logging of firewall activities (c.f. S 4.47 *Logging of firewall activities)*
   - Contingency planning for the firewall (see also Chapter 3.3)

- Data backup (see also Chapter 3.4 Data Privacy Protection)

6. Operation of clients connected to the firewall

   Alongside the safeguards described in chapter 5 additional safeguards outlined in S 5.45 *Security of WWW-browsers* should be observed

There can be various reasons for deciding against the installation of a firewall. For example, not only the purchase costs or the high administration expenditure, but also the fact that the existing remaining risks cannot be accepted. If an Internet connection is nonetheless desired, a stand-alone system can alternatively be installed (see S 5.46 *Installing stand-alone systems for Internet usage*).

The safeguards package for "Firewall" is presented in the following.

Organisation:

- S 2.70 (1) Developing a firewall concept
- S 2.71 (1) Establishing a security policy for a firewall
- S 2.72 (1) Requirements on a firewall
- S 2.73 (1) Selecting a suitable firewall
- S 2.74 (1) Selection of a suitable packet filter (in case of procurement)
- S 2.75 (1) Selection of a suitable application gateway (in case of procurement)
- S 2.76 (1) Selection and implementation of suitable filter rules
- S 2.77 (1) Secure configuration of other components
- S 2.78 (1) Secure operation of a Firewall

Hardware & Software:

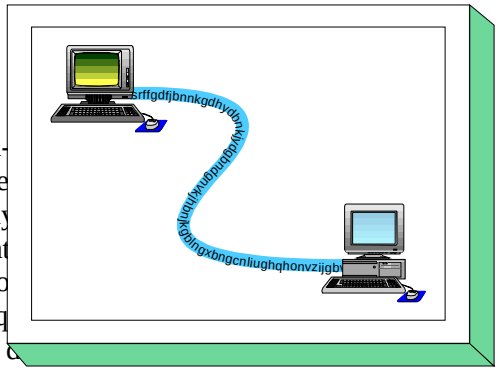
- S 4.47 (1) Logging of firewall activities
- S 4.93 (1) Regular integrity checking
- S 4.100 (1) Firewalls and active content
- S 4.101 (1) Firewalls and encryption

Communications:

- S 5.39 (1) Secure use of protocols and services
- S 5.59 (1) Protection against DNS spoofing
- S 5.45 (2) Security of WWW browsers
- S 5.46 (1) Installing stand-alone-systems for Internet use
- S 5.70 (1) Network Address Translation (NAT)
- S 5.71 (1) Intrusion Detection and intrusion response systems

❒

7.4 E-Mail



Description

Electronic mail service (e-mail in short) allows the world-
electronic messages within very brief periods of time. An e
(from/to), subject (title or reference), text body and, occasionally
only allows information to be exchanged quickly, convenient
possible to forward business transactions to other parties fo
Depending on the context in which e-mail is used, different req
availability, integrity and mandatory nature of the transmitted
use.

Threat Scenario

The following typical threats are assumed as regards IT baseline protection of files exchanged via e-mail:

Organisational shortcomings:
- T 2.7 Unauthorised use of rights
- T 2.9 Poor adjustment to changes in the use of IT
- T 2.19 Inadequate encryption key management
- T 2.54 Loss of confidentiality through hidden pieces of data.
- T 2.55 Uncontrolled use of electronic mail
- T 2.56 Inadequate description of files

Human Failure:
- T 3.1 Loss of data confidentiality/integrity as a result of IT user error
- T 3.3 Non-compliance with IT security measures
- T 3.8 Improper use of the IT system
- T 3.13 Transfer of incorrect or undesired data records

Technical Failure:
- T 4.20 Data loss due to exhausting storage medium
- T 4.32 Failure to dispatch a message
- T 4.37 Lack of time authenticity in E-mail

Deliberate Acts:
- T 5.2 Manipulation of data or software
- T 5.7 Interception of lines
- T 5.9 Unauthorised use of IT systems
- T 5.21 Trojan Horses
- T 5.23 Computer viruses
- T 5.24 Replay of messages
- T 5.25 Masquerade
- T 5.26 Analysis of the message flow
- T 5.27 Repudiation of a message
- T 5.28 Denial of services
- T 5.43 Macro viruses
- T 5.72 Misuse of e-mail services
- T 5.73 Impersonation of a sender
- T 5.74 Manipulation of alias files and distribution lists
- T 5.75 Overload due to incoming e-mails
- T 5.76 Mail bombs
- T 5.77 Unauthorised monitoring of e-mails

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

As regards e-mail systems, the following essential aspects need to be investigated:

- E-mail software is used to transmit, receive and process e-mail.
- This e-mail software transmits and receives e-mail to/from a mail server. The mail server maintains a mailbox for every user. For the further exchange of information, the mail server communicates with gateways which forward the messages to other mail systems.

A comprehensive security policy (refer to S 2.118 *Determination of a security policy for the use of e-mail*) needs to be prepared for the implementation of security measures for the exchange of electronic mail. The operation of e-mail systems entails the implementation of security measures for the mail server as well as the clients in use. The security precautions and instructions to be observed by users are of particular importance.

The package of measures for the area of e-mail is listed in the following:

Organisation:
- S 2.30 (2) Provisions governing the designation of users and of user groups
- S 2.42 (2) Determination of potential communications partners
- S 2.46 (2) Appropriate key management (optional)
- S 2.118 (1) Determination of a security policy for the use of e-mail
- S 2.119 (1) Regulations concerning the use of e-mail services
- S 2.120 (1) Configuration of a mail centre
- S 2.121 (2) Regular deletion of e-mails
- S 2.122 (2) Standard e-mail addresses
- S 2.123 (2) Selection of a mail provider

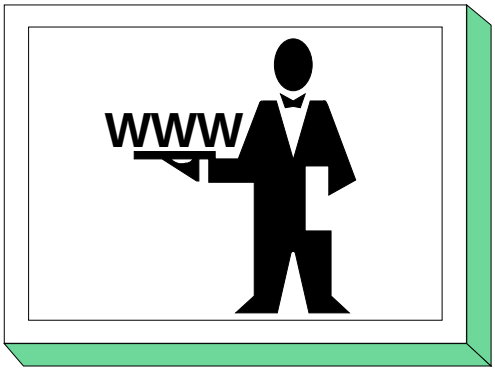
Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.10 (1) Selection of a trustworthy administrator and his substitute
- S 3.11 (1) Training of maintenance and administration staff

Hardware & Software:
- S 4.33 (1) Use of a virus scanning program when exchanging of data media and data transmission
- S 4.34 (2) Using encryption, checksums or digital signatures (*optional*)
- S 4.44 (2) Checking of incoming data for macro viruses
- S 4.64 (1) Verification of data before transmission / elimination of residual information
- S 4.65 (2) Testing of new hardware and software

Communications:
- S 5.22 (2) Compatibility check of transmission and reception systems (optional)
- S 5.32 (1) Secure use of communications software
- S 5.53 (2) Protection against mail bombs
- S 5.54 (2) Protection against mail overload and spam
- S 5.55 (2) Checking of alias files and distribution lists
- S 5.56 (1) Secure operation of a mail server
- S 5.57 (1) Secure configuration of mail clients
- S 5.63 (2) Use of PGP (optional)
- S 5.67 (3) Use of a time stamp service (optional)

Contingency Planning:
- S 6.23 (2) Procedure in case of computer virus infection
- S 6.38 (2) Backup copies of transferred data (optional)

7.5 WWW server



Description

A WWW server is an IT system using an information database and providing WWW clients with files. A WWW client, also called a browser, displays the information from a WWW server on the user's computer. The most well-known browsers are Mosaic, Netscape, Internet Explorer, Hot Java and Lynx. If the users inform the browser (e.g. with a mouse click) which document they would like to read, the program creates a network connection to the corresponding WWW server. The latter then sends the required document via the network to the client, which then displays it on the screen or prints it.

The WWW service is based on HTML (Hypertext Markup Language), a simple programming language which makes it possible to manage text with formatting (including determining headings, indenting, bold or italic sections of text), as well as images, even video and audio sequences. Individual documents are linked through what are known as hyperlinks. These can be a reference to another document on the same WWW server or another WWW server, to another section of the same text, to an image or something similar. Such links are normally marked in the text, usually through underlining or a different colour. Images and other embedded elements can also represent hyperlinks. The address of a WWW document (text, image, etc.) is the so called URL (Uniform Resource Locator).

The security of WWW use is mainly based on

- the security of the WWW server,
- the security of the WWW client and
- the security of the communication link between the two.

In order to secure a WWW server, it must be ensured that

- the WWW server only passes on information to authorised users,
- all the information offered on the WWW server is intended to be passed on,
- the security of the WWW server cannot by undermined either by authorised or by unauthorised users.

Threat Scenario

For baseline protection, the following threats are seen as typical for a **WWW server**:

Organisational shortcomings:

- T 2.1 Lack of, or insufficient, rules
- T 2.2 Insufficient knowledge of requirements documents
- T 2.4 Insufficient monitoring of IT security measures
- T 2.7 Unauthorised use of rights (here: to change information stored on a www server)
- T 2.9 Poor adjustment to changes in the use of IT (here: of information stored on a www server)
- T 2.28 Violation of copyright (here: by unauthorized transfer or publication of documents, graphics or software)
- T 2.32 Inadequate line bandwidth (here: poor reachability)
- T 2.37 Uncontrolled usage of communications lines (ActiveX, Java)

Human Failure:

- T 3.1 Loss of data confidentiality/integrity as a result of IT user error
- T 3.37 Unproductive searches
- T 3.38 Errors in configuration and operation

Technical Failure:

- T 4.10 Complexity of access possibilities to networked IT systems
- T 4.22 Software vulnerabilities or errors
- T 4.39 Software conception errors

Deliberate Acts:

- T 5.2 Manipulation of data or software
- T 5.19 Abuse of user rights
- T 5.20 Misuse of administrator rights
- T 5.21 Trojan Horses
- T 5.23 Computer viruses
- T 5.28 Denial of services
- T 5.43 Macro viruses
- T 5.48 IP spoofing
- T 5.78 DNS spoofing
- T 5.87 Web spoofing
- T 5.88 Misuse of active contents

Recommended measures

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules"), as described in chapters 2.3 and 2.4, is recommended.

In this chapter, only the threats and safeguards specific to a WWW server are described. In addition, chapter 6.1 Server-supported Network must be implemented to ensure the security of the organisation's own network.

In order to ensure that the connection of the WWW server to public networks (such as the Internet) is secure, attention should be paid to chapter 7.3 Firewall. This is also the case for the connection of several Intranets to an extensive Intranet. The controlled connection of external connection points (e.g. of telecommuting workstations via ISDN) is dealt with in chapter 9.3 Telecommuting.

A WWW server should be installed in a separate server room. The appropriate safeguards are described in Chapter 4.3.2. If no server room is available, the WWW server can alternatively be set up in a server cabinet (see chapter 4.4 Protective Cabinets).

In order to set up a WWW server successfully and securely, a number of safeguards must be implemented. The steps and measures involved are described below:

1. Creating a concept for the WWW server (see S 2.172 *Developing a concept for using the WWW*) and determining a WWW security strategy (see S 2.173 *Determining a WWW security strategy*):
   - Determining the security objectives
   - Adapting the network structure
   - Basic requirements
   - Organisational regulations
2. Implementing the WWW server (see S 2.175 *Setting up a WWW server*):
   - Implementing the IT baseline protection safeguards for the WWW computer (for example, see chapter 6.2 for WWW servers based on Unix)
   - Using secure communication connections (see S 5.65 *Use of S-HTTP* and S 5.66 *Use of SSL*)
   - Java, ActiveX (see S 5.69 *Protection against active content*)
3. Operating the WWW server (see S 2.174 *Secure operation of a WWW server*):
   - Regular checks
   - Adaptation to changes and tests
   - Access protection for WWW files (S 4.94 *Protection of WWW files*)
   - Logging at the WWW server
   - Contingency planning for the WWW server (see also Chapter 3.3)
   - Data backup (see chapter 3.4 *Data backup policy*)
6. Secure operation of WWW clients

   Alongside the safeguards described in chapter 5 additional safeguards outlined in S 5.45 *Security of WWW-browsers* should be observed
   - Using secure communication connections (see S 5.65 *Use of S-HTTP* and S 5.66 *Use of SSL*)
   - Protection against viruses, macro viruses, active contents (see S 4.33 *Running a virus scan program before and after data transfer* and S 5.69 *Protection against active content*)

The following describes the safeguards for the area "WWW server". For reasons of redundancy, safeguards from other chapters will not be repeated here.

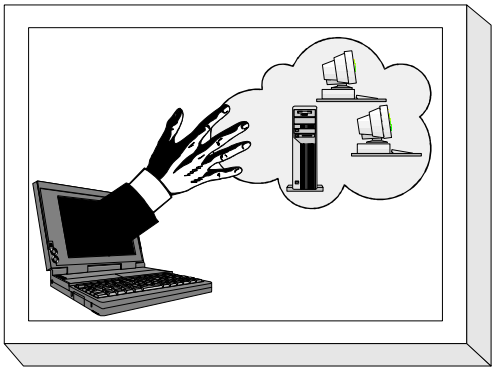
Organisation:
- S 2.35 (1) Obtaining information on security weaknesses of the system
- S 2.172 (1) Developing a concept for using the WWW
- S 2.173 (1) Determining a WWW security strategy
- S 2.174 (1) Secure operation of a WWW server
- S 2.175 (2) Setting up a WWW server
- S 2.176 (2) Selection of a suitable Internet service provider

Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.10 (1) Selection of a trustworthy administrator and his substitute
- S 3.11 (1) Training of maintenance and administration staff

Hardware & Software:
- S 4.33 (1) Use of a virus scanning program when exchanging of data media and data transmission
- S 4.34 (2) Using encryption, checksums or digital signatures (*optional*)
- S 4.44 (2) Checking of incoming data for macro viruses
- S 4.64 (1) Verification of data before transmission / elimination of residual information
- S 4.65 (2) Testing of new hardware and software
- S 4.78 (1) Careful modifications of configurations
- S 4.93 (1) Regular integrity checking
- S 4.94 (1) Protection of WWW files
- S 4.95 (1) Minimal operating system
- S 4.96 (2) Deactivating DNS
- S 4.97 (2) One service per server
- S 4.98 (1) Restricting communication to a minimum with packet filters
- S 4.99 (2) Protection against subsequent changes to information

Communications:
- S 5.45 (2) Security of WWW browsers
- S 5.59 (1) Protection against DNS spoofing
- S 5.64 (2) Secure Shell (optional)
- S 5.65 (2) Use of S-HTTP (optional)
- S 5.66 (2) Use of SSL (optional)
- S 5.69 (1) Protection against active content

7.6 Remote Access



Description

Remote access enables a user to log on from a local computer to a remote computer network and use its resources as if a direct LAN link existed. The services used here are known as Remote Access Service (RAS). RAS ensures that remote users can access the network resources.

In general, RAS is used in the following situations:

- to link individual stationary workstations (e.g. so that individual staff can work from home as telecommuters),
- to link mobile computers (e.g. to support staff working in the field or on business trips),
- to link entire LANs (e.g. to link up local networks of remote locations or branch offices),
- management access to remote computers (e.g. for remote maintenance).

RAS offers a simple solution in such scenarios: the remote user establishes a connection with the corporate network e.g. over the telephone network using a modem. This direct connection can exist for as long as is necessary and can be viewed as a leased line which is only active on demand.

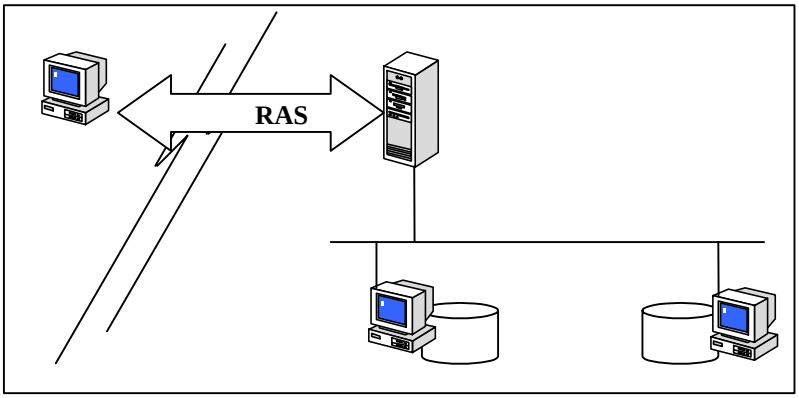


Figure: Remote Access to Resources

Establishment of a RAS connection generally requires three components as follows:

1. A computer within the corporate network on which RAS software has been installed and which is ready to accept RAS connections. This is known as the *RAS server* or *access server*.
2. A remote computer on which RAS software has been installed and which initiates the RAS connection. This is known as the *RAS client*.
3. The communication medium over which the RAS connection is established. In most scenarios the RAS client uses a telecommunications network to establish the connection. The very minimum that is required, therefore, is a telephone line and a modem to go with it. Depending on the RAS architecture, different connection technologies can be used server-side.

RAS is implemented as a client/server architecture: the RAS client can be configured so that it automatically establishes the RAS connection when corporate network resources are required by dialling the phone number of the computer on which the RAS server software is installed.

Alternatively, the RAS connection can be initiated manually by the user. Some operating systems, e.g. Windows NT, also allow the RAS to be activated immediately following system logon.

There are two basic ways of establishing a connection to the remote LAN (see Safeguard S 2.185 *Selection of a suitable RAS system architecture*):

1. Direct dial-up to the access server, which in this case is part of the remote LAN;
2. Dial-up to an access server of an Internet Service Provider (ISP) and access to the remote LAN over the Internet.

From the point of view of security, the following security objectives apply to RAS access:

1. *Access security.* The remote user must be uniquely identified by the RAS system. The identity of the user must be established through an authentication mechanism every time that a connection is established to the local network. In the context of system access, additional control mechanisms must be employed to ensure that system access by remote users is properly controlled (e.g. restricting access to certain times or to permitted remote connection points only).
2. *Access control*. Once the remote user has been authenticated, the system must be able to restrict the interactions of the user with the system. This requires that the authorisations and restrictions which have been specified for local network resources by authorised administrators are also enforced for remote users.
3. *Security of communications.* Where local resources are accessed remotely, user data have also to be transmitted over the established RAS connection. In general the security requirements which apply in the local network with regard to protection of communications (confidentiality, integrity, authenticity) must also be implementable for data which is transmitted over RAS connections. However, protection of RAS communications is especially critical since communications can be transmitted using a number of communications media which cannot generally be assumed to be under the control of the operator of local network.
4. *Availability.* Where remote access is used for mainstream business activities, the availability of RAS access is particularly important. The smooth flow of business processes may be impaired in the event of total failure of RAS access or if connections have insufficient bandwidth. This risk can be reduced to a certain extent through the use of alternative or redundant RAS connections. This applies especially where the Internet is used as the communications medium, as here there are generally no guarantees of either connection or bandwidth.

Threat Scenario

The client/server architecture of RAS systems means that both the RAS client and the RAS server are exposed to specific risks due to the type of operational environment and the manner of use.

- RAS clients do not have to be stationary (e.g. home PC), but can also be mobile (laptops). However, the client location will normally not be under the control of the LAN operator so that, especially where the client is mobile, it must be assumed that the environment is insecure and is exposed to specific threats. In particular, the threats which have to be considered here include physical threats, such as theft or damage. Sections 4.5 *Working place at home (telecommuting)*, 5.3 *Laptop PCs* and 9.3 *Telecommuting* should be considered here.
- RAS servers are generally part of the LAN to which remote users wish to log on. They are under the control of the LAN operator and can therefore be covered by the security provisions which apply locally. As the main task of the RAS server is to ensure that only authorised users can access the connected LAN, the threats to which the RAS server is exposed should be viewed as falling within the area of attacks where the objective is unauthorised access to the LAN.

At this point we advise against considering the dangers to the client and server completely separately since, for example, if a RAS client were to be compromised, the RAS server would automatically be endangered. Moreover it should be borne in mind that, for example in the Windows environment, every RAS client can also be operated as a RAS server, so that the threats which apply to RAS servers apply equally to a RAS client.

The following typical threats are assumed for the IT baseline protection of a RAS system:

Force Majeure

- T 1.1 Loss of personnel
- T 1.2 Failure of the IT system
- T 1.10 Failure of a wide area network

Organisational Shortcomings

- T 2.2 Insufficient knowledge of requirements documents
- T 2.16 Non-regulated change of users in the case of laptop PCs
- T 2.19 Inadequate key management for encryption
- T 2.37 Uncontrolled usage of communications lines
- T 2.44 Incompatible active and passive network components
- T 2.49 Lack of, or inadequate, training of teleworkers
- T 2.64 Lack of or defective rules for the RAS system

Human Error

- T 3.30 Unauthorised private use of telecommuting workstations
- T 3.39 Improper administration of the RAS system
- T 3.40 Inappropriate use of authentication services with remote access
- T 3.41 Improper use of remote access services
- T 3.42 Insecure configuration of RAS clients
- T 3.43 Inappropriate handling of passwords
- T 3.44 Carelessness in handling information

Technical Failure

- T 4.35 Insecure cryptographic algorithms
- T 4.40 Unsuitable fitting out of the RAS client operational environment

Deliberate Acts

- T 5.7 Line tapping
- T 5.8 Manipulation of lines
- T 5.22 Theft of a mobile IT system
- T 5.39 Infiltrating computer systems via communication cards
- T 5.71 Loss of confidentiality of classified information
- T 5.83 Compromising cryptographic keys
- T 5.91 Disabling of RAS access security mechanisms
- T 5.92 Use of the RAS client as RAS server
- T 5.93 Permitting use of RAS components by third parties

Recommended Countermeasures (S)

To implement IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended.

A RAS system consists of several components which from the outset should be protected as individual components. Quite apart from the RAS functionality, these should be viewed as normal IT systems or network switching elements which need to be protected according to the suggestions made in the relevant safeguard modules. RAS servers are computers which are normally fully under the control of an organisation and perform the important task of controlling access to the internal network. The RAS functionality is generally superimposed on an operating system which in most cases offers additional services as well. Hence the security of RAS access also depends on there being no security weaknesses either at operating system or service level.

As well as protecting the RAS system components, however, it is also necessary to draw up a RAS security policy which must be integrated into the existing security policy. At the same time as implementing existing security requirements, the RAS system requires that new, RAS-specific security rules are defined.

A RAS system will generally be used in the environment of other systems which serve to control access to the internal network from outside. Examples of other systems with which a RAS system has to work are firewall systems and remote maintenance systems. For this reason, when implementing the RAS-specific safeguards, the safeguards from the relevant modules of the affected systems must also be considered. The modules which should be considered include:

- 4.5 Working place at home (telecommuting)
- 7.3 Firewalls
- 8.1 Private branch exchanges
- 9.3 Telecommuting

Secure RAS access depends on a series of safeguards being taken, starting at the design stage, and then moving on to procurement and operation. The steps involved here and the safeguards which should be considered at each of the steps are listed below.

1. A RAS concept must be prepared up front, based on the security requirements for the existing IT systems and the requirements arising from the planned situations under which RAS will be used.

1.1 To tailor the concept to the particular application, the requirements must be determined at the start. For this purpose a requirements analysis must be performed (see S 2.183 *Performing a RAS requirements analysis*).

1.2 On the basis of the requirements thus determined, a RAS concept can then be defined (see S 2.184 *Development of a RAS concept*).

1.3 To implement the concept, a RAS system architecture must be defined (see S 2.185 *Selection of a suitable RAS system architecture*), which is tailored to the organisation's RAS requirements and the RAS concept to be implemented.

2. Before the RAS system can be procured, the requirements relating to the RAS product must be derived from the RAS concept and the choice of a suitable RAS product must be based on these (see S 2.186 *Selection of a suitable RAS product*).

3. The security-relevant safeguards for the implementation of the RAS concept may be broken down into the following areas:

3.1 definition of security guidelines for use of RAS (see S 2.187 *Definition of a set of RAS security guidelines*),

3.2 installation and initial configuration (see S 4.110 *Secure installation of the RAS system* and S 4.111 *Secure configuration of the RAS system*), and

3.3 the ongoing operation of the RAS system (see S 4.112 *Secure operation of the RAS system*).

Typically, RAS servers and RAS clients must always be considered with RAS systems. As the users of a RAS system essentially contribute to its secure operation, they must be prepared for the use of RAS access and be instructed in the use of the RAS software. Here in particular their attention must be drawn to the dangers which exist when RAS access is used from home or on the road (see S 3.4 *Training before actual use of a program* and S 3.5 *Education on IT security measures*).

Tunnel protocols are often used as a means of protecting RAS connections. These allow the establishment, building on an existing connection, of a communication channel between IT systems or networks which is sealed off through access control and encryption. Because this channel is sealed off from the outside world the term Virtual Private Network (VPN) is frequently employed (see S 5.76 *Use of suitable tunnel protocols for RAS communication*).

The safeguards package for the "Remote Access" module is presented below.

Infrastructure
- S 1.29 () Adequate siting of an IT system (server)

Organisation
- S 2.2 () Resource management
- S 2.25 () Documentation on the system configuration
- S 2.40 () Timely involvement of the staff/factory council
- S 2.183 () Performing a RAS requirements analysis
- S 2.184 () Development of a RAS concept
- S 2.185 () Selection of a suitable RAS system architecture
- S 2.186 () Selection of a suitable RAS product
- S 2.187 () Definition of a set of RAS security guidelines

Personnel
- S 3.4 () Training before actual use of a program
- S 3.5 () Education on IT security measures
- S 3.10 () Selection of a trustworthy administrator and his substitute
- S 3.11 () Training of maintenance and administration staff

Hardware and software
- S 4.110 () Secure installation of the RAS system
- S 4.111 () Secure configuration of the RAS system
- S 4.112 () Secure operation of the RAS system
- S 4.113 () Use of an authentication server within RAS access

Communication
- S 5.68 () Use of encryption procedures for network communications
- S 5.76 () Use of suitable tunnel protocols for RAS communication

Contingency Planning
- S 6.70 () Creation of a contingency plan for failure of the RAS system
- S 6.71 () Data backup for a mobile IT system

8 Telecommunications

This chapter defines IT baseline protection for the following types of telecommuncation:

8.1 Telecommunications System (Private Branch Exchange, PBX)

8.2 Fax Machine

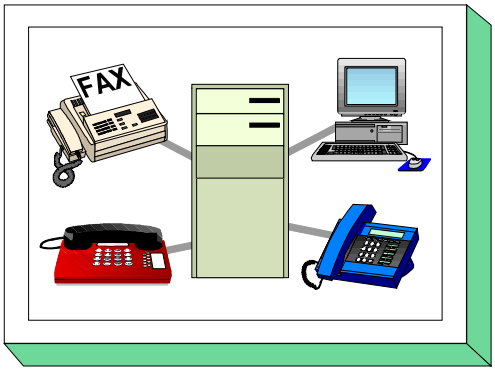
8.3 Answering Machine

8.4 LAN connection of an IT system via ISDN

8.5 Fax Servers

8.6 Mobile Telephones

8.1 Telecommunications System (Private Branch Exchange, PBX)



Description

A private digital ISDN telecommunications facility (switching device for connections between incoming and outgoing lines for the purpose of exclusive data exchange, in the following referred to as *private branch exchange* - PBX) is both a communications basis for its proper domain and an interface with the public network. It is used to transmit speech and images (fax) and increasingly serves as a transmission medium for LAN coupling and electronic mail systems. If it is used as a LAN, the provisions of Chapter 6.1, *Server supported Network*, must be observed.

For the purposes of this Chapter, it is assumed that a person responsible for the PBX has been designated who is able to take the fundamental security decisions and initiate security safeguards.

Threat Scenario

The following typical threats (T) are assumed as regards IT baseline protection of a private branch exchange:

Force Majeure
- T 1.4 Fire
- T 1.7 Inadmissible temperature and humidity

Organisational shortcomings:
- T 2.6 Unauthorised admission to rooms requiring protection

Human Failure:
- T 3.6 Hazards posed by cleaning staff or outside staff
- T 3.7 Failure of the PBX due to operating errors

Technical Failure:
- T 4.6 Voltage variations / overvoltage / undervoltage

Deliberate Acts:
- T 5.1 Manipulation/destruction of IT equipment or accessories
- T 5.11 Loss of confidentiality of data stored in PBX installations
- T 5.12 Interception of telephone calls and data transmissions
- T 5.13 Eavesdropping of rooms
- T 5.14 Call charges fraud
- T 5.15 "Inquisitive" staff members
- T 5.16 Threat posed by internal staff during maintenance/administration work
- T 5.17 Threat posed by external staff during maintenance work
- T 5.44 Abuse of Remote Access Ports for Management Functions of Private Branch Exchanges

Here, consideration is given to those threats which may impair the functioning of an institution. Thus, the focus is not on legal data privacy aspects. These are already covered, for a major part, by existing operating agreements and/or service agreements. Nevertheless, IT baseline protection does, of course, also contribute to the protection of person-related data.

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

The central devices of a PBX facility should be installed in a room which meets the requirements laid down for a server room (Chapter 4.3.2), or for a technical infrastructure room (Chapter 4.3.4). For provision of a PBX with cables, see Chapter 4.2.

In the following, the safeguard group "Private Branch Exchange" is set out:

Infrastructure:

- S 1.2 (2) Regulations governing access to distributors
- S 1.9 (2) Fire sealing of trays
- S 1.12 (2) Avoidance of references to the location of building parts requiring protection
- S 1.13 (3) Layout of building parts requiring protection
- S 1.22 (2) Physical protection of lines and distributors (*optional*)
- S 1.23 (1) Locked doors
- S 1.25 (2) Overvoltage protection (*optional*)
- S 1.27 (2) Air conditioning (*optional*)
- S 1.28 (1) Local uninterruptible power supply [UPS] (*optional*)
- S 1.30 (2) Safeguarding of data media containing data on telecommunications charges

Organisation:

- S 2.4 (2) Maintenance/repair regulations
- S 2.16 (2) Supervising or escorting outside staff/visitors
- S 2.17 (2) Entry regulations and controls
- S 2.26 (1) Designation of an administrator and his deputy
- S 2.27 (1) Dispensing with remote maintenance of the PBX (*optional*)
- S 2.28 (3) Availability of external telecommunications advisory services (*optional*)
- S 2.29 (2) PBX operating instructions for users
- S 2.40 (2) Timely involvement of the staff/factory council
- S 2.105 (1) Obtaining PBX-annexes

Personnel:

- S 3.10 (1) Selection of a trustworthy administrator and his substitute
- S 3.11 (1) Training of maintenance and administration staff
- S 3.12 (2) Informing all staff members about possible PBX warning notices, warning symbols and acoustic alarm signals
- S 3.13 (2) Increasing staff awareness of potential threats to the PBX

Hardware & Software:

- S 4.5 (2) Logging of PBX administration jobs
- S 4.6 (2) Audit of the PBX configuration (target/performance reconciliation)
- S 4.7 (1) Change of preset passwords
- S 4.8 (1) Protection of the PBX operator's console
- S 4.10 (2) Password protection for PBX terminals
- S 4.11 (2) Screening of PBX interfaces
- S 4.12 (1) Disabling of unneeded user facilities

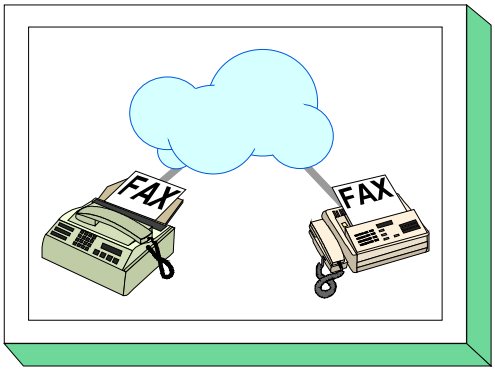
- S 4.62 (2) Use of a D-channel filter (*optional*)

Communications:
- S 5.14 (1) Shielding of internal remote accesses
- S 5.15 (1) Shielding of external remote accesses

Contingency Planning:
- S 6.10 (2) Contingency plans for breakdown of data transmission
- S 6.26 (2) Regular backup of PBX configuration data
- S 6.28 (3) Agreement on the delivery deadlines for "vital" PBX units (*optional*)
- S 6.29 (2) PBX base line for emergency calls (*optional*)
- S 6.30 (3) Emergency circuit (*optional*)

❒

8.2 Fax machine



Description

This chapter deals with information transfer via facsimile (fax). The transmission standard (e.g. CCITT group 3) was not used for differentiation purposes for the selection of safeguards as part of IT baseline protection. In this module the technical basis to be considered are common stand-alone fax machines, but not fax cards or fax servers (see chapter 8.5 Fax server).

Threat Scenario

The following typical threats are assumed for fax information transfer as part of IT baseline protection:

Organisational Shortcomings
- T 2.20 Inadequate supply of printing consumables for fax machines

Human Failure
- T 3.14 Misjudgement of the legal force of a fax

Technical Failure
- T 4.14 Fading of special fax paper
- G 4.15 Fax transmission errors

Deliberate Acts
- T 5.7 Line tapping
- T 5.30 Unauthorised use of a fax machine or fax server
- T 5.31 Unauthorised reading of fax transmissions
- T 5.32 Evaluation of residual information in fax machines and fax servers
- T 5.33 Impersonation of wrong sender on fax transmissions
- T 5.34 Deliberate re-programming of the destination keys on fax machines
- T 5.35 Deliberate overload through fax transmissions

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended. In the following, the countermeasure package for "fax machines" is set out:

Infrastructure

- (1) Adequate siting of a fax machine

Organisation

- S 2.47 (2) Designating a person in charge of the fax system
- S 2.48 (2) Designating authorised fax operators (optional)
- S 2.49 (2) Procurement of suitable fax machines (if required)
- S 2.50 (2) Appropriate disposal of consumable fax accessories and spare parts
- S 2.51 (3) Producing copies of incoming fax messages (*optional*)
- S 2.52 (3) Supply and monitoring of consumable fax accessories
- S 2.53 (3) Deactivation of fax machines after office hours (*optional*)

Personnel

- S 3.15 (1) Information for all staff about the use of faxes

Hardware & Software

- S 4.36 (2) Blocking fax recipient numbers (optional)
- S 4.37 (3) Blocking fax sender numbers (optional)
- S 4.43 (2) Fax machine with automatic envelope sealing system (*optional*)

Communication

- S 5.24 (1) Use of a suitable fax cover sheet
- S 5.25 (2) Using transmission and reception logs
- S 5.26 (2) Announcing fax messages via telephone (optional)
- S 5.27 (2) Acknowledging successful fax reception by telephone (optional)
- S 5.28 (2) Acknowledging correct fax origin by telephone (optional)
- S 5.29 (2) Periodic checks of destination addresses and logs

Contingency Planning

- S 6.39 (3) Listing dealerships for re-procurement of fax products (*optional*)

❒

8.3 Answering Machine

Description

This chapter deals with answering machines which, in addition
local telephone network in the building. They normally serve to
the form of speech in case the called party is not personally ava
recording techniques: fully analogue, fully digital and a combi
the currently widespread remote inquiry feature makes it re
machines as IT systems and carries considerable threat potential

Threat Scenario

The following typical threats are assumed for answering machines as part of IT baseline protection:

Force Majeure
- T 1.8 Dust, soiling

Organisation deficiencies
- T 2.1 Lack of, or insufficient, rules
- T 2.5 Lack of, or inadequate, maintenance
- T 2.6 Unauthorised admission to rooms requiring protection

Human Failure:
- T 3.15 Improper use of answering machines

Technical Failure:
- T 4.1 Disruption of power supply
- T 4.18 Discharged or fatigued emergency power supply in answering machines
- T 4.19 Information loss due to exhausted storage medium

Deliberate Acts:
- T 5.36 Deliberate overloading of answering machines
- T 5.37 Determining access codes
- T 5.38 Misuse of remote inquiry

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

The safeguards package for an "Answering Machine" is presented in the following.

Infrastructure:
- S 1.23 (3) Locked doors (*optional*)
- S 1.29 (3) Adequate siting of an IT system (*optional*)

Organisation:
- S 2.4 (3) Maintenance/repair regulations (*optional*)
- S 2.11 (2) Provisions governing the use of passwords (security codes in this case)
- S 2.54 (1) Procurement/selection of suitable answering machines
- S 2.55 (1) Use of a security code (*optional*)
- S 2.56 (1) Avoidance of confidential information on answering machines
- S 2.57 (2) Regular playback and deletion of recorded messages
- S 2.58 (3) Limitation of message time (*optional*)

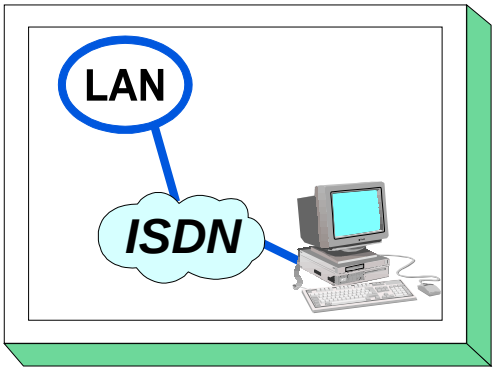
Personnel:
- S 3.16 (2) Briefing personnel on the operation of answering machines

Hardware & Software:
- S 4.38 (1) Deactivation of unnecessary service features
- S 4.39 (3) Deactivation of answering machines for periods of absence (*optional*)

Contingency Planning:
- S 6.40 (3) Regular battery checks/replacements (*optional*)

❒

8.4 LAN connection of an IT system via ISDN



Description

ISDN (Integrated Services Digital Network) is a digital telecommunications network which allows the operation of a variety of services such as telephony and facsimile, as well as the transmission of data and images.

This chapter deals with the integration of a remote IT system into a local network via a public ISDN network. The remote IT system is linked by means of an ISDN adapter card possessing an S_0 interface to the LAN via a router which is connected to a public ISDN network via an S_{2M} interface.

This type of integration of remote IT systems constitutes a typical possibility for telecommuting workstations as well.

Threat Scenario

The following typical threats are generally assumed as regards baseline protection of an IT system integrated into a LAN via ISDN:

Force Majeure
- T 1.2 Failure of the IT system
- T 1.10 Failure of a wide area network

Organisational Shortcomings:
- T 2.1 Lack of, or insufficient, rules
- T 2.6 Unauthorised admission to rooms requiring protection
- T 2.7 Unauthorised use of rights
- T 2.9 Poor adjustment to changes in the use of IT
- T 2.19 Inadequate key management for encryption
- T 2.22 Lack of evaluation of auditing data
- T 2.24 Loss of confidentiality of sensitive data of the network to be protected
- T 2.32 Inadequate line bandwidth
- T 2.37 Uncontrolled usage of communications lines

Human Error:
- T 3.1 Loss of data confidentiality/integrity as a result of IT user error
- T 3.6 Hazards posed by cleaning staff or outside staff
- T 3.8 Improper use of the IT system
- T 3.9 Improper IT system administration
- T 3.13 Transfer of incorrect or undesired data records
- T 3.16 Incorrect administration of site and data access rights

Technical Failure:
- T 4.8 Discovery of software vulnerabilities
- T 4.25 Still active connections

Deliberate Acts:
- T 5.2 Manipulation of data or software
- T 5.7 Line tapping
- T 5.8 Manipulation of lines
- T 5.9 Unauthorised use of IT systems
- T 5.10 Abuse of remote maintenance ports
- T 5.14 Call charges fraud
- T 5.16 Threat posed by internal staff during maintenance/administration work
- T 5.17 Threat posed by external staff during maintenance work
- T 5.18 Systematic trying-out of passwords
- T 5.25 Masquerading
- T 5.26 Analysis of the message flow

- T 5.39 Infiltrating computer systems via communication cards
- T 5.48 IP Spoofing
- T 5.61 Misuse of remote access to management functions on routers
- T 5.62 Misuse of resources via remote IT systems
- T 5.63 Manipulation via the ISDN D-channel

Recommended Countermeasures (S)

To implement IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended.

The safeguard package for integration of an IT system into a LAN via ISDN is described in the following. The primary objective in this context is to ensure reliable communications. Further safeguards required for the communicating IT systems are specified in the related chapters (refer to Chapter 6 for routers, and Chapter 5 for remote IT systems).

The following measures are additionally recommended:

Infrastructure:
- S 1.43 (2) Secure siting of ISDN routers

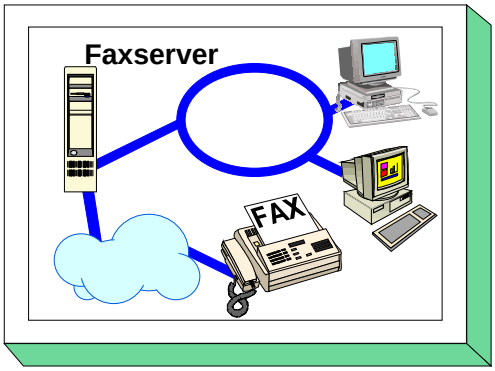
Organisation:
- S 2.4 (2) Maintenance/Repair Regulations
- S 2.9 (2) Ban on Using Non-Approved Software
- S 2.35 (2) Obtaining information on security weaknesses of the system
- S 2.42 (1) Determination of potential communications partners
- S 2.46 (2) Appropriate key management
- S 2.64 (2) Checking the log files
- S 2.106 (2) Purchase of suitable ISDN cards
- S 2.107 (2) Documentation of the configuration of ISDN cards
- S 2.108 (2) Relinquishment of remote maintenance of ISDN gateways (optional)
- S 2.109 (1) Assigning rights for remote access
- S 2.204 (1) Prevention of insecure network access

Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures

Hardware and software:
- S 4.7 (1) Change of preset passwords
- S 4.34 (1) Using encryption, checksums or digital signatures (*optional*)
- S 4.59 (1) Deactivation of ISDN board functions which are not required
- S 4.60 (1) Deactivation of ISDN router functions which are not required
- S 4.61 (1) Use of security mechanisms offered by ISDN components
- S 4.62 (2) Use of a D-channel filter (*optional*)

Communications:
- S 5.29 (2) Periodic checks of destination addresses and logs
- S 5.32 (1) Secure use of communications software
- S 5.47 (1) Configuration of a Closed User Group (*optional*)
- S 5.48 (1) Authentication via CLIP/COLP
- S 5.49 (1) Callback based on CLIP/COLP
- S 5.50 (1) Authentication via PAP/CHAP

8.5 Fax server



Description

This chapter deals with information transfer via facsimile (fax). When selecting safeguards in the area of IT baseline protection, it should be borne in mind that no distinction has been made between different transmission standards (e.g. CCITT Group 3). This module only considers fax traffic generated using a fax server. A fax server in this sense is an application which is installed on an IT system and provides services on a network enabling other IT systems to send and/or receive faxes.

Fax servers are usually integrated into existing E Mail systems. Thus, it is possible for incoming fax documents to be delivered to users by E Mail. Outgoing documents are passed to the fax server either via a printer queue or else by E Mail. If the fax server is integrated into an E Mail system it is also possible to send out "serial letters" either by fax or by E Mail. If the recipient has access to E Mail then he receives the message free of charge by E Mail, otherwise it comes by fax. The document sent or received by a fax server is a graphics file which cannot be directly edited in a word processing system. However, archiving is possible in either case. This can be done either through the fax server software or else in document management systems.

Fax server applications are available for a number of operating systems, e.g. for various UNIX derivatives, Microsoft Windows NT and Novell NetWare. The threats and safeguards associated directly with whichever operating system is used are not considered in this module. Those aspects are considered in Section 6.1 and the section that is specific to the particular operating system.

Fax servers also often have a binary transfer mode capability. This enables any data which is not in fax format to be transmitted. These transmissions do not constitute fax transmissions. Therefore any special threats and safeguards relating to this service are not considered in this section. If the binary transfer mode is permitted, then Section 7.2 *Modems* should also be used.

Threat Scenario

The following typical threats are assumed for fax information transfer over a fax server as part of IT baseline protection:

Organisational Shortcomings
- T 2.7 Unauthorised use of rights
- T 2.9 Poor adjustment to changes in the use of IT
- T 2.22 Lack of evaluation of auditing data
- T 2.63 Uncontrolled use of Faxes

Human Failure
- T 3.3 Non-compliance with IT security measures
- T 3.14 Misjudgement of the legal force of a fax

Technical Failure
- T 4.15 Fax transmission errors
- T 4.20 Data loss due to exhausted storage medium

Deliberate Acts
- T 5.2 Manipulation of data or software
- T 5.7 Line tapping
- T 5.9 Unauthorised use of IT systems
- T 5.24 Replay of messages
- T 5.25 Masquerading
- T 5.27 Repudiation of a message
- T 5.30 Unauthorised use of a fax machine or fax server
- T 5.31 Unauthorised reading of fax transmissions
- T 5.32 Evaluation of residual information in fax machines and fax servers
- T 5.33 Impersonation of wrong sender on fax transmissions
- T 5.35 Deliberate overload through fax transmissions
- T 5.39 Infiltrating computer systems via communication cards
- T 5.90 Manipulation of address books and distribution lists

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules"), as described in Sections 2.3 and 2.4, is recommended.

As a first step a comprehensive set of security guidelines for the fax server should be prepared (see S 2.178) and a suitable fax server should be procured (see S 2.181 *Selection of a suitable fax server*). These should be used as the basis for developing appropriate procedures. Finally, Fax Officers should be appointed for the fax server (see S 3.10 *Selection of a trustworthy administrator or deputy* and S 2.180 *Setting up a fax mail centre*). Both the security guidelines and the procedures based on them and the appointment of Fax Officers should be effected in writing. These specifications should then be implemented in the form of specific security measures. As well as secure operation of the fax server, it

is especially important that the users should adhere to the relevant security precautions and instructions.

The safeguard package for the "Fax server" application is listed below:

Organisation
- S 2.30 (2) Provisions governing the configuration of users and of user groups
- S 2.64 (1) Checking the log files
- S 2.178 (1) Creation of security guidelines for the use of faxes
- S 2.179 (1) Procedures controlling the use of fax servers
- S 2.180 (1) Configuration of a fax mail centre
- S 2.181 (1) Selection of a suitable fax server

Personnel
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.10 (1) Selection of a trustworthy administrator or deputy
- S 3.11 (1) Training of maintenance and administration staff
- S 3.15 (1) Information for all staff about the use of faxes

Hardware & Software
- S 4.36 (2) Blocking fax recipient numbers (optional)
- S 4.37 (2) Blocking fax sender numbers (optional)

Communication
- S 5.24 (1) Use of a suitable fax cover sheet
- S 5.25 (2) Using transmission and reception logs
- S 5.26 (2) Announcing fax messages via telephone (optional)
- S 5.27 (2) Acknowledging successful fax reception by telephone (optional)
- S 5.28 (2) Acknowledging correct fax origin by telephone (optional)
- S 5.73 (1) Secure operation of a fax server
- S 5.74 (1) Maintenance of fax server address books and distribution lists
- S 5.75 (1) Protecting against overloading the fax server

Contingency Planning
- S 6.69 (1) Contingency planning and operational reliability of fax servers

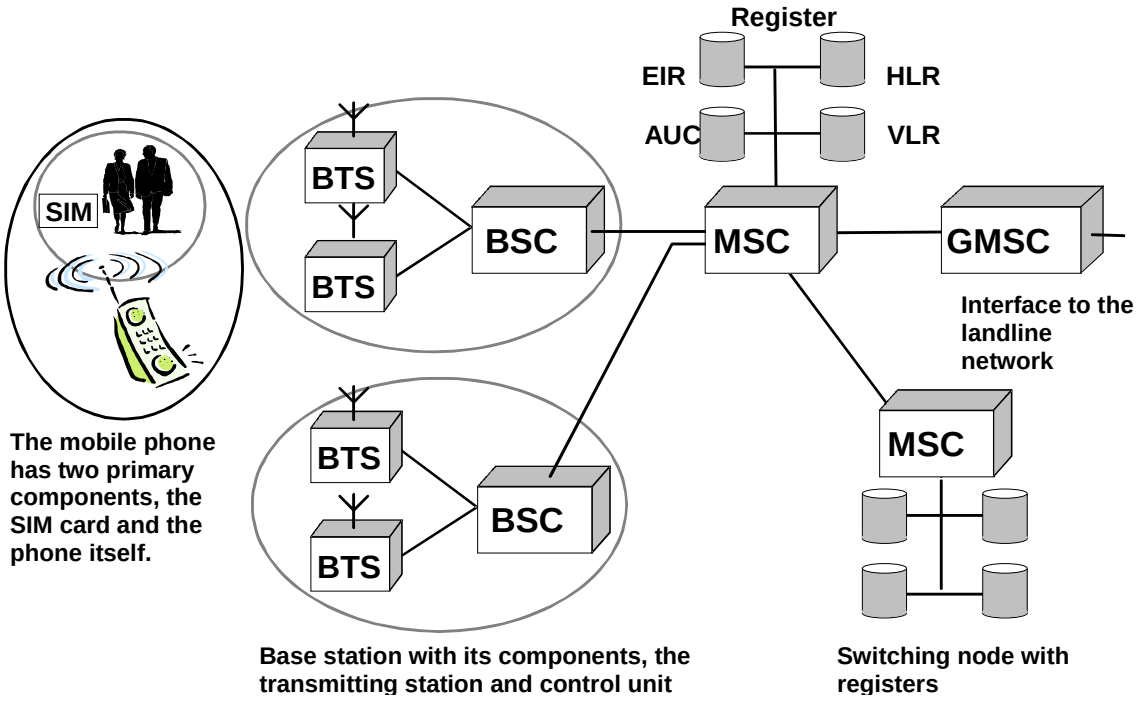
8.6 Mobile Telephones

Description

Over the last few years mobile telephones have become an indispensable element of the communications infrastructure. This raises the issue of how they can be used securely.

This chapter considers digital mobile telephone systems based on the GSM standard (D and E networks). To ensure that they can be used securely, a number of components and their interaction need to be considered (see diagram):

- Mobile telephone
- Base station
- Landline network



Mobile telephone

A mobile phone consists of two components, the mobile transceiver itself and the identification module, the Subscriber Identity Module (SIM) card. This enables the GSM network to distinguish between user and mobile terminal.

The mobile transceiver is characterised by its internationally unique serial number or International Mobile Equipment Identity (IMEI). The user is identified by his customer number (International Mobile Subscriber Identity or IMSI), which is stored on the SIM card and is assigned to the subscriber by the network provider at the time that the subscriber enters into a contract with the network provider. This must be distinguished from the telephone number that is assigned to the subscriber (the Mobile Station ISDN Number or MSISDN). This distinction enables a subscriber to use different mobile transceivers with the same SIM card.

The information stored on the SIM card includes the subscriber-specific call number (MSISDN). The cryptographic algorithms for authentication and encryption of user data are also implemented on the SIM card. In addition, short text messages, call charge information and a personal telephone directory can also be stored on the card.

SIM Toolkit

Since 1999, mobile phones and SIM cards with extended menu functionality have been available on the market. This new standard "SIM Toolkit" defines new functions between SIM card and mobile transceiver. As such, it is now possible to download new data and programs provided by the network provider on a regular basis. In this way SIM Toolkit allows some completely new services to be implemented. For example, it provides the card provider with the means to tailor the menu structure of the mobile phone to individual customers' requirements. Thus, if the customer would like to make a hotel reservation or make the travel arrangements for a business trip using his mobile phone, the menu structure of the mobile phone is appropriately modified by the service provider. However, this does require that both the card and also the mobile terminal support the SIM Toolkit standard.

Base station

Every network provider maintains a large number of transmitting stations also called Base Transceiver System (BTS). Each of these stations can cover an area having a radius of between 250m and 35km, depending on the transmitter power and terrain conditions. The coverage area of a transmitting station is referred to as a radio cell. Several radio cells are controlled from one control station or Base Station Controller (BSC). The combination of transmitting stations and control station in turn is referred to as Base Station Subsystem (BSS) or base station for short.

The base station thus constitutes the interface between the network and the mobile phone. It is here that channels for signalling data and user data are made available. The base station is controlled via the Mobile Switching Centre (MSC). This switching node assumes all the technical functions of a landline network switching node, for example, path search, signal path switching and processing of supplementary services. If there is a requirement for a connection to a subscriber in the landline network, this is forwarded by the MSC to the landline network over a switching path (the Gateway Mobile Switching Centre, GMSC).

The encryption of the data on the radio interface, i.e. between mobile phone and base station, can be viewed as a special feature of the GSM network as opposed to the landline network. This should protect the subscriber against unauthorised passive monitoring.

Registers

In order that the network provider is in a position to provide all the services for which demand exists, it must store various items of data. For example, it must know which subscribers are using its network and which services they wish to use. This data, such as the name of the subscriber, his customer number and the services he requires, are stored in the Home Location Register (HLR). If a connection is to be established, for example from a landline network terminal to a mobile phone, the network provider needs to know where the subscriber is and whether his mobile phone is switched on. This information is held in the Visitor Location Register (VLR) and the HLR. To check whether the subscriber is entitled to use the mobile communication network (i.e. he has taken out a card contract), the network provider maintains an identification register at the Authentication Centre (AUC). This holds the security code of the SIM card as well as the PINs determined by the subscriber.

The network provider can also maintain an equipment register, the Equipment Identification Register (EIR), which holds details of all the mobile transceivers permitted on the network broken down into three groups known as the white, grey and black lists. The white list is a register of all the mobile phones which are functioning reliably, the grey list contains all the phones which may possibly be

defective, while the black list holds details of all the phones which either have a fault or have been reported stolen. However, not all network providers maintain an equipment register.

In order that the network provider can prepare billing details of the services used by customers, the call data must be stored. This includes, for example, details of communication partners (e.g. call numbers dialled), time and duration of the connection and the location identifiers of the mobile terminals.

Call establishment

As soon as the owner switches on his mobile phone, it registers with the network provider via the nearest base station. The subscriber is identified to the network provider by means of his SIM card and cryptographic algorithms installed on this card. Authentication is effected with the aid of a key which is known only to the network provider and the subscriber. The network provider logs and stores data on the identity of the user, the serial number of the mobile phone and the identity of the base station over which he has registered. This occurs even if no conversation takes place. Moreover, information is stored on every number dialled, irrespective of whether a connection is established. As a result the network provider knows which subscribers are on the network so that connections can now be established from and to subscribers.

Landline network

The conventional public telephone network with its connecting paths is referred to as the landline network.

As every mobile phone connection also entails the use of landline networks, a number of threats relating to the landline network apply also where mobile communication networks are used. The line-connected part of the GSM network is a special instance of an ISDN network. Hence, most of the threats and safeguards which apply to ISDN are applicable to GSM as well. Section 8.4 *LAN connection of an IT system via ISDN* is therefore also relevant to data transmission over GSM.

This chapter considers those security characteristics of mobile phones which are relevant to persons using them. The intention is to present a systematic approach as to how to draw up a concept for the use of mobile phones within an organisation and ensure that this is implemented and integrated.

Threat Scenario

For IT baseline protection, the following typical threats are assumed to affect the use of mobile phones:

Organisational Shortcomings:
- T 2.2 Insufficient knowledge of requirements documents
- T 2.4 Insufficient monitoring of IT security measures
- T 2.7 Unauthorised use of rights

Human Error:
- T 3.3 Non-compliance with IT security measures
- T 3.43 Inappropriate handling of passwords
- T 3.44 Carelessness in handling information
- T 3.45 Inadequate checking of the identity of communication partners

Technical Failures:
- T 4.41 Non-availability of the mobile communication network
- T 4.42 Failure of the mobile phone

Deliberate Acts:
- T 5.2 Manipulation of data or software
- T 5.4 Theft
- T 5.80 Hoaxes
- T 5.94 Misuse of cards
- T 5.95 Bugging of indoor conversations over mobile phones
- T 5.96 Tampering with mobile phones
- T 5.97 Unauthorised transfer of data over mobile phones
- T 5.98 Interception of mobile telephone calls
- T 5.99 Analysis of call data relating to the use of mobile phones

Recommended Countermeasures

To implement IT baseline protection, selection of the required packages of safeguards ("modules") is recommended, as described in Sections 2.3 and 2.4.

In order to be able to use mobile phones securely and effectively, the use of mobile phones should be regulated within the organisation from the outset and security guidelines should be drawn up on the subject (see S 2.188).

The detailed package of safeguards which has been prepared for the use of mobile phones is summarised below.

Organisation:
- S 2.4 (2) Maintenance/repair regulations
- S 2.22 (3) Escrow of passwords
- S 2.188 (1) Security guidelines and rules for the use of mobile phones
- S 2.189 (1) Blocking of the mobile phone in the event of its loss
- S 2.190 (2) Setting up a mobile phone pool (optional)

Hardware and Software:
- S 4.114 (1) Use of the security mechanisms provided on mobile phones
- S 4.115 (2) Safeguarding the power supply of mobile phones

Communications:
- S 5.78 (3) Protection against mobile phone usage data being used to create movement profiles (optional)
- S 5.79 (3) Protection against call number identification during use of mobile phones (optional)
- S 5.80 (3) Protection against bugging of indoor conversations using mobile phones (optional)
- S 5.81 (2) Secure transmission of data over mobile phones

Contingency Planning:
- S 6.72 (2) Precautions relating to mobile phone failures

9 Other IT Components

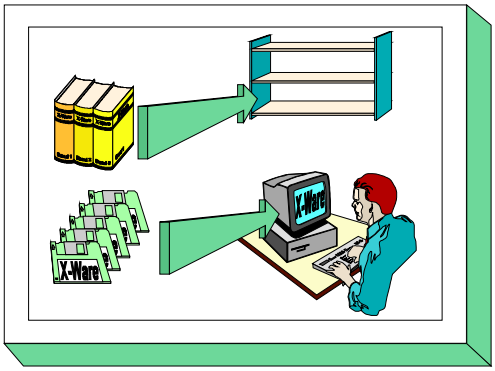
This chapter defines IT baseline protection in the following modules:

9.1 Standard software

9.2 Databases

9.3 Telecommuting

9.1 Standard software



Description

Standard software is software offered on the market and which is generally available from specialist outlets, e.g. catalogues. It is characterised by the fact that it is intended to be installed by the user and that it can be easily adapted to suit the specific needs of the user.

This chapter deals with an approach to handling standard software with regard to security. The entire lifecycle of standard software is considered: drawing up a requirements catalogue, preselection of a suitable product, test, release, installation, licence administration and deinstallation.

The quality management system of the developer of the standard software is not covered in this chapter. It is assumed that the software has been developed in accordance with the usual quality standards.

The described procedure serves as orientation for establishing a security process as far as standard software is concerned. If applicable, the procedures listed here can also be compared with a process already carried out, or they can be partly reduced for present interests.

Threat Scenario

The following typical threats are assumed for "standard software" as part of IT baseline protection:

Organisational shortcomings:
- T 2.1 Lack of, or insufficient, rules
- T 2.3 A lack of compatible, or unsuitable, resources
- T 2.26 Lack of, or inadequate, test and release procedures
- T 2.27 Lack of, or inadequate, documentation
- T 2.28 Violation of copyright
- T 2.29 Software testing with production data

Human Failure:
- T 3.3 Non-compliance with IT security measures
- T 3.38 Errors in configuration and operation

Technical Failure:
- T 4.8 Discovery of software vulnerabilities
- T 4.22 Software vulnerabilities or errors

Deliberate Acts:
- T 5.21 Trojan Horses
- T 5.23 Computer viruses
- T 5.43 Macro viruses

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

The safeguards package for the module "Standard Software " is presented in the following. Depending on the nature and scope of the standard software, it must be considered whether only individual safeguards have to be reduced. M 2.79 to S 2.89 provide a detailed description of how the lifecycle of standard software can be shaped. These are supplemented by the other safeguards stated.

Organisation:
- S 2.9 (2) Ban on using non-approved software
- S 2.10 (2) Survey of the software held
- S 2.35 (1) Obtaining information on security weaknesses of the system
- S 2.40 (2) Timely involvement of the staff/factory council
- S 2.66 (2) The importance of certification for procurement
- S 2.79 (1) Determining responsibilities in the area of standard software
- S 2.80 (1) Drawing up a requirements catalogue for standard software
- S 2.81 (1) Preselection of a suitable standard software product
- S 2.82 (1) Developing a test plan for Standard Software
- S 2.83 (1) Testing Standard Software
- S 2.84 (1) Deciding on and developing the installation instructions for standard software
- S 2.85 (1) Approval of standard software
- S 2.86 (2) Guaranteeing the integrity of standard software
- S 2.87 (2) Installation and configuration of standard software
- S 2.88 (2) Licence management and version control of standard software
- S 2.89 (3) De-installation of standard software
- S 2.90 (2) Checking delivery

Personnel:
- S 3.4 (1) Training before actual use of a program

Hardware & Software:
- S 4.34 (2) Using encryption, checksums or digital signatures (*optional*)
- S 4.78 (2) Careful modifications of configurations

Contingency Planning:
- S 6.21 (3) Backup copy of the software used (*optional*)

❒

The following essential steps must also be taken for *databases*:

1. Determining the requirements to be fulfilled by the database software.

   First prepare a requirements catalogue to allow the selection of a suitable standard database software (S 2.80 and S 2.124).

2. Training administrators

   Before the database software is used in a productive environment, the responsible administrators must be trained (S 3.11). If possible, this should be done before procuring the software package.

3. Design a database concept

Before using the database software, design a database concept which describes the installation and configuration of the database software, the suitable concept for database users and their access rights, as well as the application-specific database. Depending on the capacity and environment of the database as well as the selected standard database software, such a concept can be very extensive (S 2.125, S 2.128, S 2.129 and S 2.126).

4. Operating the database

   Commissioning and operation of the database include the implementation of the database concept, as well as continuous monitoring of the DBMS in order to ensure the availability, data integrity and protection of confidential data. The most important safeguards here concern documentation (S 2.25, S 2.31, S 2.34), administration (S 2.130, S 2.133) and utilisation of the database.

5. Contingency planning

   In addition to the general safeguards relating to this topic, it is important to consider database-specific circumstances in order to keep data losses and recovery times within reasonable limits in the event of a system crash or database crash. (S 6.32, S 6.49, S 6.50).

The safeguard package for databases is listed in the following:

Organisation

- S 2.22 (2) Escrow of passwords
- S 2.25 (1) Documentation of the system configuration
- S 2.31 (1) Documentation on authorised users and on rights profiles
- S 2.34 (1) Documentation of changes made to an existing IT system
- S 2.65 (2) Checking the efficiency of user separation on an IT System
- S 2.80 (1) Drawing up a requirements catalogue for standard software
- S 2.111 (2) Keeping manuals at hand
- S 2.124 (1) Selection of suitable database software
- S 2.125 (1) Installation and configuration of a database
- S 2.126 (1) Creation of a database security concept
- S 2.127 (2) Inference prevention
- S 2.128 (1) Controlling access to a database system
- S 2.129 (1) Controlling access to database information
- S 2.130 (1) Ensuring the integrity of a database
- S 2.131 (1) Separation of administrative tasks for database systems
- S 2.132 (1) Rules for configuring database users / user groups
- S 2.133 (2) Checking the log files of a database system
- S 2.134 (2) Guidelines for database queries
- S 2.135 (3) Save transfer of data to a database

Personnel

- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.10 (1) Selection of a trustworthy administrator and his substitute
- S 3.11 (1) Training of maintenance and administration staff
- S 3.18 (2) Log-out obligation for PC users

Hardware & Software

- S 4.1 (1) Password protection for IT systems
- S 4.7 (1) Change of preset passwords
- S 4.67 (3) Locking and deleting database accounts which are no longer required
- S 4.68 (1) Ensuring consistent database management
- S 4.69 (2) Regular checks of database security
- S 4.70 (3) Monitoring a database
- S 4.71 (2) Restrictive utilisation of database links
- S 4.72 (2) Database encryption (optional)

- S 4.73 (2) Specifying upper limits for selectable data records

Communication
- S 5.58 (1) Installation of ODBC drivers

Contingency Planning
- S 6.32 (1) Regular data backup
- S 6.48 (2) Procedures in case of a loss of database integrity
- S 6.49 (1) Data backup in a database
- S 6.50 (1) Archiving database
- S 6.51 (3) Restoring a database

❒

The following essential steps must also be taken for *databases*:

1. Determining the requirements to be fulfilled by the database software.

   First prepare a requirements catalogue to allow the selection of a suitable standard database software (S 2.80 and S 2.124).

2. Training administrators

   Before the database software is used in a productive environment, the responsible administrators must be trained (S 3.11). If possible, this should be done before procuring the software package.

3. Design a database concept

   Before using the database software, design a database concept which describes the installation and configuration of the database software, the suitable concept for database users and their access rights, as well as the application-specific database. Depending on the capacity and environment of the database as well as the selected standard database software, such a concept can be very extensive (S 2.125, S 2.128, S 2.129 and S 2.126).

4. Operating the database

   Commissioning and operation of the database include the implementation of the database concept, as well as continuous monitoring of the DBMS in order to ensure the availability, data integrity and protection of confidential data. The most important safeguards here concern documentation (S 2.25, S 2.31, S 2.34), administration (S 2.130, S 2.133) and utilisation of the database.

5. Contingency planning

   In addition to the general safeguards relating to this topic, it is important to consider database-specific circumstances in order to keep data losses and recovery times within reasonable limits in the event of a system crash or database crash. (S 6.32, S 6.49, S 6.50).

The safeguard package for databases is listed in the following:

Organisation

- S 2.22 (2) Escrow of passwords
- S 2.25 (1) Documentation of the system configuration
- S 2.31 (1) Documentation on authorised users and on rights profiles
- S 2.34 (1) Documentation of changes made to an existing IT system
- S 2.65 (2) Checking the efficiency of user separation on an IT System
- S 2.80 (1) Drawing up a requirements catalogue for standard software
- S 2.111 (2) Keeping manuals at hand
- S 2.124 (1) Selection of suitable database software
- S 2.125 (1) Installation and configuration of a database
- S 2.126 (1) Creation of a database security concept
- S 2.127 (2) Inference prevention
- S 2.128 (1) Controlling access to a database system
- S 2.129 (1) Controlling access to database information
- S 2.130 (1) Ensuring the integrity of a database
- S 2.131 (1) Separation of administrative tasks for database systems
- S 2.132 (1) Rules for configuring database users / user groups
- S 2.133 (2) Checking the log files of a database system
- S 2.134 (2) Guidelines for database queries
- S 2.135 (3) Save transfer of data to a database

Personnel

- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.10 (1) Selection of a trustworthy administrator and his substitute
- S 3.11 (1) Training of maintenance and administration staff
- S 3.18 (2) Log-out obligation for PC users

Hardware & Software

- S 4.1 (1) Password protection for IT systems
- S 4.7 (1) Change of preset passwords
- S 4.67 (3) Locking and deleting database accounts which are no longer required
- S 4.68 (1) Ensuring consistent database management
- S 4.69 (2) Regular checks of database security
- S 4.70 (3) Monitoring a database
- S 4.71 (2) Restrictive utilisation of database links
- S 4.72 (2) Database encryption (optional)

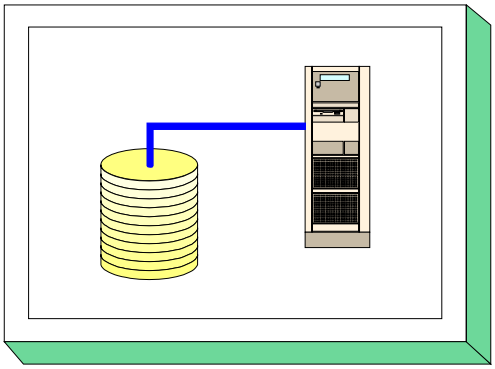
- S 4.73 (2) Specifying upper limits for selectable data records

Communication
- S 5.58 (1) Installation of ODBC drivers

Contingency Planning
- S 6.32 (1) Regular data backup
- S 6.48 (2) Procedures in case of a loss of database integrity
- S 6.49 (1) Data backup in a database
- S 6.50 (1) Archiving database
- S 6.51 (3) Restoring a database

❒

9.2 Databases



Description

Database systems (DBS) are commonly accepted computer-aided techniques of organising, generating, manipulating and managing large amounts of data. A database system consists of the *database management system* (DBMS) and a certain number of *databases*. A database is a collection of data representing facts on a specific application in the real world. The DBMS acts as an interface between users and the database, allowing efficient and centrally monitored access to data, and ensuring the pemanent availability of this data.

Database management systems now form an indispensable part of IT applications. Without a DBMS, it would not be possible to manage the vast amounts of data which need to be collected, processed and evaluated. The concept of a DBMS is based on a particular *database model*. The most important database models are described in the following:

Hierarchical database model

This is the oldest existing variant, also regarded as the database model of the first generation. This database model is structured like a tree. The nodes and leaves in this structure represent the files. A node or leaf has exactly one predecessor, and data is always accessed sequentially. The access routes are determined by the tree structure (and file structure respectively).

Relational database model

The relational database model involves strict separation between the data and the methods of accessing it. The data is stored in the form of tables, where each row represents a data record (also termed tupel) and each column represents an attribute of the data record. Tupels can be related to other tupels in different tables, which is marked by a corresponding relationship. As opposed to the hierarchical model, the relational database model does not impose any restrictions on access to data.

SQL (Standard Query Language), standardised by the ISO, is the database language provided with all relational database systems.

Object-oriented database model

Object-oriented database models are an extension of classical database models and involve an object-oriented (OO) technique. In this case, objects with similar attributes are grouped into classes which, in turn, can be assigned class hierarchies. Only defined methods can be used to modify the objects, the inheritance of methods and attributes playing a key role in object-oriented design. Standard data types such as "Integer" and "Character" can be supplemented with type constructors allowing the definition of complex values.

This chapter only provides a treatment of databases based on the relational database model, as it is currently the most prevalent.

A database system generally provides simultaneous access for different users. It therefore has to process several user requests (transactions) in parallel and guarantee a distinct level of fault tolerance. Of central importance are four requirements which are called the ACID-principle:

- Atomicity

From the view of a user, a transaction will either be completed as a whole or not at all. If there is an error or interruption, all changes made so far will be undone. This is ensured in the DBMS with appropriate recovery measures.

- Consistency

  All integrity conditions in the database are maintained. A transaction leads the database from a consistent state into another consistent state. This can be ensured by appropriate synchronisation mechanisms in the database.

- Isolation

  Every transaction is isolated from all other transactions. This also implies that a transaction can access only data that are part of a consistent state of the database.

- Durability

  If a transaction has been reported to the user as successfully completed, all changes made in the database will survive subsequent hardware or software failures (unless the database is destroyed as a whole).

These requirements are fulfilled by almost all commercially available DBMS systems.

Database systems are based on standard commercial software offered by a variety of manufacturers. The first step in acquiring a database for processing data is to select a suitable standard software package. The related threats and safeguards stated in Chapter 9.1 *Standard Software* must also be considered here.

Databases cannot be treated separately from the environment in which they are used. A stand-alone PC is just as feasible as a mainframe or a network of Unix systems. For this reason, the threats and safeguards described in Chapter 5 *Non-networked systems*, Chapter 6 *Local Area Networks* and Chapter 7 *Data Transfer Systems* should be taken into consideration in accordance with the type of environment involved. To prevent redundancies, this chapter does not repeat descriptions of threats and safeguards unless they are of particular importance.

Threat Scenario

The following threats are assumed to be applicable to the IT baseline protection of databases:

Force Majeure
- T 1.1 Loss of personnel

Organisational shortcomings:
- T 2.3 A lack of compatible, or unsuitable, resources
- T 2.22 Lack of evaluation of auditing data
- T 2.26 Lack of, or inadequate, test and release procedures
- T 2.38 Lack of, or inadequate, implementation of database security mechanisms
- T 2.39 Complexity of a DBMS
- T 2.40 Complexity of database access
- T 2.41 Poor organisation of the exchange of database users
- T 2.57 Inadequate storage of media in the event of an emergency

Human Failure:
- T 3.6 Hazards posed by cleaning staff or outside staff
- T 3.16 Incorrect administration of site and data access rights
- T 3.23 Improper administration of a DBMS
- T 3.24 Inadvertent manipulation of data

Technical Failure:
- T 4.26 Failure of a database
- T 4.27 Circumvention of access control via ODBC
- T 4.28 Loss of data in a database
- T 4.29 Loss of data in a database caused by a lack of storage space
- T 4.30 Loss of database integrity/consistency

Deliberate Acts:
- T 5.9 Unauthorised use of IT systems
- T 5.10 Abuse of remote maintenance ports
- T 5.18 Systematic trying-out of passwords
- T 5.64 Manipulation of data or software in database systems
- T 5.65 Denial of services in a database system

Recommended Countermeasures (S)

For the purpose of IT baseline protection, we recommend the complete implementation of the safeguard packages (modules) summarised in Chapters 2.1 and 2.4.

It is advisable to install the database server in a separate server room. The appropriate measures are described in Chapter 4.3.2. If an office is used simultaneously as a server room, the safeguards described in Chapter 4.3.1 must also be implemented.

If the database server is installed in a protective cabinet, also refer to Chapter 4.4 Protective Cabinets.

The following essential steps must also be taken for *databases*:

1. Determining the requirements to be fulfilled by the database software.

   First prepare a requirements catalogue to allow the selection of a suitable standard database software (S 2.80 and S 2.124).

2. Training administrators

   Before the database software is used in a productive environment, the responsible administrators must be trained (S 3.11). If possible, this should be done before procuring the software package.

3. Design a database concept

   Before using the database software, design a database concept which describes the installation and configuration of the database software, the suitable concept for database users and their access rights, as well as the application-specific database. Depending on the capacity and environment of the database as well as the selected standard database software, such a concept can be very extensive (S 2.125, S 2.128, S 2.129 and S 2.126).

4. Operating the database

   Commissioning and operation of the database include the implementation of the database concept, as well as continuous monitoring of the DBMS in order to ensure the availability, data integrity and protection of confidential data. The most important safeguards here concern documentation (S 2.25, S 2.31, S 2.34), administration (S 2.130, S 2.133) and utilisation of the database.

5. Contingency planning

   In addition to the general safeguards relating to this topic, it is important to consider database-specific circumstances in order to keep data losses and recovery times within reasonable limits in the event of a system crash or database crash. (S 6.32, S 6.49, S 6.50).

The safeguard package for databases is listed in the following:

Organisation:
- S 2.22 (2) Escrow of passwords
- S 2.25 (1) Documentation on the system configuration
- S 2.31 (1) Documentation on authorised users and on rights profiles
- S 2.34 (1) Documentation on changes made to an existing IT system
- S 2.80 (1) Drawing up a requirements catalogue for standard software
- S 2.111 (2) Keeping manuals at hand
- S 2.124 (1) Selection of suitable database software
- S 2.125 (1) Installation and configuration of a database
- S 2.126 (1) Creation of a database security concept
- S 2.127 (2) Inference prevention
- S 2.128 (1) Controlling access to a database system
- S 2.129 (1) Controlling access to database information
- S 2.130 (1) Ensuring the integrity of a database
- S 2.131 (1) Separation of administrative tasks for database systems
- S 2.132 (1) Rules for configuring database users / user groups
- S 2.133 (2) Checking the log files of a database system
- S 2.134 (2) Guidelines for database queries
- S 2.135 (3) Save transfer of data to a database

Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.10 (1) Selection of a trustworthy administrator and his substitute
- S 3.11 (1) Training of maintenance and administration staff

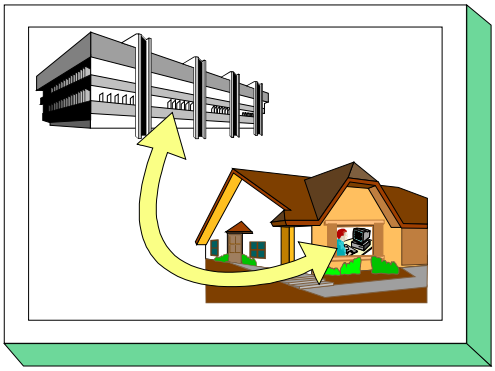
Hardware & Software:
- S 4.1 (1) Password protection for IT systems
- S 4.7 (1) Change of preset passwords
- S 4.67 (3) Locking and deleting database accounts which are no longer required
- S 4.68 (1) Ensuring consistent database management
- S 4.69 (2) Regular checks of database security
- S 4.70 (3) Monitoring a database
- S 4.71 (2) Restrictive utilisation of database links
- S 4.72 (2) Database encryption (optional)
- S 4.73 (2) Specifying upper limits for selectable data records

Communications:
- S 5.58 (1) Installation of ODBC drivers

Contingency Planning:
- S 6.32 (1) Regular data backup
- S 6.48 (2) Procedures in case of a loss of database integrity
- S 6.49 (1) Data backup in a database
- S 6.50 (1) Archiving database
- S 6.51 (3) Restoring a database

❒

9.3 Telecommuting



Description

In general, telecommuting comprises activities which are performed from a remote location for an employer or client with the help of communications links to that employer or client.

There are different types of telecommuting, such as working at satellite offices, neighbourhood offices, mobile telecommuting, and working at one's own residence. In the last case, a distinction is made between exclusive telecommuting and alternate telecommuting, i.e. working exclusively at home, or partly at home and partly at an institution.

This chapter deals with the types of telecommuting performed partly or exclusively at home. It is assumed that the home workstation and institution are linked by means of a telecommunications line allowing an exchange of data and, if required, access to data at the institution.

The measures recommended in this chapter fall under four different categories:

- Organisation of telecommuting
- Remote computer used by the telecommuter
- Communications link between the remote computer and institution
- Computer at the institution used for communication with the remote computer

The safeguards recommended in this chapter concentrate on additional security requirements for IT systems used for telecommuting. In particular, security requirements are formulated for the technical components of telecommuting (remote computers, communications links and communications computers); these requirements must be met by appropriately configured IT systems. The related modules in Chapter 5 and the safeguards for the home working-place mentioned in Chapter 4.5 also need to be considered for the IT systems used.

Threat Scenario

The following typical threats are assumed as regards IT baseline protection of telecommuting:

Force Majeure
- T 1.1 Loss of personnel

Organisational shortcomings:
- T 2.1 Lack of, or insufficient, rules
- T 2.2 Insufficient knowledge of requirements documents
- T 2.4 Insufficient monitoring of IT security measures
- T 2.5 Lack of, or inadequate, maintenance
- T 2.7 Unauthorised use of rights (on the workstations at home and at the institution)
- T 2.8 Uncontrolled use of resources
- T 2.22 Lack of evaluation of auditing data
- T 2.24 Loss of confidentiality of sensitive data of the network to be protected
- T 2.49 Lack of, or inadequate, training of teleworkers
- T 2.50 Delays caused by a temporarily restricted availability of teleworkers
- T 2.51 Poor integration of teleworkers into the information flow
- T 2.52 Longer response times in the event of an IT system breakdown
- T 2.53 Inadequate regulations concerning substitution of teleworkers

Human Failure:
- T 3.1 Loss of data confidentiality/integrity as a result of IT user error
- T 3.3 Non-compliance with IT security measures
- T 3.9 Improper IT system administration
- T 3.13 Transfer of incorrect or undesired data records
- T 3.16 Incorrect administration of site and data access rights
- T 3.30 Unauthorised private use of telecommuting workstations

Technical Failure:
- T 4.13 Loss of stored data

Deliberate Acts:
- T 5.1 Manipulation/destruction of IT equipment or accessories
- T 5.2 Manipulation of data or software
- T 5.7 Interception of lines
- T 5.8 Manipulation of lines
- T 5.9 Unauthorised use of IT systems
- T 5.10 Abuse of remote maintenance ports
- T 5.18 Systematic trying-out of passwords (on the workstations at home and at the institution)
- T 5.19 Abuse of user rights
- T 5.20 Misuse of administrator rights

- T 5.21 Trojan Horses
- T 5.23 Computer viruses
- T 5.24 Replay of messages
- T 5.25 Masquerade
- T 5.43 Macro viruses
- T 5.71 Loss of confidentiality of classified information

Recommended Countermeasures (S)

For the implementation of IT baseline protection, selection of the required packages of safeguards ("modules") as described in chapters 2.3 and 2.4, is recommended.

A sufficiently reliable form of telecommuting is only achieved if IT security measures from several areas are allowed to overlap and complement each other. If any one of these areas is neglected, secure telecommuting can no longer be ensured. The individual areas and essential measures are:

- *Infrastructural reliability of the remote workstation*: Measures to be implemented at the remote workstation are described in Chapter 4.5 titled "Working Place at Home".
- *Organisation of telecommuting*: Secure telecommuting requires organisational regulations and measures for governing staff activities. These are listed in the following under the general headings "Organisation" and "Personnel". Particular attention needs to be paid to the obligations and assignments of telecommuters, and rules concerning the usage of communications facilities. They are described in the following measures:
  - S 2.113 *Requirements documents concerning telecommuting*
  - S 2.116 *Regulated use of communications facilities*
  - S 2.117 *Regulation of access by telecommuters*
  - S 3.21 *Training and further education of telecommuters as regards security-related issues*
- Security *of the telecommuting workstations*: The remote computer must be configured so as to allow secure use even in an unsecure operational environment. In particular, only one authorised person should be able to use the remote computer in the online and offline states. The related measures are summarised under the general headings "Hardware/software" and "Contingency measures". In particular, the security requirements in S 4.63 *Security requirements for remote computers* should be observed.
- *Secure communications between telecommuting workstations and an institution*: As communications take place via public networks, special security requirements concerning the exchange of data between telecommuting workstations and an institution need to be observed. These are described in S 5.51 *Security-related requirements for communications links between telecommuting workstations and the institution*. For the linkage of a remote computer via the public network, refer to Chapter 8.4 titled "LAN linkage of an IT system via ISDN".
- *Protection of communications computers at institutions*: To a certain extent, these computers constitute a publicly accessible interface via which telecommuters can make use of information technology and data at the institution. As misuse by unauthorised parties needs to be prevented here, special security requirements described in S 5.52 *Security requirements for communications computers* must be met.

The package of measures for the area of telecommuting is listed in the following:

Organisation:
- S 2.9 (2) Ban on using non-approved software
- S 2.22 (2) Escrow of passwords
- S 2.23 (3) Issue of PC Use guidelines (*optional*)
- S 2.64 (2) Checking the log files (on the workstations at home and the institution)
- S 2.113 (2) Requirements documents concerning telecommuting
- S 2.114 (2) Flow of information between the telecommuter and the institution
- S 2.115 (2) Care and maintenance of workstations for telecommuting
- S 2.116 (1) Regulated use of communications facilities
- S 2.117 (1) Regulation of access by telecommuters

Personnel:
- S 3.4 (1) Training before actual use of a program
- S 3.5 (1) Education on IT security measures
- S 3.21 (1) Training and further education of telecommuters as regards security-related issues
- S 3.22 (2) Regulations concerning substitution of telecommuters

Hardware & Software:
- S 4.3 (2) Periodic runs of a virus detection program
- S 4.30 (2) Utilisation of the security functions offered in application programs
- S 4.33 (1) Use of a virus scanning program when exchanging of data media and data transmission
- S 4.44 (2) Checking of incoming data for macro viruses
- S 4.63 (1) Security-related requirements for telecommuting computers

Communications:
- S 5.51 (1) Security-related requirements for communications links between telecommuting workstations and the institution
- S 5.52 (1) Security-related requirements for communications computers

Contingency Planning:
- S 6.13 (2) Development of a data backup plan
- S 6.22 (2) Sporadic checks of the restorability of backups
- S 6.23 (2) Procedure in case of computer virus infection
- S 6.32 (1) Regular data backup
- S 6.38 (2) Back-up copies of transferred data
- S 6.47 (2) Storage of backup copies as part of telecommuting

❒

T 1 Threats Catalogue - Force Majeure

T 1.1 Loss of personnel

T 1.2 Failure of the IT system

T 1.3 Lightning

T 1.4 Fire

T 1.5 Water

T 1.6 Burning cables

T 1.7 Inadmissible temperature and humidity

T 1.8 Dust, soiling

T 1.9 Loss of data due to intensive magnetic fields

T 1.10 Failure of a wide area network

T 1.1 Loss of personnel

Illness, accident, death or a strike can result in an unforeseen loss of personnel resources. It also needs to be borne in mind that when a person terminates his employment in the normal manner, the remaining time that he is available for work can be shortened, for example, by his taking holidays during the notice period.

In all cases, the result may be that critical tasks are no longer performed due to the loss of manpower in IT applications. This is especially critical if the person concerned holds a key position in the IT area and cannot be replaced by alternative staff due to lack of technical expertise. IT operations could be disrupted as a result.

A loss of personnel resources could also mean that specialist knowledge and/or secret information is lost, preventing the person's duties being taken over by to replacement staff.

Examples

- Due to prolonged illness, the Network Administrator was away from work. In the company concerned, at first the network ran without any problems. However, when the system crashed after two weeks no one was able to sort out the problem. As a result the network was out of service for several days.
- While the Administrator was on holiday, it was necessary for backup purposes to access the backup tapes in the data backup safe. The access code to the safe had been changed only recently and only the Administrator knew the new code. It was not possible to restore the data for several days as it was necessary first to find out the Administrator's whereabouts.

T 1.2 Failure of the IT system

Failure of a single component in an IT system can result in failure of the entire IT operation. Such failures are especially likely to occur where faults develop in components which are central to the IT system, e.g. air-conditioning, power supply, LAN server or data transmission facilities.

Technical failure (e.g. T 4.1 *Disruption of power supply*) should not necessarily be assumed to be the cause when an IT system fails. Failures are often also the result of human error (e.g. T 3.2 *Negligent destruction of equipment or data*) or wilful action (e.g. T 5.4 *Theft*). Loss or damage may also be caused by force majeure (e.g. fire, lightning, chemical accident), although in such cases the scale of the damage is likely to be considerably higher.

If any time-critical IT applications are run on an IT system, the consequential damage following a system failure may be expected to be extensive unless there are alternatives available.

Examples

- Due to voltage spikes in the power supply, the power unit for an important IT system is destroyed. As the IT system concerned is an older model, replacement parts are not available immediately. Repairs take a whole day to perform and during this time the entire IT operation is at a standstill.
- Firmware is imported onto an IT system for which it is unsuited. The IT system will no longer start without errors and has to be repaired by the manufacturer.

T 1.3 Lightning

In the case of a thunderstorm, lightning is the major threat to a building and the IT facilities accommodated there. With a voltage of several hundred thousand volts, lightening strikes can have currents of up to 200,000 ampere. This enormous electric energy is released and dies away within a period of 50 - 100 µs. A lightening strike with the above parameters, which hits at a distance of about 2 km, still causes voltage peaks in the power lines of the building, which can lead to the destruction of sensitive electronic devices. Such indirect damage will increase with decreasing distance.

If a building is directly hit by lightning, damage will be caused by the dynamic energy of the lightening strike. This may include physical damage to the structure (roof and façade), damage caused by resultant fire, or overvoltage damage to electric devices.

The German Meteorological Service provides information on the risk of lightning in the various regions.

T 1.4 Fire

Apart from the direct damage caused by fire to a building or its equipment, there may be consequential damage, the impact of which can attain disastrous dimensions, especially for IT systems. Damage from the fire-fighting water does not occur at the direct site of the fire. Such damage can also be found in lower parts of the building. The burning of PVC generates chlorine gases which, together with air moisture and the fire-fighting water, form hydrochloric acid. In the event that such chlorine gases are spread via the air conditioning system, this may lead to damage of sensitive electronic devices in other areas far away from the site of the fire.

A fire is caused not only by negligent handling of combustible material (e.g. Christmas candles, welding, soldering, etc.), but also by improper use of electric devices (e.g. unattended coffee machines, overload on multiple plug adapters).

The following, *inter alia*, can facilitate the spreading of a fire:

- wedging of fire doors;
- improper storage of combustible material;
- lack of fire detection devices;
- deficient fire prevention (e.g. lack of fire insulation along cable routes).

Example:

In the early 90s, a mainframe computer centre in the Frankfurt region was hit by a disastrous fire, leading to the complete breakdown of the installations.

T 1.5 Water

The uncontrolled flow of water into buildings or rooms may, for instance, result from:

- rain, floods, inundation
- disruption of water supply and sewerage systems;
- defects in the heating system;
- defects in the air conditioning systems connected to the water supplies;
- defects in the sprinkler systems; and
- water used for fire fighting.

Regardless of how water enters buildings or rooms, the danger is that it will damage, or make inoperable, the supply facilities or IT components (short circuit, mechanical damage, rust, etc.). When central supplies for the building (main power distributor, trunk distribution frame for telephone, data) are accommodated in basement rooms without automatic water removal, the subsequent ingress of water can cause considerable damage.

T 1.6 Burning cables

When a cable catches fire, either by spontaneous ignition or igniting/kindling, this can have various effects:

- the connection may be interrupted;
- aggressive gases may evolve;
- cables with non fire-resistant or self-extinguishing insulation material may aid in the fire's spread, fire sealing not being able to prevent this completely, merely delaying the spread of the fire;
- in the case of close-packed lines, there may be smouldering fires which can remain undiscovered for a prolonged period of time, resulting in the spreading of the fire long before it fully breaks out.

T 1.7 Inadmissible temperature and humidity

Every device has a temperature range within which its proper functioning is ensured. If the room temperature exceeds that range in either direction, the result may be a discontinuity of service and failure of devices.

In a server room, for instance, the devices accommodated there will consume electric power and thus heat up the room. If ventilation is insufficient, the admissible operating temperature of the devices may be exceeded. In case of solar radiation, room temperatures of more than 50° C are not improbable.

The windows of a server room shouldn't be frequently opened for ventilation. In Spring or Autumn, for instance, this could cause large temperature fluctuations leading to drastic cooling down and subsequent impermissible rises in humidity.

Example:

In a Bonn-based agency, the entire control and evaluation electronics system of a security facility was accommodated in a room whereby just enough space to open the doors of the equipment lockers was left. For security reasons, both the cabinets and the room were provided with massive, tight-fitting doors.

After completion of the installation in Autumn, the operation was free of problems. The following summer, however, unaccountable malfunctions emerged. These were soon followed by total system crashes, without any discernible systematic causes in either case. Several days of searching for faults, involving great expenditure in technical and staffing terms, and carried out with the doors open, yielded no results. It was only by accident that the cause of failure, an overheating of the facilities with outside temperatures of more than 30° C, was finally found, and was remedied with the installation of an air conditioning system.

T 1.8 Dust and dirt accumulation

Although electronics play an increasing role in IT, it still relies on mechanical components. These include diskettes, hard disks, removable hard disks, disk drives, printers, scanners etc., plus fans for processors and power units. The demands made on these items are ever more exacting as requirements for quality and speed increase. Even apparently trivial impurities can cause a device to develop a fault. In most cases, safety mechanisms provided in the devices will switch them off promptly. While this may keep down the damage, repair costs and downtime, nevertheless the device concerned will still be out of action.

Example:

A server had been placed in a media room which also contained a photocopying machine and a normal paper fax machine, and first the processor fan and then the power unit fan failed due to the high level of dust in the room. The failure of the processor fan caused the server to crash sporadically. Eventually the power unit fan failed also, causing the power unit to overheat and short circuit. This in turn induced the total failure of the server.

T 1.9 Loss of data due to intensive magnetic fields

Typical data carriers with a magnetic storage medium include floppy disks, removable disks, cartridges and tapes. Information is added to them by means of read/write heads. Such magnetised data media are sensitive to interfering magnetic fields, and for this reason they should not be brought into the vicinity of such radiation.

The data loss caused by this radiation depends in part on its intensity. This is particularly critical for files which, due to their internal formatting, are rendered completely useless even due to small variations (e.g. Postscript files, data bases).

Examples of sources of magnetic interference are:

- Electromotors
- Transformers
- Magnetic ID-card reading units.

T 1.10 Failure of a wide area network

If time-critical IT applications are executed on IT systems connected via wide area networks, the damage and consequential damage arising from a network failure is severe if no counter-measures are implemented (e.g. linkage to a second communications network).

Due to the liberalisation of the domestic German telecommunications market, Deutsche Telekom AG is not the only company which now offers services for data and voice communications. Many other network providers, some of them very small, compete mutually and with Deutsche Telekom by offering low communications rates. Customers should therefore inform themselves about the actual quality of this service by requesting detailed information on backup strategies and contingency measures from the network providers.

T 2 Threats Catalogue Organisational Shortcomings

T 2.1 Lack of, or insufficient, rules

T 2.2 Insufficient knowledge of requirements documents

T 2.3 A lack of compatible, or unsuitable, resources

T 2.4 Insufficient monitoring of IT security measures

T 2.5 Lack of, or inadequate, maintenance

T 2.6 Unauthorised admission to rooms requiring protection

T 2.7 Unauthorised use of rights

T 2.8 Uncontrolled use of resources

T 2.9 Poor adjustment to changes in the use of IT

T 2.10 Data media are not available when required

T 2.11 Insufficient bandwidth planning

T 2.12 Insufficient documentation on cabling

T 2.13 Inadequately protected distributors

T 2.14 Impairment of IT usage on account of adverse working conditions

T 2.15 Loss of confidentiality of sensitive data in the UNIX system

T 2.16 Non-regulated change of users in the case of laptop PCs

T 2.17 Inadequate labelling of data media

T 2.18 Improper delivery of data media

T 2.19 Inadequate key management for encryption

T 2.20 Inadequate supply of printing consumables for fax machines

T 2.21 Inadequate organisation of the exchange of users

T 2.22 Lack of evaluation of auditing data

T 2.23 Security flaws involved in integrating DOS PCs into a server-based network

T 2.24 Loss of confidentiality of sensitive data of the network to be protected

T 2.25 Reduction of transmission or execution speed caused by Peer-to-Peer functions

T 2.26 Lack of, or inadequate, test and release procedures

T 2.27 Lack of, or inadequate, documentation

T 2.28 Violation of copyright

T 2.29	Software testing with production data
T 2.30	Inadequate domain planning
T 2.31	Inadequate protection of the Windows NT system
T 2.32	Inadequate line bandwidth
T 2.33	Siting of Novell Netware Servers in an insecure environment
T 2.34	Absence of, or inadequate activation of Novell Netware security mechanisms
T 2.35	Lack of auditing under Windows 95
T 2.36	Inappropriate restriction of user environment
T 2.37	Uncontrolled usage of communications lines
T 2.38	Lack of, or inadequate, implementation of database security mechanisms
T 2.39	Complexity of a DBMS
T 2.40	Complexity of database access
T 2.41	Poor organisation of the exchange of database users
T 2.42	Complexity of the NDS
T 2.43	Migration of Novell Netware 3.x to Novell Netware Version 4
T 2.44	Incompatible active and passive network components
T 2.45	Conceptual deficiencies of a network
T 2.46	Exceeding the maximum allowed cable/bus length or ring size
T 2.47	Insecure transport of files and data media
T 2.48	Inadequate disposal of data media and documents at the home work place
T 2.49	Lack of, or inadequate, training of teleworkers
T 2.50	Delays caused by a temporarily restricted availability of teleworkers
T 2.51	Poor integration of teleworkers into the information flow
T 2.52	Longer response times in the event of an IT system breakdown
T 2.53	Inadequate regulations concerning substitution of teleworkers
T 2.54	Loss of confidentiality through hidden pieces of data.
T 2.55	Uncontrolled use of electronic mail
T 2.56	Inadequate description of files

T 2.57	Inadequate storage of media in the event of an emergency
T 2.58	Novell Netware and date conversion to the year 2000
T 2.59	Operation of non-registered components
T 2.60	Strategy for the network system and management system is not laid down or insufficient
T 2.61	Unauthorised collection of person related data
T 2.62	Inappropriate handling of security incidents
T 2.63	Uncontrolled use of Faxes
T 2.64	Lack of or defective rules for the RAS system
T 2.65	Complexity of the SAMBA configuration
T 2.66	Lack of or inadequate IT Security

T 2.1 Lack of, or insufficient, rules

The importance of organisational regulations and requirements for IT security objectives increases with both the level of information processing and the protection requirements of the information to be processed.

Ranging from the assignment of responsibilities to the distribution of control functions, the spectrum of regulations can be very broad. The effects of a lack of, or insufficient documents detailing requirements, are described in T 2.2 ff.

The following **examples** illustrate the potential deleterious effects of regulatory deficits:

- Insufficient resource management, e.g. the mere failure to re-order printing paper, can seriously impair on-schedule operations in a computing centre.
- In addition to the procurement of hand-held fire extinguishers, their maintenance must also be provided for so that they are ready for operation in case of fire.

T 2.2 Insufficient knowledge of requirements documents

Determining requirements documents alone does not guarantee undisturbed IT operations. The requirements documents which apply to a certain person must be known to that person. The damage which can be caused by insufficient knowledge of the existing requirements documents should not be excused by the statement: "I didn't know it was my responsibility" or "I didn't know what to do".

Examples:

- If employees are not informed of the handling procedure of incoming floppy discs, the danger is that a computer virus may be spread throughout the company/agency.
- Waste paper bins of different colours were distributed within a federal agency, of which one colour was intended for the disposal of documents. Most employees were not aware of this requirements document.

T 2.3 A lack of compatible, or unsuitable, resources

Insufficient provision of resources can disrupt IT-related operations considerably. An insufficient amount of required resources, or failure to provide them in due time, can result in a discontinuity of service.

Similarly, it may happen that unsuited or even incompatible resources are procured which consequently cannot be used.

Examples:

- The forthcoming transition to the year 2000 can cause compatibility problems in the hardware and software used.
- For a newly leased *Datex P* line the payment for the installation initially fails to be transferred to the network operator and the connection is therefore not enabled. As a result, commissioning of the IT procedure intended to use this line is delayed.
- An unsuitable resource is, for instance, a graphical user interface that is installed on a computer with insufficient performance.
- An example of incompatible resources are interconnecting cables of varying pin assignment for connecting printers.
- The main memory or hard-disk space on a computer is not sufficient to allow the operation of a database using new standard database software.

T 2.4 Insufficient monitoring of IT security measures

Following the introduction of IT security measures (e.g. data backup), their consistent realisation is often incumbent on the users. Where no monitoring, or inadequate monitoring, of IT security measures takes place, neither abuse nor effectiveness can be verified. A due reaction is thus not possible.

In addition, there are IT security measures which can be effective only when appropriate controls are implemented. These include, for example, auditing functions, the security capabilities of which will take effect only after evaluation of the auditing data.

Example:

An administration desk of a computer system is connected to a console printer. All user input from the console is to be logged to the printer. It is only by means of an analysis of the print-outs that any improper action by the administration can be detected. Where such an analysis fails to be made by an independent person, logging will be ineffective.

T 2.5 Lack of, or inadequate, maintenance

Operability of the system used must be ensured on a continuing basis. Regular maintenance can enhance assurance of continuous service. Lack of, or insufficient maintenance can result in incalculable damage and late effects.

Examples:

- Due to a lack of maintenance, the batteries of an uninterruptible power supply (UPS) system are no longer sufficient (too little acid), and thus t he UPS system cannot ensure power supply for a sufficiently long period.
- Due to deficient maintenance, the pressure of fire extinguishers has dropped to a point where they no longer retain their fire-fighting effect.
- Overheating results in the failure of a laser printer because a ventilation grid has not been properly cleaned.

T 2.6 Unauthorised admission to rooms requiring protection

If unauthorised persons enter protected rooms, hazards may be entailed not only by deliberate acts, but also by inadvertence. Disruption is caused merely by the fact that checks must be made for potential damage as a result of the unauthorised access. In this context, domestic rooms used for business purposes should also be considered as security areas.

Example:

Temporary help is employed to substitute for cleaning staff on vacation. The stand-in cleaner, without any instructions to this effect, decides to clean the computing centre. She opens the emergency exit and thus trips the alarm.

T 2.7 Unauthorised use of rights

Rights of admission and of access to hardware and software are applied as organisational measures to ensure secure and proper use of IT systems and processes. If such rights are granted to the wrong person, or if a right is abused, the result may be a variety of hazards which can impair the confidentiality and integrity of data or the availability of computer performance.

Example:

During the absence of the archive keeper, a work scheduler who is not authorised to have access to the data medium archives takes some magnetic tapes for the purpose of making backup copies. Due to such uncontrolled removal of media, the inventory list of the data medium archives is not updated, and the tapes cannot be located during this period.

T 2.8 Uncontrolled use of resources

Resources - of any type - may only be used for their designated purpose. The persons responsible for the procurement and use of resources must both prevent their uncontrolled use and monitor their correct use. Inadequate control of the use of resources can entail multifarious risks.

Examples:

- Use of private data media by staff members may lead to virus infection of company PC's.
- Use of wrong cleaning products can damage the VDUs.
- The wrong type of ink for an ink jet printer can result in the soiling or malfunction of the printer.

T 2.9 Poor adjustment to changes in the use of IT

The rules created for IT applications and the application environment are subject to permanent change. This is due to changes in the staff, moving of employees to different rooms, usage of new hardware or software, or changes in the supply chain. The following examples show that risks may be incurred if the required organisational adjustments are not properly taken account of:

- Staff members forget to transfer the necessary file access rights to the person who is to take over from them while they are on holiday. This can cause delays in IT operations.
- On account of alterations to a building, changes are made to the previous escape routes. Due to insufficient information provided to the staff, the building cannot be evacuated within the required time.
- When an IT procedure is modified, a large quantity of printing paper will be required. If the procurement unit is not informed, continuity of IT operations and service will be impaired.
- On their arrival, electronic documents are not scanned automatically for macro viruses, as this problem is not known yet, or no virus scanning programs are available.
- Before electronic documents are transferred, no care is taken to ensure that they have been stored in a format which is readable by the recipient.

T 2.10 Data media are not available when required

Correct use of data media is of particular importance to IT processes. Even minor faults - e.g. insufficient marking, unsuitable storage site, lack of input or output acknowledgements in the data media archive - can be the reason why a data medium cannot be located within the required time. The resultant delays can cause significant damage.

Examples:

- By mistake, backup tapes are stored in an external data backup archive. A required data recovery is delayed considerably as it is not possible to obtain the tapes immediately.
- By mistake, backup tapes with different contents are labelled identically. The archive keeper inadvertently releases the most recent tape for deletion. Consequently, only an outdated backup will be available.

T 2.11 Insufficient bandwidth planning

A mistake frequently made when planning networks is to dimension bandwidth solely on the basis of the current requirements. This approach fails to take account of the fact that

- the need for expanding a network can never be ruled out;
- the bandwidth of the network has to be enlarged due to increasing data transfer requirements.
- due to new requirements to be met by the given network, other cables have to be installed;

Expansion of the network will be possible only to the extent permitted by the installed cables or by the availability of space for additional cables. Especially in the case of covered wiring (piping, plaster-covered conduit subways, etc.), even where space is available, it is often impossible to insert additional cables without damaging new or old cables. The only alternative here is to pull out the existing cables and to draw in all cables, old and new, at the same time. The resulting operational hindrance and costs can be considerable.

T 2.12 Insufficient documentation on cabling

If, as a result of insufficient documentation the precise location of lines is not known, the consequence may be damage to these lines caused by construction work outside or within a building. This can entail prolonged downtime periods or even life-threatening hazards, e.g. due to electric shock.

Insufficient documentation can, however, also make it more difficult to test, maintain and repair lines and jumpers, i.e. in case of changes to the area of new terminal equipment (relocation, new access).

Example:

In a larger-sized agency, cabling for the IT facilities was carried out by an external firm. The compilation of documentation was not included in the service package. Since no maintenance agreement was concluded with that firm after the completion of cabling, the required documentation was not available to the agency. Network expansion could only be achieved with considerable delays.

T 2.13 Inadequately protected distributors

Distributors of the supply mains are often freely accessible and kept unlocked in corridors and staircases. Thus, any person can open these distributor boxes, make manipulations, and possibly cause a power failure.

T 2.14 Impairment of IT usage on account of adverse working conditions

A workplace not organised according to ergonomic requirements or the operational environment (e.g. dust or noise nuisances) may be the reason why no use, or no optimum use, can be made of the available IT facilities.

For the major part, the conceivable faults do not have a direct impact on IT facilities. Rather, staff members will be affected in such a way that they cannot perform their tasks with due concentration. Such affects can be due to extensive noise, unorganised customer visits, inappropriate room lighting or bad air conditioning First signs of these disturbances are a decrease in efficiency and an increase in small errors (incorrect spelling, etc.) This will not only affect the direct results of work, i t will also introduce errors into stored data and reduce the data integrity.

T 2.15 Loss of confidentiality of sensitive data in the UNIX system

By means of various UNIX programmes it is possible to read/extract user-related data held in the IT system. This also covers data which can furnish information on the user performance profile. Therefore, attention must be paid both to privacy protection aspects and to the risk that such information may facilitate abuse.

Example:

With a simple program which, at certain intervals analyses the information provided by the *who* command, any user can extract a precise utilisation profile for an account. In this way it is possible, for instance, to establish the periods of absence of the system administrator(s) in order to exploit these absences for illicit acts. Also, it can be established which terminals are approved for privileged access.

Other programs with similar abuse possibilities are *finger* or *ruser*.

T 2.16 Non-regulated change of users in the case of laptop PCs

A change of the users of portable PCs such as laptops or *notebooks* is often affected by the mere handing over of the computer. As a result, users frequently fail to check whether the computer still holds sensitive data or is carrying a virus. Also, after a certain lapse of time, it will no longer be possible to establish who has used the portable PC at what time and who is using it at present. Thus, non-regulated change of users without memory checks or proper documentation can result in reduced availability of the computer, and in the loss of confidentiality of the residual data on the hard disk.

T 2.17 Inadequate labelling of data media

If the exchanged data media are not labelled properly, the recipient is frequently unable to identify the sender, the stored information, or its purpose. If the same sender is stated on several data media, inadequate labelling might lead to disruption of the correct sequence.

Example:

A floppy disk containing data with a main focus on integrity of data is sent from user ‘A’ to recipient ‘R’. The next day user ‘A’ recognises that there were errors within the data. He sends a corrected version and announces the new version to the recipient by telephone. The second floppy disk overtakes the first one in the mailing process, and as a result of insufficient labelling, the recipient assumes that the first floppy disk received carries the wrong data.

T 2.18 Improper delivery of data media

If data media are delivered improperly, confidential data stored on these media may fall into the hands of unauthorised parties or fail to reach their correct destination on time.

Examples:

- Faulty addressing can cause the data media to be delivered to an unauthorised recipient
- Inadequate packaging can cause the data media to be damaged and/or allow unauthorised access which might not be discovered immediately
- lack of allocation of responsibilities at the receiving end may lead to delayed processing of the data medium
- Unspecified or incorrect types of dispatch might delay the arrival of data media
- lack of allocation of responsibilities by the responsible party at the transmitting end may cause a delay in the delivery of data media.

T 2.19 Inadequate key management for encryption

If cryptographic systems are used for protecting the confidentiality of data to be transferred, inadequate key management can undermine the required protection if:

- cryptographic keys are generated or stored in an unprotected environment
- unsuitable or easily-guessed cryptographic keys are used
- encryption or decryption keys are not sent to the communication partner by means of a safe avenue.

Examples:

- The simplest **negative example** of this can be the dispatch of encrypted information **and** the cryptographic key on the same floppy disk, provided that the encryption method is known.
- Cryptographic keys are usually generated by random processes and may be post-worke.If the source of random numbers is unsuitable, insecure keys may be produced.
- It is vital for security that the cryptographic keys generated are not weak, particularly in the case of masterkeys. Weak keys can be keys that are easily guessed or keys which are unsuitable for encryption (e.g. weak and semi-weak DES keys). If it is not checked whether keys are weak when they are derived from masterkeys, then weak keys may come into active use.
- If identical partial keys are used in the triple DES algorithm, the triple DES encryption only has the effect of a simple DES encryption. The gain in security is lost.

However, it is not only the disclosure but also the loss of cryptographic keys that can cause substantial problems. Cryptographic keys can

- be lost or forgotten,
- cease to be available, for example if the person in possession of the key has left the firm, or
- be destroyed in that they are accidentally deleted or in that they are changed, e.g. through a data media failure or bit errors.

If keys are no longer available, data protected by them can no longer be decrypted or tested for its authenticity.

T 2.20 Inadequate supply of printing consumables for fax mT 2.21 Inadequate organisation of the exchange of users

In the case that several users work on one IT system at different times, an exchange of users is inevitable. If this is not adequately organised and administered, it may not fulfil security requirements. This can be open to abuse if:

- current applications are not closed correctly,
- current data are not saved,
- data remain in the main storage or in temporary files,
- the previous user does not log off,
- the new user does not correctly log on to the IT system.

T 2.21 Inadequate organisation of the exchange of users

In the case that several users work on one IT system at different times, an exchange of users is inevitable. If this is not adequately organised and administered, it may not fulfil security requirements. This can be open to abuse if:

- current applications are not closed correctly,
- current data are not saved,
- data remain in the main storage or in temporary files,
- the previous user does not log off,
- the new user does not correctly log on to the IT system.

T 2.22 Lack of evaluation of auditing data

Auditing data provide a possibility to detect a posteriori a breach of security or an attempt to do so. Auditing data can thus be used to identify the perpetrator in case of damage. A further important function of the auditing data is deterrence. If auditing data are evaluated on a regular basis, intentional attacks can be detected at an early stage. If the auditing data are not, or are inadequately evaluated and this becomes known, they lose their function as a deterrent.

Many IT systems or applications lack sufficient possibilities for auditing. In some cases auditing is not provided for at all and in other cases it is often not possible to make distinctions in the auditing according to events.

Example:

On a stand-alone Windows 95 computer it is not possible to log the activities of one or more users on a user-specific basis. Therefore, it cannot be determined if security has been impaired or an attempt to impair security has occurred.

T 2.23 Security flaws involved in integrating DOS PC's into a server-based network

When integrating DOS PC's into a server-based network, security flaws may arise in a network which would normally be secure.

If, for example, DOS-PCs are connected to a UNIX-network, then the use of UNIX services such as *telnet*, *ftp*, NFS, RPC's, and X-Windows is possible. The security problems arising are basically no different to those on a pure UNIX network.

However, when integrating DOS-PCs into a server-based network, additional uncontrolled network access may be created. Every network access point can be misused to tap into the network. By using appropriate software, Sniffer, this is also possible with a PC connected to the network. In this case it is very easy to listen to, and to misuse, all kinds of information, such as passwords and file contents that are transmitted over the network.

A PC user can also generally administer the PC himself. If he/she configures it to feign a false identity, he/she can use approved services such as NFS or RPC's to gain access to directories and files of other users from the server. This information can then be read, copied, forged or deleted without the knowledge of others.

DOS PCs integrated into a Windows NT network create a potential threat to the security of this system. Therefore, when copying files from the server to the hard disk of a PC, information relevant to the security of the system will be stored in a physically unsatisfactory manner, or when copying files to a local floppy disk drive, such information may be sent on to external destinations without being recorded by the auditing functions of the server. On the other hand there is the danger of importing a computer virus from a floppy disk drive which is not adequately protected.

T 2.24 Loss of confidentiality of sensitive data of the network to be protected

If a network that is not protected by a firewall is connected to an external network such as the Internet, various data from the internal network including mail addresses, IP numbers, computer and user names, can be retrieved by the external network. From this data, information can be deduced about the internal network architecture and its users. The more information an invader has about potential targets of attack, the more opportunities he has to infiltrate If an invader knows, for instance, user names of an IT system, he can try to guess the associated passwords or find them through dictionary hacking (see also T 5.18 *Systematic Trying Out of Passwords)*.

T 2.25 Reduction of transmission or execution speed caused by Peer-to-Peer functions

If one of the operating systems WfW, Windows 95 or Windows NT constitutes the basis for the user interface in a server-based PC network, single Peer-to-Peer functions may restrict the transmission bandwidth in the server-based network, as the same physical medium is being shared. For example, the file access from a server will be delayed considerably if large files are being copied from PC to PC using peer to peer functions.

Within a Peer-to-Peer network a single PC can be configured as Server, meaning it can act as an application server or as a file server for other computers. During its work the Peer-to-Peer functions cause an additional system load, reducing the performance of the computer significantly.

T 2.26 Lack of, or inadequate software test and release procedures

If new hardware or software is inadequately tested or not tested at all, and released without installation instructions, errors in the hardware or software may either not be identified or essential installation parameters may not be recognised or considered. These hardware, software or installation errors resulting from software and release procedures that are inadequate or lacking altogether, can result in a considerable threat to IT operation.

In the confidence that you will be able to install new hardware or software without difficulty, it is often not considered that the potential damage is completely out of proportion to the costs of carrying out a proper test- and release procedure. Programs or IT systems that have been inadequately tested and that still contain errors are integrated in the production environment. These errors then have a disruptive effect on programs that had until then been working satisfactorily.

Examples of such damage are listed below:

- Programs or program updates cannot be used effectively because more resources (e.g. RAM, disk space) than expected are needed to achieve a reasonable processing speed.. If this is not detected during test runs it can lead to considerable amounts of unusable investments. Decisions against further investments often lead to the result that a software product, which was ordered and paid for regularly, could never be used.
- Routine procedures can be badly held up after the installation of new software. The benefit originally envisaged when the program was installed only becomes apparent much later, as the key staff were not trained or informed about the new program functions.
- If a new, updated DBMS software version containing bugs is loaded, the database will no longer be available, and a loss of data might occur.

T 2.27 Lack of, or inadequate documentation

Various forms of documentation may be considered: the product description, the administrator and user documentation required to use the product, and the system documentation.

If documentation on the IT components used is inadequate or lacking, this can have significant effects both on the selection and decision-making processes regarding a product, and in terms of damage occurring during actual operation.

If the documentation is inadequate in the case of damage such as hardware failure or malfunctioning of programs, error diagnosis and rectification may be delayed considerably or rendered completely impractical.

Examples:

- If a program stores working data in temporary files without sufficient documentation of that process, this can lead to the situation that temporary files are unsuitably protected and confidential information being exposed. If these files are not sufficiently protected against user access, or if sectors which are only used temporarily are not correctly deleted physically, information can become accessible to unauthorised persons.
- When a new software product is installed, existing configurations are changed. Other programs which have run correctly hitherto are then incorrectly parameterised and crash. If the changes resulting from the installation of new software were described in detail, the error could be located and eliminated in less time.

T 2.28 Violation of copyright

The use of unlicensed software can be a violation of copyright and lead to both civil and criminal penalties.

Agencies and companies where pirate copies are used may be made liable for damages by the copyright owner under corporate liability, irrespective of the type of offence (intention or gross negligence).

Example:

In an organisation a large number of graphical user interfaces were used without the necessary licences. The costs of having them retrospectively licensed, and the damages payable to the copyright owner, far outweighed the cost of the licences.

T 2.29 Software testing with production data

Frequently it happens that software tests are being performed with production data. The main reasons given for this are that the only way to make a definitive assessment of the functions and performance of the product is to compare it directly with existing, operating data. Additional reasons for doing this are inadequate security awareness, exaggerated confidence in the software under test, and ignorance of potential damage.

Testing with production data may result in the following problems:

- Software is tested with copies of production data in an isolated test environment:

  If new software is tested with data which has not been made anonymous, unauthorised employees or third parties who have been put in charge of testing the software may gain access to files carrying information which are confidential.

- Software is tested with production data in actual operation:

  Software which malfunctions under test may, as in the before-mentioned case, lead not only to impaired confidentiality but also to a loss of integrity and availability of production data.

  Because different programs may be incompatible, side effects can arise which may lead to significant impairments in other system components. In the case of networks this may range from loss of performance through to a crashing of the network.

  If software under test performs incorrectly or operating errors are made, production data may be inadvertently modified. It is possible that such a modification may not be able to be identified. To avoid redundancy, databases are increasingly shared by different programs, so that these errors potentially have an effect on other IT applications as well. When damage occurs there are not only costs involved in reconstructing the data but, existing working data must also be checked for integrity.

T 2.30 Inadequate domain planning

Inadequate planning of domains and their trust relationships in a Windows NT network can lead to a situation in which trust relationships exist for domains which should not be regarded as trustworthy. Thus, it may be possible for users of the domains concerned to access resources of the trusting domain without this being intended or even recognised. This can occur particularly if the access rights of the trusting domain were configured in a relatively broad way on the assumption that no other domain could access the local resources.

Conversely, the absence of trust relationships between domains can lead to a situation in which users have to authenticate themselves in an unnecessarily explicit way in the case of outside domains, leading to confusion when there is a lack of co-ordination of passwords between these domains. The user now has to remember a large number of passwords that can lead to security being impaired when he/she notes down such passwords.

T 2.31 Inadequate protection of the Windows NT system

Windows NT is supplied with very extensive access rights to the file system and to the registry. If these access rights are not set out more strictly after installation according to local security requirements, every user effectively has access to all files and to the entire registry, i.e. access protection is eliminated de facto.

Furthermore, Windows NT is not able to check access to floppy disk drives, CD-ROM drives and tapes. As a result data can be imported and exported improperly if access to these data media has not been restricted or at least checked at an organisational level by additional safeguards.

T 2.32 Inadequate line bandwidth

A mistake frequently made when planning networks is to dimension bandwidth solely on the basis of the current requirements, disregarding the fact that the network will be subject to ever-increasing bandwidth requirements, e.g when new IT systems are integrated into the network or when the amount of transmitted data increases.

When the bandwidth of the network is no longer sufficient, the transmission rate in the network is severely restricted for all users. File access in remote IT systems is slowed down considerably, for example, when the available network bandwidth has to be shared with other users, initiating a high amount of network traffic(capacity is subject to a high level of utilisation by other users), such as applies when large files are transferred from one IT system to another.

Example:

An organisation with several sites installs a network based on ISDN-S_0 lines for data communication. After the installation of a GUI based Intranet, the data communication nearly broke down. Finally, only a switch to S_{2M} communication channels provided the necessary network bandwidth.

T 2.33 Siting of Novell Netware Servers in an insecure environment

Siting of Novell Netware servers in an insecure environment (e.g. corridors, unlocked server rooms) creates a considerable threat to IT security.

Direct input into the server-console or loading of NLMs (Netware Loadable Modules) can cause deactivation of the installed security measures, without the administrative personnel i.e. IT security-management being aware of this.

Example:

By loading special NLMs, it is possible to create a user equivalent to a supervisor. That is to say, an existing user can get the same privileges as a supervisor.

T 2.34 Absence of, or inadequate activation of Novell Netware security mechanisms

The network operating system Novell Netware 3.x has a number of security mechanisms which protect against unauthorised access to server files.

However, these security mechanisms will not be activated automatically. They must be set-up by the system administrator after the primary start of the server.

If the security mechanisms of a Novell Netware server are not installed, or if they are insufficiently installed, unauthorised access to files which have to be protected are likely to be considerably easier.

T 2.35 Lack of auditing under Windows 95

On a stand-alone Windows 95 computer it is not possible to log the activities of one or more users on a user-specific basis. Therefore, it cannot be determined if security has been impaired or an attempt to impair security has occurred.

Note:

The content of this threat has been integrated into T 2.22 Lack of evaluation of auditing data and is no longer used in any modules in version 1999 of the IT Baseline Protection Manual.

T 2.36 Inappropriate restriction of user environment

Various operating systems (e.g. Windows 95, Windows NT) and PC-security products offer the possibility of restricting the user environment on an individual basis for each user. Principally, two different possibilities exist to do this:

1. Certain functions are permitted and all others are prohibited.
2. Certain functions are prohibited while all others are permitted.

In both cases, there is the possibility of restricting the user in such a way that he/she may no longer be able to carry out essential functions, or that sensible and efficient work with the PC is no longer possible.

T 2.37 Uncontrolled usage of communications lines

During the use of communications cards in an IT system (fax, modem or ISDN cards), it is not always clearly evident whether any further data is also transmitted in addition to the user and protocol data. Once activated, a communications card is generally able to establish a connection to an undesired terminal, without any user activity. In addition, third parties may have access to remote functions which are not known to the user.

Examples:

- While configuring a fax card for the first time, the user is prompted by the installation program to enter the country code for Sweden.. This could imply that the manufacturer of the card wants information on the use of his/her product, possibly for marketing reasons.
- A large number of modem cards support remote access to IT systems. Although such access can be protected by certain mechanisms, some of which are integrated in the cards themselves (call-back option and call-number authentication), the related default settings, however, have not been made. An IT system configured like that can therefore be completely manipulated at will by external parties via the modem card.

T 2.38 Lack of, or inadequate implementation of database security mechanisms

Database software normally includes a number of security mechanisms that allow data to be protected against unauthorised access and similar intrusions. However, most of these mechanisms do not activate automatically and need to be activated manually from the database administrator. If none of these mechanisms is used, neither the confidentiality nor the integrity of the data can be guaranteed. In such cases, it is usually not possible to identify and log security violations. The consequences of this can range from the manipulation and loss of data to the destruction of the database.

Example:

In the case of the MS Access database, activation of the password is optional. Due to this it is quite possible to gain unauthorised access to the database and to therefore also have unauthorised access to all kinds of data stored inside the database. In this case, any auditing of database access is not possible.

T 2.39 Complexity of a DBMS

The selection and use of standard database systems requires careful planning, installation and configuration of the database management system (DBMS), thus ensuring trouble-free operation. The following examples are intended to elucidate the large variety of potential threats involved here.

Selection of an unsuitable standard database system:

- The selected DBMS cannot be executed in the designated runtime environment. This might be due to the fact that the DBMS is only compatible with a particular operating system or that the hardware used does not fulfil the minimum requirements.
- The selected DBMS constitutes a security risk because the security mechanisms provided by the manufacturer are not sufficient for ensuring the required availability, integrity and confidentiality of the data.

Incorrect installation or configuration of the standard database system:

- Further threats might be posed if the security measures recommended by the manufacturer are ignored or incorrectly implemented.

  Example: The log files of a database system were not mirrored, or the mirrored log files were not stored to another hard disk. A head crash causes inevitable destruction of the database.

- The physical distribution of the data is not sufficient (if the DBMS provides for physical distribution).

  Example: Inside an Oracle database the files per tablespace are limited. If all the data is being managed in the system tablespace, files can no longer be added once this maximum number has been attained. As the system tablespace also holds the data dictionary, this problem can only be solved through a complete reinstallation of the database.

- Parameters that are set incorrectly can prevent access to certain data.

  Example: Incorrect country settings in a database software program can prevent certain country-specific special characters from being displayed.

Poor database concept:

- Missing database relations between individual tables can impair the consistency of data and the integrity of the database.
- If application-specific data is not stored on separate physical media, the failure of a single hard disk can lead to the failure of all applications.
- If no database triggers or s*tored procedures* are used, inconsistencies might arise in the data if an application, itself, does not take this into account..
- The poor concept regarding the use of database triggers and *stored procedures* can impair the integrity of data and result in uncontrolled manipulations.

T 2.40 Complexity of database access

A database management system (DBMS) is used to access one or more databases. This access can take place directly or via an application. To ensure the integrity of a database, all access to it must be controlled from a central point of administration. The complexity of such access procedures can result in the following problems:

Incorrectly designed user environment

- If access rights for database users are too restrictive, this might prevent certain tasks from being accomplished.
- If access rights for users are too loosely defined, this might lead to the unauthorised manipulation or browsing of data. This will also violate the integrity and confidentiality of the database.
- If users are allowed to access a database directly (instead of via an application), this might damage the integrity of the database through data manipulations whose consequences cannot be foreseen by the users.
- If database objects are not protected explicitly by the accessing applications through the use of an appropriate concept of authorisation and access, this could result in the manipulation of such database objects (e.g. a modification of table fields or indices). The database could be destroyed as a result.

Remote access to databases

- If a database is made accessible within a network, inadequate security safeguards for remote access procedures might allow the manipulation and unauthorised browsing of data. This will also violate the integrity and confidentiality of the database.

Database queries

- The total number of possible database queries must be restricted for each user and certain queries must be prohibited explicitly. Otherwise the confidentiality of sensitive data might be violated (particularly in the case of statistical databases).
- If database queries from a certain application are not implemented in accordance with the SQL standard, the DBMS might not be able to execute and may therefore reject such queries (especially if database management systems from different vendors are in use).
- Database queries which have not been specified precisely may supply incorrect or unexpected results if the database objects have been modified.

  Example: The query "SELECT * FROM table" returns all the attributes/fields of a tupel/data record. If a field is now added to, or deleted from this table, fatal consequences may arise for applications which make use of this query.

T 2.41 Poor organisation of the exchange of database users

In situations where several users of a database share the same workstation, inadvertent or deliberate data manipulations might result if the changes between these users are poorly organised or undertaken incorrectly. Here too, the confidentiality of the data is no longer guaranteed.

Example:

If an application that accesses a database is not exited correctly before a change of user occurs, the different authorisation profiles of the affected users will give rise to the afore-mentioned threats. This will also subvert the logging function of the database that records the data modifications, and also those tasks performed under the active user ID. However this ID will no longer correspond to the user who is actually logged in.

T 2.42 Complexity of the NDS

NDS (Netware Directory Services) allows the installation of a shared, decentralised directory database of all logical and physical resources within a network. Each network resource is represented by a unique entry in this database, regardless of the actual location of the resource. Access to the network or a network resource is not performed via a particular Netware 4.x server (as opposed to Novell Netware 3.x), but via a directory service of the Novell network (refer to S 2.x5 *Design of an NDS concept*).

The NDS is the central resource management component of Novell Netware 4.x, and subsequently, high demands are placed on the correct functioning of this component. The complex possibilities of administration here can result in the impairment of the availability, confidentiality and integrity of the data, and give rise to the following threats:

- Access to the network by a user requires authentication to the NDS. This login takes place on the nearest Netware 4 server that contains the master partition of the directory tree, or at least a copy of it. If an insufficient number of copies is present in the network, all users will require authentication on the same server. Each login places an additional load on the server and the network. This can result in delayed response times during login procedures and impair the availability of resources.

  If no copies of the master partition have been placed on other Netware 4 servers, the occurrence of an error in the NDS database makes it impossible to log into the network.
- The higher the number of organisations and sub-organisations within a directory tree, the greater the administrative effort required. In addition to that, the localisation of network resources becomes more and more complicated for the administrators and for the users
- If a location in a WAN does not hold a copy of the related local partition, a failure of the WAN makes it impossible to log into the network from that location.
- The higher the number of copies of a partition created in a WAN, the greater the volume of traffic in the WAN will be, due to the fact that the login date needs to be changed in all copies of the partition each time a user logs in.
- The various versions and patch levels of Novell Netware Version 4 can also hold different versions of the *DS.NLM* module. However, this information is used by the Netware 4-servers to filter requests for modification to the NDS database. This can prevent the Netware 4 servers from notifying each other of changes to the NDS data, thus resulting in inconsistencies.

T 2.43 Migration of Novell Netware 3.x to Novell Netware Version 4

If both Netware 3.x and Netware 4.x servers are present in a network, a distinction can basically be made between two different types of scenario:

- The Netware 3.x servers were migrated, and thus integrated in the NDS
- Netware 3.x and Netware 4.x servers operate in parallel operation mode

The following real threats can arise in this context:

- During the migration of a Netware 3.x server, most of its NLMs will be replaced so that it can be controlled by the Netware administrator from a Netware 4.x server. Elaborate measures would be required in order to separate such a migrated Netware 3.x server from its appropriate Netware 4.x server so that it is capable of acting again as an independent Netware 3.x server within the network.
- If no bindery emulation was activated on the Netware 4.x server after the migration of a Netware 3.x server users will no longer be able to log into the Netware 4 network with the old client software.
- If the Netware 3.x servers operate separately as an independent network, a great deal of administration is required, because in this case all users will be administrated not only from all the Netware 3.x servers, but also the NDS.

T 2.44 Incompatible active and passive network components

Incompatible active network components can cause problems with communications protocols which have not yet been standardised completely, such as ATM or Tag switching. In such cases, the manufacturer needs to employ proprietary implementations to offset the missing, or partially available standards and allow for the use of the affected communications protocol.

Incompatibilities of this type can be caused if existing networks are extended with active network components from another vendor or networks are built using components from different vendors.

If active network components with different implementations of the same communications protocol are running parallel within the same network, this may impair the availability of the entire network, individual segments, or some services within the network. Two different cases can be distinguished depending on the type of incompatibility:

- Implementations of a communications protocol which are not able to operate with each other, can make communication between the related components impossible.

  Example: ATM components might use different signalling protocols which are not able to operate together, e.g. in compliance with UNI (User Network Interface) Version 3.0 and UNI Version 3.1.

- Even if active network components are able to operate together in principle, certain services might be implemented in different ways. As a result, these services may be unavailable or at least not available in some segments of the network, although communication outside the scope of these services is still possible.

  Example: Proprietary implementations of redundant LAN emulation servers for ATM networks are in existence. If an ATM network consists of two ATM switches, one of which possesses such a proprietary implementation while the other does not, communication based on LANE (LAN Emulation) is still possible, but the service implemented on a proprietary basis cannot be used.

A combination of incompatible, passive network components can also impair the availability of a network. Twisted-pair cables available in 100-ohm and 150-ohm designs cannot be used parallel without the use of the proper converter. An unsuitable combination of active and passive network components can also impair availability if, for example, a network access protocol is used for a medium which has not been foreseen for this purpose. For instance, ATM is not able to work with a 50-ohm coaxial cable.

T 2.45 Conceptual deficiencies of a network

Correct planning of the installation and expansion of a network decisively determines the success of all network operations. Progressively shorter innovation cycles in IT pose a particular challenge to networks which cannot meet the new requirements due to their design, and therefore easily create bottlenecks:

- A network must be designed in accordance with the requirements of network users (e.g. workgroups) as regards the confidentiality of data and the integrity of the network. Otherwise, confidential data of a particular workgroup could be read by other, unauthorised network users. The confidentiality of data can also be violated through the relocation of individual workgroup members or entire workgroups if it is not possible to configure new confidential domains in the network or reconfigure existing ones. This threat also applies to the integrity of the network or segments thereof.

  Example: A subnetwork separated by a router was configured for a workgroup that had special requirements as regards the confidentiality and integrity of data. Because of the routing of cables this segment was confined to one single building. If several members of this workgroup were later relocated to a different building, they would then need to communicate via the standard, productive network. As a result, the confidentiality and integrity of the data could no longer be ensured.

- If new applications with higher bandwidth demands than were foreseen during the planning phase are placed within the network, this can easily impair the availability of the entire network if conceptual deficiencies in its infrastructure no longer allow adequate scaling (loss of availability due to overload). Depending on the existing segmentation of the network, the loss of availability might only affect individual segments.

  Example: For historical reasons, many existing networks which have been expanded during the course of time contain, in many cases, backbone segments with a lower maximum bandwidth, such as Token-Ring or Ethernet segments. The restricted transmission rates in these backbone segments affect the availability of the entire network during periods when the load is high.

- Networks intended exclusively to connect proprietary systems can also suffer a loss of availability if they are connected to non suitable systems (loss of availability due to network components which cannot operate together).

  Example: Proprietary networks are used primarily in the mainframe sector for connecting mainframes with their terminals. Such networks are often intended for terminal or printer operation only and are not suitable for other architectures (e.g. Ethernet). This applies to the installed cables as well as the active network components. If an attempt is made to exceed this scope, the proprietary network usually becomes unavailable. One possibility of integrating two different architectures is to create a connection via a gateway.

- The use of active network components which are not designed for use with certain protocols might prevent the use of these protocols or of additionally required services.

  Example: A network consisting exclusively of active components which only support IP routing or IP switching does not allow a Novell NetWare network operating system to be run on a SPX/IPX basis.

- The use of passive network components which impose restrictions on the possible network access protocols might prevent future scaling of the network.

  Example: A network consisting exclusively of 50-ohm coaxial cables does not allow the use of ATM. Networks consisting of 150-ohm twisted-pair cables do not allow the use of 100-ohm Ethernet components. Such conceptual deficiencies, partly historical in nature, require costly changes to the network infrastructure.

Although a network can have a neutral design with respect to applications, systems and services, the use of highly heterogeneous components can give rise to high maintenance requirements which might exceed the scope of ability of the operating personnel. This can impair the availability of the network if failures or malfunctions on passive or active network components cannot be remedied quick enough due to a lack of personnel capacity.

T 2.46 Exceeding the maximum allowed cable/bus length or ring size

In accordance with the types of cable, topology and transmission protocols involved, maximum cable and bus lengths, as well as maximum ring sizes for networks have been stipulated in order to ensure the functions of the network as defined by applicable standards. Excessively long cables and buses, as well as excessively large rings, prolong signal transmission times beyond the limit specified for the type of transmission protocol involved, thus reducing the availability of the network segment or the communications bandwidth.

The phenomena which can occur depend on the type of the access control method used:

- In the case of network segments which use the CSMA/CD (Carrier Sense Multiple Access/Collision Detection) access method, all stations have the same access rights to the medium, although it can only be used by one station at a time. For this purpose, every station first checks whether the medium is free for use (carrier sense). If so, the station starts the transmission of data. If several stations carry out this procedure in a parallel context (multiple access), a collision occurs and is recognised by all sending stations (collision detection), whereupon the medium is checked again and transmission is repeated.

  If the maximum defined signal propagation delay is exceeded on the medium, collisions might not be detected in the specified time interval (collision detection). This means that one end appliance already started to transfer data while another end appliance still assumes the transfer medium to be free. In this case, so-called late collisions occur, thus corrupting the affected data packet and, depending on the length of the data packet, the medium may be blocked beyond reasonable limits. This can severely impair the effective transmission bandwidth of the medium. Although individual data packets might be discarded in this process, the network access protocol normally prevents data from being lost. For example, Ethernet and Fast Ethernet use the CSMA/CD communication protocol.

- Transmission techniques based on the token passing procedure use a special data packet (named token) to determine which station may occupy the medium. A station which receives this token occupies the medium and, in accordance with the token passing procedure in use, passes the token on to the next station. This ensures that the medium is only occupied by a single station at one time.

  Synchronous data transmission at a constant bit rate is a characteristic of network segments using token passing procedures. When the medium is busy, the relevant time intervals are used to transmit the data packets. When the medium is free, these time intervals are used to forward the token. If the maximum signal propagation time is exceeded, the constant bit rate specified for the transmission protocol in use can no longer be guaranteed, thus causing a break down of all communication. For example, Token Ring and FDDI use the token passing procedure.

Increasing the cable length not only prolongs signal propagation time but also increases the signal attenuation. If the cable length exceeds the maximum value specified in the applicable standard, the resulting signal attenuation could be high enough to prevent the system from distinguishing between the various signal levels as specified in the standard. In this case, communication can no longer be ensured along the entire length of the wires or optical fiber cables that are in use.

T 2.47 Insecure transport of files and data media

During the transport of documents, data media and files between the institution and other locations, such as the workstation at home, there is a danger that these items may be:

- lost
- stolen
- viewed or manipulated, or
- given to an unauthorised recipient.

Damage, loss of confidentiality, or manipulation may cause serious damage particularly in the case of unique items of which copies do not exist.

T 2.48 Inadequate disposal of data media and documents at the home work place

If a proper disposal of data media and documents from the working place at home is not possible, it could be possible for third parties to fully or partially extract data from documents and data carriers which have been disposed of. The consequential damage depends on the value of the information extracted.

T 2.49 Lack of, or inadequate, training of teleworkers

At their home working place teleworkers have to rely mainly on themselves. This means that they have to be more familiar with the IT systems in use than their colleagues at the institution who are usually able to receive quick assistance from IT specialists on location. If a telecommuter is not adequately familiar with the IT systems in use, this may result in longer down times when problems arise. For example, when an IT specialist needs to travel from the institution to the telecommuter's working place at home in order to solve the problem there.

Example:

The teleworker should be able to create backup copies on his own. If an additional storage medium (e.g. tape drives) are provided to a teleworker he should also be trained with the use of the medium.

T 2.50 Delays caused by a temporarily restricted availability of teleworkers

Usually, teleworkers do not observe fixed working periods at their home working place. Only certain stand-by periods at home are agreed upon. In the case of alternate teleworking, working periods are divided among work at home and work at the institution. If information needs to be obtained from, or provided to a teleworker, this will cause a delay in operations, due to a restricted availability of the teleworker. Even a transfer of information via E-mail does not necessarily shorten response times, as it is not guaranteed that the telecommuter will read the mail in certain time intervals.

T 2.51 Poor integration of teleworkers into the information flow

As telecommuters work primarily at home and are thus not present at the institution on a daily basis, they have less opportunity to participate in a direct exchange of information with superiors and colleagues. As a result, they may remain partially unaware of certain internal affairs, which would lead to a reduced affiliation with the institution.

Furthermore in case of an inadequate information flow, there is the possibility that some information required from security aspects will be not be properly received or will arrive too late from the teleworker . One possible scenario here involves a delay in the forwarding of messages concerning computer viruses.

T 2.52 Longer response times in the event of an IT system breakdown

In the occurrence of an IT-system breakdown at the teleworker's home which cannot or must not be repaired by the teleworker, either an IT system specialist will have to visit the teleworker at home, or the affected IT system will have to be transported to the institution to be repaired. This would take some time, and the teleworker has to therefore be aware of increased idle times. Similar problems can occur during maintenance or during the installation of new components/software.

T 2.53 Inadequate regulations concerning substitution of teleworkers

In general, all tasks of a teleworker suppose and suggest that he/she is able to work largely on an independent basis. One potential risk here is, that it maybe difficult to find a substitute for a telecommuter who has fallen sick. In particular, it may be difficult to arrange a transfer of documents and of data from the affected teleworker's home workstation to the substitute's if there is no immediate possibility of accessing the teleworker's home working place.

T 2.54 Loss of confidentiality through hidden pieces of data.

During electronic data communication or transmission of data media, information that should not leave the institution is frequently passed. The possible reasons for an inadvertent transfer of information are listed below: .

- A file contains some pieces of text formatted in a hidden or non visible mode. Such pieces of text can include statements, which are not addressed to a recipient.
- Files created with standard software, including text processor or spreadsheet programs can contain additional information such as the structure of directories, version numbers, creator, modification time stamp, last time of printing, document name and document descriptions.
- If a file is copied to a floppy disk, an entire physical memory block will be filled. If the original file does not require a complete memory block , the IT system fills up the unused section of the block with discretionary 'hidden' data.
- All current releases of Winword offer the possibility of using the 'quick-saving' option for all created documents This ensures only that the modifications of a document will be saved. This takes less time as compared to a complete saving procedure, in which Winword has to save a completely modified file . However, a complete saving procedure requires less storage on the hard disk than does a 'quick-save' procedure. The decisive disadvantage, however, is the fact that a file can contain textual fragments which were not foreseen for distribution by the author.

Examples:

- Due to the use of a different editor, a user accidentally discovered several URLs, followed by a user name and a password from a file which was ready and prepared for sending. The address of a WWW-document is called URL (Uniform Request Locator). The access to a WWW-page can be password-protected
- Presentation slides built with Microsoft Powerpoint were handed over as files to a third party by a public authority. Later it was detected, that it was not only the presentation slides, but that it also included information about the user environment, such as information about the newsgroup subscribed to by the user and which articles from the newsgroups he had already read. Among other things the PowerPoint file contained the following entries:

  alt.drugs! s21718 0

  alt.sex s125 0

T 2.55 Uncontrolled use of electronic mail

Uncontrolled use of electronic messages includes the threat that unwarranted persons can get access to sensitive information or that they may not arrive at the intended recipient on time.

Examples:

- An incorrect address may be the reason for an electronic message being sent to an unauthorised recipient

  If distribution lists are not maintained in regular terms electronic mail may be sent to certain recipients, who should have been excluded from the distribution list.

- An incorrect sending mode can cause problems during the transmission or receiving of messages. If a file had not been converted into 7-bit ASCII format by *uuencode*, it might be converted incorrectly and thus become unreadable for the recipient During transmission the relaying of messages may be erased from one of the participating IT systems if the file set is too large

- Missing or insufficient requirements documents at the recipient's end may cause a delay in the processing of a received electronic message.

- Lack of, or insufficient allocation of responsibilities by the responsible party sending the message, might cause a delay in the assured delivery of data on schedule.

T 2.56 Inadequate description of files

If files intended for electronic transmission are not adequately described, the recipient is often not able to ascertain their origin, contents or purpose.

If several e-mails are received from the same sender that lack, or contain inadequate marking, an incorrect sequence in sending may lead to the misinterpretation of the messages.

Example:

Sender S sends an e-mail containing several files to recipient R. The next day, S detects that one file still contains some errors and subsequently sends a corrected version accompanied by a request to delete the previous e-mail. After R has deleted the previous e-mail, he/she becomes aware that the current e-mail contains only the corrected file, and nothing else.

T 2.57 Inadequate storage of media in the event of an emergency

If data need to be recovered following damage to an IT system, it is often necessary to copy the data backups first to separate storage media. This applies, in particular, to complex data structures such as databases, as the recovery of data here is not always a smooth and error-free process. If the available storage capacity is insufficient, a hasty reaction in during an emergency may result in an additional loss of data.

Example:

At a company running a large database application, the database management system (DBMS) indicated an inconsistency in the database. Thereby, the system management took the database out of operation and restored the most recent backup of the data in the production system. However, only the log and configuration files of the apparently corrupt database had been backed up. As a result of this action, all modifications of the data since the last backup were lost - an unknown error in the DBMS had prevented the recovery of these changes. A subsequent analysis of the log and configuration files showed that the database had, in fact, remained consistent. If sufficient disk space had been available, the old productive system could have been ready for operation again without any loss of data, following identification and elimination of the apparent inconsistency.

T 2.58 Novell Netware and date conversion to the year 2000

Under Novell Netware, dates are currently stored in two-digit format, while the number 19.. is affixed only for the purpose of visual representation.

That means that the date conversion 1999/2000 will cause the sequence of '00' to be interpreted incorrectly as the year 1900 by the running Netware server. According to a statement of Novel, the date will be set automatically to 1980 after a restart of the server.

This conversion results from the fact that after a restart, the value of (19)**00** is interpreted as an invalid date, for which reason the standard value of (19)**80** (the year of birth of IBM PCs) is selected as the valid date.

Although this particular behaviour will not destroy stored data, it will cause errors within all time-controlled programs for user accounts with an expiration date, as well as time-driven processes such as data backups, and could, in turn, result in a loss of data. Above all, considerable problems would occur in the NDS if the date was suddenly set back. However, it is also important that the BIOS for the computer is year-2000 compatible and the transition from 31.12.1999 to 1.1.2000 can take place automatically.

These errors currently affect (according to reports from June 1999) versions NW 2.x, NW 3.x up to version 3.2 and NW 4.x of Novell Netware.

Further details on the response of Novell products to the transition to the year 2000 are available on the Internet under the following URLs, for example: http://www.novell.de/jahr2000/ and http://www.novell.com/year2000/. Programs can also be found to test whether Netware Software in use is year-2000-compatible. Similarly, an overview is provided, showing which Novell programs have been tested for their year-2000 compatibility and what the results were.

T 2.59 Operation of non-registered components

As a rule, all components of a network should be known to the system administration. On an organisational level, it should be guaranteed that new components are registered with and released by the system administration, for example through automatic reporting from the purchasing organisation or a corresponding request from the organisational unit operating the components.

Non-registered components are a security risk as they are not integrated in organisational in-house processes and controls. On the one hand, this can cause problems for the users of non-registered components (e.g. loss of data, as the system is not integrated into the data backup). On the other hand, it can also jeopardise other network components. For example, weaknesses can arise through unrecorded access points to the network if they are poorly protected against unauthorised access or not even protected at all. In particular, as such components are not controlled by the network management and/or the system management, errors in the configuration of the local system can lead to a gap in security.

Example:

The administrator uses the system management system to maintain the passwords (community names) for the network management system in use which is based on SNMP. A workgroup buys a new network PC but forgets to report this to the central administration. At installation, the password (community name) for the local SNMP demon is set to "public". This password is well-known. Perpetrators can now start an SNMP-based attack, as they have full access to the SNMP data. A PC compromised in this way can serve as a starting point for further perpetration to the internal network. For example, password sniffers could be installed.

T 2.60 Strategy for the network system and management system is not laid down or insufficient

If no general organisational management strategies are laid down for the areas of network management and system management, mistakes in the coordination of individual subdomains can cause serious problems through errors in the configuration, which can cause the system to completely collapse at network level. This is particularly the case in medium and large networks with several management domains.

For this reason, it is imperative that you lay down and enforce a management strategy. The following gives several examples of problems caused when the strategy for the network management and system management has not been laid down or is insufficient.

Requirements are not analysed before the management strategy is laid down

In order to determine a strategy for the network management and the system management, you must first analyse the requirements. Without determining the requirements of the management (for example: Which manageable network switching elements exist? How often is the software to be updated?), it is not possible to formulate demands of the management strategy. As the management strategy also has an impact on the software to be purchased, this can lead to wrong decisions.

If, for example, a management product is introduced whose range of functions is too restricted, this can also cause problems in security, as the necessary function has to be provided "manually". In large systems, this can easily lead to errors in the configuration.

Purchasing unmanageable components

If a computer network is administered with the help of a network management system and/or a system management system, you must ensure that new components can be integrated into the relevant management system so that they can be included in the management. If this is not the case, you will need additional time for administration, if nothing else, as the management strategy that was laid down must be enforced for the components which are not administered with the management system. However, as these components are in particular not integrated in the automatic administrative processes of the management systems, errors can occur in the configuration . This can lead to a security risk through uncoordinated configurations.

Uncoordinated management of related areas (communities, domains)

If a computer network administered by a management system contains several administrative areas which are each looked after by their own system manager, then the management strategy must define their competence unambiguously. Otherwise, uncoordinated management of individual components can cause security problems.

On the one hand, for example, if individual components such as network switching elements are wrongly managed by two administrative areas (this can

happen, for instance, if users fail to use different SNMP passwords (community strings)), then the uncoordinated setting of configuration parameters may lead to gaps in the security.

On the other hand, if components (such as printers) are used by two administrative areas together and if, for example, the confidentiality of the other administrative area (e.g. Windows NT network releases) was not set up correctly, this can inadvertently lead to security problems if an unauthorised third person is permitted access.

Non-integrated administrative software

In the administration of medium and large systems, after the management system has been introduced, it may be the case that new components are to be integrated into the system whose administration requires functions which the management system in use does not support. This applies in particular to the area of application management. If administrative software that cannot be integrated into the management system is used for the administration of the new components (e.g. via a programming interface or through the implementation of what are known as gateways), then it is impossible to integrate the components into the management system. Thus the new components are not subject to the "automatic" management, making it necessary to manage them "manually". The strategy laid down for the management must now be applied to two systems. However, this can lead to configuration errors which can cause gaps in the security.

T 2.61 Unauthorised collection of personal data

When management systems are used, a large amount of auditing data usually arises which, as a rule, is produced and evaluated automatically. This is particularly true for the areas of network and system monitoring. Without keeping detailed records of the system activities it is, for example, also impossible to detect security violations. One requirement is that the monitoring system can determine when certain data has been accessed and which user has accessed it. Therefore, a record of the monitored activities must be kept for each user. As a rule, the management strategy determines for the whole organisation, in agreement with the data security officer, which user activities should be monitored for security reasons. You must inform the affected users of this correspondingly. Within the framework of the system revision, you must check that the requirements laid down by the management strategy are adhered to. It is possible that the management system, while performing a normal function, draws up temporary log files which are then stored in the poorly-protected area for log files. The log files are then potentially accessible at least as long as they exist and may also contain user information.

T 2.62 Inappropriate handling of security incidents

In practice, the possibility of a potentially extremely damaging security incident can never be eliminated, even where extensive security measures have been implemented. If appropriate action is not taken in response to a security incident, considerable damage or loss could occur or the situation could even develop into a catastrophe.

Examples include:

- New computer viruses containing damaging functionality at first occur on a sporadic basis but afterwards they are found on a wide scale. Without an appropriate and rapid response, entire organisational units can be put out of action. This is what happened when the "Melissa" virus appeared. **Non-productive time**
- The material held on a Web server changes inexplicably. If this is not investigated as a possible sign of a hacker attack, further attacks on the server could result in considerable loss of image. **Impaired company image**
- Inconsistencies are found in the log files of a firewall. Unless this is investigated as a hacking attempt, external adversaries could actually penetrate the firewall.
- New security weaknesses in the used IT systems become known. If this information is not obtained in good time and the necessary countermeasures are not taken speedily, there is a danger that the security weaknesses will be misused by either internal or external perpetrators.
- There are signs that corporate data has been manipulated. If the opportunity to follow up the manipulations is overlooked, undetected manipulations could result in extensive consequential damage, such as, for example, incorrect stock levels, false book-keeping or unchecked outflows of funds. **Consequential damage**
- Failure to take action when there is evidence that confidential corporate data has been compromised could result in additional confidential information being leaked.

These examples illustrate how important it is that security incidents are reported promptly to the responsible persons, action is taken quickly and those potentially affected are informed of how to minimise the damage or prevent it.

Again, in the absence of defined appropriate procedures for handling security incidents, it is possible for incorrect decisions to be made with the result, for example, that **Wrong decisions**

- representatives of the press obtain incorrect information;
- the systems or components affected are not switched off even though there are serious security weaknesses;
- systems or individual components are switched off completely even though the security weaknesses concerned are relatively minor;
- there is no provision for backup measures, e.g. for replacement of compromised components, cryptographic procedures or keys.

T 2.63 Uncontrolled use of faxes

Where usage of fax machines or fax servers is uncontrolled, there is a danger that sensitive danger could fall into the hands of unauthorised persons or fail to reach the intended destination in time.

Examples:

- An incorrect address could result in a fax being sent to an unauthorised recipient. **Incorrect addressing**

  If address books and distribution lists are not maintained, faxes could be sent to recipients who should not be on the distribution list.

- Defective administration of a fax server could result in incoming faxes been delivered to employees who should not see them.

- Lack of or inadequate organisational procedures at the recipient's end could cause a delay in the processing of a received fax. **Unreliable processing**

- Lack of, or inadequate organisational procedures at the originator's end could have the result that a promised deadline for sending a message by fax is missed.

- Lack of awareness amongst users of the need for responsible use of fax servers could result in a draft document which should not have left the organisation being sent out.

T 2.64 Lack of or defective rules for the RAS system

If no rules or only inadequate ones have been set for the RAS system, this constitutes a considerable threat to the system as a whole. As a RAS system is composed of a number of components, the first set of threats comes from the "Organisational shortcomings" area of the various individual components, as set forth in the relevant module descriptions.

In the RAS environment, the threats outlined below deserve special mention.

- A RAS system should not be allowed to "grow organically". Instead, use of RAS access should be preceded by careful planning, irrespective of how complex access is designed to be. Experience shows that especially where RAS access is continually extended, complex hardware and software scenarios can come about which it is then no longer possible to keep under control. This can result in security settings that are incorrectly selected, incompatible with each other or which cancel each other out.

Lack of or inadequate planning of the RAS system

- In the absence of a universal and binding security policy, it is usually left to individual administrators and RAS users to make the security settings which seem appropriate to them. This can result in incompatible security settings which either prevent connections from being established or else allow insecure connections to be established. But since in many cases IT systems which are linked up via RAS have the same access possibilities as IT systems which are actually on the LAN, one result may be that the security of the LAN is compromised.

Lack of a RAS security concept

- The security of a RAS system is based on the interaction of the physical components (computers, network switching elements), their connection structure (distribution over the network, connection topology) and the configurations of the relevant software components. The rules specified in the RAS security concept and their implementation through corresponding configuration settings can, however, only deliver the required security if the system that is actually installed agrees with the planned system. But in practice changes are often made to the physical design during the installation phase, for example, due to a lack of detailed information during the planning phase. If these changes are not recorded, documented and analysed for possible effects on IT security, then the security of the LAN can be endangered through incompatibilities of system structure and configuration of the RAS system.

Installation which does not comply with the rules

- If no rules or only inadequate ones have been set for the use of RAS, this constitutes a special threat. RAS users generally act on their own initiative when using RAS. If there are no dedicated rules on the use of RAS or if the users do not know about them, then security weaknesses can be created unknowingly by the user. Rules whose adherence is the sole responsibility of the individual user may not always be adhered to in their entirety, for example due to a lack of technical understanding.

Lack of or defective rules for use of RAS

Examples

- *Incompatible security settings*. The RAS system administrator only allows triple-DES encrypted connections, but a user has not configured any encryption for the RAS client. A connection is therefore not established.

- *Installation which deviates from plan.* Due to incompatible links between RAS server and the interface with the telecommunications provider (e.g. ISDN terminal device connection linked to ISDN system connection) or inappropriate cable arrangement, a decision is made during installation of the RAS system to install an additional small ISDN PBX which offers compatible connections to both sides. As this additional device was not included in the plan, it gets left out of the RAS security concept. When a RAS connection is established it is now possible, for example, to access the device for remote maintenance using a procedure that is protected only with a standard password.

T 2.65 Complexity of the SAMBA Configuration

SAMBA is a freeware software package for UNIX operating systems which, amongst other things, provides file, print and authentication services over the Server Message Block (SMB) and Common Internet File System (CIFS) protocols. The most important examples of SMB/CIFS clients are definitely the operating systems in the Microsoft Windows family. With SAMBA it is possible, for example, for Windows 9x or Windows NT computers to access shared files on a UNIX server directly. This obviates the need to take a detour over the FTP or NFS protocols or to install additional software on the client. In the current version, SAMBA simulates a whole range of Windows NT server functions so that in many cases it is possible to use a UNIX system with SAMBA in lieu of such a server.

Unnoticed side-effects

On the server side, most of the SAMBA configuration settings are defined in the file *smb.conf*; in particular, the shared directories and printers are entered here together with various settings relating to authentication. A whole range of parameters are available for this purpose. These are set in the individual sections of file *smb.conf*. A given function of the SAMBA server is generally controlled via a combination of several parameters. Depending on the particular instance, the interaction of these parameters can be very complex, so that there is a danger that the Administrator could incorrectly interpret the effect of a particular parameter combination. In particular, there is a danger that if one parameter is modified this could have unnoticed side-effects that compromised the security of the server.

Directory and file access permissions

The problem described above is aggravated during configuration of directory and file permissions. Here it is necessary to consider not only the settings contained in file *smb.conf*, but also the access rights to the (UNIX) file system on which the directories and files are held. The actual rights which are valid for the user during access via SAMBA can be influenced by file *smb.conf* in two different ways. Firstly, it is possible to specify direct access restrictions for the individual shares of a SAMBA server (e.g. via the parameter *valid users*). Secondly, file *smb.conf* contains parameters (e.g. *force user*) by means of which it is possible to configure how directory- and file-based access restrictions affect a user's current access rights. It is easy to make a mistake in the configuration, with the result that users are given excessively wide access rights to directories and/or files.

Example:

The Administrator of a SAMBA server assigns directory- and file-based access rights to the local file system of the server. This entails setting appropriate permissions and ownerships for all the shared areas. However, file *smb.conf* contains the line

```
force user = root
```

. This means that the file system is accessed under the "root" user account, irrespective of which user has logged on to the server. The result is that virtually all the directory-and file-based access restrictions are ignored.

T 2.66 Lack of or Inadequate IT Security Management

Uncoordinated approach

The complexity of the IT systems used in many enterprises today and the trend towards networking these systems makes it imperative to proceed in an organised fashion with regard to planning, implementation and monitoring of the IT security process. Experience shows that it is not sufficient simply to arrange for safeguards to be implemented, as often the individuals concerned, especially the IT users, do not have the technical expertise and/or time that are needed to implement them properly. As a result, security measures frequently fail to be implemented at all so that it is impossible to attain a satisfactory level of security. Even if a satisfactory level of security is achieved, it must be continuously nurtured if it is to remain current.

Shortcomings in overall organisation

Inadequate IT security management is often a symptom of a poor overall organisation of the IT security process and hence of IT operations as a whole. Examples of specific threats which result from inadequate IT security management include the following:

- *Lack of personal responsibility*. If no IT security Management Team has been set up in an organisation or if no IT Security Officer has been appointed and personal responsibilities for implementing individual measures have not been clearly defined, then it is likely that many IT users will decline to take responsibility for IT security, maintaining that it is the responsibility of those above them in the organisational hierarchy. Consequently safeguards which at the outset nearly always require extra work on top of one's normal duties remain unimplemented.
- *Inadequate support from management.* Usually IT Security Officers are not members of an organisation's management team. If the latter does not unambiguously support the IT Security Officers in their work, this could make it difficult to effectively require that the necessary measures are implemented, including by IT users who are above them in the organisational hierarchy. In these circumstances, there is no guarantee that the IT security process will be fully implemented.
- *Inadequate strategic and conceptual requirements.* In many organisations the job of drawing up an IT security concept is commissioned, its content is known to only a few insiders and its requirements are either deliberately or unconsciously not adhered to in those parts of the organisation where organisational effort would be required in order to implement it. To the extent that the IT security concept contains strategic objectives, these are often viewed simply as a collection of declarations of intent, and insufficient resources are made available to implement them. Frequently it is falsely assumed that in an automated environment security is automatically generated. Sometimes spurts of activity are triggered in response to a damaging incident in the organisation or in other organisations with a similar structure, but at best only a subset of the issues are properly addressed.
- *Insufficient or misdirected investment.* If the Management of an organisation is not kept informed of the security status of the IT systems and applications and of existing shortcomings through regular IT security

reports which lay down clear priorities, it is probable that insufficient resources will be made available for the IT security process or that these will be applied in an inappropriate manner. In the latter case it is possible to have an excessively high level of security in one sub-area and serious deficiencies in another. Another common observation is that expensive technical security systems are incorrectly used, rendering them ineffective or even transforming them into security hazards.

- *Impracticability of safeguard concepts.* To achieve a consistent level of IT security it is necessary that those in positions of responsibility within an organisation co-operate with each other. Inadequate strategic direction and unclear objectives sometimes result in different interpretations of the importance of IT security. This can have the result that the necessary co-operation is ultimately not forthcoming due to the supposed non-necessity or inadequate prioritisation of the "IT security" task, and hence that the implementability of the IT security measures cannot be taken for granted.
- *Failure to update the IT security process*. New IT systems or new threats have a direct impact on the IT security position within an organisation. Without an effective review concept, the IT security level will fall over time. Thus, what was once really secure slowly gives way to a dangerous illusion of security because people are often not aware of the new threats.

T 3 Threats Catalogue Human Failure

T 3.1	Loss of data confidentiality/integrity as a result of IT user error
T 3.2	Negligent destruction of equipment or data
T 3.3	Non-compliance with IT security measures
T 3.4	Inadmissible connection of cables
T 3.5	Inadvertent damaging of cables
T 3.6	Hazards posed by cleaning staff or outside staff
T 3.7	Failure of the PBX due to operating errors
T 3.8	Improper use of the IT system
T 3.9	Improper IT system administration
T 3.10	Incorrect export of file systems under UNIX
T 3.11	Improper configuration of sendmail
T 3.12	Loss of data media during transfer
T 3.13	Transfer of incorrect or undesired data records
T 3.14	Misjudgement of the legal force of a fax
T 3.15	Improper use of answering machines
T 3.16	Incorrect administration of site and data access rights
T 3.17	Incorrect change of PC users
T 3.18	Sharing of directories, printers or of the clipboard
T 3.19	Storing of passwords for WfW and Windows 95
T 3.20	Unintentional granting of read access for Schedule+
T 3.21	Improper use of code keys
T 3.22	Improper modification of the registry
T 3.23	Improper administration of a DBMS
T 3.24	Inadvertent manipulation of data
T 3.25	Negligent deletion of objects
T 3.26	Inadvertent sharing of the file system
T 3.27	Improper time synchronisation
T 3.28	Inadequate configuration of active network components
T 3.29	Lack of, or unsuitable segmentation
T 3.30	Unauthorised private use of telecommuting workstations
T 3.31	Unstructured data organisation

T 3.32	Violation of basic legal conditions for the use of cryptographic procedures
T 3.33	Improper use of cryptomodules
T 3.34	Unsuitable configuration of the management system
T 3.35	Disabling the server while in operation
T 3.36	Misinterpretation of events
T 3.37	Unproductive searches
T 3.38	Errors in configuration and operation
T 3.39	Improper administration of the RAS system
T 3.40	Inappropriate use of authentication services with remote access
T 3.41	Improper use of remote access services
T 3.42	Insecure configuration of RAS clients
T 3.43	Inappropriate handling of passwords
T 3.44	Carelessness in handling information
T 3.45	Inadequate checking of the identity of communication partners

T 3.1 Loss of data confidentiality/integrity as a result of IT user error

Through inappropriate actions, it is possible for IT users to cause or enable a loss of data confidentiality or integrity. The extent and nature of the damage induced will depend on the sensitivity of the data involved. Examples of such inappropriate actions are as follows:

- Printouts containing person related data are accidentally left lying on the network printer.
- Floppy disks are sent out without data previously stored on them being physically deleted.
- Due to incorrectly administered access rights, a staff member is able to modify data without being able to assess the critical impact of such a violation of integrity.
- New software is tested using non-anonymous data, giving unauthorised staff members access to protected files or confidential information. It is also possible that third parties could gain access to this information if the disposal of "test printouts" is not handled correctly.
- Data stored on partially intact file systems can fall into unauthorised hands when hard disks are dismounted, lent, sent for repair or taken out of service.

T 3.2 Negligent destruction of equipment or data

Negligence, but also untrained handling, may lead to the destruction of equipment or data which can severely disrupt further operation of the IT system. This can also be caused by improper use of IT applications, leading to incorrect results or inadvertent modification or deletion of data. Careless use of a single deletion command can delete entire file structures.

Examples

- Users who switch off the computer when an error message is displayed instead of correctly closing all running applications or consulting an expert, can cause serious integrity errors in stored data.
- Moisture arising from spilt coffee or from plants being watered can cause short-circuits in the IT system.
- A user who has a developed a habit of running the delete command *rm* under UNIX without activating the parameter (*-i*) which ensures that the user is asked to confirm any deletion before execution of the command or who actually disables the confirmation prompt with *-f* runs a high risk of accidental deletion of files. The same applies to the command *del *.** under MS-DOS.

T 3.3 Non-compliance with IT security measures

Due to negligence and insufficient checks, persons frequently fail to perform, in part or full, recommended or prescribed IT security measures. Damage may be caused which otherwise could have been prevented, or at least minimised. Depending upon the position of the given person and on the importance of the disregarded measure, severe damage could occur here.

IT security measures are frequently disregarded due to the lack of security awareness. A typical sign is the disregarding of recurrent error messages after a certain habituation period.

Examples:

- The keeping of floppy disks in a locked desk does not afford sufficient protection against unauthorised access if the key is kept in the office e.g. on top of a cupboard or inside a card box.
- Passwords which need to be kept secret are kept on a piece of paper near a terminal or a PC.
- Although the purpose of data backups to minimise potential damage is widely known, losses of data do occasionally occur when unexpected deletion of data takes place and recovery is not possible due to lack of backups. This is particularly illustrated by the damage reported to BSI, resulting from computer viruses, for instance.
- Access to a computer centre should take place exclusively through a door secured by an entry control system (e.g. magnetic strip reader). However, the emergency exit door can be used as an additional entrance and exit although it may only be opened in an emergency..

T 3.4 Inadmissible connection of cables

In addition to technical defects, the main reason for inadmissible connections is incorrect cabling, e.g. when carrying out cable assignment for jumper distributors and splice distributors. Inaccurate documentation and insufficient labelling of cables often results in an unintentional error in the set-up and complicates the detection of deliberately incorrect assignments.

Due to inadmissible connections, data may be transmitted additionally or exclusively to wrong addressees. The normal line can be mutilated.

T 3.5 Inadvertent damaging of cables

The risk of inadvertent damage increases with the lack of protection provided in the layout of cables. Such damage does not necessarily result in an immediate breakdown of connections. It is also possible that inadmissible connections are established accidentally. Typical examples of such damage are:

within the building:

- an unembedded flexible device cable is yanked out with the foot;
- damaging of concealed (buried) cables by drilling or nailing;
- incursion of water into windowsill ducts;
- incursion of water into conduit subways (floor ducts) during cleaning of the building;
- damaging of exposed lines (on walls or floors) during the transport of bulky or heavy objects.

externally:

- damage caused during below-grade construction, through both manual excavation and excavator use;
- incursion of water into underground lines/buried cables.

Example:

In a pedestrian precinct, the charwoman employed by a small shop had made a habit of pouring the used water directly in the PTT-cable inspection manhole. Although the water evaporated, the dirt and soap residues deposited on the cables had to be removed with great expenditure of time and effort when work had to be carried out.

- damaging of cables by rodents;
- damaging of ducts and cables by roots (the roots of a tree are strong enough to crush cables);
- damage caused by the exceeding of admissible traffic loads (pipes may burst, cables may be sheared).

T 3.6 Hazards posed by cleaning staff or outside staff

Hazards posed by cleaning staff and external staff range from improper handling of technical equipment, or the attempt to "play" on the IT system, to the theft of IT components.

Examples:

Cleaning staff may accidentally detach a plug-in connection; water may seep into equipment; documents may be mislaid or even removed with the garbage.

T 3.7 Failure of the PBX due to operating errors

Apart from technical failure due to defective components, power failure or sabotage, there are various other factors which may result in the breakdown of a PBX. For instance, insufficiently trained maintenance staff may modify the configuration of the system which could result in such a failure. The same effect can occur if alarm signals or abnormal operating performance are not recognised in time, or when generally simple routine repairs are carried out improperly or rashly.

T 3.8 Improper use of the IT system

Improper use of the IT system involving negligence or ignorance of IT security measures jeopardises the security of the system. These can be avoided if users are sufficiently informed about the correct operation and function of the IT system.

Examples:

Rights granted too generously; passwords that can be easily guessed ; inadvertent deletion; data media containing backup copies are accessible to unauthorised persons; the terminal is not locked during temporary absence, etc. etc.

T 3.9 Improper IT system administration

Improper IT system administration can jeopardises the security of the system if it results in circumvention of or failure to observe IT security measures.

Insecure network access

Improper administration exists, for example, if network access points (daemon processes) which are not necessary for the regular operation of the IT system or which represent a particularly large threat due to their error-proneness are created or not disabled.

Unnecessary access rights

Under no circumstances should access accounts be used when working on the system which possess more privileges than are absolutely necessary for the work, as this raises the danger of loss or damage due to viruses and Trojan horses unnecessarily.

Improper modifications

It is extremely rare that standard installations of operating systems or system programs have all the features of a secure installation. Inappropriate modifications to specific security requirements can pose a considerable risk here.

Special care must be taken with systems which, if poorly administrated, could affect the protection of other systems (e.g. firewalls).

Every modification of security settings and extension of access rights constitutes a potential threat to overall security.

Examples

Inadequate logging

In addition to the instances mentioned under T 3.8 *Improper use of the IT system*, the System Administrator may create threats due to the incorrect installation of new or existing software. Other instances of incorrect management are: failure to use auditing functions or to analyse existing log files, granting of overgenerous access rights, failure to review access rights at regular intervals, multiple assignment of the same log-in name or UID, and failure to use the available security tools, e.g. failure to use a *shadow* file for passwords under UNIX.

Ageing of passwords

The older a password is, the less effective it becomes. The reason for this is that the probability of a successful attack increases steadily over time.

Special care must be taken over the administration of a firewall system as the protection of many other systems depends on it.

T 3.10 Incorrect export of file systems under UNIX

Exported disks can be mounted from any computer whose name is specified in files */etc/exports* or */etc/dfs/dfstab*. The user of such a computer can assume any UID and GID. As long as directories have not been exported with the option *root=*, UID 0 (*root*) constitutes an exception which, on access to an NFS server, is normally mapped to a different UID (e.g. to the UID of the user *nobody* or *anonymous*). Hence only files which belong to *root* can be protected.

There are no adequate protective measures available in protected environments for the use of the NFS protocols for the export of file systems or the distribution of system files using NIS. Such use therefore constitutes a threat to the integrity of the systems.

T 3.11 Improper configuration of *sendmail*

Errors in the configuration or software of *sendmail* have repeatedly led to security leaks in the affected IT systems in the past (typically: *Internet* worm).

Example:

Through various publications it has become known that it is possible to obtain user IDs and group IDs which are set with the options *u* and *g* (normally *daemon*). To do this a pipe has to be indicated in the address fiels (From:) so that the mail is sent back. In the mail itself an error message has to be generated. Therefore, if you send an E mail containing

cp/bin/sh/tmp/sh

chmod oug + rsx/tmp/sh

to an unknown recipient and use '*/bin/sh*' as the sender address, that message will be returned as undeliverable which, in this case, is equivalent to the execution of a small shell-script. By means of this script, a shell with a set *suid* bit will be generated which has the user and group ID defined in *sendmail.cf*.

T 3.12 Loss of data media during transfer

If data media are dispatched without robust packaging (mailing envelopes etc.) damage to the packaging might lead to loss of this data media (particularly floppy disks). The loss could also occur during the mailing process, e.g. due to negligence on the part of the postman. If, for example, a floppy disk is dispatched together with a letter inside an envelope which is considerably larger, the floppy disk might be overlooked and disposed of inadvertently by the recipient of the envelope.

T 3.13 Transfer of incorrect or undesired data records

It is possible that data media intended for dispatch might contain data from earlier transactions not meant for disclosure to the recipient. If this data is not physically and intentionally deleted, it will be possible for the recipient to view it.

If the data to be transferred is located within a directory containing additional data requiring protection, there is the danger that they will be transferred inadvertently to the data medium as well (e.g. by *copy* *.*) and become accessible to the (unauthorised) recipients.

If data records have to be sent directly via data networks instead of ‘storage’ media (e-mail via the Internet, modem links, Intranets, X400 service), communication programs offer the possibility to use short descriptions for complex address and distribution lists for multiple dispatch. If such distribution lists are not kept centrally or not updated at regular intervals, data records might be sent to addresses of persons who are no longer authorised.

T 3.14 Misjudgement of the legally binding of a fax

If fast decisions are required, postal dispatches are frequently avoided by transmitting important documents/information to the business partner by fax. The parties involved here often do not take into account that these documents are not always considered legally binding in case of a lawsuit. Customers do not have to accept orders, promises need not be kept. Deadlines for legal remedies can expire, even though the fax was sent in time.

T 3.15 Improper use of answering machines

There is a risk of the incorrect use of an answering machine. Some answering machines are fundamentally prone to incorrect use; because they have function keys with double or even triple assignments for example. This problem is compounded by the keys being so small and close together that incorrect handling becomes almost inevitable.

It may happen that an answering machine will ignore incoming calls as a result of incorrect use. This could happen, for example, if the machine is turned off or the outgoing message is deleted inadvertently by the pressing of a button.

T 3.16 Incorrect administration of site and data access rights

Access rights to an IT system, to stored data and to IT applications should only be granted to the extent required to carry out the necessary tasks. If these rights are administered incorrectly, it can result in a disruption of the operation. if the necessary access rights were not granted or to security leaks if more rights were granted than required.

Example:

As a result of incorrect administration of access rights, a clerk is able to gain access to auditing data. By deleting specific entries, he is able to cover up his attempts to manipulate the computer because they will not appear in the log file any longer.

T 3.17 Incorrect change of PC users

If several users work on one single PC, it may happen that the previous user does not log off and the new user does not log on correctly as a result of negligence or convenience. Those concerned mostly justify this by stating that the time required for a restart of the IT system is too long and not considered to be acceptable.

However, this incorrect behaviour leads to a situation whereby the auditing of all user log-on and user log-off procedures and therefore also accountability will (partially) fail. The audit data no longer provide reliable information as to who used the computer at a certain time.

Example:

A PC is alternately used by three users in order to calculate travelling expenses. After the first user has carried out the log-on procedure, the change in user is then no longer correctly registered as the log-on/off procedures are not carried out for reasons of convenience.

Because of irregularities, checks are made as to who carried out which transactions on the computer. According to the audit data only one user worked on the PC, the perpetrator can not be identified and the user who logged on correctly is made responsible.

T 3.18 Sharing of directories, printers or of the clipboard

When using the file or print manager or the clipboard on a computer running *Windows for Workgroups*, operative errors are possible when sharing directories, printers or pages of the clipboard. This can result in resources being shared unintentionally. The necessary password protection may be applied incorrectly or not at all if the user has not been sufficiently informed of the peer-to-peer functionality in Windows for Workgroups.

When using Windows 95, access rights have to be granted explicitly for a sharing, so that every user has to decide if and to whom access will be allowed. For Windows NT only one administrator can share files or directories.

As shared resources (except for the pages of the clipboard) are generally visible to all participants, other participants can detect and abuse this situation. It is possible for confidential data to be read, changed or deleted without authorisation. For instance, if a directory was shared with write access and without password protection, it would be possible to store files in that directory until the capacity of the hard disk was exhausted.

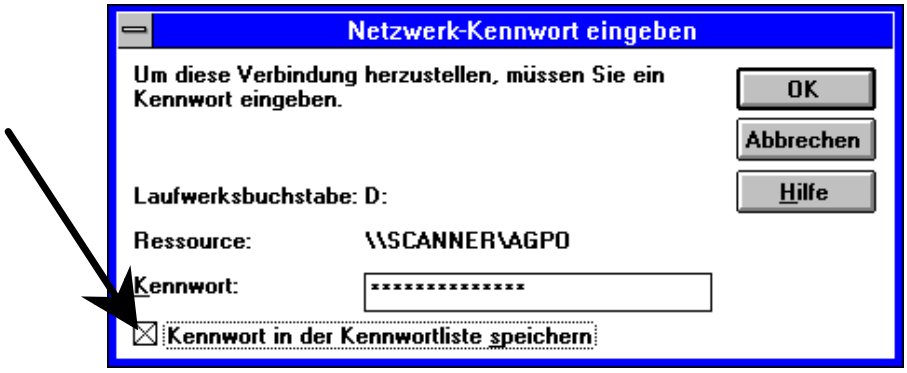
It should be noted that a shared directory will be shared automatically, if the option "Share during next start-up " is activated, without the user noticing this. For Windows 95 and Windows NT, the deactivation of the sharing must not be forgotten. In this case, the sharing must be deactivated explicitly, otherwise it will remain active even after a restart of the system.

Example:

After installation of the WfW user interface within a server-based LAN which was not accompanied by training, about 10% of all users shared the entire hard disk (root directory C:\).

T 3.19 Storing of passwords for WfW and Windows 95

For Windows 95 and WfW, access to directories, printers or pages of the clipboard which were shared by another party is facilitated by keeping the necessary passwords inside the file [*account name*].*pwl*. To do this, the option "Save password in the password list" can be selected. If this option is activated, the result may be that passwords are stored unintentionally. If Windows 95 is used within a NetWare network environment, the passwords will be automatically stored in the [*account name*].*pwl*. file. Access rights however, are only granted at the user level.



Should a third party get access to the WfW or Windows 95 computer he/she would have direct access to the password list ([*account name*].*pwl*). The passwords kept for access to resources of other parties are protected by the WfW or Windows 95 password. If this is deactivated or widely known or if WfW or Windows 95 is already active without a screen lock, unauthorised persons can establish connections to other computers.

Note:

Programs are now offered through the Internet which allow decoding of PWL files for WfW without knowledge of the password. The passwords stored in these files can often be discovered as plain text inside of the windows-specific temporary swap file *386spart.par*. For this reason, an appropriate site access protection or data access protection at file level has to be installed.

T 3.20 Unintentional granting of read access for Schedule+

The WfW package contains the program *mail* and the appointment planer *Schedule+*. If a shared post office is used by several users, *Schedule+* may also be used for joint appointment planning. Access privileges for one's own diary can be granted here. The access right "display vacant/occupied time blocks" is activated by default for the private calendar for each party of the same post office. Unless this right is explicitly withdrawn, the time arrangement but not the contents of the private calendar could be viewed by others. The private user, however, may assume that his vacant/occupied time blocks cannot be viewed by others as he has not granted any access rights.

T 3.21 Improper use of code keys

Experience shows that errors in the operation of mechanical code locks relatively often lead to a situation in which the cupboard can no longer be opened properly. Improper use can occur during input and are particularly frequent when the code is changed. In order to make the data media or IT equipment being stored accessible again, a specialist key cutting service has to be commissioned, with the result that, in addition to the loss arising from the lack of availability of the data media or equipment, substantial repair costs can also be incurred. In the worst-case a new protective cupboard has to be provided.

T 3.22 Improper modification of the registry

Windows 95 allows restricting the user environment of a PC on a global or on an individual basis. Generally this can be done by the use of the system guideline editor (*POLEDIT.EXE*) or the registry editor (*REGEDIT.EXE*). These programs should only be used with great care. Any changes to the registr should only be made by trained personnel and with the greatest care, as a system can very quickly be put into a state whereby work with the PC is no longer be possible. In the worst case the operating system will have to be reinstalled or certain hardware components will have to be reinitialised (by the installation of appropriate drivers).

T 3.23 Improper administration of a DBMS

Negligent or improper administration of a database management system (DBMS) can cause the following hazards:

- Loss of data
- (intentional or inadvertent) manipulation of data
- Unauthorised access to confidential data
- Loss of database integrity
- Database crash
- Destruction of the database

The hazards mentioned above, can also result from access rights granted too widely, the irregularity or lack of database monitoring, inadequate data backups, invalid but not yet deactivated IDs, etc.

T 3.24 Inadvertent manipulation of data

The more extensive the access rights on a database for a specific user, the greater the risk of inadvertent manipulation of data. In principle, this cannot be prevented by any application. The fundamental reasons for inadvertent manipulation of data include:

- The lack of or poor technical knowledge
- The lack of or poor knowledge of the application
- Too widely granted access rights
- Negligence (e.g. leaving a workstation without correct termination of the application)

T 3.25 Negligent deletion of objects

Novell Netware 4.x makes it possible, for the first time, to delete the Admin object which will be created automatically during installation. This object, which replaces the Supervisor familiar from Netware 3.x, is created during the very first installation of a Netware 4 network and initially possesses all administration rights. Its ability to delete this object creates the following potential threats:

- If no replication of the administrator (***"repl.-admin")*** is created as an object inside NDS, it could become impossible to administer the NDS or individual containers. This would make it necessary to re-install the NDS and to re-create all the contained objects, which could lead to a complete breakdown of the Netware 4 network.
- In a decentrally administered Netware 4 network, administrators are usually configured at the organisational level (container level). The IRF (inherited rights filter) makes it possible to restrict or disable the inheritance of rights by other administrators to subordinate organisations, so that only the decentral administrator possesses all rights. If this administrator isdeleted from the NDS, an entire organisational unit can no longer be managed, because the other administrators do not have access to this container. Because of the decentral administration *(distribution of administrative tasks)* it is no longer possible to manage the container from other administrators.

T 3.26 Inadvertent sharing of the file system

Novell Netware Version 4 distinguishes between object access rights and file access rights. Object access rights imply all rights to create, to modify, to view and to delete objects within the NDS. File access rights imply reading, writing, deletion etc. of files and directories. The NDS object "Server" acts as the sole interface between the object system and file system.

For this reason, every user registered as a supervisor for a server object also gets supervisor-rights for the entire, related file system, because the supervisor attribute cannot be filtered by an IRF (inherited rights filter). As a result, the user might inadvertently gain access to confidential data.

T 3.27 Improper time synchronisation

Novell Netware 4.x allows several servers to interact within a network. To ensure smooth operation of network services, for example, for the creation of date and time stamps of files, review and auditing, and to guarantee time restrictions for login procedures, it is very important for all servers to indicate the same time of day. Changes to a directory tree also carry a time stamp in Novell Netware Version 4; which determines the processing sequence when the NDS is updated. For this reason, it is important to maintain identical times for all Netware 4 servers in a network.

Potential threats:

- If the internal hardware clock of a computer is not checked and, if necessary, adjusted prior to an installation of a Netware 4 server on that computer, it might not be possible for the new server to match itself with the remaining Netware 4 network, thus giving rise to the danger of the NDS malfunctioning.
- If the time source fails within a network which uses the single-reference procedure for time synchronisation, a replacement time is no longer available. This allows uncontrolled changes to file access rights and object access rights.
- NDS modifications whose time stamps lie far ahead in the future due to an incorrect system time are only executed on the actual attainment of these future deadlines. This might result in errors and problems which are hard or impossible to comprehend, due to the large time span between the issue and execution of the modifications.
- If, after the installation of the server, a radio clock is connected without prior deactivation of the automatic switch between summer and winter time, this will result in an additional adjustment by one hour.

T 3.28 Inadequate configuration of active network components

Throughan inadequate configuration of the network components, the availability of the entire network or segments of it, or the confidentiality of information and the integrity of data can be impaired. The following types of incorrect configuration need to be distinguished in particular:

- Active network components used for building VLANs (virtual LANs) implement a logical segmentation of the network. An incorrect configuration could lead to the breakdown of communications within a VLAN, between individual VLANs or even between all of them. Depending on the VLAN strategy employed by the manufacturer in question, this influences the allocation of mutually communicating systems to identical VLANs, and also VLAN routing, if this is supported by the active network components.

  Example: In case of VLANs which can only communicate with each other via routers, the central infrastructure servers which provide file and printing services, for example, are not allocated also to the VLANs of the workstation systems. In addition to this no routers are connected. In this situation some of the workstation systems can no longer use the services of the central infrastructure servers, as these servers are located within an inaccessible subnetwork.

- A network can be divided into subnetworks through the use of routers. These routers must be configured appropriately to allow communications between the subnetworks, i.e. the routers have to keep routes between individual subnetworks in routing tables. Routing tables can be managed statically or dynamically. In both cases, any communication between individual subnetworks will not be possible, if the routing tables do not specify a route between these subnetworks. A misconfiguration can be caused by an incorrect definition of static routing tables or by an incorrect configuration of the routing protocols (for example RIP or OSPF) used for an automatic update of dynamic routing tables.

  Example: A router-to-router connection is configured by static entries of the IP addresses in the corresponding routing tables. This communication line will become no longer available, if there is a change in the IP address of one of these routers, or an additional router is inserted.

- Active network components capable of filtering protocols and network addresses can prevent communications based on certain protocols or communications between systems having certain network addresses with this technique. Incorrect configuration of the respective filters in use can result in an undesired communications breakdown, depending on the type of incorrectly configured filters and the type of incorrect configuration.

  Filters configured incorrectly can also result in an establishment of connections allowing the infiltration of IT systems within the protected network. Depending on the nature of the infiltration, this might impair the availability of individual network components or even the entire network.

Furthermore, a manipulation of the connecting path may lead to a re-routing, to modifications, or to a monitoring of the data packets.

Examples:

A multiport repeater is configured in such a way that only systems with particular MAC addresses can be connected to certain ports. After the replacement of a network card on one of the stations and the resulting change in the MAC address, this system can no longer be connected to the network (loss of availability).

An unsuitable configuration for active network components (particularly for VLANs or filtering rules) can expand broadcast-domains to an unnecessarily large extent and give rise to superfluous network connections. This could allow confidential data to be viewed by unauthorised parties.

T 3.29 Lack of, or unsuitable segmentation

Local networks can be segmented physically by active network components, or logically by means of an appropriate VLAN configuration. In this case the connected IT systems of a network are distributed among various segments. This not only improves the load sharing within the network, but also facilitates the administration.

However, the following specific threats can arise here:

- Loss of availability

  The higher the number of IT systems within a layer-2 segment, the greater the network load in this segment. This can severely impair the availability of the network segment or even cause an overload situation or a breakdown. In the case of CSMA/CD-based network access protocols (e.g. Ethernet) this also results in more frequent collisions which reduce the available bandwidth. Inadequate segmentation can also take place, if systems are separated by active network components based on layer 2 or 3, causing high network traffic by communicating with each other.

- Insufficient protection of confidentiality

  To ensure that confidential data is protected, the number of users granted access to it should be restricted to a minimum. Consequently, the size of broadcast-domains should be kept as small as possible. However, if the specific segments have been configured inadequately, unauthorised users might also be able to view and examine confidential data during transmission.

Examples:

- Two IT systems which exchange high amounts of data are separated by a router. This might result in unsuitable segmentation, as data needs to be transmitted via the router, which is relatively slow.
- Two IT systems exchanging passwords and other sensitive information frequently are separated by a bridge. This means that the network traffic could be monitored in both segments. Limitation of the network traffic between the two IT systems to one segment would protect the confidentiality of the data to a greater extent.

T 3.30 Unauthorised private use of telecommuting workstations

At home, it is easier to make private use of telecommuting workstations, as the employer only has restricted possibilities of monitoring such usage. This might result in the installation of software which has not been checked, or that data infected by computer viruses will be stored on the telecommuting workstation . Unauthorised use of the telecommuting workstation is possible for the telecommuter as well as relatives and guests. In particular, children and adolescents might be tempted to use the professional workstation to play games, without the telecommuter even being aware of this. Potential damages are for example: erased hard disks resulting in a complete loss of data, which would entail re-installation expenses and a re-entry of data.

T 3.31 Unstructured data organisation

Inadequate instructions and/or a lack of training for staff members can result in a confusing organisation of data on the data media in use. This can lead to various problems such as:

- Waste of disk space through multiple storing of the same data
- Hasty or non-deletion of data, because nobody knows any longer what kind of data is stored in which files
- Unauthorised access, if files are placed in directories or on data media which are made accessible to third parties
- Inconsistent version numbering of different directories and IT systems

Example:

A new staff member with little IT experience was not briefed on the importance of structured data organisation. Problems occurred shortly thereafter, because the staff member had stored all files in the root directory, without creating a single subdirectory.

T 3.32 Violation of basic legal conditions for the use of cryptographic procedures

Various general legal conditions must be observed in relation to the use of cryptographic products. In some countries, for example, cryptographic procedures are not allowed to be used without approval. This can mean that, if encoded data records are sent to such countries, the recipient may not be able to read them because they cannot employ the necessary cryptomodules or may even commit an offence.

In addition, there are severe restrictions on exporting products with strong cryptography in a large number of countries. This particularly applies to the USA. When export is restricted, the functionality of coding products which are strong in themselves is often intentionally reduced (by reducing the diversity of the code). Such intentionally-weakened procedures do not even offer sufficient protection for average protection requirements. This is for instance the case for standard PC software from the USA such as Internet browsers (SSL), in which the length of the code is reduced to only 40 bits. Some export rulings even require parts of the code to be deposited, so that the cryptomodules are in principle unrestricted but foreign intelligence still has the possibility of accessing the files if necessary.

On the other hand, such restrictions, which are valid for use within certain countries or for export, can prevent data worth protecting from being encoded or cause it to be protected with low-quality cryptoproducts. This can both open the door to perpetrators and at the same time violate national law. For example, data protection laws may require the use of adequate cryptographic procedures for the protection of personal data.

T 3.33 Improper use of cryptomodules

In practice, improper use of cryptomodules has already caused damage in many cases. This improper use can have various consequences.

- Data is not encoded before transmission because the plain-text mode in the cryptomodule was activated accidentally.
- When cryptographic codes are entered, parts of the code are entered incorrectly. The result is that neither the originator (who failed to notice the false entry) nor the recipient (who has no way of knowing the real code) can decode the data with the incorrectly-entered code.
- The electricity supply is accidentally cut off during the process of encoding the data. This has the result that only parts of the data are encoded while other parts are not. In such a case, it may no longer be possible to decode the data because the process was stopped due to an unforeseen error.
- Some of the encoding parameters are entered incorrectly. This can result in an insufficient number of secure cryptoalgorithms or insecure cryptographic codes being used.
- If the users are involved in producing the code, in that they are asked to enter random characters, it is also improper use to select strings of characters that are known or can easily be guessed (words) rather than random characters.

Such improper use of a cryptomodule can interfere with the confidentiality, the integrity and the availability of the data. Examples include:

- Data is not encoded or no longer encoded, even though it may be necessary to encode it to preserve confidentiality.
- Encoded data can no longer be decoded because improper use has made it impossible to use the cryptomodule in accordance with the rules.
- Data is either intentionally or unintentionally encoded in such a way that it can no longer be reconstructed because the necessary cryptographic code is not known.
- Correctly-encoded data is changed in such a way that the data can no longer be decoded.

T 3.34 Unsuitable configuration of the management system

In order for a network management system and/or a system management system to be used securely, all components involved must be configured consistently. Although the individual components are usually managed from a central entity (management console), the management system is made up of a number of individual components which are distributed among the network components to be managed. A consistent configuration of such a system can be subdivided into two areas:

- On the one hand, the configuration of the system components (e.g. computer, router) set with the help of the management system must be consistent as a whole. A server should, therefore, be configured in such a way that all authorised client computers have access but no others do.
- On the other hand, the management software itself must be configured consistently.

If the consistency of the configuration is damaged, either intentionally or unintentionally, then the components cease to work together smoothly, which can cause security problems. For example, a server may become inaccessible or access rights may become too relaxed.

T 3.35 Disabling the server while in operation

If a network is managed through a management system, then there are servers with special tasks (particularly in the area of system management). As a rule, databases with management information are kept on what are known as management servers. If such servers are simply disabled while in operation, then data such as that contained in the computer's memory is no longer written onto the file system. The consequence of this is that inconsistencies may also occur in the management data when the computer is next switched on. Large management systems therefore tend to use databases which use what are known as transaction mechanisms to ensure that the information is converted back into an (old) consistent state. This reduces the risk but does not completely remove it and can even be used for perpetration (exploitation of an old configuration with less restricted access rights).

T 3.36 Misinterpretation of events

When a management system is used, it is the task of the system administrator in charge to analyse and interpret the messages of the management system in order to take appropriate measures. As a rule, the messages of the management system are based on monitoring mechanisms which automatically search system protocols of various types according to certain rules. In the process, it is not easy to automatically recognise abnormalities from the wide range of auditing data that occurs and to produce relevant messages for the system administrator. In addition, an error here may not be discovered. The incoming messages must therefore always be viewed and interpreted by the system manager, as the messages (in the case of an error) are based on symptoms of errors and their (automatic) interpretation. A system administrator must also be able to recognise false alarms and incorrect messages. If the administrator incorrectly interprets system messages, countermeasures intended to correct the situation may actually make things worse.

T 3.37 Unproductive searches

The Internet offers millions of information sites, documents and files. In order to navigate in the enormous amount of information on offer, a simple mouse click can be used to follow up cross-references. This enables users to rapidly switch to further information sites, which then have cross-references to even more sites. Navigating from one site to another using cross-references is called "surfing" and can lead to extremely time-consuming searches.

In many organisations, Internet services have been introduced without thoroughly examining the goals connected with them and the expected effects. The training and assistance for the users are often inadequate, leading to unproductive searches in the diversity of information offered on the Internet. Both the users and those responsible for IT often fail to realise how much such queries cost. A consultancy firm estimates that surfing and unnecessary or long research in the Internet causes personnel and communication costs of several million that could be avoided each year.

T 3.38 Errors in configuration and operation

Configuration errors arise when parameters and options with which a program is started are set incorrectly or incompletely. This includes access rights which are laid down incorrectly. Operational errors are not only incorrect for individual settings, but IT systems or applications are handled incorrectly. An example of this is starting programs which are not necessary for the purpose of the computer but could be misused by a perpetrator.

Examples of current configuration or operation errors are saving passwords on a PC on which software from the Internet is run without being checked (such software was used in the spring of 1998, for example, to spy out T-Online passwords), or loading and implementing defective ActiveX Controls. These programs, one of whose tasks is to make WWW sites more attractive through dynamic contents, are run with the same rights that the user has - they can therefore delete, alter or send data at will.

Many programs which were intended to relay data in an open environment without restrictions can, in the case of false configuration, provide potential perpetrators with data that they can misuse. In this way, for example, the *finger* service can inform them how long a user has already been sitting at a computer. This also includes WWW browsers which transmit a series of information to the WWW server whenever a query is made (e.g. the version of the browser and the operating system in use, the name and the Internet address of the PC). In this context, cookies should also be mentioned. These are files in which the operators of WWW servers store data concerning the WWW user in the user's computer. This data can be called up when the server is next visited and be used by the operator of the server to analyse the server's WWW sites that the user has already visited.

The use of a Domain Name System (DNS), which is responsible for transcribing an Internet name such as *rechner1.universitaet.de* into the corresponding numeric address, is a further source of danger. On the one hand, an incorrectly-configured DNS enables you to query a large quantity of information regarding a local network. On the other hand, perpetrators can send forged IP numbers by taking over the server, enabling them to control all data traffic.

A great threat is also posed by executable contents in E-mails or web pages. This is known under the name content security problem. Files that are downloaded from the Internet can contain a code which is implemented without consulting the user when they are just "viewing". This is the case, for example, for macros in Winword files and was exploited to produce what are known as macro viruses. Even new programming languages and programming interfaces such as ActiveX, Javascript or Java, which were developed for applications in the Internet, also have the potential to cause damage if the control function is used incorrectly.

T 3.39 Improper administration of the RAS system

Improper administration of RAS components constitutes a potential risk which should not be overlooked. Once they get to a certain size and structure, RAS systems are complex systems which only trained system administrators can configure correctly and securely. Administrative errors generally have a pronounced effect on the stability and security as an administrator possesses privileged rights in the system. Some of the problems which can occur with RAS systems are set out below.

- Security-relevant routine tasks on the RAS client are frequently neglected. These include, for example, regular data backups or scanning for computer viruses. In particular, mobile RAS clients are taken around by their users and are therefore only seldom available to system administration staff. While it is possible for remote administration to be performed during an established RAS session, depending on usage profile, connection times may be too short to carry out systematic remote maintenance. But if the regular administrative tasks are not performed, different clients may have different configurations.

Neglect of security-relevant routine tasks

- Remote administration of computers can be performed with the aid of commonly used software products and is often possible simply using mechanisms provided by the operating system. The use of unauthorised software (by the user or the administrator), often means that either non-permitted protocols are used over a RAS connection or that settings are made which do not comply with the security guidelines in force and can therefore open up security loopholes.

Unauthorised use of software for remote administration

- If computer virus checking is performed exclusively on the server, encryption of data client-side can be a problem. Many application protocols can be processed over RAS connections so that transport of e-mail, Web content or files is possible. Encrypted data can in this case no longer be checked for viruses using anti-virus software installed on the server.

Encryption and virus protection

- There is no anti-virus software installed on the RAS client or such software is out of date or disabled. As RAS clients are frequently operated in insecure environments with the result, for example, that the exchange of data media is in practice uncontrolled, computer viruses constitute a particularly serious threat. In particular, the danger exists that computer viruses or Trojan horses can find their way into the LAN through the RAS client.

Inadequate virus protection on RAS clients

- If functions which place heavy demands on bandwidth are performed over RAS connections, then there is a danger that the user will terminate a RAS session and start another one because he believes there is a fault on the line. But in reality it is simply a case of the response time being unacceptably slow because the bandwidth is inadequate. This can not only result in inconsistencies in the application data due to unexpected termination of a connection, but repeated attempts by users to establish a connection followed by termination of the connection can also increase the loading on the RAS system.

Long response times due to insufficient bandwidth

- A general danger found when administration is inadequate is that hardware or software components used for communication, upon which the RAS connections rely, are configured either incorrectly or so that they are incompatible. Incorrect configuration can range here from incorrect security settings through to incompatible communication protocols. The consequences of incorrect configuration are just as diverse, for example, users are unable to log on when they need to or unauthorised third parties can successfully establish a connection.

Incorrectly configured components for communication

Examples

- An employee working out in the field regularly uses the replication mechanism of a groupware product to update his local copy of a technical reference database. Because the replication mechanism is incorrectly configured, replication is always initiated after the RAS connection has been established so that connection using a mobile phone modem always appears to "hang" after successful logon.
- A company uses a software management system which regularly installs new software updates on the individual users' computers. Due to a configuration error, the mobile RAS clients are included in this procedure. After a connection has been successfully established, the entire bandwidth is then taken up by the management software attempting to install a substantial update package on the computer.

T 3.40 Inappropriate use of authentication services with remote access

Inconsistent RAS user administration

The RAS user's identity must be determined during logon. This typically entails the use of authentication mechanisms which are based on user administration facilities involving the storage of authentication data. RAS systems offer several options for the storage of user data: separate user administration facilities, use of the user administration facilities of the operating system, use of authentication servers (with separate user administration). If different user administration systems are used for RAS and the operating system, it is possible if there are lapses in organisational processes for inconsistencies to come about in the two sets of data. This can lead to the establishment of connections which are not permitted and to unauthorised data access. Separate administration is therefore not recommended.

Example

- When an employee leaves the organisation, his user account is not deleted in the RAS user administration software. The former employee can therefore continue to dial in via RAS access and access all generally accessible data. Access can also be used to initiate other attacks.

Storage of authentication data on the RAS client

Many client components for remote access allow the data necessary for authentication to be locally stored after it has been entered once so that when further connections are subsequently established it is no longer necessary for the user to enter the data. However, this procedure can be dangerous if the RAS client is subject to unauthorised access. The authentication mechanism can then no longer perform its intended role. As a result, unauthorised persons may be able to access the local network which can be accessed over a RAS link from the client concerned, thus endangering the security of these local network. Storage of keys for data encryption or digital signatures on the RAS client carries a similar risk.

T 3.41 Improper use of remote access services

Unless users receive appropriate training it is possible, as with every other IT system, for security problems to develop as a result of users' (usually unintentional) mistaken actions while using RAS or in the environment in which RAS is used (e.g. violation of IT security guidelines or incorrect configuration).

Moreover, stationary and mobile IT systems on which RAS client software is installed are often used not just to access a LAN. In particular, if the RAS connection is established over the Internet, then often Web and e-mail services are used over these IT systems. In many cases external networks are accessed, for example, when employees working in the field log on to customer networks using mobile RAS clients. This can result in exposure to the threats described below.

- As a minimum, establishment of connections which have not been approved causes unnecessary loading of the system, as an authorisation check has to be performed in every case. In this way, system resources are tied up unnecessarily. When this is combined with incorrect configuration settings, the result may that an attempt at unauthorised access succeeds.

Unapproved RAS connections established

- Amongst other possibilities, RAS clients can be used for Internet access. One potential danger here is that unless special precautions (e.g. secure configuration or PC firewall) are taken, it may be possible to access the client computer from the Internet. This means that the computer is exposed to potential attacks. Thus, for example, an aggressor could disable data encryption or change other RAS configuration data so that secure RAS communication is no longer possible. Similar problems (viruses, Trojan horses) can arise where software has been downloaded from the Internet and stored on the RAS client.

Use of the RAS client on the Internet

- If a RAS client is connected to an external LAN (e.g. customer network or private home network), often there will be interfaces from that LAN to other networks, e.g. the Internet or local subnets. Depending on the security requirements covering LAN administration, uncontrolled access to the RAS client may be possible (see also T 5.39 *Infiltrating computer systems via communication cards*).

Connection of the RAS client to an external network

Examples

- During a business trip an employee logs on to the corporate network over the Internet. Before the connection is established with the RAS system, he loads an executable file from a Web server. In addition to its "official" functionality, the file also contains a malicious section of code which attempts to influence the security mechanisms in the RAS configuration (e.g. disabling of encryption) and to access data in the corporate network where an existing RAS connection has been previously discovered.
- An employee working out in the field connects his laptop to the network of a customer. In order to be able to exchange data with the customer, he makes some local directories shared so that they can be accessed from the

network. By mistake the file in which the employee has stored his authentication data is also transmitted during the exchange of data.

T 3.42 Insecure configuration of RAS clients

Limited scope for administration with RAS clients

The security of the RAS system depends both on the secure configuration of the RAS server and also on the RAS client. Even if the configuration of the server is under the full control of an administrator, the RAS clients will often be outside of the organisation. This means that the computer can only loosely be included in administrative processes. Especially where mobile RAS clients are used, users can also be given certain administrative rights to enable them to resolve problems with RAS access by changing the RAS configuration parameters, either by themselves or by being guided over the telephone.

The limited ability of the system administrators to exercise control over RAS clients may result in these being insecurely configured. Examples are:

Insecure configuration of the browser

- Browsers are frequently not at all straightforward to configure, and often this results in incorrect settings. If security mechanisms are disabled (e.g. Java, JavaScript and/or ActiveX are activated), it is possible for unreliable software to get onto the client.
- Another problem is the installation of non-permitted software on the RAS client, as this may contain security loopholes or allow the introduction of computer viruses or Trojan horses.
- Often RAS users will fail to make proper use of the available security mechanisms are or else they will make the wrong settings (see also T 5.91 *Disabling of RAS access security mechanisms*).

Use of incompatible authentication mechanisms

- Other problems may arise if incompatible authentication mechanisms are used between RAS client and RAS server. Thus, for example, the authentication protocol MS-CHAP of a Windows 3.11 RAS client is incompatible with the MS-CHAP protocol of a Windows NT 4.0 server. The result is that the client cannot establish a connection with the server.

T 3.43 Inappropriate handling of passwords

Even the use of well thought out authentication procedures will be of little avail if the users are careless in handling the necessary access-granting means. Whether the access-granting means used are passwords, PINs or authentication tokens, in practice they are often disclosed to other persons or not kept safe.

Passing on of passwords or token

Often users disclose their passwords to other users for reasons of convenience. Passwords are frequently shared within teams so that it is easier for individual staff to access shared files. The obligation to use a password is often experienced as onerous and, to make life easier, passwords are never changed or else all staff use the same password.

Loss of an authentication token

Where a token-based procedure (e.g. smart card or one-time password generator) is used for user authentication, if this is lost there is a danger that the token could be used by unauthorised persons. An unauthorised user might thus be able to establish a remote access connection using this token.

Too many different passwords

Where large numbers of different passwords and PINs are used, often users cannot remember them all. Frequently this results in passwords being forgotten, which sometimes means that extra work is required in order to be able to continue working with the system. Again, authentication tokens can get lost. With very secure IT Systems, the loss of passwords or tokens can even result in loss of all user data.

Password under the keyboard

Often passwords are written down in order to prevent their being forgotten. This is not a problem as long as they are carefully looked after so that they are protected against unauthorised access. Unfortunately this is not always the case. A classic example is to keep the password written underneath the keyboard or on a sticker attached to the screen. Keeping authentication tokens underneath the keyboard is also a popular habit.

Passwords which are too simple

Another means of avoiding forgetting passwords is to choose "suitable" passwords. But if users are able to choose their passwords themselves and have not been made sufficiently aware of the problems, they will often choose trivial passwords such as "4711" or the names of friends.

Examples:

- It was established in one company using spot checks that many passwords were not suitable or were not being changed sufficiently frequently. Technical means were employed to ensure that passwords were changed every month and also contained numbers or special characters. It turned out that one administrator was choosing his passwords as follows:

  january98, february98, march98 etc.

- In a government organisation it was discovered that users whose offices faced the street often used the same password, the name of the hotel over the road which, with its large illuminated letters, dominated the view out of the window.

T 3.44 Carelessness in handling information

It is frequently observed that although a number of organisational or technical security procedures are in place, these are undermined through careless handling of the technology. A typical example of this is the almost proverbial sticker on the monitor which contains a list of all the access passwords. Abundant other examples of carelessness, dereliction of duty or recklessness in handling information that needs to be kept secure are also to be found.

Examples:

- Employees often divulge confidential information about their company over mobile phones on trains or in restaurants. This information is not only heard by the person the other end but also by everyone around. Examples of particularly interesting internal information divulged in this way include

  Allowing information to be overheard

- why a contract with another company was lost or
- how many millions planning errors in the strategy department have cost and how this could depress the share price of the company if anyone were to find out about it.

- Often it is necessary during business trips to take a notebook, an organiser or data storage media along with one. During breaks, these are gaily left behind in the meeting room, the train compartment or the car. The data stored on these mobile IT systems is often not backed up anywhere else. If the IT system is then stolen, the data is lost for ever. In addition, a thief may be able to make good money from the sale of potentially explosive data that he has been able to access easily due to lack of encryption or access protection.

  Allowing information to fall into the wrong hands

- One reason for taking a notebook or files on business trips is to be able to make productive use of travelling time. This practice often provides fellow travellers with interesting insights, as it is virtually impossible on a train or aircraft to prevent a person in the next seat from also being able to read the documents or the screen.

  Allowing other people to read information

  Premises which are open to the public, e.g. hotel foyers, hotel business centres or train compartments, generally provide little in the way of privacy protection. If the user enters passwords or has to make changes to the configuration, an adversary could acquire this information and misuse it.

- Articles appear at regular intervals in the press about public bodies and companies whose dustbins in the rear yard contain highly explosive documents. For example, pay information for all the employees in one company and the ex-directory phone numbers of a company's board of directors have become public knowledge by this means.

  Explosive information in waste containers

- When IT systems develop faults, they are sent quickly for repair. Often once a system has developed a fault it is no longer possible to delete data that is stored on it. When a failure occurs the top priority is usually to have a working machine again as soon as possible. For this reason, many specialist suppliers offer a special customer service which involves simply exchanging defective components and sending customers home with a system that works.

  Exchange of components during repair

However, there have been a number of cases where such dealers were able to resolve the problem quite quickly during subsequent examination and the next customer was then generously given the now repaired machine - including all the data belonging to the original customer.

T 3.45 Inadequate checking of the identity of communication partners

Thoughtless disclosure of internal information

During personal conversations, on the phone or using e-mail, many people are prepared to pass on a lot more information than they would do in writing or if they had a larger audience. Often it is tacitly assumed that the communication partner will treat the content of the conversation or e-mail as confidential. There is also a disinclination to enquire as to the identity of a caller as this will appear impolite. The same considerations deter people from querying the reason for the call or enquiring as to the person on whose behalf the caller is ringing ("I work for XY Bank and need some detailed information on your income level.") Such behavioural patterns can be exploited through "social engineering" (see also T 5.42 *Social engineering*).

Example:

There are many cases known in which journalists have phoned up important people and pretended to be other important people. In this way they have succeeded in obtaining information from celebrities or public figures which was not intended for the public. This has proved to be dynamite where the information was transmitted directly over the radio so that it was not possible to reverse publication.

T 4 Threats Catalogue Technical Failure

T 4.1	Disruption of power supply
T 4.2	Failure of internal supply networks
T 4.3	Inoperability of existing safeguards
T 4.4	Impairment of lines due to environmental factors
T 4.5	Cross-talk
T 4.6	Voltage variations / overvoltage / undervoltage
T 4.7	Defective data media
T 4.8	Discovery of software vulnerabilities
T 4.9	Disruption of the internal power supply
T 4.10	Complexity of access possibilities to networked IT systems
T 4.11	Lack of authentication possibilities between NIS Server and NIS Client
T 4.12	Lack of authentication possibilities between X Server and X Client
T 4.13	Loss of stored data
T 4.14	Fading of special fax paper
T 4.15	Fax transmission errors
T 4.16	Fax transmission errors
T 4.17	Technical defects of fax machines
T 4.18	Discharged or fatigued emergency power supply in answering machines
T 4.19	Information loss due to exhausted storage medium
T 4.20	Data loss due to exhausting storage medium
T 4.21	Transient currents on shielding
T 4.22	Software vulnerabilities or errors
T 4.23	Automatic CD-ROM-recognition
T 4.24	File name conversion when backing up data under Windows 95
T 4.25	Still active connections
T 4.26	Failure of a database
T 4.27	Circumvention of access control via ODBC
T 4.28	Loss of data in a database

T 4.29 Loss of data in a database caused by a lack of

T 4.30 Loss of database integrity/consistency

T 4.31 Failure or malfunction of a

T 4.32 Failure to dispatch a message

T 4.33 Poor-quality or missing authentication

T 4.34 Failure of a cryptomodule

T 4.35 Insecure cryptographic algorithms

T 4.36 Mistakes in encrypted data

T 4.37 Lack of time authenticity in E-mail

T 4.38 Failure of components of a network management system or system management system

T 4.39 Software conception errors

T 4.40 Unsuitable fitting out of the RAS client

T 4.41 Non-availability of the mobile communication network

T 4.42 Failure of the mobile phone

T 4.1 Disruption of power supply

Despite high assurance of a continuity of supply, power supply will be disrupted from time to time. For the major part such failures, with a duration of less than one second, are so short that people will not notice them. However, IT operations can be disrupted even by failures of more than 10 ms. In the Federal Republic of Germany, approximately 100 network downfalls of this type were recorded in 1983 as nation-wide measurements were carried out at some 60 measuring points. Of these, five failures lasted for up to 1 hour, and one had a duration of more than one hour. These interruptions were due exclusively to failures of the supply network. In addition, interruptions may be caused by disconnection for unannounced maintenance/repair purposes or by cables damaged during foundation works.

Not only direct power consumers (PC, lighting, etc.) depend on power supply. All infrastructure installations nowadays are either directly or indirectly dependent on electric power. For instance: elevators, pneumatic dispatch systems, air-conditioning, intruder and fire detection devices, and telephone private branch exchanges. Even water supply in high-rise buildings is currently dependent on electric power due to the pumps needed for generation of pressure in the upper storeys.

Example:

In a large Southern German industrial plant, the entire power supply was interrupted for several hours on account of technical problems at the power utility. This resulted in an interruption of production and in the failure of all computers of the development divisions that had no auxiliary power supply.

T 4.2 Failure of internal supply networks

Supply network failure, such as:

- electricity,
- telephone and
- air conditioning / ventilation

can all lead to immediate breakdown of the IT operation. Disruption can also be caused by failure in the following areas:

- heating,
- water,
- feeders for fire-fighting water,
- sewarage,
- pneumatic dispatch,
- gas,
- reporting and control devices (intruders; fire; housekeeping control engineering) and
- intercom systems

These disruptions may occur with a substantial delay in regard to the original failure.

These networks are mutually dependent to various degrees, so that malfunctions in any one of them could also have an impact on others.

Examples:

- Power failure does not only have a direct impact on IT processes, but also affects other networks using electrically operated automatic controls. Even sewerage pipes may be provided with electric lifting pumps.
- By means of modern telecommunications facilities (ISDN technology), it is possible to build up LANs. Glitches within the telecommunications network will automatically affect the pertinent LAN.
- An outage of water supply may impair the functioning of air conditioning systems.
- Failure of the air conditioning system can impair utilisation of the building due to excessive heating or cooling, or on account of insufficient air exchange.

T 4.3 Inoperability of existing safeguards

Due to technical defects or external factors (e.g. on account of ageing, operating errors, deficient maintenance, manipulation, power failure), safety devices may become inoperative, resulting in their protective effect being greatly reduced or neutralised altogether. **Examples** include:

- defective door locks;
- inadequately functioning fire extinguishers;
- soiled fire detection devices;
- damaged keys or ID cards;
- jamming bolt contacts on doors;
- burn-in of static pictures (freezing frames) in control monitors;
- wedging of fire exit doors.

T 4.4 Impairment of lines due to environmental factors

The channel capacity of cables with electric signal transmission can be adversely affected by electric and magnetic fields. Whether this will lead to actual disruption of signal transmission will basically depend on three factors:

- frequency range, intensity, and duration of exposure;
- cable shielding; and
- safeguards during data transmission (redundancy, error correction).

In many instances, impairment can be identified in advance:

- Along high-tension lines and in the vicinity of large engines, strong inductive fields are generated. (railroad, production plant, elevator)
- In the vicinity of transmitter installations, electro-magnetic fields can exist (broadcasting, police/fire department, service radio, paging systems, wireless networks)
- Portable telephones ("mobiles") exceed the disruption sensitivity of many IT systems due to the strength of their transmission (2 to 4 watts).
- Cables influence each other by mutual induction.

Irrespective of merely electrical or magnetic factors, other environmental conditions may have an effect on a cable:

- high temperatures (during process control);
- aggressive gases, and
- high mechanical stress (e.g. during provisional layout on floors, lines to mobile devices).

T 4.5 Cross-talk

Cross-talk is a special form of line impairment. In this case, the fault is not generally caused in the environment, but by currents and voltages of signals transmitted over adjacent lines. The intensity of this effect depends on the cable structure (shielding, cable capacity, insulation quality) and on the electrical parameters for information transmission (current, voltage, frequency).

Not every line affected by cross-talk will, in turn, necessarily have an effect on others. This phenomenon is encountered in the (analogue) telephone network. There, calls of other network participants can be heard. However, these often do not respond to the request "to clear the line" because cross-talk is confined to one direction. Checking one's own lines for coupled-in, other-source signals does not yield any information on whether one's own signals cause cross-talk in other lines and whether they can thus be monitored.

The main differences compared to other line faults is that, apart from disruption of signal transmission on adjacent lines, exploitable information may be available on other lines due to cross-talk.

T 4.6 Voltage variations / overvoltage / undervoltage

Variations in the supply voltage may result in malfunctions and damage of IT systems. Such variations range from extremely short and minor incidents, which have little or no effect on IT systems, to complete failure or destructive overvoltage. This may be triggered in all sectors of the power supply network, ranging from the utility network to the circuit to which the respective devices are connected.

T 4.7 Defective data media

Failure of or defects in individual data media due to technical deficiencies or damage are quite common. Such media include mass storage devices such as hard disks, tapes, and cartridges. Hard disks can be destroyed by crashes of the read/write head, while tapes and cassettes can be damaged by direct mechanical impacts. Again, CD's can be rendered useless by surface scratches. Diskettes are particularly vulnerable to failure: it is not an uncommon occurrence for reading from, or writing to, a diskette to suddenly become no longer possible.

Examples

- In a medium-sized company there was a build-up of dust due to building work. The dust particles found their way to the magnetic disk of the computer used in that firm, causing a head crash as a result of which some data was destroyed.
- Faults started inexplicably occurring on the laptop of a field service employee although the laptop was always transported carefully packed. It turned out that the hard disk of the laptop had been damaged by a magnet which was used to secure a folding table on his train.
- During data backup of a multimedia PC, some ZIP diskettes were temporarily stacked on its speakers. The magnets in the speakers destroyed parts of the data media.

T 4.8 Discovery of software vulnerabilities

Software vulnerabilities includes unintentional program errors which are not known to the user or not yet known and constitute a security risk to the IT system. Security loopholes are constantly being found in existing software, including in widely used or quite new software.

Examples

Some examples of known software vulnerabilities are as follows:

- A *sendmail bug* under UNIX which enabled any user to execute programs and modify files by using the *sendmail* UID and GID.
- The *gets* routine under UNIX. This was used by the *fingerd* program to read a line, without any check being made of the boundaries of variables. Thus, by means of an overflow it was possible to modify the stack in such a way that a new shell could be started.
- cgi scripts which are supplied with www servers. Remote users were able to access sensitive information over the www server.
- A bug in the DNS software allowed temporarily stored DNS data to be falsified.
- Incorrect implementations of the TCP/IP stack. These enabled entire networks to be paralysed due to oversize or otherwise manipulated packets.

T 4.9 Disruption of the internal power supply

Use of a mobile IT system, e.g. a laptop, pre-supposes that the system has a power supply unit independent of the mains. Such a unit, which generally uses rechargeable batteries, will usually last for several hours of operation. After that period, sufficient power supply is no longer ensured so the IT system will have to be de-activated or connected to the supply mains. The majority of mobile systems constantly check the supply voltage and indicate any critical voltage drop. If such a message is disregarded, the system may all of a sudden become inoperative, and the results of the latest transactions that are stored only in the main memory, will be lost.

T 4.10 Complexity of access possibilities to networked IT systems

As opposed to stand-alone systems where the log-in process is essentially responsible for access control, and which can thus be corrupted only by inadequately defined or insufficient passwords, network computers have many complex processes allowing multifarious forms of access. Thus, for instance, under Unix *sendmail* allows for the introduction of texts (mails) into the network computer; *FTP* allows a log-in, albeit restricted, which in instances (*anonymous FTP*) is not even protected by a password; while *telnet* allows a complete log-in.

For security reasons server systems such as Windows NT or Novell Netware avoid the transmission of plain-text passwords. However, this security mechanism will be deactivated when using services such as FTP or Telnet as plain-text passwords are used.

Apart from the fact that all these processes can constitute a security flaw on account of an incorrect or faulty configuration, there is, of course, also a much greater probability that a security-related programming error could exist in one of the processes due to its size.

T 4.11 Lack of authentication possibilities between NIS Server and NIS Client

If the NIS domain name is known, any computer can be signed on as a client, and all NIS maps can be read, in particular the *password* map.

If administrator privileges can be gained on a system, a NIS server process (*ypserv*) can be started on a privileged port. The client process *ypbind* is then restarted on the target system. If the server process responds faster than the original NIS server arbitrary information can be transmitted to the client.

T 4.12 Lack of authentication possibilities between X Server and X Client

Without suitable security mechanisms, such as, for example, "magic cookies" or use of Secure Shell, the X Windows system especially should only be used in a trusted environment. Without security enforcing functions it is possible for any participating user to corrupt both the X client and the X server. The X server process, which is responsible for the input and output on a computer, has no means of detecting the identity of the owner of the X client process which is communicating with it. In this way all X clients can access all data input on an X server, and the X server has no means of telling from which X client it is receiving data. Thus, for example, the *meltdown* program simulates optical "melting" of the screen of any X server, while it equally possible to read data of an *xterm* client or to send own data to that client, i.e. make screen copies from another computer that runs on X Windows.

Examples

- With the *xspy* tool it is possible to automatically record keyboard inputs remotely on an *xterm* client.
- Windows which are displayed by an aggressor on an X server are visually no different from those of the intended X client. In this way an aggressor could implant false information or provoke the input of sensitive information with the aid of "imposter" windows.

T 4.13 Loss of stored data

The loss of stored data can have a major influence on IT applications. The loss or forgery of application data or customer databases could threaten the existence of private enterprises. In government agencies, the loss or forgery of important data can delay or even preclude administrative work and specialist tasks.

Stored data can be lost for a variety of reasons:

- Demagnetisation of magnetic data media due to ageing or unsuitable environmental conditions (temperature, air moisture),
- Interference of magnetic data media by extraneous magnetic fields
- Destruction of data media by force majeure, e.g. fire or water
- Inadvertent deletion or overwriting of files
- Technical failure of external storage (headcrash)
- Faulty data media
- Uncontrolled changes in stored data (loss of integrity)
- Deliberate deletion of files with computer-viruses etc.

T 4.14 Fading of special fax paper

Fax machines using the thermal printing technique require special paper on which the print can become illegible due to the text fading or the paper blackening after just a short period of time. Furthermore, this type of paper can become discoloured upon contact with text markers or adhesives, thus making the text illegible.

T 4.15 Fax transmission errors

Malfunctions on the transmission path

During fax transmission, faults can occur either on the transmission path or on any of the terminal devices involved. As a result, it is possible for fax transmissions to be incomplete, illegible or to fail to reach their intended recipients. Decisions which depend on this information could be inappropriate, resulting in loss or damage.

Delivery to the wrong recipient

There is also a danger that the fax could be sent to the wrong recipient. This could be due to faulty switching in the public telecommunications network. It is also possible on conventional fax machines for the wrong call number to be dialled or for the shortcut destination keys to be incorrectly programmed. When a fax server is used, it is possible for a recipient's call number to be incorrectly input or for an incorrect version of it to be held in the address book. As a result, confidential information could be disclosed to unauthorised parties. The amount of damage this could cause depends on the confidentiality of the information. Moreover, the originator of the fax will incorrectly assume that the fax message has been transmitted successfully to the intended addressee. The resulting time delay could prove detrimental.

Example:

A well-known German company lost a major order because the offer was accidentally sent to the wrong recipient.

Note:

Threats T 4.16 *Fax transmission errors* and T 4.17 *Technical defects on fax machines* have been amalgamated in threat T 4.15 *Fax transmission errors*.

T 4.16 Fax transmission errors

Errors along the transmission route or within the connected devices could cause losses or illegibility in the information by the time it has reached the recipient. Decisions based on this information could thus prove detrimental.

T 4.17 Technical defects on fax machines

Technical defects can cause a fax machine to malfunction or reproduce information incorrectly/incompletely. Thus the availability and integrity of the transmitted information are at risk. This is especially dangerous if the defect is not obvious and the incompleteness of the information is not detected in time.

T 4.18 Discharged or fatigued emergency power supply in answering machines

Answering machines with a digital memory are equipped with a battery or accumulator which allows the memory contents to be retained in case of a power failure. If the capacity of the battery or accumulator is exhausted before the end of a power failure, this generally results in the deletion of the outgoing message and, in the case of digital recordings, the messages already in the memory.

T 4.19 Information loss due to exhausted storage medium

If the storage medium (digital memory or audio tape) in the answering machine is full of recorded messages, this makes it impossible to record further messages or causes earlier messages to be overwritten with new ones. Information loss is the result in both cases.

T 4.20 Data loss due to exhausting storage medium

Every storage medium has a limited capacity for holding data. When this limit has been reached, the result may be the loss of data and services becoming no longer available, such as:

- Users unable to save any more data;
- Incoming email is rejected;
- Incoming or outgoing fax transmissins are rejected, or
- It is no longer possible to keep audits or audit data that have not yet been evaluated and are then overwritten.

The capacity of the storage medium can suddenly be exhausted due to various reasons, e.g. due to errors in the application program, increased storage requirements of the users or a malicious attack intended to specifically reduce the existing storage space, thus preventing audit trails from being kept.

T 4.21 Transient currents on shielding

If IT appliances supplied by electricity via a TN-C network are connected with double-sided shielding, the result may be transient currents on the shielding (an explanatory diagram is to be found in S 1.39 *Prevention of transient currents on shielding*).

The reason for this is the nature of the TN-C network, whereby protective (PE) and neutral (N) conductors are led together to the various distribution points as a PEN conductor. The separation into N and PE conductors only takes place in the distribution. This installation is permissible according to VDE 0100!

If the interface shieldings of appliances (supported by different distribution points) that are connected with PE are connected together by shielded data lines, the result is a parallel connection of the PEN conductor between the distributors and the shielding between the interfaces. The transient current flowing over the shielding can lead to damage of the interfaces and to the risk of personal injury when working on the data lines.

No transient currents flow over the shielding of data lines between appliances which are connected to the same distribution in a TN-C network or between appliances which are connected to various distributions in a TN-S network.

With regard to TN-CS networks, some parts are designed as a TN-C network, others as a TN-S network. As long as data lines with double-sided shielding are only led within one section, the same will apply as in the relevant networks. However, if IT appliances in different areas are connected via data lines with double-sided shielding, transient currents can also flow in the TN-S area.

T 4.22 Software vulnerabilities or errors

The same applies to standard software as for all other software: the more complex it is, the more frequently errors occur. It should be noted that high expectations of the user and standard software appearing in too short intervals can also lead to the manufacturer publishing its product before it is ready and free of errors. If these software errors are not detected, the errors resulting from the use of the software can have serious consequences.

Examples:

- The strength of the security functions in the standard software (such as passwords or encryption algorithms) is frequently overestimated by the user. These security functions can often not permanently withstand a well-planned attack. For example, this applies to the encryption functions which are integrated into a number of word processing programs. For almost all of them, the Internet provides numerous tools to overcome this encryption.
- The appearance of a certain word in the spell-check of a word-processing program consistently caused a crash.
- Standard software often contains undocumented functions, such as so-called "gagscreens", features that the product developer leaves behind for posterity. On the one hand, this uses up additional IT resources and on the other hand this points out that the entire functionality of the product cannot be settled down to the last detail.
- Most of the warning messages from the Computer Emergency Response Teams in the last few years have been concerned with security-relevant programming errors. These are errors which introduced during software development and make it possible for the software to be misused by perpetrators. Most of these errors were caused by buffer overflows. These are errors in which a routine for reading characters does not check whether the length of the character string entered corresponds with the length of the memory area. This makes it possible for perpetrators to transmit an exceptionally long character sequence, so that additional commands are stored behind the memory area reserved for the entry and are executed. These commands can, for example, be programs.
- A large number of other warning messages have been caused by **denial-of-service attacks** (DoS), which can cause the computer to crash through errors in individual routines which are used for network data processing (see, for example, CERT Advisory 97.28 on IP Denial of Service Attacks: Teardrop and Land-Attack).

T 4.23 Automatic CD-ROM-recognition

If CD-ROM-recognition is activated under Windows 95, CDs are automatically recognised and the file *AUTORUN.INF* is automatically executed, provided this file is located in the root directory of the CD. This file can automatically execute any program (e.g. with harmful functions) saved on the CD-ROM.

Whether or not this option is enabled, can be recognised, for example by the fact that Explorer automatically blends in the title of the CD-ROM in front of the CD drive letter. As a side-effect, energy-saving functions usually are no longer activated.

T 4.24 File name conversion when backing up data under Windows 95

If backup programs that do not support long file names are used under Windows 95, all long file names must be converted before backup via use of the supplied program LFNBK.EXE and option /B in convention 8.3. Thereafter, the backup program should be invoked. Finally, the original filenames can be restored with LFNBK.EXE /R.

This process should be applied with care, however, since on one hand, information can be lost when converting names, and on the other hand files may no longer be restored as soon as the directory structure of the PC has changed after backup. This can lead to a loss of data.

T 4.25 Still active connections

An ISDN communications adapter might actually fail to close down a connection established previously via the communications software. If such a defect is suspected, it can be verified easily by calling the corresponding ISDN subscriber number.

Example:

Before leaving on a 2-week vacation, a network administrator established an ISDN data connection with his Internet provider. On completion of the session, the ISDN connection was not terminated properly. On returning from his vacation, the network administrator was surprised to see the large bill he had received for ISDN services

T 4.26 Failure of a database

If a database fails, for example, due to a hardware/software error or an act of sabotage, this could have far-reaching consequences, depending on the function and significance of the database. In this case, all applications which rely on the data in the affected database are rendered unusable. As a result, users of these applications can no longer perform some or all of the tasks assigned to them, unless these tasks are able to be carried out manually. Depending on the type of task, which can only be performed electronically with the help of a database, this can have the following consequences:

- Financial loss
- Security pitfalls which might be severe enough to affect personal well-being (for example, in the case of medical databases)
- Partial or complete disruption of operations

T 4.27 Circumvention of access control via ODBC

Existing access control of databases can be circumvented if databases are accessed via ODBC (Open Database Connectivity) and if the ODBC drivers were installed incorrectly. This might result in the violation of confidential data and the manipulation of data in general.

T 4.28 Loss of data in a database

Loss of data in a database can be caused by a wide variety of factors, including inadvertent manipulation of data (for example, through unintentional deletion of data), database crashes and deliberate intrusions.

As a result, the availability and completeness of the data is no longer guaranteed, and the following consequences might arise:

- Applications which rely on the data in the database can no longer be executed or offer only partial function..
- The correlation of data is lost.
- Considerable time and effort are required to recover lost data.

Depending on the cause of the data loss, it can be difficult or even impossible to determine precisely which data has been lost. This can lead to further financial losses and security risks.

Example:

When a database model is changed, the old tables and structures must first be saved and deleted. Then the new tables are created. The occurrence of an error during any of these procedures can easily cause data to be lost or render it incapable of transfer.

T 4.29 Loss of data in a database caused by a lack of storage space

Every storage medium has a limited capacity for holding data. This also applies to databases which need to incorporate a physical storage medium to allow the long term storage of data. Once this storage medium is exhausted, the database might crash and result in a loss of data. The consequences of this are described in T 4.28 *Loss of data in a database*.

The capacity of a storage medium can suddenly be exhausted for a variety of reasons, e.g. errors in application programs, increased memory requirements by users, as well as deliberate intrusions aimed at lowering the storage capacity in order to disable auditing:

T 4.30 Loss of database integrity/consistency

A loss of database integrity or consistency means that data are still present in a database but have become partly corrupted or unintelligible. As a result, the data cannot be correctly processed any more. This database integrity and consistency can be impaired in a variety of ways, for example, through inadvertent data manipulations (e.g. unintentional modifications to data), inadequate checks of the synchronisation of transactions, and deliberate intrusions.

The following consequences can arise as a result:

- Certain tasks which rely on the correctness of the data in the database can no longer be performed fully or at all.
- The information in the database as a whole is corrupted.
- Considerable time and effort are required to restore the integrity and consistency of the database.

Depending on the factor responsible for the loss of database integrity/consistency, it can be difficult or even impossible to determine exactly which data were modified. This can lead to further financial losses and security risks.

Example:

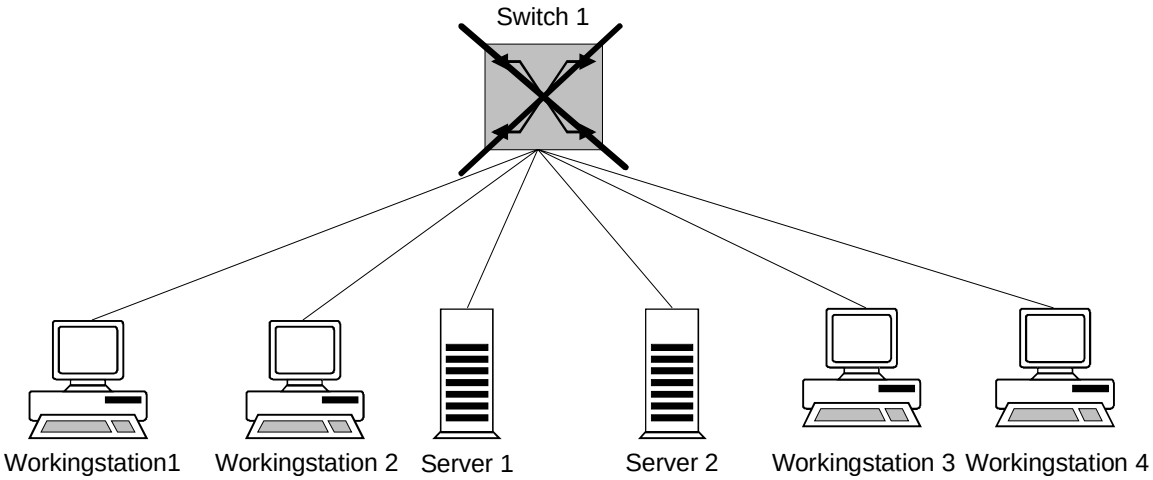
To save space and time, a database file is created in the */tmp* file system on a Unix server. This file is deleted subsequently during a nightly *cron* job, as a result of which the entire database becomes useless.

T 4.31 Failure or malfunction of a network component

A failure or malfunction of active network components impairs the availability of the entire network or sections of it. Three different situations can be distinguished:

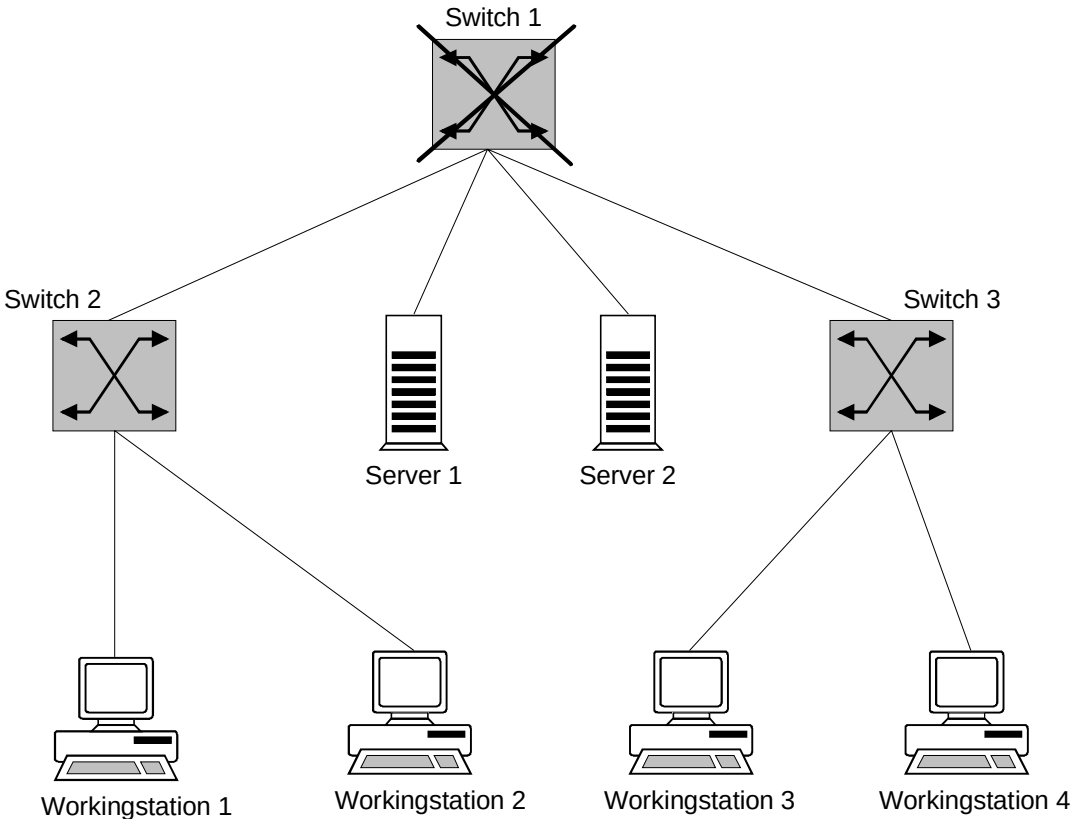
- With a failure or malfunction of the entire network component, the network is rendered inaccessible for all the stations connected to it. With such a failure or malfunction of just a single port, only the station connected via this port is no longer able to access the network.

  Example: A failure of the central switch 1 as shown in the diagram below results in a complete breakdown of communications between the connected stations.



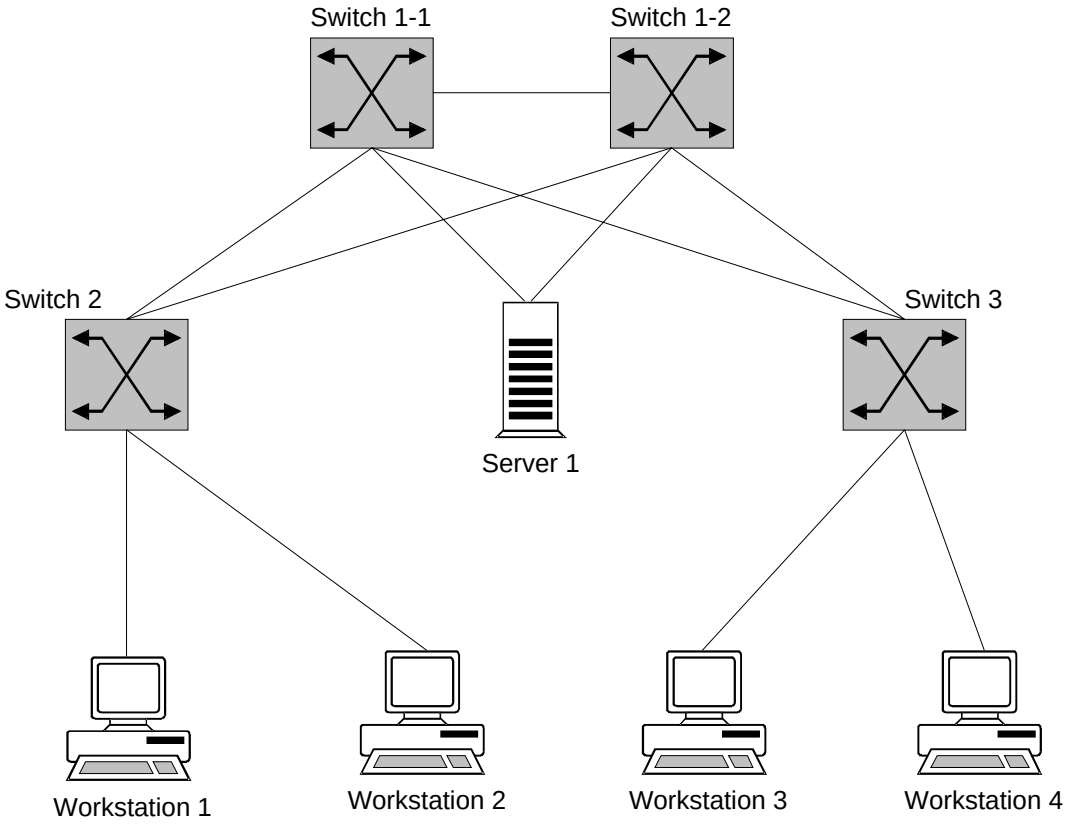
- Another situation involves active network components which are not connected directly to the network segments of mutually communicating workstation and server systems, but which are located in the signal path between these systems. If no redundant signal paths are present between the workstation and server systems in question, a failure or malfunction of one or more such components might fully or partially disrupt communications between these systems.

  Example: If switch 1 fails as shown in the diagram below, then workstations 3 and 4 can no longer communicate with the two servers or the remaining workstations.



- The last situation involves active network components which are not necessarily located in the signal path between the workstation and server systems, due to the existence of a second, redundant signal path. Some of these active network components might have been installed for the purpose of redundancy or load balancing. With a failure or malfunction of one or more of these components, communications between the workstation and server systems is still possible, but the available bandwidth in the network is restricted, because redundant signal paths might no longer be available or load balancing in the network might be impaired.

  Example: Failure of one of the redundant switches 1-1 or 1-2 as shown in the diagram below can restrict the available bandwidth for communications between the workstations and the server.

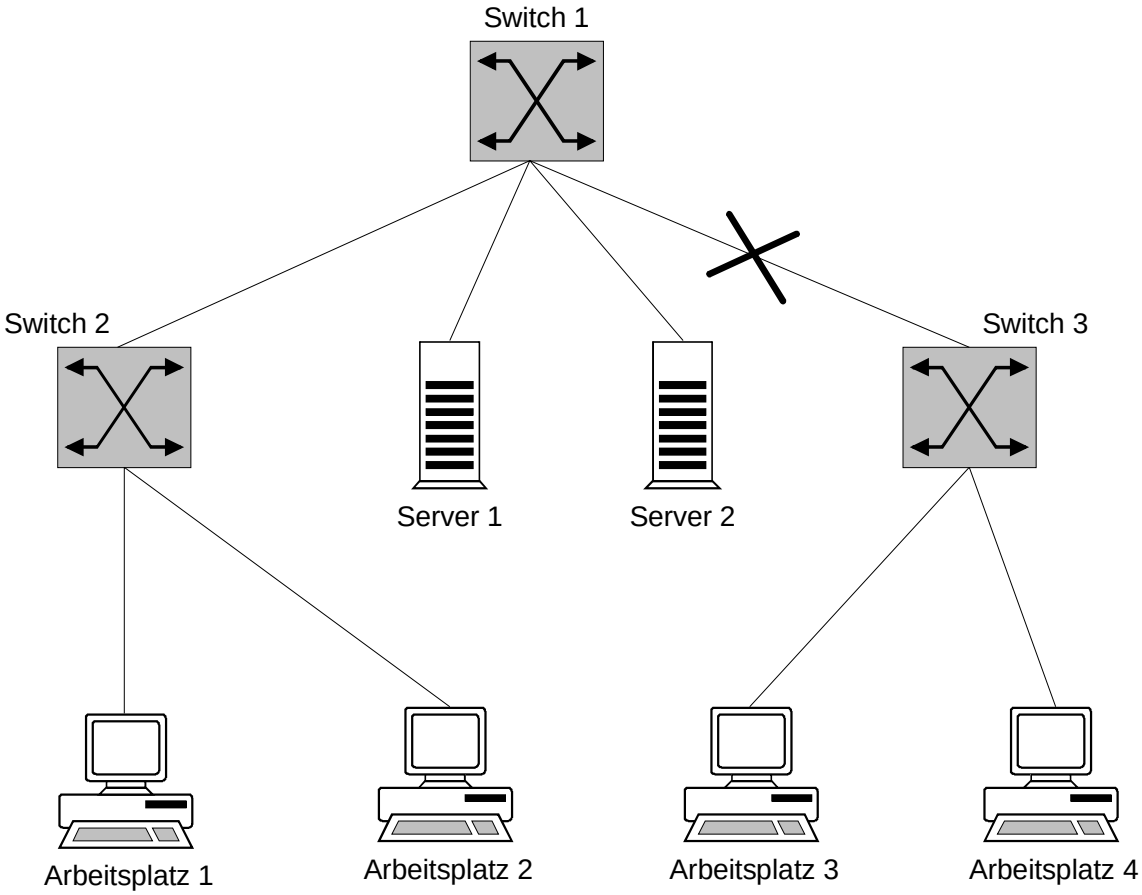


The MTBFs (Mean Time Between Failure) quoted by the manufacturers of the components can be used to estimate the risk of failure.

In the case of hubs, there are basically two different techniques of establishing connections between individual modules, and therefore between the segments connected. As regards products with a passive backplane - the element which establishes connections between modules - these backplanes provide only the electrical connections . The control unit as such is integrated in the individual modules. In the case of products with an active backplane, this element provides additional functions such as configurable communications between the modules, signal amplification etc. In general, active network components with an active backplane are more susceptible to malfunctions than active network components with a passive backplane. The failure of an active backplane leads to a complete breakdown of communications within the affected network component. In contrast, passive backplanes are designed in such a way that only mechanical violence or force majeure (e.g. lightning) can damage them. In many cases, component faults can be attributed to the related power supply units, as the components require a stable power supply. For this reason, many components are delivered with redundant power supply units or can be refitted with them. The failure of a passive network component can impair the availability of a network to the same extent. This applies, for example, to cables and connectors which link segments together. Such a threat can arise as a result of improper cable installation (e.g. non-observance of the maximum bending radius), incorrect installation of connectors (particularly in

the case of optic fibers) and interference due to electromagnetic incompatibility.

Example: If a damaged cable or connector disrupts the link between switches 3 and 1 as shown in the diagram below, workstations 3 and 4 are still able to communicate with each other, but no longer with the servers or workstations 1 and 2. The communication between workstations 3 and 4 will still be possible.



T 4.32 Failure to dispatch a message

The exchange of data via E mail is fast and convenient, but not always reliable. Messages are lost on a regular basis due to hardware and software errors in the IT systems involved, or interference in transmission lines. These technical problems can have multiple reasons. Cables can be damaged, active components can be defective, or communications software can be incorrectly configured. E mails can also be lost because the recipients address was incorrect. The biggest problem in this case is that users are often not informed about failures to deliver E mail. Mechanisms designed to automatically indicate failures to deliver messages are not completely reliable.

Many E mail programs offer options such as "Confirm dispatch" or "Confirm receipt". However, such confirmations should not be overvalued. Often, these confirmations are not issued on the arrival of E mail at the recipient's workstation, but on arrival at the mail server. No indication is given of whether or not this server successfully forwards the E mail to the intended recipient. Furthermore, indication of successful transmission of E mail is often not provided if the corresponding option has not been activated on the recipient's workstation.

T 4.33 Poor-quality or missing authentication

Authentication mechanisms can be used to authenticate users or components, or to determine the origin of data. If authentication mechanisms are missing or if the quality is too poor, there is a risk that

- unautorised persons can gain access to IT systems or data,
- the causes of problems cannot be identified or
- the source of data cannot be determined.

Gaps occur in the security

- when users are authenticated, for example if users choose passwords which are easy to guess or if they never change their password,
- when components are authenticated, for example if default passwords are not replaced by individually-chosen ones following the installation of an IT system, if the passwords which are permanently entered in many IT systems are never changed again, or if the passwords are not kept safely and nobody can remember the vital password after the system has crashed.
- in the choice of procedure, for example if it is completely useless or gaps in the security are known which are not reacted to while the system is in operation.

T 4.34 Failure of a cryptomodule

If you use a cryptomodule to protect the confidentiality of data that needs to be protected, it is particularly important that the cryptomodule functions perfectly. The failure of a cryptomodule used in such a way can have various causes:

- a technical error which impairs the module's ability to function,
- a power cut following which the cryptographic codes stored in volatile memory are deleted, so that the cryptomodule is no longer able to encode properly,
- intentional or unintentional destruction through mechanical influence, improper use or similar actions.

The failure of a cryptomodule can also result in various types of damage. Of particular interest are:

- It is no longer possible to protect a data transmission path using cryptographic procedures, making it temporarily impossible to preserve the confidentiality of the data. This is particularly critical if the failure is not noticed and, as a result of the malfunction, data is no longer encoded, although the users rely on the cryptomodule to guarantee that the data is confidential.
- Encoded data can no longer be decoded until the required cryptomodule becomes available again. This can lead to problems in the availability of IT applications which process the decoded data.
- If the cryptomodule ceases to work correctly but does not completely fail, data is encoded incompletely or incorrectly. In both cases, it can mean that the recipient (if the data is transmitted) or the user (if the data is stored locally) can no longer decode the data correctly. Without suitable data backup, this could mean that all of the data is lost.

T 4.35 Insecure cryptographic algorithms

The extent to which cryptographic processes increase security basically depends on two parameters: secure cryptographic algorithms must be used and the secret codes must be treated confidentially (for the compromising of cryptographic codes see G 5.83).

Insecure cryptographic algorithms are characterised by the fact that a potential perpetrator with justifiable resources is able to discover how the cryptographic process works. In the case of encoding algorithms, this means that it is possible to ascertain the original plain text from the encoded text without any additional information. Here, you must take into account that relevant resources for the perpetrator include available performance, aids such as analysis tools, prior knowledge, time available, knowledge concerning weaknesses, etc. Therefore, if you use insecure cryptographic algorithms, perpetrators may be able to get round the cryptographic protection.

However, you need to examine each case separately in order to determine whether a cryptographic algorithm is insecure. Nevertheless, there are several criteria which indicate insecurities:

- If secret codes with actual lengths of less than 60 bits are used in symmetric cryptographic techniques, then they can be cracked using a huge number of computers to try out every possible code. With the increasing performance of computers, it is to be expected that this limit will increase to 80 bits in the future.
- If algorithms whose security is based on the problem of factorising large numbers are used in asymmetric cryptographic techniques and signature procedures, it is now thought that code lengths of less than 768 bits should be considered insecure. This is founded on the progress in the development of efficient factorisation algorithms which currently make it possible to factorise numbers with approximately 500 bits using huge numbers of computers. At the same time, it must be taken into account that opto-electronic accelerators may be developed to perform a considerable proportion of the calculations in these processes, which would speed things up considerably.
- Hash functions which convert character strings of any length into a hash value with a constant bit length can be considered insecure if the constant length of the hash value is less than 128 bits, as it would otherwise be possible to calculate two character strings which produce the same hash value.
- Cryptographic algorithms developed by inexperienced developers that have not been investigated scientifically should be considered potentially insecure, as many years of experience are needed to develop secure cryptographic algorithms.
- Unpublished cryptographic algorithms which run remarkably quickly in software should also be considered potentially insecure. Experience shows that secure algorithms are usually based on complex mathematical functions.

- In the application of cryptographic processes, random numbers are often required. Poor generators of random numbers could cause the values produced to be predictable. This could, for example, cause cryptographic check sums, which are supposed to guarantee the integrity of a message, to become worthless.

For example, these criteria affect the DES algorithm for symmetric coding, which is used frequently world-wide. This uses an effective code length of 56 bits. The so-called triple DES algorithm, carried out three times in a row with two codes, has an effective code length of 112 bits and can be considered sufficiently secure at the moment. The RSA algorithm, an asymmetric procedure based on the factorisation problem, is also affected. If this is operated with a code length of under 512 bits, potential insecurities are to be expected. For the next few years, a code length of over 1024 bits is seen to be sufficiently secure.

A common example of an insecure but extremely fast algorithm is what is known as the XOR function, which uses a simple method of linking constant values to the original plain text. This is a high-performance algorithm which, however, can be cracked extremely quickly. The XOR function can, on the other hand, be the most secure coding algorithm there is, if the data to be encoded are XOR-ed with unpredictable random values (One-Time-Pad).

For inexperienced users it is practically impossible to determine whether a cryptographic algorithm is sufficiently secure. Therefore, you should only use algorithms that are known to have been developed by experts or have undergone years of scientific investigations.

T 4.36 Mistakes in encoded data

If data which is in an encoded form is changed, it may no longer be possible to decode the data correctly. According to the mode of operation of the encoding routines, this can mean that only a few bytes are decoded incorrectly or that all data following the error is decoded incorrectly. If there is no data backup, this can cause the data to be lost entirely.

Errors in the encoded data can occur in various ways:

- When the encoded data is transmitted, a transmission error occurs that cannot be corrected.
- A permanent error occurs in the storage medium (floppy disk, hard disk).
- A computer virus manipulates the data.
- A third person intentionally manipulates the data, for example by manipulating the encoded data in a few places with an editor.

In serious cases, such as when bits are lost or a large amount of data is altered and the error is propagated, the data cannot be reconstructed even if you know the cryptographic process and the code used for encoding.

An error in the cryptographic codes used can be even more serious. Even if a single bit of a cryptographic code is altered, the result is that all of the data encoded with it can no longer be decoded. If the cryptographic code has no data backup, this data is lost for good.

T 4.37 Lack of time authenticity in E-mail

An E-mail can contain various information about time, such as the time a message was sent, the transmission time or the time it was received. These are not tamperproof, though. For example, the time a message was sent can be falsified by adjusting the system time on the computer from which the message was sent. While an E-mail is on it's way from the sender to the recipient, the mail header, in particular the entries for time, date and address of the mail server, can be falsified at will. A further attack to be mentioned is the systematic and purposeful corruption and diversion of SMTP packets.

T 4.38 Failure of components of a network management system or system management system

It is possible for various components in a network management system or a system management system to fail. Some of the problems that this causes are described in the following section.

Failure of managed components

If components managed by a network management system or a system management system fail while the system is in operation, then depending on the type of management system, this can result in the management information ceasing to be updated automatically. As a rule, for example in the case of network management systems, the system administrator is only informed of the failure of the component. If, for example, the failure of the component is observed or deliberately caused by perpetrators, they can bring their own computer into the system outside the LAN and pass it off as the failed component (IP spoofing). This computer can be used for further perpetration whereby it has the rights of an internal computer (such as entering false management information).

Failure of monitoring components

If parts of a management system fail while the system is in operation (also unnoticed), then the system components monitored or managed by these components are no longer connected to the management system. New instructions from the management then cease to be implemented on these computers. The consequence of this is that inconsistent system configurations arise, which can then cause security problems.

Unavailability of the central management station

If the central management station in a network managed by a management system fails, the system can no longer be managed centrally. If the station is unavailable for a long period of time, for example because the hardware cannot be replaced at short notice due to missing maintenance contracts, routine functions such as data backup may no longer be performed. If uncoordinated manual alterations are made to the individually-managed systems, this will lead to inconsistencies and maybe even security problems.

Failure of network switching elements during the transmission of management information

When a management system is used to manage a computer network, it is necessary to exchange so-called management information between the individual components of the management system. The information is transmitted via the local area network. Local area networks usually (depending on the network technique used) consist of several subnetworks which are linked together by network switching elements such as routers. In the process, the network switching elements pass on data from one subnetwork to another. If the switching elements fail, this corresponds to the affected subnetworks being separated physically. It is then no longer possible to exchange management information. Yet there is usually a subnetwork

which can still be managed from the management station in use at the time and a subnetwork which can no longer be managed. Depending on how long the switching element cannot be reached, this leads to inconsistencies and security problems.

T 4.39 Software conception errors

When programs and protocols are planned, conception errors may occur which affect security. From a historical point of view, these errors are entirely comprehensible. For instance, the developers of the protocols used in the Internet surely did not expect, at the end of the sixties, that these protocols would one day become the basis for a world-wide computer network that is extremely important commercially.

Examples of conception errors include the open transmission of data in the Internet, making it possible to read and alter data (such as passwords) or send packets using the Internet address assigned to another computer. A special case of this is what is known as the FTP bounce attack which exploits the fact that the link used for data transmission with an FTP protocol can be established with any computer. In serious cases, it is even possible to overcome firewalls in this way using dynamic packet filters (see CERT advisory 97-27). There are most certainly further errors in the Internet protocols which will be published in the future.

Another example of a conception error is the so-called DNS spoofing (see also G 5.78 *DNS spoofing*). The Domain Name System is the central information service in the Internet, which makes it possible to transcribes the easily-remembered computer names such as www.amazon.com into the corresponding Internet address. DNS spoofing involves a perpetrator attempting to assign the wrong computer to a computer name so that users seeking information are misdirected.

Another example of a conception error is that it is possible to send large numbers of advertising E-mails anonymously (mail spamming). This is often done by using other mail severs as so-called remailers, so that any counteraction from the recipient comes to nothing. These attacks are obviously due to the lack of opportunities for authentication currently offered by the Internet.

T 4.40 Unsuitable fitting out of the RAS client operational environment

Often RAS connections cannot be established due to incompatibility of the technical equipment. But even where the technology is compatible the connection can fail if dial-in points for the relevant service provider are lacking or cannot be accessed. The threats which can occur in this area include the following:

- The power parameters between RAS client and remote location are incompatible (220V/110V).
- The modem connections between RAS client and remote location are incompatible.
- The switched network that is normally used (telecommunication service provider, Internet service provider) is not available at the remote location.
- The remote phone number is transmitted incorrectly or in an incompatible manner to the RAS server (where authentication is effected using Calling Line Identification Protocol, CLIP).

Moreover, it is virtually impossible to consider all the possible technical problems which can occur in any operational environments when planning the RAS system.

T 4.41 Non-availability of the mobile communication network

The availability of mobile communication networks is significantly lower than that of landline networks. Like all systems which cannot guarantee 100% availability, mobile communication networks are often not available in the places and at the times when they are needed the most urgently. Again, not all mobile communication networks are designed to ensure blanket coverage.

The most frequent cause of inadequate availability of mobile communication networks is where there are gaps in radio coverage, i.e. areas which do not fall within the catchment area of any network provider. However, if demand is very high, it is also possible for parts of the network to be overloaded. This can mean that the reception or transmission of messages is prevented.

Another possibility is that noise pulse generators could cause radio interference in a geographically defined area so that reception of mobile radio signals is not possible there. There are also devices which can be purchased precisely for this purpose. However, in Germany use of such devices is illegal.

Example:

The call handling capacity of a transmitting station is not sufficient when after a major accident a huge number of people simultaneously all try to notify the emergency services or inform their staff by mobile phone.

T 4.42 Failure of the mobile phone

A mobile phone could become unusable for reasons such as the following:

- The battery is exhausted because the user forgot to re-charge it.
- The battery has lost its ability to store charge.
- The user has forgotten the PIN so that he cannot use the mobile phone any more.
- Components such as the display, keypad or SIM card are faulty.

If a mobile phone is exposed to harmful environmental conditions, its functional performance can be impaired. Mobile phones can sustain damage through exposure to excessively high or low temperatures, dust or moisture.

Examples:

- An employee embarking on an extended business trip took with him a mobile phone plus accessories from a mobile phone pool. While on the road it transpired that he had unfortunately packed the wrong battery charger. As he was unable to re-charge the mobile phone he could not use it any more during the rest of his trip.
- The mobile phone is left in a parked vehicle. This not only increases the risk of theft, but may also expose the phone to harmful environmental conditions. When a vehicle is exposed to direct sunshine, it is possible for the temperature to climb to over 60ºC behind the window glass. This can result in damage to either the battery or to the display.

T 5 Threats Catalogue Deliberate Acts

T 5.1	Manipulation or destruction of IT equipment or accessories
T 5.2	Manipulation of data or software
T 5.3	Unauthorised entry into a building
T 5.4	Theft
T 5.5	Vandalism
T 5.6	Attack
T 5.7	Line tapping
T 5.8	Manipulation of lines
T 5.9	Unauthorised use of IT systems
T 5.10	Abuse of remote maintenance ports
T 5.11	Loss of confidentiality of data stored in PBX installations
T 5.12	Interception of telephone calls and data transmissions
T 5.13	Eavesdropping of rooms
T 5.14	Call charges fraud
T 5.15	"Inquisitive" staff members
T 5.16	Threat posed by internal staff during maintenance/administration work
T 5.17	Threat posed by external staff during maintenance work
T 5.18	Systematic trying-out of passwords
T 5.19	Abuse of user rights
T 5.20	Abuse of Administrator rights
T 5.21	Trojan horses
T 5.22	Theft of a mobile IT system
T 5.23	Computer viruses
T 5.24	Replay of messages
T 5.25	Masquerading
T 5.26	Analysis of the message flow
T 5.27	Repudiation of a message
T 5.28	Denial of services
T 5.29	Unauthorised copying of data media
T 5.30	Unauthorized use of fax machine

T 5.31	Unauthorised reading of incoming fax transmissions
T 5.32	Evaluation of residual information in fax machines
T 5.33	Impersonation of wrong sender on fax machines
T 5.34	Deliberate re-programming of the destination keys on fax machines
T 5.35	Overload due to incoming fax transmissions
T 5.36	Deliberate overloading of answering machines
T 5.37	Determining access codes
T 5.38	Misuse of remote inquiry
T 5.39	Infiltrating computer systems via communication cards
T 5.40	Monitoring rooms using computers equipped with microphones
T 5.41	Misuse of a UNIX system with the help of uucp
T 5.42	Social engineering
T 5.43	Macro viruses
T 5.44	Abuse of Remote Access Ports for Management Functions of Private Branch Exchanges
T 5.45	Trying Out Passwords under WfW and Windows 95
T 5.46	Masquerading under WfW
T 5.47	Deleting the Post Office
T 5.48	IP Spoofing
T 5.49	Abuse of Source Routing
T 5.50	Abuse of the ICMP Protocol
T 5.51	Abuse of routing protocols
T 5.52	Misuse of administrator rights in Windows NT systems
T 5.53	Deliberate misuse of protective cabinets for reasons of convenience
T 5.54	Deliberately causing an Abnormal End
T 5.55	Login Bypass
T 5.56	Temporary free-access accounts
T 5.57	Network analysis tools
T 5.58	Hacking Novell Netware
T 5.59	Misuse of administrator rights in the Novell Netware network 3.x
T 5.60	By-passing system guidelines

T 5.61	Misuse of remote access to management functions on routers
T 5.62	Misuse of resources via remote IT systems
T 5.63	Manipulation via the ISDN D-channel
T 5.64	Manipulation of data or software in database systems
T 5.65	Denial of services in a database system
T 5.66	Unauthorised connection of IT systems to a network
T 5.67	Unauthorised execution of network management functions
T 5.68	Unauthorised access to active network components
T 5.69	Higher risk of theft from a working place at home
T 5.70	Manipulation by family members or visitors
T 5.71	Loss of confidentiality of classified information
T 5.72	Misuse of e-mail services
T 5.73	Impersonation of a sender
T 5.74	Manipulation of alias files and distribution lists
T 5.75	Overload due to incoming e-mails
T 5.76	Mail bombs
T 5.77	Unauthorised monitoring of E mails
T 5.78	DNS spoofing
T 5.79	Unauthorised acquisition of administrator rights under Windows NT
T 5.80	Hoaxes
T 5.81	Unauthorised use of a cryptomodule
T 5.82	Manipulation of a cryptomodule
T 5.83	Compromising cryptographic keys
T 5.84	Forged certificates
T 5.85	Loss of integrity of information that should be protected
T 5.86	Manipulation of management parameters
T 5.87	
T 5.88	Misuse of active contents
T 5.89	Hijacking of network connections
T 5.90	Manipulation of address books and distribution lists
T 5.91	Disabling of RAS access security mechanisms
T 5.92	Use of the RAS client as RAS server

T 5.93 Permitting use of RAS components by third parties

T 5.94 Misuse of cards

T 5.95 Bugging of indoor conversations over mobile phones

T 5.96 Tampering with mobile phones

T 5.97 Unauthorised transfer of data over mobile phones

T 5.98 Interception of mobile telephone calls

T 5.99 Analysis of call data relating to the use of mobile

T 5.1 Manipulation or destruction of IT equipment or accessories

Various motives

External - as well as internal - perpetrators may for various reasons (revenge, malice, frustration) try to manipulate or destroy IT equipment, accessories, documents, or the like. The later such manipulations are detected, the greater the knowledge acquired by the perpetrator and the more far-reaching the impact on a work operation, the more effective they are. The effects range from unauthorised viewing of sensitive data to the destruction of data media or IT systems, which could result in these being out of action for prolonged periods.

Example:

An employee in a company used his knowledge of the fact that an important server was sensitive to excessive operating temperatures and blocked the vent slots for the power unit fan with an object placed behind the server. Two days later the hard disk in the server sustained a fault induced by overheating and the server was out of action for several days. The attacker subsequently claimed that it was a simply a matter of an oversight.

T 5.2 Manipulation of data or software

There are a number of ways in which data or software can be manipulated: through incorrect data acquisition, changes to access rights, modification of accounting data or of correspondence, changes to the operating system software etc. A perpetrator can only manipulate data and software to which he has access. The more access rights a person has, the more serious manipulations he will be able to carry out. If such manipulations are not detected in time, smooth IT operations may be seriously impaired.

Data or software can be manipulated out of revenge, to intentionally create some damage, to obtain personal gains or for financial reasons.

Example:

In 1993, the software used for specific financial services of a Swiss financial institution was manipulated by a staff member. This made it possible for him to obtain sizeable amounts of money illegally.

It is a by no means uncommon occurrence for customer databases to be copied by staff on leaving a company. Other risks include the malicious destruction of databases or threatening to destroy databases.

T 5.3 Unauthorised entry into a building

Unauthorised entry into a building precedes various hazards to IT systems such as theft or manipulation. Therefore, countermeasures would also be effective against the respective consequential threats.

The direct effect of unauthorised entry can be material damage. Windows and doors would be opened by force and damaged and would have to be repaired or replaced.

T 5.4 Theft

Theft of IT equipment, accessories, software, or data not only causes costs for replacement and for restoration of operability, but also losses resulting from lack of availability. In addition to that, damage can be caused by a loss of confidentiality and its sequels.

T 5.5 Vandalism

Vandalism is very similar to an attack, with the difference that vandalism is not purposive and focused, but, in most cases, an expression of blind rage.

Such acts may be committed by both external perpetrators (e.g. disappointed burglars, demonstrations which have got out of control) and internal perpetrators (e.g. frustrated employees or staff members under the influence of alcohol). The actual hazard posed by vandalism is more difficult to assess than the hazard posed by an attack, because vandalism is generally not motivated by a conscious effort. Personal problems or a bad climate in the organisation may be the underlying reasons.

T 5.6 Attack

There are multiple technical possibilities for carrying out an attack: throwing bricks; use of explosives; use of firearms; arson. Whether an IT operator will be exposed to the risk of attack, and to what extent, will depend on the site and environment of the building and also, to a great extent, on his tasks and on the political/social climate. IT operators working in controversial political fields are more at risk than others. IT operators near areas frequently used for demonstrations will be at greater risk than those in remote places. When assessing the risk of politically motivated attacks, advice can be obtained from the local criminal police office or from the federal criminal police office.

Examples:

- During the 80s, a bomb attack was committed against the computer centre of a large federal authority in Cologne.
- Almost every year, an internal revenue office in the Rhine region was paralysed for several hours on account of bomb threats.
- In the late 80s, an attempted attack by the RAF against the computer centre of a major German bank was reported.

T 5.7 Line tapping

Due to the low risk of detection, tapping of lines is a potential threat to IT security which should not be overlooked. No cable is entirely proof against tapping. It is simply that different cables require different amounts of effort to tap. Whether a line is actually being tapped can only be determined using sophisticated measuring technology.

Capabilities and motivation of the attacker

The decision to intercept a line essentially depends on whether the obtainable information is worth the technical (financial) expenditure and the risk of being detected. This question can only be answered by knowing what capabilities the attacker has and what his particular interests are. Therefore, definitive identification of the targeted information, and thus of the lines which might be intercepted, is not possible.

Automatic analysis of HTTP connections

The transmission of credit card numbers or passwords on the Internet is especially susceptible to eavesdropping as the position of the data entered by the user in the data packets transmitted is determined by the HTTP protocol, which is not at all sophisticated. It is thus a relatively simple matter to perform an automatic analysis of HTTP connections.

Password sniffer programs can be used to collect passwords during transmission to a system. This enables the perpetrator to then access this IT system in order to perform additional attacks locally on the computer at a later time.

Examples

- It is wrong to assume that messages sent by *electronic mail* are the equivalent of letters in the classical sense. As E mail messages can be read throughout their route through the network, it is more appropriate to consider them as being like postcards.
- Some manufacturers supply sniffer programs along with their operating systems for the purpose of debugging networks. However, these can be used to intercept data as well.

T 5.8 Manipulation of lines

Apart from the interception of lines (cf. T 5.7 *Line tapping*), lines may be manipulated in the pursuit of other objectives as well.

- Frustrated employees could manipulate lines in such a way that non-permitted connections are established within and outside the organisation's own IT set-up. The aim here is often simply to disrupt IT operations.

Non-permitted connections

- Lines could be manipulated so that they can be used privately at the expense of the network operator. Apart from the charges incurred as a result of use of communication lines which are liable to charges, lines and resources would be blocked by such private use.

Private usage

- As a result of the manipulation of lines, it might become possible for data transmitted over those lines to be modified to the advantage of the perpetrator. The effects of manipulation can be especially damaging in processes relevant to accounting, in payroll applications, and in all IT applications which directly or indirectly relate to the management of material assets.

Manipulation of transmitted data

T 5.9 Unauthorised use of IT systems

Without mechanisms for the identification and authentication of users, any control over unauthorised use of IT systems is practically not possible. Even for IT systems provided using identification and authentication mechanisms in the form of user IDs and password verification, there is a risk of unauthorised use, if passwords and user IDs get disclosed.

In order to guess the secret password, unauthorised persons could enter a possible password during the log-in process. Afterwards, the response of the IT system would show, whether the password was correct or not. In this way, passwords could be detected by trial.

However, taking a suitable word as a password and trying out all user IDs is a much more efficient approach. If the number of users is large enough, a valid combination is often found in this manner.

If the identification and authentication function can be abused, it is even possible to initiate automatic attempts by developing a program which systematically tests all conceivable passwords.

Example:

In 1988, the *Internet* worm exploited a vulnerability of the respective UNIX operating system to find valid passwords although the passwords were stored encrypted. To achieve this, the program tried all entries of a dictionary by encrypting them with the local encoding function and comparing them with the stored encrypted passwords. Where a correspondence was found, a valid password had been detected.

T 5.10 Mißbrauch von Fernwartungszugängen

Bei unzureichend gesicherten Fernwartungszugängen ist es denkbar, daß Hacker Zugang zum Administrierungsport des IT-Systems erlangen. Sie können somit nach Überwindung des Anlagenpaßwortes ggf. **alle** Administrationstätigkeiten ausüben. Der entstehende Schaden kann sich vom vollständigen Anlagenausfall, über schwerste Betriebsstörungen, den Verlust der Vertraulichkeit aller auf der Anlage vorhandenen Daten bis hin zum großen direkten finanziellen Schaden erstrecken.

T 5.11 Loss of confidentiality of data stored within PBX installations

Within PBX installations, personal and in-house data are stored on hard disks for a prolonged period of time. In this case, personal data are: charging infomation, configuration data, privileges and, in instances, data for electronic telephone directories, passwords and job account numbers.

Such data can be read and modified by the administration staff. The nature and extension of such tampering depends on the type of the given installation and, where provided for, on the granting of rights. Administration staff have this possibility both at the site and through remote maintenance. In case of external remote maintenance, the person entrusted with this task (normally the manufacturer) has this possibility at any time!

The hard disks are often taken to the PBX manufacturers for an upgrade of system software. This means that personal data can be read by the respective manufacturer.

T 5.12 Interception of telephone calls and data transmissions

By abusing user facilities, it may be possible for colleagues to listen in on telephone calls. One example is the add-on (three-party) conference. If subscriber A receives a call for subscriber B, he might try, in secret, to establish a three-party conference, instead of passing the call on. Subscriber B would not be aware of this fact if he had a telephone set without a display.

In addition, it is possible for third parties to listen in on calls by activating disabled user facilities which are partly not allowed in Germany. One example is the add-on witness feature. Such an activation requires in-depth knowledge of the system.

T 5.13 Eavesdropping of rooms

In general two different types of unauthorised bugging of rooms have to be distinguished. In the first type, the threat is directly represented by the terminal. In this case particularly intelligent terminals with installed microphones, such as answering machines, ISDN cards, or multimedia PCs are affected. Terminals of this kind can, assuming the relevant functions are installed, be activated via the public network to switch on the installed microphones. A well-known example of this is the so-called "baby-watch function" of answering machines (c.f. 8.3 *Answering machine*).

The second type is to make use of the PBX system itself in connection with appropriately equipped terminals. This threat arises from the abuse of the "voice calling" user facility in conjunction with the "handsfree conversing" option. This function, of an intercom switching centre with simplex transmission if applied in this way, can, under certain circumstances, also beused for the bugging of a room.

T 5.14 Call charges fraud

Numerous reports of call charges fraud by hackers concerning PBX systems have recently been reported in the press. Such manipulations can be carried out in various ways. On the one hand. it may be that existing features of a PBX system can be abused for this purpose. For example, call redirections or dial-in options which can be remotely programmed are suitable for this. On the other hand, rights can be granted in such a way that incoming "exchange lines" occupy outgoing "exchange lines". As a result, when a certain number is dialled from outside, the caller can be directly connected with the "exchange". However, this takes place at the expense of the PBX system provider.

Another type of call-charges fraud can be caused by the user himself. By various means, e.g. making telephone calls from other people's telephone sets, reading out other people's identifiers (passwords) or modifying personal privileges, an attempt can be made to make calls at the expense of the employer or of other staff members.

T 5.15 "Inquisitive" staff members

"Inquisitive" staff members can, by abusing user facilities of the PBX, try to

- divert calls intended for colleagues to their own telephone;
- accept calls intended for others;
- read the call and last-number re-dial memory of other persons; and
- tap telephone calls.

T 5.16 Threat posed by internal staff during maintenance/administration work

To their own advantage, or as a favour for colleagues, internal staff might, during maintenance or administration work, try to modify privileges (e.g. international dialling authorisation) or to activate user facilities. System crashes can be caused through ignorance. Also, improper handling of hardware components might result in their destruction. In addition, maintenance staff may have full or restricted access to the stored data (read and write).

T 5.17 Threat posed by external staff during maintenance work

An IT system can be manipulated in any way during maintenance work. The threat is primarily due to the fact that the owner is often not able to understand and follow the effected modifications. Moreover, an external maintenance engineer, just like an internal one, usually also has access to all data stored in the system.

T 5.18 Systematic trying-out of passwords

Passwords which are too simple can be found out by systematically trying them out.

Example:

A study made by Klein (Klein, Daniel V. 1990, USENIX Security Workshop Proceedings, Portland, August 1990) of 15,000 accounts yielded a success rate of 24.2 per cent; the following password options were tried out:

About 130 variations of the log-in name (first and last names) and of other personal data from the */etc/passwd* file; frequent names, names of well-known persons, names and places in movies, from sports events and from the Bible; abusive common invectives/swear-words, and words from foreign languages; different variations of these words, e.g. changes from upper and lower case, insertion of special characters and check symbols, reversing of the sequence of letters, repeated letters (e.g. *aaabbb*), or frequent abbreviations (e.g. *rygbv* for the colours of the rainbow) and pairs composed of two short words.

All these combinations and more can be tried out by any user of the UNIX system in which the password file is freely accessible, using the *crack* PD program. Moreover, for passwords that are too short, it is highly probable that the password can be found out by systematically trying out all combinations.

T 5.19 Abuse of user rights

Abuse of rights takes place when someone deliberately exploits - rightfully or illicitly obtained - facilities in order to harm a system or its users.

Example:

For many systems, it is possible for any user to read the */etc/passwd* file so that he can obtain information on the personal data contained in that file. In addition, he can try, by means of a dictionary attack (cf. T 5.18 *Systematic trying-out of passwords*), to guess the encrypted passwords. If group privileges are granted too generously, particularly in the case of system groups such as *root*, *bin*, *adm*, *news* or *daemon*, abuse - for instance, modification or deletion of third parties' files - can be easily effected.

T 5.20 Abuse of Administrator rights

Abuse of Administrator rights occurs when superuser (*root*) privileges, acquired either rightfully or illicitly, are deliberately used to harm the system or its users.

Example:

No restrictions for *root*

Since *root* in UNIX systems is not subject to any restrictions, the Administrator is able to read, modify or delete any file, regardless of access rights. Moreover, he can assume the identity of any user of his system, without this fact being perceived by any other user; thus, it is possible for him, by feigning another person's identity, to send mail messages or to read and/or delete mail messages intended for others.

Superuser files

There are a number of ways in which superuser privileges can be abused. These include misuse of incorrectly administered superuser files (files with *root* as owner and *s*-bit set) and of the *su* command.

Automatic mounting

Automatic mounting of exchangeable data media can also constitute a threat, since as soon as the medium is placed in the drive, it is mounted. Then anybody has access to the files stored there. If any *s*-bit programs are stored on the mounted drive, any user can obtain superuser rights.

Access to the console

Depending on the UNIX version and the hardware used, if the console can be accessed then it is possible to activate monitor mode or else to boot up in single-user mode. This allows the configuration to be manipulated.

Software errors

A software error could mean that a given application is only able to process a limited amount of data. If too much data or too many parameters are passed to this application, areas of main memory could be overwritten with alien code. This could result in commands being executed with the rights of the application. This was possible, for example, under SunOS 5.5 with the command *eject*, which possessed SetUID rights which to all intents and purposes were equivalent to superuser rights.

T 5.21 Trojan horses

Application programs and script languages

A Trojan horse is a program with a hidden, undocumented function or effect. The user therefore has no influence on the execution of that function, making its effect similar to that of a computer virus. However, unlike computer viruses, Trojan horses are not self-reproductive. Any kind of application software can be used as carrier for a Trojan horse. Script languages, like batch files, ANSI control sequences, Postscript etc., which are interpreted by the operating system or by an application program, can also have Trojan horses planted in them.

The more privileges the originator program has, the more damage the Trojan horse can cause.

Examples

Altered login programs

- A modified login program can contain a Trojan horse which sends the user's user name and password to an aggressor over the network and then passes it to the correct log-in program. Such Trojan horses have appeared recently on several online services like AOL or T-Online.

Back Orifice* and *NetBUS

- The *Back Orifice* program is a client/server application which enables the client to maintain a Windows PC remotely over the network. In particular, it is possible for data to be read and written and also for programs to be executed. There is a risk that this program could be integrated into another application program and thus used as a Trojan horse. If the Trojan horse starts up when there is a network connection, then an adversary can use the remote maintenance function of Back Orifice to gain access to the user's PC unnoticed. The NetBUS program, which has similar functions, should also be mentioned here.

Manipulated programs and libraries

- It is possible using root kits for different UNIX variants which contain manipulated versions of the programs *ps*, *who*, *netstat* etc. to keep so-called back doors open for prolonged periods, allowing penetration of the system to go unnoticed so that traces of the attack are covered up. Often the files */sbin/in.telnetd*, */bin/login*, */bin/ps*, */bin/who*, */bin/netstat* and the C Libraries are replaced in this way.

Current directory in the search path

- Another source of danger in UNIX systems is the "." in the *$PATH* environment variable. If the current working directory (.) is included as a path in the *PATH* variable, the programs located there are executed first. Thus, while listing of the contents of a directory the superuser could unintentionally execute a modified "*ls*" program with root rights contained there.

T 5.22 Theft of a mobile IT system

Mobile use of an IT system carries the risk of new threats to which stationary IT systems are less exposed. Mobile systems such as laptops are normally not used in a room secured by protective measures. They are carried in cars or on public transport, set down in other people's offices during breaks and left unattended in hotel rooms.

Because of these environmental factors, mobile use of IT systems intrinsically exposes them to a higher risk of theft. It is not totally uncommon for mobile IT systems to be "accidentally" stolen, e.g. there might be a laptop in the boot of a car that happens to be stolen.

Insufficient access protection

If a mobile IT system should be stolen it is also possible that any existing boot protection (boot/BIOS password) may be surmounted. For IT systems which do not have boot protection but whose protection relies exclusively on the authentication mechanism of the operating system (user name, password), an aggressor can access the data on the hard disk by booting up from a diskette or CD-ROM.

Higher threat potential with remote access

If the mobile IT system is integrated into a remote access system and automatic RAS connection (auto-dial, storage of authentication data) is enabled, an unauthorised third party could access resources on the destination LAN.

Example

The managing director of a large company had his laptop stolen during a business trip. The material loss was trivial as it was possible to obtain a new laptop within a day. Far more painful, however, was the loss of important customer data which had been stored on the laptop. No backup of this information existed as it had only been entered during the business trip.

Examples of destructive functions of computer viruses

- Every year on March 6th the boot virus Michelangelo overwrites the first tracks of a hard disk with stochastic material, thus rendering the hard disk useless.
- The multi-partite virus Onehalf encrypts a maximum of half of the contents of a hard disk. If the virus is removed, the encrypted data becomes inaccessible.
- The Word macro virus WAZZU inserts the word "Wazzu" at random points in infected documents.
- The Word macro virus Melissa appeared on 26 March 1999 and spread all over the world in the course of the following weekend. This virus is contained in a Word 97 or Word 2000 file which is sent by an infected computer via Microsoft Outlook to up to 50 address entries stored in each address book. In some relatively large organisations the virus completely overwhelmed the mail system.

- W32.Mypics.Worm is a computer worm written in Visual Basic which propagates itself automatically on Windows 95/98 and Windows NT computers. It contains a destructive function which is activated as soon as dates reaches the year 2000. One of its effects is to alter the computer's BIOS settings so that it no longer boots up correctly.

T 5.23 Computer viruses

A computer virus is a *program with a destructive function*. The damage lies particularly in the loss or corruption of data or other programs, which can have significant consequences. Such program functions can be triggered intentionally as well as accidentally.

The definition of a computer virus does not directly refer to a possibly implemented destructive function:

> *A computer virus is a non-independent, self-reproducing routine which thereby manipulates system sectors, programs and their environments in a manner which cannot be controlled by the user. (In addition to this, the virus might also include destructive functions.)*

Similar to its biological equivalent, the property of reproduction leads to the designation "virus". There are numerous possibilities of manipulation. Particularly frequent is the overwriting or attachment of the virus code to other programs or to sectors of the operating system.

In principle, computer viruses can occur on all operating systems. However, the largest threat is posed in the area of IBM-compatible personal computers (PCs). Presently, roughly 20,000 viruses (including their variants) are known to exist worldwide on the most commonly used operating systems in this area (MS-DOS, PC-DOS, DR DOS, NOVELL DOS etc.).

Special computer viruses for the Windows 3.x, Windows NT, Windows 95, OS/2 and Unix operating systems are of little significance in practice. In the case of hardware typical for PCs, however, the hard disks of these computers could be infected by DOS boot viruses if the boot sequence begins with the floppy disk drives.

Roughly 100 special computer viruses are known to exist for Apple computers, for which corresponding virus scanning programs are also available.

Types of computer virus

There are three basic types of computer virus:

- Boot viruses
- File viruses
- Macro viruses

Hybrids and special forms of these three types are also known to exist. Additional distinguishing features are the stealth mechanisms, with which viruses are often equipped in order to avoid detection by users and scanning programs

Boot viruses

"Booting" is the loading of the operating system. This procedure also involves the execution of certain program routines which are independent, but which

are located in inaccessible sectors which are not visible in the directories on the hard disks or floppy disks. Boot viruses overwrite these sectors with their own program code. The original contents are moved to a different location of the data media, and executed after the execution of the virus code during the start-up of the computer. As a result, the computer apparently starts in the usual manner, but the boot virus is loaded into the computer's main memory even before the operating system is loaded, and stays there during the whole power-on time of the computer. Consequently, the virus is able to infect the boot sector of every write-enabled floppy disk used during the computer's power-on time. Boot viruses can only infect other computers during booting, or through attempts at booting with infected floppy disks.

File viruses

Most file viruses attach themselves to program files. However, this happens in such a way that when the file is opened, the virus code is activated first, followed by the original program. The program then appears to run as usual and the virus is not immediately detected. Nevertheless, primitive, overwriting viruses are also known to exist, which attach themselves to the beginning of the host program in such a way that the program no longer runs correctly. File viruses are spread by the execution of infected programs.

In the case of hybrid boot and file viruses, so called multi-partite viruses have become important. These viruses can spread through the starting of an infected program as well as during booting (or attempted booting) from an infected floppy disk.

Macro viruses

Macro viruses are also placed within files, although they do not infect the applications, but the files generated by these applications. All kinds of application programs can be effected including those in which generated files not only single control characters, but also programs and other objects, can be embedded. Particularly Microsoft Word and Excel files are affected by such viruses. These applications offer a powerful macro programming language, which can easily be abused for the implementation of viruses, also by users who are not very skilled with these programs.

Macros are programs with whose help the application program can be expanded with additional functions which have been cut to fit the application (e.g. production of a fair copy from the draft of a text). These macros can only be executed with the relevant application program (Winword, Excel etc.) when the document is processed, either due to activation by the user or if the macro starts automatically. If, for example, a Word file is received by a WWW browser which automatically opens the document with Microsoft Word, a macro can be activated. As data files are often distributed as conventional program files via data media and networked IT systems, the threat posed by macro viruses is now larger than that posed by boot and file viruses.

Examples of destructive functions of computer viruses

- On every March 6th, the boot virus called Michelangelo overwrites the first tracks of a hard disk with stochastic contents, thus rendering the hard disk useless.

- The multi-partite virus named Onehalf encrypts a maximum of half of the contents of a hard disk. If the virus is removed, the encrypted data are rendered unavailable.
- The Winword macro virus named WAZZU inserts the word "Wazzu" at random points in infected documents.

T 5.24 Replay of messages

In this form of attack, an aggressor records a message and replays it unchanged at a later time.

Examples

- An adversary records the authentication data (e.g. user ID and password) during a user's logon dialogue and uses this information to obtain access to a system by feigning a false identity (see also T 5.21 - *Trojan horses*).
- An employee places an authorised order several times with the intention of causing financial loss to his employer.

T 5.25 Masquerading

Manipulation of the originator field or I/O address

Masquerading is used by an aggressor to assume a false identity. Thus he can obtain a false identity by spying out the user ID and password (cf. T 5.9 - *Unauthorised use of IT systems*) or by manipulating the originator field of a message or the I/O address within the network. Other ways of obtaining a false identity are to manipulate the calling number display (Calling Line Identification Presentation) on an ISDN line or the originator identifier of a fax originator (CSID - Call Subscriber ID)

A user who believes he is communicating with a different person can be easily induced to disclose sensitive information.

Intruding on an existing connection

An aggressor can also use masquerading to try to connect to an existing connection without having to authenticate himself, as this step has already been taken by the original participants in the communication.

T 5.26 Analysis of the message flow

By a traffic flow analysis, a perpetrator tries to find out who, at what time and how often, has sent what data volumes to whom. Even if an eavesdropper cannot read the contents of the message, it is possible to draw conclusions about the behaviour of users. The information regarding the date and time a message is created can be analysed to a personality profile of the sender. Address collectors from address companies also search for e-mail and postal addresses to which unsolicited advertising can be sent.

Within ISDN (Integrated Services Digital Network), the D-channel of a connection, used for signalling between terminal devices and the exchange, is particularly vulnerable to intrusions. An analysis of the signalling by a protocol sniffer not only allows the drawing of conclusions about the behaviour of a user (e.g. who phones when, to whom, and for how long?), but also can be used to prepare more complex attacks via the D-channel.

T 5.27 Repudiation of a message

In any form of communication a communication partner can deny having received a message (repudiation of receipt). This is of particular importance in the case of financial transactions. A communication partner can deny having received a message sent by post just as a fax or e-mail.

Example:

An electronic order was placed for an urgently needed spare part. After a week of shutdown, a complaint about non-delivery was lodged. The supplier denies ever having received such an order.

A communications subscriber can also repudiate transmission of a message, e.g. deny having sent an order.

T 5.28 Denial of services

Such an attack aims to prevent IT users from using functions or devices which are normally available to them. This attack often takes place in connection with distributed resources, with the attacker using these resources to such a degree that other users are prevented from carrying out their work. Shortage of the following resources can intentionally take place: processes, CPU time, disk space, inodes, directories.

This can be carried out, for example, by:

- starting any number of programs simultaneously,
- starting numerous programs at the same time which use a lot of CPU time,
- occupation of all free inodes within a UNIX system so that no new files can be created,
- creation of a large number of small files in a directory on a DOS PC so that no new files can be created inside this directory,
- deliberately overloading the network,
- cutting off network connections.

T 5.29 Unauthorised copying of data media

When data media are replaced or transported, the information on them might be transferred from a secured environment via an insecure route to an insecure environment at the receiving end. In such cases, unauthorised persons could make copies of this information more easily than in the original environment.

Example:

Confidential engineering results are to be transported from a development laboratory in town X to the production site in town Y. If the data media are mailed without any supervision or control, the information on them might be copied illegally and perhaps sold to a competitor, without any indication of such an exposure of information.

T 5.30 Unauthorised use of a fax machine or fax server

Unauthorised access to a fax machine or fax server can be exploited for manipulative purposes. On top of the cost of fax transmissions (charges and consumables), loss or damage could also result from an unauthorised person using the device under false pretences (sending out letters bearing the company letterhead from the corresponding fax connection).

Steps must also be taken to ensure that unauthorised persons cannot access incoming fax transmissions.

Examples

- A fax machine is situated in the corridor so that anybody walking by can read or help himself to faxes unchecked.
- The access authorisations to stored fax data on a fax server are set incorrectly so that unauthorised persons can read other people' faxes.

T 5.31 Unauthorised reading of fax transmissions

Where fax machines are placed in places with free access there is a danger that incoming faxes could be read by unauthorised persons. Again, if the distribution list used within the organisation is inaccurate, unauthorised persons could obtain knowledge of the information contained in confidential fax transmissions.

Access rights too loosely defined

If the access rights to a fax server are not granted very strictly, it may be possible for unauthorised persons to read incoming and outgoing fax transmissions which pass over the fax server.

Manipulated address books

Fax servers contain so-called address books. These eliminate some of the work involved in sending a fax as users do not have to enter the recipient's call number every time they send a fax to him, but merely to select his name. If the call number entered in the address book for a given recipient is incorrect, then every time this entry is used the fax will be sent to the wrong recipient. A lot of address books also provide facilities for combining several addresses into a single group. The user who wishes to send a fax to the members of such a group only has to specify the group as the recipient, rather than each member of the group individually. But if the group contains addresses which should not be there, the corresponding recipients could obtain access to all fax transmissions which are sent using this group definition. The assignment of incorrect addresses may be due to carelessness or it could be the result of deliberate manipulation.

Incoming faxes sent to a fax server have to be distributed to recipients. This can be done either by printing out the incoming faxes and manually forwarding them to recipients or the fax server can distribute the faxes automatically over the network.

Unauthorised reading of documents on the printer

Where incoming faxes are distributed manually and the printer used to print out the faxes is located in an area with open access or the process of distributing faxes within the organisation is flawed, it is possible for them to be read by unauthorised persons.

Manipulated assignment tables

In order to forward fax transmissions automatically, the fax server requires an assignment table which specifies to which user or to which user group incoming faxes, for example from a particular originator or sent using a particular call number should be sent. If an unauthorised person is included in such an assignment table, either out of carelessness or as a result of deliberate manipulation, he will receive faxes which are not intended for his eyes.

T 5.32 Evaluation of residual information in fax machines and fax servers

Fax machines

Depending on the technology a fax machine uses to store, process and print information, it may contain varying amounts of residual information after receiving a fax message. This information can be reconstructed by persons having access to the fax machine or the relevant components.

Thermo-transfer printers

In the case of fax machines which use thermo-transfer techniques, incoming fax messages are first written onto an intermediate foil, which is then used to print the information. This foil is a consumable and must be replaced regularly; it is therefore designed to be easily removable. If an unauthorised person gains possession of this foil (by theft or on disposal) he will be able to reproduce the contents with a minimum of technical effort. Thus he would be able to view several hundred pages' worth of information.

Intermediate data storage in the fax machine

Most fax machines have an intermediate memory (document memory, buffer) in which outgoing faxes can be read until they have been successfully sent and incoming faxes can be stored temporarily until they have been printed. Depending on the fax machine, this memory can contain a large number of fax pages which can usually be printed by anyone who has access to the fax machine.

Fax server

Residual information on hard disks

Fax servers are applications installed on IT systems which are generally fitted with at least one hard disk or can access a disk drive over the network. Fax transmissions are stored on this until they can be delivered to the recipient. Modern operating systems also work with swap files which, too, can contain residual information. There is a danger here that this information can be evaluated without permission when this fax server is accessed. For example, if a hard disk fails during the warranty period, it has to be returned to the dealer or manufacture in order to make a claim under the warranty. However, the hard disk could still contain data to which unauthorised persons could in this way obtain access. If the hard disk is faulty, it is often not possible to delete the data using software tools.

Inadequate protection of main memory

If a workstation or the fax software installed on it is not adequately protected, it is possible to access fax data on the fax client without authorisation. Information can also be read by unauthorised persons through access to the workstation's hard disk.

T 5.33 Impersonation of wrong sender on fax transmissions

Similar to writing letters using a false name and letterhead, it is possible to send faked fax messages. This can cause damage if the recipient assumes that the information is authentic and thus legally binding (c.f. T 3.14 *Incorrect assessment of the legal force of a fax*).

Examples

- Signatures can be scanned in from other signed documents and printed out onto the fax template or copied into the fax as a graphic file when the fax server is used. On the fax received a signature reproduced in this way looks no different from an authentic signature.
- The call number of the transmitting fax connection is generally sent during the transmission. It is possible, however, to feign a different call number. The reception logs should not therefore be viewed as a reliable proof of the identity of the sender.

T 5.34 Deliberate re-programming of the destination keys on fax machines

To avoid the repetetive input of recurring fax numbers, some fax machines are equipped with programmable destination keys. During the transmission of fax messages to such recipients, the stored destination number is usually not checked. If unauthorised persons are able to re-program the destination keys and promptly forward the fax messages arriving at the new destination to the correct recipient, all fax traffic along this route can be monitored easily, perhaps without ever being detected.

T 5.35 Overload through fax transmissions

Overloading by incoming fax messages can occur if there are not enough fax lines or telecommunications lines or channels. Furthermore, a fax connection can be intentionally blocked if

- long faxes are sent continuously (possibly containing information which is of no interest to the recipient);
- sending of faxes is deliberately continued until the fax machine runs out of paper and the buffer memory is exhausted.

Overload due to incoming fax transmissions

A fax server can also become overloaded if faxes continue to be sent to it until the storage space available on the hard disk is exhausted. However, it should be borne in mind that a single faxed A4 page occupies approx. 70 KB. Given the size of hard disks today, this means that a huge volume of incoming faxes is needed to exhaust capacity. Moreover it should be borne in mind that there is only a limited number of lines or channels available and every fax transmission also requires time to process the fax protocol. Overloading of the fax server in this way is only possible if the hard disk selected has too little capacity or the fax server is also used to archive faxes.

Overload due to outgoing fax transmissions

Unlike conventional fax machines, it is entirely possible for a fax server to be overloaded due to outgoing fax transmissions. Thus a fax server's processing capacity could become completely exhausted by a very large number of serial fax transmissions, which would then mean it was no longer available to receive incoming faxes.

T 5.36 Deliberate overloading of answering machines

It is possible for a perpetrator to fill (e.g. with useless information) the limited storage medium of an answering machine (digital storage or audio cassette) during a call, making additional recordings impossible or causing existing messages to be deleted (also refer to T 4.19 *Information loss due to full storage medium*).

T 5.37 Determining access codes

Almost all modern answering machines are equipped with a number of functions in addition to the recording of messages. Typical examples are: remote inquiry, call redirection, room monitoring, or telecontrol of connected electrical devices. These functions can be controlled remotely while the answering machine is being called (in the case of dial pulsing with an additional remote control device, in the case of multi-frequency dialling system directly with the telephone keys). The use of this remote inquiry and control feature is generally protected by a security code (code number, PIN). This access code is also transmitted from the remote inquiry device to the answering machine with tones of different frequencies.

If third parties were able to find out that access code, it would be possible for them to influence the answering machine via the remote control as if it was their own answering machine. The consequential damage would depend on whether a third party monitored sensitive messages or misused other features.

Example:

According to recent reports, the access codes of some answering machines have been increasingly cracked by using a standard PC and a connected modem to try out all possible number combinations within a very short time.

T 5.38 Misuse of remote inquiry

If third parties get to know the access code of an answering machine, they can use the remote inquiry to abuse a large number of the functions of the answering machine. The most sensitive functions which can be accessed and therefore abused with remote inquiry are:

- Room monitoring

  The room monitoring function activates the microphone of the answering machine, thus bugging the room. A fact that should be mentioned is that very few types of answering machine clearly indicate bugging by an acoustic signal, the standard indicator only consists of one LED.

  If this function is activated in an abusive manner during the absence of the called party, an activated monitoring of the room will not be noticed after the called party returns. All conversation inside that room will be bugged without being noticed.

- Unauthorised monitoring or deletion of stored messages

  Incoming messages can be monitored (without authorisation) and also deleted. The consequential damage depends on the sensitivity of the recorded information.

- Modifying or deleting of stored outgoing messages

  Some types of answering machine allow the deletion of the outgoing message by a remote inquiry, thus putting the answering machine out of action. It is also possible to confuse callers by specific incorrect information.

- Modification of stored call numbers used for the call-transfer or call-forwarding mode

  The facility call-notification makes the answering machine dial a preset telephone number automatically after receiving a call. If the called subscriber responds, a particular acoustic signal or reminder text is sent by the answering machine to indicate that a call has been recorded. Some answering machines then automatically replay the recorded call. Mostly however, the replaying of the call has to be activated by first entering a security code. In the call-forwarding mode, the calling party is routed to a preset telephone number.

  On deactivation of the call notification or call-forwarding mode, these functions will not be executed any more, this means that the user can no longer be notified of important calls. By re-programming these functions, it is possible to re-route calls arbitrarily, e.g. to an information service with charges.

- Re-winding and fast-forwarding a tape

  Some answering machines with an analogue recording unit allow a remote fast-forwarding or re-winding of the tape. Fast-forwarding the tape to the end prevents the recording of subsequent calls. Re-winding the tape causes the messages already recorded to be erased by subsequent ones.

- Modes of telecontrol

  Some answering machines allow electrical equipment to be turned on and off remotely. The damage arising from misuse of this feature depends on the function and significance of the connected equipment.

- Turning off the answering machine

  Some answering machines can be turned off remotely so that their functions are no longer available.

T 5.39 Infiltrating computer systems via communication cards

A communications card (e.g. an ISDN card or an internal modem, but also an external modem) is capable of automatically receiving incoming calls. Depending on the installed communications software and its configuration, this makes it possible for callers to access the connected IT system without being detected.

An external computer can be connected as a terminal to a server via a communication card. If the user logs off after a terminal session but the line stays connected, an external computer can be used for access just like the local terminal. This allows third parties, who have access to this computer, the opportunity to try out user IDs and passwords. It is even more dangerous if the line is interrupted without the user at the local terminal being logged-off automatically. The next caller could then work with the same user ID, without any need to log on to the system Through this, he gets complete access to the IT system without any identification or authentication.

T 5.40 Monitoring rooms using computers equipped with microphones

Nowadays, many IT systems are equipped with microphones. The microphone on a computer connected to a network can be used by all persons who have access rights to the relevant device files (e.g. */dev/audio* for UNIX and an entry in the registry for Windows NT). If these access rights are not granted carefully, unauthorised persons might be able to misuse the microphone for eavesdropping.

T 5.41 Misuse of a UNIX system with the help of uucp

The UUCP (UNIX-to-UNIX copy) software package allows an exchange of ASCII and binary files between IT systems and the execution of commands on remote IT systems. UUCP was originally implemented on UNIX systems but is now available for many other operating systems. During communication via UUCP, IT users at remote computers get privileges for the local computer. If these rights are not granted carefully, or restricted to a bare minimum, the local system is in danger of being misused. Masquerading via UUCP, e.g. by feigning a host using the relevant password, is also conceivable.

T 5.42 Social engineering

Social engineering is a method of "bugging" information which is not generally accessible. Perpetrators often pose as insiders by using pertinent keywords during conversations and thus receive information useful for other purposes.

"Sounding" can be performed by telephone call where perpetrators pose as:

- A secretary whose superior needs to urgently complete a task but has forgotten the correct password
- An administrator who is calling because of a system error and needs to know the user password to eliminate this error
- A telephone technician who needs to know certain details, e.g. the subscriber number a modem is configured for and the settings of this modem
- An external person wanting to speak to Mr. X who is not on the premises. The information that Mr. X will be away for three days also implies that Mr. X's account will remain unused and unobserved during this period.

If queries are subsequently raised, the inquisitive caller was "just an assistant" or "somebody important".

T 5.43 Macro viruses

With the exchange of files (e.g. by data media or e-mail), there is a danger that, in addition to the actual file (text file, spreadsheet etc.), other macros connected to the document or embedded editor commands are also transmitted. These macros can only be executed with the relevant application program (Winword, Excel etc.) when the document is processed, either due to activation by the user or if the macro starts automatically. If a document is received by a WWW browser which automatically opens the document, a macro can be activated.

As the macro languages have a large instruction set, there is a danger that a macro with a damaging effect is added to a document (e.g. a virus).

In practice, the danger, especially for documents for Winword or Excel from Microsoft, rose significantly all over the world. For a user, therefore,it is not clear that files for Word profiles (*.DOT) which might contain macros, can be renamed to *.DOC files and then appear as ordinary document files not containing any macros. However Microsoft Word processes these kinds of files nearly the same way, without any notification to a user of that fact (exception: Winword starting from version 7.0.a)

In the meantime, macro viruses for Word are the number one in the rank of all reported virus infections. It must be noted that micro viruses can occur on all operating systems where Winword can be installed (Windows version 3.1 and 3.11, Windows 95, Windows NT, Apple Macintosh)

Example:

The Winword macro virus "Winword Nuclear" was spread through the Internet via the file WW6ALERT.ZIP. The macro virus causes the text "STOP ALL FRENCH NUCLEAR TESTING IN PACIFIC!" to be added to all printouts, but also attempts to delete system files.

T 5.44 Abuse of Remote Access Ports for Management Functions of Private Branch Exchanges

Private branch exchanges have remote access ports for management functions. It is possible to execute all administration and maintenance tasks as well as other management functions such as alarm signalling and processing via these access ports.

Such remote access ports are particularly useful and sometimes indispensable in connected PBX installations (corporate networks). It is possible to distinguish between two types of remote access:

- "Modem" access via dedicated management ports and
- Direct dialling via DISA (Direct Inward System Access).

. Furthermore, in more recent logging procedures such as QSig and some of the other proprietary protocols, management functions are already contained within the signalling spectrum. This results in the potential for abuse.

In the case of insufficiently secured access ports for remote maintenance, it is conceivable that hackers could gain access to the PBX's management programs. Consequently, once they had mastered the system password they would perhaps be able to perform **all** administration tasks. The resultant damage may range from failure of the complete system, via the most serious operating malfunctions, loss of confidentiality of all data present on the system, through to huge direct financial loss, e.g. through call charges fraud.

T 5.45 Trying Out Passwords under WfW and Windows 95

Within a peer-to-peer network under WfW, access rights to directories are realised by the allocation of passwords. No distinction is made between individual users. Access to a shared directory and the files stored inside is only granted if the correct password is entered. This is not the case for Windows 95 used within NetWare networks. Therefore, in principle, it is possible to determine the access passwords to shared directories by trial and error under WfW. As there is no restriction on the number of unsuccessful attempts when entering passwords, this promises to be very successful if a certain systematic approach is used.

T 5.46 Masquerading under WfW

WfW is not able to identify users reliably as every user of a WfW computer can change the computer name and the log-on name. Therefore masquerading is easily possible. Thus, a potential perpetrator may share a directory with damaging programs inside with all employees working under WfW and connected to the same network, using a false name on his computer. He can also try to get unauthorised access to the directories of others. The person to whom damage is caused will be misled about the true identity of the person concerned. In the same way, a perpetrator could easily carry out communication functions under WfW (e.g. using the telephone function) using a false name and mislead the recipient about the identity of the true sender. It is also possible to prevent a specific computer from logging on under WfW by logging on in its name ahead of it under WfW.

Under Windows 95 and Windows NT, it is possible to prevent the user from changing the log-on name or the computer name via the appropriate system guidelines.

T 5.47 Deleting the Post Office

If a common post office is used by several users under *mail*, it may be deleted, without authorisation, by circumventing all WfW security functions if there is no guarantee of adequate access protection to one of the computers known to the post office (e.g. via a BIOS password).

T 5.48 IP Spoofing

IP spoofing is a method of infiltration in which incorrect IP numbers are used to act out a false identity to the IP system being attacked.

Within many protocols of the TCP/IP family, authentication of the IT systems communicating with each other takes place only via the IP address which is easily falsified. If one also exploits the fact that the sequence numbers used by computers for synchronisation when making a TCP/IP connection are easy to guess, it is possible to send packets using any sender address at all. Thus, appropriately configured services such as *rlogin* can be used. In this case, however, an invader must possibly take into account the fact that he will not receive an answer packet from the computer which is being used improperly.

Additional services which are threatened by IP spoofing are *rsh*, *rexec*, X-Windows, RPC-based services such as NPS and TCP-Wrapper which is otherwise a very worthwhile service for setting up access monitoring for TCP/IP networked systems. Unfortunately, the addresses used in level 2 of the OSI model such as Ethernet or hardware addresses are also easy to falsify and therefore provide no reliable basis for authentication.

In LAN's in which the Address Resolution Protocol (ARP) is used, many more effective spoofing attacks are possible. ARP is used to find the 48 bit hardware or Ethernet address belonging to a 32 bit IP address. If a corresponding entry is not found in an internal table in the computer, an ARP broadcast packet is transmitted with the unknown IP number. The computer with this IP number then transmits an ARP answer packet back with its hardware address. As the ARP answer packets are not secure against manipulation, it is usually sufficient to gain control over one of the computers in the LAN in order to compromise the entire network.

T 5.49 Abuse of Source Routing

Abuse of the source routing mechanism and protocol is a very simple protocol-based method possibility for attacks. In an IP packet it is possible to prescribe the route by which the packet is intended to reach its target, or the route the answer packets should take. The description of the route may, however, be manipulated during the transmission so that the secure routes provided for by the routing entries are not used (e.g. via the firewall), whilst other uncontrolled routes are.

T 5.50 Abuse of the ICMP Protocol

As a protocol of the transport level, the Internet Control Message Protocol (ICMP) has to transport error and diagnostic information. It may be abused in several ways. On the one hand, the routing tables of a computer may be changed by way of *Redirect* packets and undesirable routes may be configured. On the other hand an invader may smuggle falsified *Destination Unreachable* packets into the connection so that the existing connection is interrupted and the availability of the network connection is no longer given.

T 5.51 Abuse of Routing Protocols

Routing protocols such as RIP (Routing Information Protocol) or OSPF (Open Shortest Path First) serve to pass on changes to routes between two networked systems to the systems concerned, thereby making s a dynamic change of the routing tables possible. It is easily possible to generate incorrect RIP packets and thus to configure undesirable routes.

The use of dynamic routing makes it possible to send routing information to a computer which usually uses this information unchecked to build up its routing tables. The invader can exploit this to change the transmission route in a particular way.

T 5.52 Misuse of administrator rights in Windows NT systems

Improper administration occurs when legitimately or non-legitimately acquired administrator authorisations and rights are deliberately used to damage the system or its users.

Example:

By improper use of the right to assume ownership of any files, an administrator, under Windows NT, can gain access to any files, even though their owner has explicitly refused him such access by means of appropriate access permissions. However, the gaining of access can be recognised by the original owner of the files, as the administrator has to make himself the owner of the files concerned in the process, and under Windows NT no function is available to undo this change again. Nevertheless, the administrator can gain access to user files without being noticed by, for example, registering with the backup operators' group and making a backup of the files he wishes to read.

There are various opportunities for exploiting administrator rights in an improper manner. These include illegal access to files, changes to the logging settings and the specifications for user accounts. Other possibilities of misuse lie in the falsification of protocol details, by altering the system time, or in the detailed tracking of the activities of individual users.

Depending on the underlying hardware, where it is possible to gain access to the console and the system cabinet, the system can be booted up. This may enable the configuration to be manipulated if boot-up can be performed by an outside medium or if another operating system can be selected.

T 5.53 Deliberate misuse of protective cabinets for reasons of convenience

One often-seen form of deliberate misuse of protective cabinets with mechanical code locks consists of not wiping the code after closing a protective cabinet, in order not to have to re-enter the code when opening it. This inappropriate behaviour reduces the protection value of the cabinet against unauthorised access, as it enables a third party to open the protective cabinet without knowing the code.

A circumstance encountered just as frequently involves protective cabinets not being locked when the room is vacated for a short period, to save individuals from having to open the cabinet when they return. This likewise reduces protection value against unauthorised access.

T 5.54 Deliberately causing an Abnormal End

A Netware ABEND (Abnormal End) occurs when the Netware operating system can no longer carry out or control network processes properly due to hardware and/or software problems. In this case, the file server is stopped and must be restarted.

If an attacker has access to a Novell Netware server-console, the input of certain parameters will allow deliberate execution of an ABEND.

The abnormal end of a Novell Netware Server can even be caused by anyone having access to the network, without an authorised login being required. By opening the program *SYS:\PUBLIC\RENDIR.EXE* with additional parameters, every workstation with an "Attached" status can provoke an ABEND on a Novell Netware Server.

T 5.55 Login Bypass

After successful login to the Novell Netware server the login-scripts (system-login-script, user-login-script) creates a personal network environment for the user.

By using options when executing *LOGIN.EXE* under Novell Netware, neither the system-login-script nor the user-login-script of the selected Novell Netware server will be activated, thereby avoiding the security settings implemented in the login-scripts. Security setting implemented in the login scripts can therefore, be circumvented. Thus, after an authorised login and with the help of map commands, it is possible for the user to "move around" on the Novell Netware server, independent of the set parameters of the login scripts (system login-scripts, user login-scripts). In conjunction with insufficient allocation of privileges, this can lead to a situation whereby the user has access to information which should normally not be available to him.

T 5.56 Temporary free-access accounts

The standard set up of a new user account does not involve a password. As far as the network operating system is concerned there is no obligation to assign a password, although this can be set up in the standard settings ("Default Account Balance/Restrictions"). The newly set-up user-accounts are openly accessible to anyone without requiring a password. The more privileged the account is on the Novell Netware server, the higher is the threat of the so-called "race on new accounts".

In this context it must be taken into account that different versions (e.g. vers. 3.75, vers. 3.76) of Netware Utilities *SYS:\PUBLIC\SYSCON.EXE* transmit an unencrypted password across the network, if the system administrator has used a new password.

T 5.57 Network analysis tools

If information transmitted in the network segment is not encrypted, it can be read in clear text with the help of network analysis tools or so-called Sniffers. It must be taken into account that these Sniffers are not to be considered as "hacking software" since many products which serve as network-managers contain such a function.

T 5.58 Hacking Novell Netware

"Hacking Novell Netware" can principally be carried out in two ways.

Firstly, a targeted attack against a user account can be carried out from a workstation in order to find out the password.

A targeted attack against a user account can take place via a so-called brute force attack, in which a workstation (status: attached) with the help of an algorithm or the provided dictionary, generates passwords and tries them out, thus attempting to login to a previously established user account.

By using the program *HACK.EXE* an authorised user can carry out an attack against the supervisor's account. By taking advantage of a weakness in the operating system, all users of the Novell Netware server can be put in a position equivalent to that of a supervisor. Also, the supervisor can be logged out or his password changed, given the supervisor is logged on when *HACK.EXE* is activated.

Furthermore, an attack can be carried out via direct manipulation of the server, for example, to generate an account equivalent to that of a supervisor.

By loading and activating NLMs (Netware Loadable Modules), which were developed as emergency tools, it is possible, for example, to create a special user whose privileges on the Novell Netware server are equivalent to those of a supervisor.

These tools, such as *SETPWD.NLM*, also function in Netware 4 networks. In this context it is, therefore, advisable to once again refer to S 1.42 *Secure siting of Novell Netware Servers*.

Most of these programs are freely available on the Internet. As regards their operation, they can be used by "amateurs" as no specific knowledge of Novell Netware is necessary.

T 5.59 Misuse of administrator rights in Novell Netware 3.x networks

A supervisor account or supervisor-equivalent account possesses complete control over the Novell Netware server, with the exception of bindery information (e.g. passwords).

It is, therefore, possible for an account with the security level "supervisor" to have access to all stored information on the server, as long as it is not protected by additional safeguards such as encryption. Authorised users of such accounts are able to read, delete or change other users' data.

T 5.60 By-passing system guidelines

If local access to a non-networked PC under Windows 95 exists, it is possible to delete the password file (*name.PWL*) belonging to a particular user ID. Access with this user ID is then possible without knowing the user password. This is critical if a non-networked Windows 95 computer is restricted for certain users, but an administrator ID (for example ADMIN) exists which possesses all privileges. By deleting *ADMIN.PWL* a restricted, but nonetheless authorised, user can thus log on as an administrator. The restrictions or guidelines set for the user are then by-passed.

T 5.61 Misuse of remote access to management functions on routers

Routers are equipped with remote access ports for management functions. All administration, maintenance and signalling tasks can be performed via these ports. Such ports are useful, and sometimes even indispensable, particularly in large networks possessing several routers and LANs linked via long-range lines.

There are two types of remote access:

- Modem access via dedicated interfaces (e.g. V.24)
- Direct access via reserved bandwidths

If SNMP (Simple Network Management Protocol) is used for network management, a fundamental lack of security measures, or a failure to implement existing measures, gives rise to threats over and above the direct misuse of unprotected remote interfaces:

- An unauthorised user intercepts data packets from an SNMP management station and modifies their parametrised values for his own purposes. The manipulated data packets are then forwarded to their original, intended destination. The receiving unit is not able to detect the manipulation of the data, and handles the information in the packet as though it had been sent directly from the management station.
- If the owner of a network management station gains access to a network administered using SNMP, it is possible for the owner to impersonate a community (an administrative area within SNMP). As a result, an unauthorised user is able to feign an authorised identity, and read all the information from the agents (objects to be managed in the network, such as routers) as well as perform all management operations. In this case, the agents are not able to distinguish between the correct and incorrect identities.

T 5.62 Misuse of resources via remote IT systems

Remote IT systems (e.g. telecommuting workstations) can usually access a large number of resources in a corporate network. This constantly poses a threat of data and program theft.

Access by remote IT systems (e.g. remote workstations) to a corporate network also gives rise to a danger of misuse of services offered within the network. Fraudulent use of communications servers (e.g. fax gateway, Internet links etc.) for private purposes in a network can result in unnecessary, extra charges.

T 5.63 Manipulation via the ISDN D-channel

The sum of all physical links between a subscriber and a digital exchange assigned to that subscriber is termed connection network. Such a connection network contains numerous distributors and transfer points, some of which are freely accessible and unprotected to a large extent (e.g. cable distributors). In the simplest case, communications with the connection network can be disrupted by mechanical damage to a connection line.

Furthermore, an ISDN protocol analyser allows communicated messages to be recorded and evaluated. If a protocol analyser is looped into the communications circuit, it also allows the manipulation of control information on the D-channel of the ISDN network. The communications components of the affected subscriber (i.e. ISDN cards, ISDN routers, telecommunications facilities, etc) might thus respond in a manner which impairs their operation or the integrity of the stored data.

T 5.64 Manipulation of data or software in database systems

In this case, data is corrupted or rendered useless through deliberate manipulation. The consequences of this are described under T 4.28 *Loss of data in a database* and T 4.30 *Loss of database integrity/consistency*.

The deliberate deletion/modification of files in a database or files of the standard database software lead to the destruction of the entire database system (refer to T 4.26 *Failure of a database*).

In principle, it is not possible to prevent users from deliberately manipulating data or destroying a database within the scope of the access rights allocated to them. However, if access rights can be circumvented (e.g. due to incorrect administration of the DBMS), then even unauthorised parties can gain access to the database and manipulate the data contained therein.

T 5.65 Denial of services in a database system

This type of intrusion is aimed at disabling the functions and services normally available to users in a database system. In addition to the examples mentioned under T 5.28 *Denial of services*, database services can be disabled, for example, by selecting large amounts of data whose evaluation paralyses the entire system, or by locking access to data records.

T 5.66 Unauthorised connection of IT systems to a network

In principle, unauthorised connection of an IT system to an existing network (by connecting to the existing cables or using the interfaces in the technical infrastructure rooms or offices) cannot be ruled out. This type of linkage cannot be prevented with available cable designs, which differ solely in terms of the time and effort required to connect to the cable and compromise the data.

The unauthorised integration of a computer into a network is often very difficult to detect, and usually goes unnoticed. This type of access allows monitoring of all data communications taking place in the affected segment and can facilitate the following activities, for example:

- Manipulation of data and software
- Monitoring of lines
- Manipulation of lines
- Replay of messages
- Masquerading
- Analysis of message flow
- Denial of services
- Unauthorised execution of network management functions
- Unauthorised access to active network components

.

T 5.67 Unauthorised execution of network management functions

Unauthorised execution of network management functions allows partial or full control of active network components. One of the factors determining the possibilities of control is the network management protocol in use (e.g. SNMP or CMIP/CMOT). This can impair network integrity, the availability of some or all network segments, as well as the confidentiality/integrity of data.

The use of a service protocol such as SNMP allows dedicated ports of active network components to be activated and deactivated. Furthermore, VLAN configuration, routing tables, router configuration as well as the filter configuration can be manipulated (refer to T 3.28 *Inadequate configuration of active network components*). In addition, the possibility of the distribution of firmware updates across the network allows unauthorised installation of software on active network components. This software might allow and facilitate the infiltration on network components in a great variety of ways.

T 5.68 Unauthorised access to active network components

Active network components normally have a serial interface (RS-232) to which an external terminal or portable PC can be connected. This allows the active network components to be administered locally as well.

Insufficiently protected interfaces might allow intruders to gain unauthorised access to network components. After passing local security checks (e.g. through entry of a password), an intruder might be able to perform all administrative functions.

By reading the configuration of active network components, the intruder can gain access to confidential information on the topology, security mechanisms and utilisation of the network. Configuration data can be read by connecting an external terminal or portable PC to the serial interface of the active network component, by accessing the active network component via the local network, or by viewing the data on a screen or display while the active network component is being administered or configured.

T 5.69 Higher risk of theft from a working place at home

The working place at home is usually not protected to the same extent as the working place in a company or agency. Due to elaborate measures such as security doors and guards, the risk of intruders in the building is far less than in private premises.

Burglaries of private residences usually have financial gain as the motive. Electronic equipment stolen in this process is usually intended for sale to third parties. Possibilities of using stolen information for monetary gain include extortion of the affected company or forwarding of the data to competitors.

T 5.70 Manipulation by family members or visitors

Workstations at home are generally accessible to family members and visitors, so that they might be able to manipulate business-related data on the workstations if the data is not protected adequately. Possible scenarios here include the installation of private software (e.g. computer games) by family members, damage to IT by children, and misappropriation of business-related data media for use by unauthorised third parties. This type of inadvertent or intentional manipulation affects the confidentiality and integrity of the business-related information, as well as the availability of data and IT services on the workstation.

T 5.71 Loss of confidentiality of classified information

In the case of classified information (such as passwords, person-related data, certain business-related and official information, research & development data) there is an inherent danger of the confidentiality of this information being impaired inadvertently or intentionally. Classified information can be tapped from various sources, including

- Internal storage media (hard disks)
- External storage media (floppy disks, magnetic tapes)
- Printed paper (hardcopies, files) and
- data communications lines.

There are various ways of actually obtaining the confidential information:

- Reading out data
- Copying data
- Reading of data backups
- Theft of data media for the purpose of evaluation
- Monitoring data transmission lines
- Viewing data on a screen.

The more classified a piece of information, the higher the incentive for third parties to obtain and misuse it.

T 5.72 Misuse of e-mail services

Misuse of e-mail systems can take place at a variety of stages: at the sending workstation, within an Intranet, on a mail server or at a receiving workstation.

If access to a user's e-mail program or an organisation's e-mail system is not adequately protected, unauthorised persons might be able to manipulate these IT systems. The resulting, unnecessary transmission expenses might also be accompanied by damage caused through the impersonation of an authorised user.

Similarly, unauthorised persons must be prevented from reading e-mail. Confidential information could thus be disclosed, lose its value or be exploited to the detriment of the recipient.

Examples:

- A department head briefly left his office with the IT system unlocked, the mail software on it still active, and user authentication already having been performed. A colleague who happened to pass by the office then played what he considered to be a great practical joke by using the department head's ID to send other colleagues "letters of notice" or work orders.
- An employee uses his own business e-mail account to disseminate private opinions which could damage the reputation of his employer.

T 5.73 Impersonation of a sender

It is relatively easy to impersonate senders when dispatching e-mail. This might result in damage if the recipient considers the information contained in the e-mail to be authentic and binding.

Example:

The commonly used Eudora mail program allows mail with an incorrectly specified sender to be forwarded to a mail server without a password check. If user authentication has not been performed, this mail is only identified as "Unverified" in the field labelled "X-Sender". However, experience has shown that very few recipients pay attention to this. Besides, most mail programs do not include this field in their standard configuration.

T 5.74 Manipulation of alias files and distribution lists

To avoid having to re-enter frequently required e-mail addresses, pseudonyms can be assigned to these addresses, or distribution lists can be prepared to allow convenient selection of a large group of recipients. Unauthorised modification to such pseudonyms and distribution lists can result in a failure to forward e-mail to the required recipient, or transfer of the e-mail to an unauthorised recipient. Particularly vulnerable in this case are centrally maintained pseudonym files and address books.

T 5.75 Overload due to incoming e-mails

An e-mail address can be blocked intentionally by being constantly sent large e-mail files (possibly with unintelligible contents). This can happen, for example, to users who have not observed Netiquette and thus made themselves unpopular in news groups. Netiquette (network etiquette) comprises rules of conduct which develop in the course of time among users of the Internet, particularly newsgroups. These rules are meant to allow efficient and satisfactory use of the Internet for everyone.

An intentionally high volume of traffic can overload the local mail system, thus rendering it inoperable. This problem can become serious enough to make the provider disconnect the user's organisation from the network.

A mail system can also be overloaded by employees engaged in the forwarding of chain-letters. During a Christmas season in the mid-Eighties, one such chain-letter campaign paralysed several IT systems worldwide. Users received an e-mail with Christmas greetings including a bitmap, and were requested to copy this mail and forward it to ten other users.

T 5.76 Mail bombs

Mail bombs are e-mails containing functions intended to disrupt IT systems. Functions like this are usually integrated into e-mail attachments. On being opened for the purpose of reading, such an attachment generates countless subdirectories or occupies a lot of hard disk space, for example. In many cases, the selective overloading of e-mail addresses by messages with usually unintelligible contents is also termed mail bombing (refer to T 5.75 *Overload due to incoming e-mails*).

T 5.77 Unauthorised monitoring of E mails

Transmission in plain text

Electronic mail (E Mail) is usually transmitted as plain text. Data which has not been protected by cryptographic means can be monitored and modified on any IT system via which it is being transmitted. In the case of E Mail sent over the Internet, a large number of IT systems could be involved without the precise routing being known beforehand. The transmission route depends on the utilisation and availability of gateways and network segments. In some cases, E Mail intended simply for transmission between two neighbouring municipal districts can be routed abroad at some point.

Storage on the mail server

Access to incoming E Mail can also be gained via the recipient's mailbox maintained on the mail server. This mailbox contains all received E Mails, not only those which have not yet been read, but depending on the configuration, it may also contain an archive of all E Mails received in recent months. As a very minimum, the system administrator in charge of the mail server will have access to the mailbox. In some cases, copies of outgoing E Mails are also stored on the mail server. Usually, however, the user's mail software stores them on the sender's computer.

Examples

- A number of Microsoft internal E Mails have been used by the other side in the anti-trust proceedings against Microsoft to undermine the company's position. Some of these E Mails contained defamatory remarks about Microsoft's competitors.
- A supplier makes services available over the Internet. To use these services, it is necessary to log on to the service provider's server. The authentication information needed for this purpose is sent to the customer by E Mail. If this E Mail is intercepted, an adversary can then log on to the service provider's server without authorisation and avail himself of its services at the expense of the registered customer.

T 5.78 DNS spoofing

To be able to communicate with another computer in the Internet, one needs to know its IP address. This address consists of 4 sets of numbers between 0 and 255, e.g. 194.95.176.226. As such numbers are not very easy to memorise, almost all IP addresses are assigned names. This method is termed DNS (Domain Name System). Consequently, the WWW server of the BSI can be addressed under *http://www.bsi.bund.de* as well as *http://194.95.176.226*, because the name is converted into the IP address during polling.

The databases in which computer names are assigned IP addresses, and vice versa, are located on name servers. Two databases are available for allocation of names to IP addresses. The first database allocates IP addresses to names, while the second database allocates names to IP addresses. These databases need not be mutually consistent! DNS spoofing is said to occur when an intruder becomes successful in forging an allocation between a computer name and an IP address, i.e. assigning a name to a false address, or vice versa.

This allows the following types of intrusion:

- r-services (rsh, rlogin, rsh)

  These services allow authentication on the basis of client names. The server knows the IP address of the client and requests its name via the DNS.

- Web spoofing

  An intruder could assign the address *www.bsi.bund.de* to a wrong computer, which would then be addressed each time *http://www.bsi.bund.de* is entered.

The ease with which DNS spoofing can be performed depends on how the attacked network has been configured. As no computer can hold all the DNS information existing in the world, it always has to rely on information from other computers. To reduce the volume of DNS requests, most name servers temporarily store information which they have received from other name servers.

Once someone has infiltrated a name server, they are also able to modify the information it holds. Direct intrusion into a name server is not considered further here. Instead, the principal shortcomings of DNS are mentioned.

The two examples below are intended to describe different techniques of DNS spoofing.

1. A user on the computer named *pc.customer.de* first intends to access *www.company-x.de* and then the competitor's server *www.company-y.de*. To allow access to *www.company-x.de*, the corresponding IP address needs to be requested from the name server *ns.customer.de*. This server does not know the address either, and then requests it from the name server of *ns.company-x.de*. This server returns the IP address, which is forwarded by *ns.customer.de* to the user and stored. If, in addition to the IP address of *www.company-x.de*, the response from *ns.company-x.de* also contains any other IP address for the computer name *www.company-y.de*, it is also

stored. If the user then tries to access *www.company-y.de*, the internal name server *ns.customer.de* no longer sends any requests to the name server *ns.company-y.de*; instead, it forwards the information supplied to it by *ns.company-x.de*.

2. Company X knows that a user on computer *pc.customer.de* intends to access a competitor's computer *www.company-y.de*. Company X prevents this by requesting the address of *www.company-x.de* from name server *ns.customer.de*. This server in turn has to request the information from name server *ns.company-x.de*, and consequently receives incorrect details on *www.company-y.de* as was the case in the first example.

These two examples are based on the assumption that name servers also accept additional data which they had not requested in the first place. New versions of certain software programs (e.g. *bind*) no longer contain this error, thus preventing intrusions by this means. However, IP spoofing can still be used to generate false DNS entries, although this type of intrusion is technically much more complicated.

T 5.79 Unauthorised acquisition of administrator rights under Windows NT

An administrator account is created during every standard installation of Windows NT (this applies to Workstation and Server versions, as well as the domain controller). As opposed to user-configured accounts, this pre-defined account can neither be deleted nor disabled; this prevents administrators from being blocked intentionally or by mistake, thus ensuring administration on a continuous basis. One problem here is that the pre-defined administrator account cannot be disabled even if the maximum number of invalid passwords specified for a block in the account guidelines is exceeded. This allows passwords to be tested using cracking programs.

There are also other methods of obtaining a password assigned to an administrator account in order to gain administrator rights: if a computer is remotely administered under the Windows NT operating system, there is a danger of the login password being transmitted during authentication procedure, thus allowing an intruder to scan the password. Even if the system has been adjusted to ensure that login passwords are only transmitted in encrypted form, it is possible for intruders to record an encrypted password and decrypt it with the help of appropriate software.

Furthermore, every password is stored in encrypted form in the registry and in a file located in the directory *%SystemRoot%\System32\Repair*, as well as on emergency diskettes or tape backups. Intruders who are able to access this file could decode the required password with the help of appropriate software.

Finally, a special type of destructive software allows intruders logged locally into a Windows NT computer to add an arbitrary user account to the "Administrators" group and thus obtain administrator rights for the holder of this account.

T 5.80 Hoaxes

False alarms

A hoax is a message which contains a warning of new spectacular computer viruses or other IT problems, resulting in widespread panic, but which has no factual basis. Usually such messages are sent by e-mail. For example, it may warn of a computer virus which damages hardware or causes infection or damage simply through opening of an e-mail (not even an attachment) and is not detected by any anti-virus software. Alongside this warning the recipient is requested to pass on the message to friends and acquaintances. Such a hoax is even more effective if a false address, such as that of a well-known manufacturer, is given for the sender.

A hoax is not a virus!

Such hoaxes should not be confused with computer viruses, which really can tamper with IT systems. It is simply a misleading message that can be deleted without causing any damage, which is what you should do. The only damage caused by a hoax is the recipient's uncertainty and irritation, and possibly the time and money spent on forwarding the hoax.

A whole range of such hoax messages have afflicted mobile phone users, whereby users have been warned that inputting certain key combinations or dialling certain call numbers on mobile phones could result in conversations being tapped or calls being charged to other persons. Because such messages contain references to particular mobile phone brands and a few technical terms, they give the impression of being serious messages. Such rumours have a way of persisting users find them disconcerting.

Example:

In the spring of 2000 the following false alarms were going the rounds by e-mail (and in some cases even by letter):

> "If you receive a message on your mobile phone telling you to call back number 0141-455xxx, under no circumstances should you do so. Otherwise your phone charges will shoot up enormously."
>
> This information was published by the "Central Office for the Suppression of Fraudulent Practices" (Office Central de Repression du Banditisme). ..."

T 5.81 Unauthorised use of a cryptomodule

If a third person succeeds in using a cryptomodule without authorisation, this can lead to various types of damage. Examples of such damage include:

- While using the cryptomodule without authorisation, a perpetrator may manage to read secret codes, alter the codes or even manipulate vital security parameters. This would mean that the cryptographic process no longer offers sufficient security.
- While using the cryptomodule without authorisation, the perpetrator may manipulate the cryptomodule in such a way that it appears to be working correctly at first sight but is actually in an insecure state.
- The perpetrator may use the cryptomodule in the form of a masquerade. If the perpetrator signs or encodes data while using the cryptomodule without authorisation, this is interpreted by the recipient of the data as if it had been done by the authorised user.

Example:

It is possible to use a cryptomodule without authorisation if users briefly leave their workplace while the cryptomodule is able to operate and not protected against unauthorised access. This is the case, for instance, if a signature chip card or encoding chip card is left in the computer. In this way, anyone who happens to go by can sign E-mails in the name of the usual user or encode files stored in the IT system in such a way that the user can no longer use them.

T 5.82 Manipulation of a cryptomodule

A perpetrator can attempt to manipulate a cryptomodule in order to read secret codes, alter the codes or even alter vital security parameters. A cryptomodule can be manipulated in various ways, for example it can contain:

- a super password which can get round all other passwords.
- unregistered test modes through which sensitive areas can be accessed at any time.
- Trojan horses, i.e. software which, alongside its actual task, performs actions which cannot be recognised directly, such as recording passwords.
- manipulated access rights to certain commands

. Other examples of such attacks include:

- modifying cryptographic codes,
- impairing the internal code generation, e.g. by manipulating the random number generator,
- modifying the processes within the cryptomodule,
- modifying the source code or the executable code of the cryptomodule,
- exceeding or falling below the permissible range of the cryptomodule's voltage supply, temperature, EMC limits, etc.

When the cryptomodule is manipulated, the perpetrator will usually try to conceal the attack so that the user believes the cryptomodule to be working correctly at first glance, although it is actually in an insecure state. There are, nevertheless, also destructive attacks in which perpetrators consciously resign themselves to destroying the cryptomodule, for example if they wish to obtain information on how the cryptomodule functions or read the cryptographic code.

A perpetrator can attempt to attack the cryptomodule at the user's site or steal it. If the user's site is poorly protected, the manipulation may be performed extremely rapidly and may thereby remain unnoticed for a long time. By stealing cryptomodules, a perpetrator can obtain important information on how a component can most easily be manipulated. The stolen components can be used to obtain sensitive information such as codes, software or knowledge of hardware security mechanisms. However, the stolen component can also be used to fake an authentic cryptomodule.

T 5.83 Compromising cryptographic codes

When cryptographic procedures are used, the gain in security depends to a large extent on how confidential the secret cryptographic codes are. With knowledge of both the code and the cryptomethod used, it is normally easy to revert the encoding and obtain plain text. A potential perpetrator will therefore attempt to ascertain the code used. Possible points of attack are:

- Unsuitable processes are used to produce the code, for example to determine random numbers or derive the code.
- The codes that are produced are exported before they are stored using a safe medium.
- During operation, codes from cryptomodules are exported through technical attacks .
- Codes left as backup are stolen.
- When cryptographic codes are entered, the codes cracked by perpetrators.
- The cryptomethods in use are cracked. In the case of symmetric cryptographic techniques such as DES, for example, it is currently possible to determine the code using huge numbers of parallel computers (brute-force attack).
- Internal perpetrators give away cryptographic codes in use.

T 5.84 Forged certificates

The purpose of certificates is to link a public cryptographic code to a person. The link of a code to the name of a person is then protected cryptographically using the digital signature of a reliable neutral organisation. These certificates are then used by a third person to check digital signatures of the person identified in the certificate or to send this person data with the code recorded in the certificate.

If such a certificate is forged, false signatures seem to be correct when checked and are associated with the person in the certificate or data is encoded and sent with a code which may be insecure. Both opportunities for attack may induce a perpetrator to bring forged certificates into circulation.

Forged certificates can be produced in various ways:

- Internal perpetrators from the neutral organisation create a certificate with false entries using their own signature code. This certificate is authentic and is verified to be correct when tested.
- Perpetrators pretend to be someone else and demand a certificate which is made out to this person, although the perpetrators are in possession of the secret code which corresponds with the public code.
- Perpetrators produce a certificate and sign it with a code of their own. The forgery is only noticed if the certificate is tested and it is possible to determine that the certificate was made out by an unreliable organisation.

Once perpetrators have somehow got hold of a certificate with wrong entries, they can pretend to be someone else when communicating with peers at any time, both when sending and when receiving messages.

T 5.85 Loss of integrity of information that should be protected

If data integrity is lost, a multitude of problems can occur:

- In the most simple case, data can no longer be read, that is to say processed.
- Data can be falsified, either accidentally or maliciously, in such a way that this results in false information being passed on. For instance, credit transfers can be made out to the wrong amount or sent to the wrong person, the details of the sender of E-mails can be manipulated, and much more.
- If encoded or compromised data records lose their integrity - and the alteration of just one bit is enough - they can no longer be decoded or unpacked.
- The same applies to cryptographic codes, where the alteration of just one bit is enough to make the code useless. Likewise, this means that data can no longer be decoded or checked for their authenticity.

Loss of integrity can occur in several ways:

- Information can be lost through the expiration of data carriers.
- Transmission errors can occur when data is transmitted.
- Computer viruses can alter or destroy entire collections of data.
- False entries can cause undesired transactions which even remain unnoticed for a long time.
- Perpetrators can attempt to manipulate data for their purposes, e.g. to gain access to other IT systems or collections of data.

T 5.86 Manipulation of management parameters

Management systems can also be used for an attack on a local computer system by deliberately causing incorrect configuration. The incorrect configuration can be caused in various ways. In the process, it is possible to manipulate both the management platform and the equipment it controls. Network management systems which use SNMP are particularly susceptible to attacks in which management parameters are deliberately configured incorrectly (e.g. through the perpetrator's own SNMP client). Depending on which parameters can be adjusted, the attacks range from simple "denial-of-service attacks" (e.g. by altering IP addresses) to data manipulation (e.g. following the alteration of access rights).

If network components are controlled through a management system, then all configuration parameters controlled by the management system should only be changed through the management system. Depending on the management system, however, it is also possible to change the configuration parameters of the components locally. If a PC is controlled through a network management system, e.g. via SNMP, then local users can alter the settings with a local SNMP client program (if they know the SNMP password) or using a local operational control (e.g. on a printer). This may just lead to inconsistencies in the network management system, but could even be deliberately used to cause gaps in the security. For example, it could later be made possible for a Windows NT computer to query records released via SNMP and the network.

T 5.87 Web spoofing

Web spoofing involves perpetrators "forging" WWW servers, that is to say, they set up their WWW sever to pretend that it is a particular, reliable WWW server. This is done by choosing a WWW address in such a way that many users assume they are connected to a particular institution just from the choice of address. Even if the correct computer name is used, Web spoofing is possible if perpetrators use DNS spoofing (see G 5.78 *DNS-Spoofing*).

Example:

- It is not the official Homepage of the White House which is found under the address www.whitehouse.com but that of a prankster.
- The XY bank has the WWW address www.xy-bank.de. Perpetrators can set up WWW sites under www.xybank.de or www.xy-bank.com which at first glance appear to be that of the XY bank. They then enter the addresses in various search machines, choosing keywords that XY customers may well search for.

  Users who call up these sites will assume that they are communicating with the WWW server of their bank. They are therefore willing to enter their account number and PIN number or other access codes. They may also read offers there which interest them but are false, such as profitable investments or property offers which they would like to accept. If the bank cannot make these offers under these conditions or cannot make them at all, the customers are at best dissatisfied and at worst, it can end in legal disputes.

Rather than trying to manipulate or imitate an existing WWW server, perpetrators can also bring their own WWW offer into the Internet and present it in such a way that each visitor has the impression of being connected to an established, serious institution.

Examples:

- Goods may be offered for the sole purpose of obtaining the credit card numbers of potential customers.
- There have been cases in which trusting customers have wanted to invest money under profitable conditions with supposed banks. They only knew of these banks via the Internet and only when the expected interest failed to arrive did they realise that it was simply a private WWW site which had in the meantime been deleted.

T 5.88 Misuse of active contents

During surfing on the Internet, WWW sites with active contents can be loaded on the user's computer (e.g. ActiveX or Java Applets). This software can be purposefully used in order to spy out confidential data from the user and return such information to the perpetrator via the Internet.

A Java-enabled browser allows Java applets to be loaded from the Internet and performed without being detecting by the user. This causes serious security risks for the Java user:

- A Java Applet can use standard network protocols (such as SMTP) in order to send data from the user's computer.
- A Java Applet can attack a Java system by corrupting its memory or it can attack a subordinate operating system by falsifying data or canceling important processes.
- A Java Applet can take up the whole storage space of the system or create high-priority messages. An attack on availability is also possible if the Java safety model is interpreted correctly.

Unlike Java, the functionality of ActiveX is barely limited. An ActiveX program can contain all commands up to the formatting of the hard disk. These small executable codes are called controls. The controls, usually distributed for illustration or entertainment can also have malicious elements which then have access to the file system of the user's computer or control other programs without being noticed by the user. ActiveX Controls can delete the hard disk, contain a virus or a Trojan horse, or search the hard disk for certain information. All of this can happen without the user or observer of the control noticing it. While the observer runs a game transmitted by the controls, this control can in the background search the E-mail for particular information.

By presetting their WWW browsers accordingly, users can ensure that only digitally-signed ActiveX controls are performed. However, such a digital signature only proves that the producer of the ActiveX control is known by a certification body and that the control provided by this producer was loaded unchanged. This says nothing about how such a control functions or if it is undamaged, and no guarantee is given for this.

T 5.89 Hijacking of network connections

Hijacking of a connection is even more serious than having a connection tapped. This entails injection of data packets into the network which result in either failure or blocking of the client. The server process is then unable to detect that a different program has now replaced the original client. When an existing connection is taken over in this way after a user has authenticated himself, the adversary can perform any actions he likes in the name of the authenticated person.

Example

There are already a number of programs which allow an existing Telnet connection to be hijacked.

T 5.90 Manipulation of address books and distribution lists

Manipulation of address books

On most fax servers it is possible to maintain address books and distribution lists. The information held in address books includes the fax numbers of recipients. It is also possible to combine several fax recipients into one group, e.g. for sending out serial fax transmissions. Such address books are very convenient to use since, once a recipient's fax number is held in store, faxes can be sent to that person without having to enter the number manually. Often users of a fax server no longer bother to check that the fax number entry held in the address book for the recipient is actually correct prior to sending out a fax. The same applies to the assignment of individual recipients to groups. Often no one bothers to check before sending out serial fax transmissions whether the members of a given distribution group are identical with the people to whom the fax should be sent.

Again, distribution lists can be used to assign incoming fax transmissions to (several) recipient(s).

Manipulation of distribution lists

As long as the possibility that an unauthorised person can alter address books and distribution lists is not ruled out, there is a risk that fax transmissions could be sent to unintended recipients or that a fax could be prevented from being sent to the intended recipient. By their nature, address books and distribution lists which are maintained centrally are especially at risk.

T 5.91 Disabling of RAS access security mechanisms

The security of RAS access depends significantly on correct use of the security mechanisms provided. However, it is generally possible to configure the RAS system (client and/or server) in such away that either weak or no security mechanisms are used. If, for example, the mechanisms used for data encryption are dynamically negotiated between client and server when a connection is established (e.g. this can occur if IPSec or SSL is used), generally this negotiation process entails the client offering the server a list of procedures supported (known as *cipher suites*) for selection, from which the server chooses one. The list of algorithms can be altered by making the appropriate configuration changes. Usually there is also a "no encryption" option.

If an unencrypted connection is one of the options allowed between clients and server, then there is a risk that protection of the data transmitted will be disabled. This is particularly problematic where users are able in the event of problems to modify the RAS system configuration settings on RAS clients to fit local circumstances.

Examples

- RAS communications are to be protected by means of IPSec running under Windows 2000. The RAS server has been configured so that IPSec encryption is requested but is not enforced, so that RAS clients can potentially also establish insecure connections. As the loss of performance associated with encryption appears unacceptable to a RAS user who is working with an older laptop, he disables IPSec encryption. The RAS connection is now established in plaintext.
- Under older Windows NT versions, encryption of the RAS connection using Microsoft Point to Point Encryption (MPPE) can only be performed if MS-CHAP has been specified as the authentication procedure. Consequently only if MS-CHAP is used are the parameters which are necessary for encryption exchanged between client and server. In order to use a standard authentication procedure, a user selects the CHAP procedure in the configuration settings. Encryption of the RAS connection is no longer possible using MPPE even though the appropriate option is enabled.

T 5.92 Use of the RAS client as RAS server

The RAS software installed on RAS clients may possibly allow the client to function as a RAS server and to accept incoming connections (e.g. Windows RAS). If this option is enabled, then anyone who knows the number of the telephone connection to which the client is connected can connect to this computer. If an aggressor succeeds in getting past the RAS authentication mechanism (for example, by trying out or guessing passwords, use of user accounts that are not password-protected, use of Guest user IDs with standard passwords), then he can access the data on the RAS client. If the client is connected over ISDN, then it is even possible to establish another outgoing connection (e.g. to the corporate network). If connection is automated (because the RAS password is stored on the machine), then the aggressor can also access data on the LAN without authorisation. It is therefore essential to prevent a RAS client from being used as a RAS server.

T 5.93 Permitting use of RAS components by third parties

If RAS components are deliberately made available to unauthorised persons, then the security of the RAS system can no longer be assured (see also T 3.30 *Unauthorised private use of telecommuting workstations*). The resulting possible threats are set out below.

Unauthorised use of RAS access

- Unauthorised RAS access could occur if the security guidelines are not adhered to. For example, it is a common occurrence for administrators to allow RAS dial-in to unauthorised persons (e.g. for use of the Internet) out of mistaken friendliness.

Passing on of passwords or token

- RAS users give authentication data or tokens to unauthorised third parties to enable them to access the LAN remotely (under their ID). Possible motives for doing this might include the fact that a colleague is not authorised under the RAS security concept to use remote access or has forgotten to apply for RAS permission in good time before a business trip. As one RAS user account is now being used by several users, in case of damage it will no longer be possible to unequivocally identify the person responsible.

Unauthorised use in the private environment

- Where telecommuting is permitted, the problem often arises that the RAS client is used by members of the family or friends of members of the family. If persons who are outside of the organisation are using the RAS client, they will generally ignore the security rules which apply to the RAS client. As a result, the security of the LAN can be compromised.

The possibility that IT systems in remote locations will be used by third parties can never be excluded as the security mechanisms of an IT system can be circumvented once physical access has occurred.

T 5.94 Misuse of cards

Loss and theft of mobile phones are everyday occurrences. In addition to loss of the phone itself, this can result in further financial loss. If an unauthorised person gains possession of a SIM card (e.g. because he finds it or steals it), he can make calls at the expense of the genuine cardholder as long as he knows the PIN or can guess it easily.

Data such as telephone directories or short messages which are stored on the mobile phone or SIM card may well be of a confidential nature. Loss of the mobile phone or card may then mean disclosure of this stored information.

There have been instances in the past where the cryptographic security mechanisms of the SIM cards provided by some network providers have proved too weak. This meant it was possible to make copies of these network providers' SIM cards. However, to do this, the adversary must have the original card. He also needs the PIN or, alternatively, the requirement to enter the PIN must be deactivated in order that the IMSI can be read.

Such an attack can easily be prevented and detected by private users. However, where a number of different people have access to the same mobile phone it is possible for such an attack to be carried out and only noticed long after the event. For example, this affects mobile phones from a pool or companies which hire out mobile phones.

T 5.95 Bugging of indoor conversations over mobile phones

Inconspicuous switching on

Mobile phones can be used to record or listen to conversations unnoticed. In the simplest case, a mobile phone can be switched on, connected to an interested third party and inconspicuously placed in a room, for example where a meeting is being held. However, as the phone has only a limited battery life and the microphone is not designed for room surveillance, such an attempt at bugging is of only limited effect.

Utilisation of features

Through skilful selection of features and combining these with additional frills, it is possible to put a mobile phone into talk mode without this being indicated by a ringing tone or other means. For example, there is one type of phone in which the mobile phone's display can be switched off by entering a particular key combination even though a call is actually connected to the device.

Manipulated mobile phones

However, specially manipulated mobile phones can also be used for this purpose. With these phones, it is not evident from looking at the phone that it is switched on. Here the mobile phone is used as a bugging device which can be activated from anywhere in the world over the telephone network, without this being detectable from the phone itself. Devices in which this special function is implemented using additional circuits are known. This manipulation is relatively easy to detect through visual inspection after taking the device apart or using special investigation methods. Operation of such devices is illegal in Germany.

T 5.96 Tampering with mobile phones

The installation of additional electronic circuitry, as described in T 5.95 *Bugging of indoor conversations over mobile phones*, is a typical hardware manipulation. In order that such tampering can be carried out, the device to be manipulated must be in the possession of the adversary for a certain period of time.

Manipulation of firmware

Another way of using mobile phones for bugging purposes is to tamper with the control software (firmware) installed on the device. This kind of tampering is a lot more difficult to detect than tampering with the hardware.

A concealed, undocumented bugging function could already be programmed (either deliberately or by accident) into the control software during development of the device.

However, it is also conceivable that the control software could be modified subsequently by a third party, for example when the device is out of the user's (short-term) control during repair or due to other reasons (loss or theft). Such manipulation requires in-depth specialist expertise which is normally available to few persons other than the firmware developers. It is virtually impossible for an outsider to demonstrate that such manipulation has taken place.

Mobile phones are becoming more flexible through extension of the mobile phone menu functions using SIM Toolkit and a new generation of SIM cards which support this functionality. Such a mobile phone can be programmed with new functions by the service provider over the cellular network. Thus, for example, the card provider can tailor the menu structure to meet the requirements of a particular customer.

However, this capability carries with it the threat that firmware could be tampered with, as the functionality that is needed to reconfigure a phone into a bugging device could already be contained as standard in the firmware. The probability that functions which will convert the mobile phone into a bugging transmitter can be called up from "outside" increases. It could also be possible for these functions to be enabled and disabled at will.

T 5.97 Unauthorised transfer of data over mobile phones

Mobile phones provide the means whereby data from one IT system, e.g. a PC or notebook, can be transported to another without a cable connection having to be established between the two devices.

Information can then be surreptitiously retrieved and transmitted in a place where IT systems can be accessed openly. If a mobile phone is connected to a modem or has an in-built modem, information held on a computer can be transmitted to virtually anywhere in the world wire-free.

This type of unauthorised data transfer can be performed either with a mobile phone that has been specially brought along for the purpose or even using an internal mobile phone. In this way large quantities of data can be passed to the outside world unnoticed. Existing bandwidth limitations which currently make the transmission of large quantities of data unattractive are likely to disappear over the next few years as new technologies come on stream. With GSM the maximum data transfer rate is currently 9600 bps, whereas next generation protocols (GPRS, UMTS) envisage significantly higher transfer rates.

Nor is it always possible to check afterwards whether such data transmission has occurred as the network provider's record of the call data may already have been deleted.

Example:

- An employee of one company is called out of a meeting with an outside party so that he can take an important phone call. The external party uses the brief interval during which he is alone in the meeting room to link up the PC installed there with his GSM modem. He then initiates a data transfer to a connection of his choice.
- Where remote access services are used over mobile phone networks, often the Calling Line Identification Presentation (CLIP) mechanism is used as an authentication feature. If the mobile phone is stolen or lost, the authentication procedure will no longer function properly. Although normally a PIN has to be entered when a mobile phone is switched on, most people leave their phones switched on. If the telephone is already switched on when it is stolen, then theoretically it can be used immediately by a third party. If the battery is re-charged in time, the point at which the phone cuts out due to lack of power can be deferred and hence the need to input the PIN because the phone has been switched on again.

T 5.98 Interception of mobile telephone calls

The easiest way of listening in on a conversation conducted over a mobile phone is simply to listen from close by. It is no rare occurrence to hear a person divulging a lot of company-internal information by talking loudly on the telephone in a public place (see also T 3.45 *Inadequate checking of the identity of communication partners*).

But generally there are also very elaborate technical means available for intercepting telephone calls.

If, for example, an adversary can gain access to the technical facilities of the network provider (lines, switching exchanges, base stations), he will then be able to listen to any telephone conversation conducted over this equipment. This applies to connections both in the mobile communication network and in the landline network. However, deliberate tapping of conversations which are assigned to a particular call number is extremely effort-intensive, due to the huge flood of data.

If the calls are connected over line-connected paths from the base station to the mobile telephone exchange, a physical attack on the cable paths is necessary. If a base station is connected to the mobile telephone exchange over an unencrypted directional radio link, as is the case with some network providers, it is possible to intercept and tap these radio signals unnoticed using antennae and special receivers. The threat is all the greater if all phone calls for the connected base station are transmitted over these directional radio links.

Telephone conversations are also transmitted bundled over directional radio relay links in the landline network. As these transmissions are generally unencrypted, conversations transmitted by this route can also be tapped with a certain amount of technical effort.

In Germany, the transmission of radio signals between mobile phone and base station is encrypted in all GSM mobile communication networks. There are special interception devices around which exploit the weakness of one-sided authentication in the GSM network (the only authentication which occurs is the authentication of the mobile phone to the base station), by pretending to mobile phones to be a base station, disabling encryption and instituting plaintext operation. Depending on the statutory requirements, in some countries encryption of transmissions can be completely disabled. It may also be possible that other security parameters such as the frequency of key changes are weaker.

Other possible ways of disabling this encryption are tampering with the mobile phone or the technical facilities of the network provider.

T 5.99 Analysis of call data relating to the use of mobile phones

With mobile communications, the signals transmitted on the radio link are not physically shielded against unauthorised passive monitoring and recording. Thus an aggressor could perpetrate an attack without the access problem which occurs on line-connected communications. A second problem which generally occurs with most radio communication services arises from the fact that for technical reasons the mobile communication partners have to be located in order to be contactable. Again, if these partners establish a connection themselves, they also give away information about their location through the act of establishing a connection. This location information could be used by the network or service provider - and also by third parties - to build up movement profiles.

If an aggressor is familiar with particular filter characteristics over a mobile phone, he could (although it would be technically effort-intensive) identify individual phone calls by means of these characteristics. These or other attacks require that the customer number (IMSI), mobile transceiver number (IMEI) and subscriber call number (MSISDN) are known.

An insider who, for example, had access to the corporate or private telephone directories in a company would be able to identify the MSISDN call number.

S 1 Safeguard Catalogue Infrastructure

S 1.1 Compliance with relevant DIN standards/VDE specifications

S 1.2 Regulations governing access to distributors

S 1.3 Adapted segmentation of circuits

S 1.4 Lightning protection devices

S 1.5 Galvanic separation of external lines

S 1.6 Compliance with fire-protection regulations and requirements imposed by the local fire department

S 1.7 Hand-held fire extinguishers

S 1.8 Room allocation, with due regard to fire loads

S 1.9 Fire sealing of trays

S 1.10 Use of safety doors

S 1.11 Plans detailing the location of supply lines

S 1.12 Avoidance of references to the location of building parts requiring protection

S 1.13 Layout of building parts requiring protection

S 1.14 Automatic drainage

S 1.15 Closed windows and doors

S 1.16 Selection of a suitable site

S 1.17 Entrance control service

S 1.18 Intruder and fire detection devices

S 1.19 Protection against entering and breaking

S 1.20 Selection of cable types suited in terms of their physical/mechanical properties

S 1.21 Sufficient dimensioning of lines

S 1.22 Physical protection of lines and distributors

S 1.23 Locked doors

S 1.24 Avoidance of water pipes

S 1.25 Overvoltage protection

S 1.26 Emergency circuit-breakers

S 1.27 Air conditioning

S 1.28 Local uninterruptable power supply (ups)

S 1.29 Adequate siting of an IT system

S 1.30	Safeguarding of data media containing data on telecommunications charges
S 1.31	Remote indication of malfunctions
S 1.32	Adequate siting of the consoles, devices with exchangeable data media, and printers
S 1.33	Safe keeping of laptop PCs during mobile use
S 1.34	Safe keeping of laptop PCs during stationary use
S 1.35	Pooled storage of a number of laptop PCs
S 1.36	Safekeeping of data media before and after dispatch
S 1.37	Adequate siting of a fax machine
S 1.38	Suitable siting of a modem
S 1.39	Prevention of transient currents on shielding
S 1.40	Appropriate siting of protective cabinets
S 1.41	Protection against electromagnetic irradiation
S 1.42	Secure siting of Novell Netware servers
S 1.43	Secure siting of ISDN routers
S 1.44	Suitable configuration of a home workplace
S 1.45	Suitable storage of business-related documents and data media
S 1.46	Use of anti-theft devices

S 1.1 Compliance with relevant DIN standards/VDE specifications

Initiation responsibility: Head of Procurement Section; planner

Implementation responsibility: Building supervisor, construction/mounting firm

For nearly all fields of technology, standards and/or regulations are in force, e.g. in Germany: DIN, VDE, VDMA, VdS guidelines. These regulatory schemes help to ensure that technical installations offer sufficient protection for the user and security for operations.

When planning and constructing buildings, remodelling/redesigning, installing technical equipment (e.g. internal supply networks such as telephone or data networks), and during the procurement and operation of equipment, the relevant standards and regulations must be strictly complied with.

Additional controls:

- Are VDE specifications taken account of in tendering procedures, purchase orders or procurement measures?

S 1.2 Regulations governing access to distributors

Initiation responsibility: Head of Site/Bldg Technical Service

Implementation responsibility: Site/Bldg Technical Service

As far as possible, distributors (e.g. for power supply, data and telephone networks) should be accommodated in technical infrastructure rooms (see Chapter 4.3.4). The measures specified for such rooms are to be met.

Access to the distributing frames of *all* supply facilities (power, water, gas, telephone, warning system, pneumatic dispatch, etc.) within the building must be **possible** and **regulated**.

Possible means that

- distributing frames will, during painting work, not be pasted over with paint or wallpaper in such a way that they could be opened only with tools or could not be located;
- distributors must not be blocked by furniture, equipment, pallets, etc.;
- keys are available for locked distributors, and that the locks are in working order.

Regulated means that it has been laid down who may open which distributor. Distributors should be locked and may be opened only by the persons responsible for the respective supply facility. Access can be regulated by various locking devices and appropriate key management schemes (on this point, cf. S 2.14 *Key Management*).

If melting fuses are built into distributors of the supply mains, appropriate spare fuses should be held in store (in the distributor). The documentation of the distributors should be in accordance with the provisions of S 2.19 *Neutral documentation in the distributors*).

All devices installed in the distributor must bear precise and intelligible legends.

Additional controls:

- Are there regulations governing access to distributors?

S 1.3 Adapted segmentation of circuits

Initiation responsibility: Head of Site/Bldg Technical Service

Implementation responsibility: Site/Bldg Technical Service

Experience shows that room allocation and the power ratings, for which an electric installation has been laid out, will, after some time, no longer match the actual situation. Thus, it is essential to review, and, where appropriate, to adjust the electric installation when rooms are to be used for different purposes and when changes and amendments are made to the technical equipment (IT, air-conditioning, lighting). This may be done by re-wiring lines. Otherwise, it may become necessary to re-install feeders, lines, distributors, etc.

Additional controls:

- Are any checks made to see whether the protection and layout of circuits meet the actual requirements?
- When was the last check made?

S 1.4 Lightning protection devices

Initiation responsibility: Head of Site/Bldg Technical Service

Implementation responsibility: Site/Bldg Technical Service

The direct impact of a stroke of lightning on a building (damage to structural elements, roof truss fire, and the like) can be prevented by installing a lightning arrester complying with the DIN/VDE 0185 standard. Besides this outside lightning protection it is mandatory to provide an internal lightning protection as an overvoltage protection. this is required because the lightning arrester does not protect the resources accommodated in the building. This can only be achieved by overvoltage protection (cf. S 1.25 *Overvoltage Protection*), the high costs of which must be justified in relation to the items to be protected.

Example:

As a result of a lightning strike, damage was caused to IT equipment (PC's, server, laser printers) to the amount of DM 20,000 in the southern German branch of a service company. As a result, the building was furnished with external lightning protection without internal lightning protection (overvoltage protection). A second lightning strike led to damage of approximately the same extent despite this external lightning protection.

Additional controls:

- Is external lightning protection actually required?
- Are there any requirements imposed by authorities or insurers?
- Is the lightning protection device regularly checked and maintained?
- Is there sufficient overvoltage protection in the building?

S 1.5 Galvanic separation of external lines

Initiation responsibility: Head of Site/Bldg Technical Service

Implementation responsibility: Site/Bldg Technical Service

Many in-house networks have a direct galvanic connection to external lines. This may be the case with telephone lines, power supply, data networks with remote data transmission connections, but also with gas and water supplies.

Through these mains connections, external voltage and overvoltage can be imported into the building. There are a number of electric, electronic or software-based measures which can protect networks against external factors. However, absolutely reliable protection cannot be guaranteed in all cases. Systematic galvanic separation of outside lines at the entry points into the building is then the last resort. This can be done, for instance, by installing a switch which will connect the line only when required (remote maintenance).

For the protection of inseparable lines (telephone, data, power, gas, water) against overvoltage, consideration should be given to installing an overvoltage protection device (c.f. S 1.25 *Overvoltage protection*).

S 1.6 Compliance with fire-protection regulations and requirements imposed by the local fire department

Initiation responsibility: Head of Site/Bldg Technical Service; site fire protection officer

Implementation responsibility: Site fire protection officer; Site/Bldg Technical Service

The existing fire safety regulations (e.g. DIN 4102) and the requirements imposed by the local fire department with regard to buildings must be strictly complied with. The local fire department may be consulted when fire safety plans are developed. It is advisable to take note of further fire protection instructions such as those contained in the "*Rooms for ADP Systems*" leaflet issued by the *Federation of Property Insurance Companies* (VdS).

S 1.7 Hand-held fire extinguishers

Initiation responsibility: Head of Site/Bldg Technical Service; site fire protection officer

Implementation responsibility: Site/Bldg Technical Service; site fire protection officer

Most fires arise from small sources of fire which initially can be kept easily under control. In offices, in particular, there is plenty of material to feed the fire and it can spread very quickly. Therefore, immediate fire-fighting is to be given a high priority.

Such immediate fire-fighting is only possible if a sufficient number of hand-held fire extinguishers of adequate size (advice to be obtained from the local fire department) are available within the building. The aim must be to place them close to areas and rooms requiring protection, e.g. server room, technical infrastructure room, document archives. Dry-powder extinguishers fit for *class of inflammability* "E" up to 1000 V are suitable for electrically-driven periphery devices. For electronically-controlled, e.g. computers, CO_2 extinguishers (*class of inflammability* "B") are adequate.

Fire extinguishers must be regularly checked and maintained. Staff members should memorise the locations of the nearest fire extinguishers. During fire drills, the staff must be briefed on the use of hand-held fire extinguishers.

Additional controls:

- Have the staff been informed about the locations of hand-held fire extinguishers?
- Is the use of hand-held fire extinguishers being practised?
- Can the hand-held fire extinguishers actually be accessed in case of a fire?
- Are hand-held fire extinguishers regularly inspected and maintained?

S 1.8 Room allocation, with due regard to fire loads

Initiation responsibility: Head of Site/Bldg Technical Service; site fire protection officer

Implementation responsibility: Site/Bldg Technical Service; site fire protection officer

A fire load is produced by any combustible material brought into a building. It is determined by the quantity and the calorific value of such material. Examples of fire loads are IT systems, furniture, carpets, and wall paper. Maximum fire loads, standardised calorific values, and further information are listed in DIN 4102.

When siting IT equipment, data media etc., the existing fire loads in the same room and in adjacent rooms should be reviewed. The data carrier archive, for example, should not be located near or above a paper storage area.

S 1.9 Fire sealing of trays

Initiation responsibility: Head of Site/Bldg Technical Service; site fire protection officer

Implementation responsibility: Site/Bldg Technical Service; site fire protection officer

In buildings with several fire cuts, it can hardly be avoided that trays will lead through fire walls and ceilings. After installation of lines, the breaches must be shielded in keeping with the fire-resistance value of the wall/ceiling. In order to provide for retrofitting, appropriate material (e.g. fire-resistant padding) should be used. The relevant VdS guidelines should be complied with.

Negative approach example:

In a multi-storey office building in Bonn, several networks were run through a common rising line from the basement to the uppermost storey. All ceiling breaches had been made with ample reserves, but had, after wiring and pipe installation, not been closed. In the basement, large quantities of paper and cloth were stored in the vicinity of the front end of the line. The rising line beginning immediately above would, in case of fire, have had the effect of a fireplace (chimney). Smoke and fire would have spread to all floors in no time.

Additional controls:

- Has the person responsible for fire protection been consulted with regard to route planning?
- Have possible alternatives been explored as regards line routing?

S 1.10 Use of safety doors

Initiation responsibility: Head of Site/Bldg Technical Service

Implementation responsibility: Site/Bldg Technical Service

Safety doors, e.g. steel sheet doors, are to be preferred to normal office doors for the following reasons:

- on account of their stability (DIN 18 103), they provide a higher degree of protection against breaking and entering (e.g. for basement and delivery entrances); and
- when designed as self-closing fire doors (FH door T30, DIN 18 082), they delay fire propagation.

In addition to the areas prescribed by the fire authorities (cf. S 1.6 *Compliance with fire-protection regulations and requirements imposed by the local fire department*), use of safety doors is advisable in rooms requiring special protection, such as server room, document archives or data media archives.

Additional controls:

- Has the use of safety doors been checked?
- Are fire and smoke doors actually closed or are they wedged open, for example?

S 1.11 Plans detailing the location of supply lines

Initiation responsibility: Head of Site/Bldg Technical Service

Implementation responsibility: Site/Bldg Technical Service

Precise location plans must be kept for all supplies (power, water, gas, telephone, warning system, pneumatic dispatch, etc.) in the building and on its associated premises, and *all* facts regarding supply lines are to be included:

- precise routing of the line (plotting on dimensioned floor plans and location plans);
- exact technical data (type and dimensions);
- any existing marking;
- use of the lines, naming the network subscribers connected to them;
- danger spots; and
- protective measures that are in place and to be reviewed.

It must be possible, by consulting these plans, to get a picture of the situation in a simple and quick way. Only then will it be possible to minimise the risk of lines being inadvertently damaged during repair/maintenance work. It will then be possible to locate a defect more quickly and to eliminate it.

It must be ensured that all work on lines is documented promptly and completely. The plans are to be kept separately, and provisions regarding access to them must be laid down as they contain sensitive data.

Additional controls:

- Who is responsible for the plans?
- Are the plans being updated?
- Are the plans stored safely and are they only accessible to authorised parties?
- Which plans are already in place?

S 1.12 Avoidance of references to the location of building parts requiring protection

Initiation responsibility: Head of Site/Bldg Technical Service

Implementation responsibility: Site/Bldg Technical Service

Building parts requiring protection are, for instance, the server room, computer centre, data media archives, air conditioning centre, distributing frames for power supply, switching and wiring/patching rooms, spare parts store.

Such areas should not have any markings regarding their use. Doorplates - such as *COMPUTER CENTRE* or *ADP ARCHIVES* - give hints to a potential offender having access to the building so that he can prepare his actions more specifically and thus with a greater chance of success..

If it is not possible to avoid the accommodation of IT systems in rooms or parts of the building which can easily be seen from outside (cf. also S 1.13 *Layout of building parts requiring protection*),adequate measures will have to be taken to prevent observation from outside or to arrange the room so that its use is not apparent to outsiders. Attention must be paid to ensuring that, for instance, not just *one* window of an entire storey is shielded against general view.

Additional controls:

- Which information on the location of building parts can be seen from outside?
- What location-related indications are provided in a building?

S 1.13 Layout of building parts requiring protection

Initiation responsibility: Project planner; agency/company management

Implementation responsibility: Construction supervisor; Head of Site/Bldg Technical Service

Rooms or building parts requiring protection should never be in exposed or particularly endangered areas:

- basement rooms are exposed to water damage;
- first-floor rooms - facing public traffic zones - are exposed to attacks, vandalism and force majeure (traffic accidents in the vicinity of the building);
- first-floor rooms of buildings with courtyards that cannot be easily observed are exposed to breaking and entering and to sabotage;
- rooms immediately below flat roofs are exposed to rainwater.

As a rule of thumb, it may be assumed that rooms or areas requiring protection will best be located in the centre of a building rather than in its outer parts.

The optimum approach is to include these aspects already in the project planning of a new building or in the room allocation plans for moving into an existing building. Where buildings are already in use, the pertinent utilisation scheme will often involve moves within the given buildings. Alternatively, consequent use should be made of the opportunities offered by changes which are to be made anyhow to room allocation.

Additional controls:

- Which rooms requiring protection are in an exposed location?

S 1.14 Automatic drainage

Initiation responsibility: Project planner; agency/company management

Implementation responsibility: Construction supervisor; Head of Site/Bldg Technical Service

All areas where water can gather and accumulate, or where running water or stagnant water is discovered belatedly or not at all, and where water can cause damage, should be provided with automatic drainage and possibly with water detectors. Such areas include:

- basement,
- free spaces under false (raised) floors,
- light shafts,
- heating system.

In case of passive drainage, i.e. through floor drains leading directly into the sewerage system of the building, backflow valves are indispensable. Without such flaps, this type of drain becomes a water inlet whenever the sewage system is overloaded. After very heavy rainfall, it will, in the majority of cases, be through this system that water leaks into the basement. The operation of the backflow valves must be examined at regular intervals.

If passive drainage is not possible because the level of the sewage system is too high or because the normal hydraulic pressure is insufficient, use may be made of pumps which are automatically activated by float switches or water sensors. When such technology is used, the following points must be particularly observed:

- The pump throughput must be of sufficient size.
- The hydraulic main of the pump must be provided with a backflow valve.
- Provisions must be made against the pump being blocked by entrained objects (suction filter etc.).
- Start-up of the pump should be automatically indicated (e.g. to the janitor of the Site/Building Technical Service).
- The functioning of the pump and the switches must be regularly tested.
- The hydraulic main of the pump must not be connected to a sewage pipe run in the immediate vicinity. If such a pipe had a leak, the water would only be pumped in a circle.

Additional controls:

- Have the rooms exposed to water risks been provided with automatic drainage?

S 1.15 Closed windows and doors

Initiation responsibility: Head of Site/Bldg Technical Service

Implementation responsibility: Site/Bldg Technical Service, staff members

Windows and outward leading doors (balconies, patios) should be closed whenever a room is unoccupied. In the basement and on the first floor and, depending on the cladding/type of facade, in upper storeys as well, they offer burglars and intruders an ideal opportunity even during working hours;

During regular working hours and a definite short absence of staff, mandatory regulations for offices need not be enforced.

Additional controls:

- Have instructions to close windows and outside doors been issued?
- Are regular checks made to see whether windows and doors have been closed by occupants after leaving the rooms?

S 1.16 Selection of a suitable site

Initiation responsibility: Agency/company management

Implementation responsibility: Site planner

When planning the site where a building is to be rented or constructed, it is recommended to consider the environmental factors with an influence on IT security in addition to the normal aspects such as space requirements and cost:

- Due to structural weaknesses, IT systems may be affected by shock/vibration stemming from close-by traffic routes (road traffic, railway, underground railway).
- Buildings located directly on primary routes (railway, motorway, trunk road) can be damaged as a result of traffic accidents.
- Closeness to optimum traffic routes, and thus escape routes, can facilitate the imposition of attacks.
- In the vicinity of transmitter installations, IT installations can be subject to disruption.
- In the vicinity of water bodies and in low plains, flooding is a probability.
- In the vicinity of power plants or factories, accidents or operating troubles (explosion, release of hazardous material) can lead to impaired availability of the building (e.g. by evacuation or the cordoning-off of large areas).

Additional controls:

- Are there any hazards caused by the location?
- How are such hazards counteracted?

S 1.17 Entrance control service

Initiation responsibility: Head of General Services Section

Implementation responsibility: Internal Services Division

Establishment of an entrance control service has far-reaching positive effects against a number of threats. However, this presupposes that some fundamental principles are observed in the performance of entrance control.

- Gatekeepers observe and/or monitor all movements of persons at the entrance.
- Unknown persons (*"even the new boss"*) will have to prove their identity to the entrance control staff.
- Before allowing a visitor to enter, the gatekeeper will check with the person to be visited.
- A visitor will be escorted to the person to be visited or will be met by the latter at the entrance.
- Gatekeepers must know the staff members. In case of termination of employment, gatekeepers must also be informed of the date from which this member of staff is to be denied access.
- A visitors' log may be kept to document access. The issue of visitor's passes is to be considered.

The working conditions for entrance control staff are to be designed with due regard to the tasks to be performed. The description of tasks must precisely define the tasks of entrance control staff (gatekeepers) in support of other protective measures (e.g. building security after business hours, activation of the alarm system, checking of outside doors and windows).

S 1.18 Intruder and fire detection devices

Initiation responsibility: Head of Site/Bldg Technical Service; site fire protection officer; IT Security Management

Implementation responsibility: Site/Bldg Technical Service

If an intruder or fire detection device is installed and if it can be expanded at reasonable cost, it should be considered whether, as a minimum, the IT core areas (server rooms, data media archives, technical infrastructure rooms, etc.) could be included in the monitoring provided by this device. Thus it will be possible to detect threats such as fire, burglary or theft in good time and to initiate countermeasures. In order to maintain the desired level of protection, the intruder/fire detection device should be maintained and tested on a regular basis.

If an intruder/fire detection device is not available or if an existing device cannot be used, local detection devices should be considered as a minimum. These work on a completely independent basis without being connected to any central facility. Alert is given at the site or by means of a simple two-wire line (possibly telephone line) located elsewhere.

Additional controls:

- Is the intruder/fire detection device regularly serviced and tested?
- Have the persons concerned been advised of the steps to be taken in case of alert?

S 1.19 Protection against entering and breaking

Initiation responsibility: Head of Site/Bldg Technical Service, IT Security Management

Implementation responsibility: Site/Bldg Technical Service

The current measures for protection against breaking and entering should be adapted to the local situation. This includes:

- protecting doors or windows through which outsiders might easily enter by means of safeguarded rolling shutters;
- special locks, additional locks and bars;
- safeguarding of basement light shafts;
- locking of unused side-entrances;
- burglar-proof emergency exits (if permitted by the local building authorities);
- locking of goods lifts and passenger lifts outside office hours.

Recommendations in this regard are provided by the local advice office of the criminal investigation department.

Regulations must be issued to the staff to inform them about which anti-burglary measures are to be observed.

Additional controls:

- Are checks carried out as to whether protective measures against burglary are being observed?

S 1.20 Selection of cable types suited in terms of their physical/mechanical properties

Initiation responsibility: Network planner; Head of Site/Bldg Technical Service; IT Security Management

Implementation responsibility: Site/Bldg Technical Service

When selecting cables, account is to be taken of technical requirements as regards transmission, and, in addition, attention must be paid to the environment in which the cables are to be run. For most cabling requirements, cables with the appropriate properties are available. The most important of these are listed here:

- indoor cables or outdoor cables;
- non-hosing cables for damp or wet areas;
- strain-relieved cables for overhead lines and extreme gradients;
- function-preserving cables in areas exposed to fire hazards;
- shielded cables for areas with strong electrical and inductive interference fields;
- armoured cables for those instances where sufficient mechanical protection cannot be ensured in any other way, e.g. in case of provisional layout on floors and walls.

Additional controls:

- Regarding the selection of cables; has the O&S officer (person responsible for operation and maintenance) been consulted with regard to known or anticipated adverse factors in the operational environment?
- Have possible alternatives regarding cable routing been considered?

S 1.21 Sufficient dimensioning of lines

Initiation responsibility: Network planner; Head of Site/Bldg Technical Service; Head of IT Section

Implementation responsibility: Site/Bldg Technical Service

Sufficient dimensions must be specified for cable runs (e.g. floor ducts, window-sill ducts, raceways, pipe ducts in outside areas) so that, there will be sufficient scope for required extensions to the network. However to prevent cross-talk (mutual interference of cables), it may be advisable to provide for minimum spacing of cables.

If, for various reasons, it is not possible to provide routes with sufficient reserves right away, attention should at least be given to providing for any required extensions to be realised as regards routing. With regard to the design of wall breaches and ceiling breaches, this will obviate subsequent measures entailing high levels of noise, pollution and costs.

This measure can be replaced by the selection of other types of cables (S 2.20 *Monitoring of existing lines* and S 5.3 *Selection of cables types suited in terms of communication technology*). As compared to many small cables, use of a small number of multicore cables can save space. Cross-talk can be prevented by using shielded cables or fibre optics.

Additional controls:

- Has consideration been given to saving space and to preventing cross-talk by selecting other types of cables?

S 1.22 Physical protection of lines and distributors

Initiation responsibility: Network planner; Head of Site/Bldg Technical Service; Head of IT Section

Implementation responsibility: Site/Bldg Technical Service

In rooms visited by the general public or in building areas which can not easily be overseen, it may be expedient to protect lines and distributors. This can be accomplished in different ways:

- concealed wiring of lines;
- steel-armoured conduits for lines;
- running lines in mechanically solid and lockable ducts;
- locking of distributors; and
- if required, additional electrical monitoring of distributors and ducts.

In case of locking, arrangements must be made which lay down the access rights, the distribution of keys and the access modalities (*what must the authorised person possibly do before having access to lines?*).

Additional controls:

- Have the number of places providing access to the cable been minimised?
- Has the length of routes requiring protection been kept as short as possible?
- Are access rights granted restrictively? Is account taken of staff turnover and substitution?
- Are access rights being regularly reviewed for authorisation/necessity?

S 1.23 Locked doors

Initiation responsibility: Head of Site/Bldg Technical Service, Head of IT Section

Implementation responsibility: Site/Bldg Technical Service, staff members

The doors of unoccupied rooms should be locked. This will prevent unauthorised persons from obtaining access to documents and IT equipment in the given room.

In some cases, e.g. open-plan offices, it is not possible to lock the office. Then, as an alternative, each staff member should lock away his/her documents (*"clear-desk policy"*) and secure his/her personal work area: desk, cabinet and PC (lock for floppy disk drive, keyboard lock), telephone.

If the computer is in operation, it is not necessary to lock the doors provided that a safeguarding feature has been installed which allows continued use of the computer only if a password is entered (password-assisted screen saver), the display has been cleared and booting of the computer can be effected only with a password.

When the computer is switched off, the office need not be locked provided that the booting of the computer can be effected only with a password.

If doors are left unlocked in the above cases, it must be ensured that all other objects such as sensitive documents or data media are kept out of general view.

Additional controls:

- Are sporadic checks made of whether offices are locked when they are left?
- Are staff members instructed to lock their offices during their absence?

S 1.24 Avoidance of water pipes

Initiation responsibility: Head of Site/Bldg Technical Service, Head of IT Section

Implementation responsibility: Head of Site/Bldg Technical Service; administrator

In rooms or areas housing IT facilities with central functions (e.g. server), water pipes of any type should be avoided. Where absolutely necessary, the only water-carrying lines installed should be coolant pipes, fire-fighting water pipes and heating pipes. Supply lines to radiators should be furnished with gate valves - where possible, outside the room/area. These valves must be closed outside the heating period.

If water pipes cannot be avoided, minimum protection can be provided by a water sump or drip pan installed under the pipeline, the drain of which leads outside the room. For this purpose, it is opportune to use the corridor as then any pipe defects can be detected at an earlier time.

Optionally, water detectors with automatic solenoid valves can be installed. Such solenoid valves should be installed outside the room/area and must be closed if de-energised.

As an additional or alternative measure, automatic drainage (S 1.14 *Automatic drainage*) may be advisable.

Additional controls:

- Is the tightness of any existing water pipes being checked on a regular basis (visual inspection)?

S 1.25 Overvoltage protection

Initiation responsibility: Head of Site/Bldg Technical Service; Head of IT Section; IT Security Management

Implementation responsibility: Head of Site/Bldg Technical Service; administrator

Depending on the quality and advancement of the external power supply network and the in-house power network, overvoltage peaks can, depending on the environment (other power consumers) and on the geographical location, be caused in the supply mains by induction or lightning. As a rule, overvoltage due to lightning has quite a destructive potential, whilst that of overvoltage due to other causes is only minor. However, all types of overvoltage can destroy IT systems.

A comprehensive overvoltage protection policy covers three stages:

- elementary protection in the building feeder;
- medium protection in storey distributors; and
- fine protection provided at the respective sockets and the plug-in connections of all other lines.

The design of elementary protection depends on the existence of external lightning arrester. The protective effect of every stage builds on the preceding stage. If one stage is left out, overvoltage protection will, in its entirety, become nearly ineffective.

If overvoltage protection cannot be ensured throughout the building, it will at least be necessary to establish an adequate protective perimeter around important IT facilities (server, etc.). In order to minimise potential damage, networks to which multiple devices are connected can, by means of optocouplers or surge arresters, be divided into small sectors protected from each other.

Irrespective of the extent and development of overvoltage protection, attention must be given to two basic requirements:

- The line between the fine-protection feature and the devices to be protected should not be longer than 20 metres. If that length is exceeded, another fine-protection device must be interposed. If a device is provided with fine protection at the entry point, the 20 m limitation does not apply.
- If overvoltage protection is to be effective, comprehensive potential equalisation is required for all electric resources covered by overvoltage protection!

Additional controls:

- Are lightning/overvoltage protection devices being checked and, in the appropriate cases, replaced, both periodically and after known actual incidents?
- Has potential equalisation been ensured throughout?
- In case of retrofitting, is consideration given to the inclusion of potential equalisation?

S 1.26 Emergency circuit-breakers

Initiation responsibility: Head of Site/Bldg Technical Service, Head of IT Section

Implementation responsibility: Site/Bldg Technical Service

Installation of emergency circuit-breakers is advisable in rooms where electrical devices are operated in such a way that, for instance, increased fire hazards exist due to the waste heat of such devices, to compact installation of equipment, or to the existence of additional fire loads. As staff is required to activate the emergency circuit-breaker, it is only worth considering in areas in which people are present all, or at least most, of the time. In areas which are only sporadically occupied, if at all, an emergency shutdown through a device for the early detection of a fire is considerably more effective.

Activation of an emergency circuit-breaker will eliminate a major source of energy for any fire, and as a result, minor fires can go out. In any case, the risk posed by voltages will be eliminated during fire-fighting operations.

A point to be borne in mind is that local systems for uninterruptable power supply (ups) will, after the external power supply has been switched off, automatically provide for power supply and that the respective devices will remain live. Therefore, when installing an emergency circuit-breaker, it must be ensured that also the UPS is switched off rather than being merely separated from the external power supply.

The emergency circuit-breaker should be installed either in the room - next to the entrance door - (possibly with a note, on the outside of the door, indicating the location of the switch) or outside the room, next to its door. In this context, however, it must be considered that such an emergency circuit-breaker may, even in the absence of a threat, be activated inadvertently or intentionally.

Negative approach example:

In the server room of a medium sized agency, about ten servers, five laser printers and other devices were installed. In terms of burglary protection, the room was provided with appropriate walls, windows and doors. An emergency circuit-breaker had not been provided. There were only two points from which it was possible to disconnect this room from the power supply: the building main distribution frame in the basement, or the distributing frame of the room. However, the latter was located on the wall opposite the entrance door and thus would have been almost inaccessible in case of fire.

S 1.27 Air conditioning

Initiation responsibility: Head of Site/Bldg Technical Service, Head of IT Section

Implementation responsibility: Site/Bldg Technical Service

In order to ensure the admissible range of the warmed up temperature of IT devices, the normal air exchange and heat transfer in a room sometimes does not suffice so that the installation of air conditioning is required. Its function is, through cooling, to keep the room temperature under the limit preset by the IT systems.

If, in addition, atmospheric humidity requirements exist, these can also be met by the air-conditioner through humidification and dehumidification. For this purpose, however, the air-conditioner will have to be connected to a water supply line. Account must be taken of S 1.24 *Avoidance of Water Pipes*.

In order to preserve the protective effect, provisions must be made for regular maintenance of the air-conditioning plant.

Additional controls:

- In which rooms used for IT purposes can increases in temperature occur?
- Are the air-conditioners in use being maintained on a regular basis?
- What are the maximum/minimum permissible temperature and humidity for the IT system?

S 1.28 Local uninterruptable power supply (ups)

Initiation responsibility: Head of Site/Bldg Technical Service; Head of IT Section; IT Security Management

Implementation responsibility: Head of Site/Bldg Technical Service; administrator

With an uninterruptable power supply (UPS), it is possible to bridge a short-term power failure or maintain the power supply long enough to allow an orderly shut-down of the connected computers. This is particularly expedient

- when large quantities of data are stored temporarily in the computer (e.g. cache memory in the network server) before their transfer to non-volatile storage;
- if, in case of power failure, large quantities of data would be lost and their subsequent re-entry would be required;
- if the stability of power supply is not sufficiently ensured.

Two types of UPS should be distinguished:

- Offline UPS: The connected power consumers are normally fed directly from the supply mains. It is only in the case of failure of the latter that the UPS will automatically switch in and take over the supply function.
- Online UPS: The UPS is permanently switched between the mains and the power consumers. The entire power supply is always provided through the UPS.

In addition to tiding over a complete breakdown of power supply and undervoltage situations, both types of UPS can also serve to smooth overvoltage. In this case, too, the 20 m limit specified in S 1.25 *Overvoltage Protection* applies with regard to overvoltage protection.

If IT equipment in a building with TN-S network (see S 1.39 *Prevention of transient current on shielding*) is supplied by a local UPS, the following should be observed: In order to maintain the protective effect of the TN-S network against transient current on shielding of data lines, the PE conductor of the power line must not be connected to the PE conductor of the output side of the UPS.

When dimensioning a UPS system, a normal by-pass time of about 10 to 15 minutes can, as a rule, be assumed. In most cases, a power failure will be remedied within 5 to 10 minutes. This leaves about 5 minutes for the orderly shut-down of the connected IT systems if the power failure should persist for some time. Most modern UPS equipment offers computer interfaces capable of initiating a timely automatic shut-down after a predefined time, in accordance with the time requirements of the IT systems and the capacity of the UPS.

For specific applications (e.g. PBX), the necessary by-pass time may be several hours.

In order to preserve the protective effect, provisions must be made for regular maintenance of the UPS system.

If it is possible to obtain uninterruptable power supply from other sources (e.g. by connection to a central UPS system), this constitutes an alternative to a local UPS system.

Additional controls:

- Are the required intervals for UPS maintenance being observed?
- Have provisions been made for automatic shut-down?
- Is the effectiveness of the UPS system being tested on a regular basis?
- Have any changes taken place with the result that the assigned capacity of the UPS system is no longer sufficient?

S 1.29 Adequate siting of an IT system

Initiation responsibility: Head of Site/Bldg Technical Service, Head of IT Section

Implementation responsibility: Site/Bldg Technical Service; IT users

When installing an IT system, attention should be paid to various requirements which enhance the lifetime and reliability of the technical equipment and take account of ergonomics. Some of them are listed here by way of example:

- an IT system should not be sited in the immediate vicinity of heaters so as to avoid overheating;
- an IT system should not be exposed to direct solar radiation;
- dust and soiling should be avoided since the mechanical components (floppy disk drives, mechanical mouse, fixed disks) might be impaired;
- direct incidence of light on the monitor should be avoided for ergonomic reasons;
- location near to a window or door will increase the risk of observation from outside.

Further advice is contained in the recommendations issued by the Industrial Injuries Insurance Institutes.

Additional controls:

- Have failures due to the location occurred in the past?
- Do the users of IT systems complain about inadequate ergonomic conditions?

S 1.30 Safeguarding of data media containing data on telecommunications charges

Initiation responsibility: PBX officer; departmental data privacy officer

Implementation responsibility: Administrators

During the operation of PBX facilities, call data are generated. This contains information on:

- time and date of a call;
- calling number and called number; and
- duration of the call.

Call data are personal data within the meaning of the relevant federal and state protection laws. This implies that also under the IT baseline protection measures proposed hereafter, a separate review must in any case be made with regard to the requirements of data protection laws (e.g. the Annex to Section 9 of the *Federal Data Protection Act* - BDSG).

Such data can be stored both on the fixed disk of the PBX itself and on an external customer billing computer. In many cases, both variants will be combined. Where possible, computers must be protected in such a way that only authorised persons can access the call data. To achieve this, the billing computer must be installed in a specially protected room (cf. Chapter 4.3.2 - *Server Room*). For systems in which call data are stored, safeguards S 1.23 *Locked doors,* S 2.5 *Division of responsibilities and separation of functions,* S 2.6 *Granting of site access authorisations,* S 2.7 *Granting of system/network access authorisations,* S 2.8 *Granting of (application/data) access rights,* S 2.13 *Disposal of resources requiring protection,* and S 2.17 *Entry regulations and controls* must be implemented as well.

Additional controls:

- Who has access to call data?
- How is access protection ensured?
- Do only users with a justified interest have access rights?
- Where are the backup copies kept, and who has access to them?
- How are data media disposed?
- For how long will stored data be kept?

S 1.31 Remote indication of malfunctions

Initiation responsibility: Head of IT Section: PBX officer; IT Security Management

Implementation responsibility: Administrators

IT equipment and support devices requiring no, or only infrequent, intervention by a human operator are often located in closed and locked rooms (e.g. server room). As a result, malfunctions which, during their initial stage, do not yet produce an effect and can be easily remedied will be detected too late, mostly on account of their impact on IT systems. Fire, malfunctions of a UPS system or failure of an air-conditioner are some examples of such "insidious threats".

Remote detection provides for earlier discovery of such malfunctions. Nowadays, many devices on which reliance has to be placed without the possibility for constantly testing or observing them, are provided with remote indication of malfunctions. The respective technical possibilities range from simple contacts through which a warning lamp can be switched on to computer interfaces with the pertinent software package for current operating systems. Often it is even possible through such interfaces to ascertain the current operational status of the connected devices and thus to take timely action to counter any failures.

Additional controls:

- Do the persons alerted by remote indication know which measures to take?

S 1.32 Adequate siting of the consoles, devices with exchangeable data media, and printers

Initiation responsibility: Head of IT Section: PBX officer; IT Security Management

Implementation responsibility: Administrators

This measure serves to protect the interfaces of an IT system against external factors in order to meet the security requirements, also in these cases, as regards stored and processed data, which are ensured within the IT system by the internal security mechanisms and by measures taken in the hardware/software field. Protection against unauthorised reading of information, which within the system is ensured by access control mechanisms, must, at these interfaces, be provided primarily by infrastructure or organisational measures.

In order to prevent manipulation of the console, of devices with exchangeable data media and of printers, these must be installed in locations which can be accessed by authorised persons only.

In particular, the following provisions apply:

- In the case of UNIX systems, unauthorised persons must not be given access to the console since they might boot the UNIX computer in single-user mode or activate the hardware monitor and thus acquire system administrator rights.
- It must be ensured that devices for exchangeable data media - such as streamers, floppy disk drives, removable disks - do not allow illicit import or reading out of files.
- Only authorised persons may have access to rooms with printers/print-outs. This can be achieved, for instance, by locating printers in a locked room and by having print-outs distributed by a trustworthy person to pigeon-holes which can be accessed only by the intended recipients. Therefore, the names of the recipients must be indicated on print-outs. This can be done automatically by means of print programs.

This measure is complemented by the following:

S 4.18 Administrative and technical means to control access to the system-monitor and single-user mode

S 4.21 Preventing unauthorised acquisition of administrator rights

Additional controls:

- Are the console, devices for exchangeable data media, and print-outs protected against unauthorised access?

S 1.33 Safe keeping of laptop PCs during mobile use

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

Since the user, in most instances, has no direct influence on the general external conditions during mobile use of a PC, he must try to ensure secure storage of the laptop PC also outside the house. In this respect, only a few indications can be given which are to be observed in mobile use:

- The time during which the computer is left unattended should be as minimal as possible.
- If a laptop PC is kept in a car, the computer should not be visible from the outside. Alternatives are to cover the computer or to lock it up in the luggage-boot. A laptop has a high material value which attracts potential thieves, especially since portable PCs can be easily sold.
- If a laptop PC is used in offices of other persons/institutions, the respective room must be locked even during short absences. If the room is left for a longer period of time, the laptop should, in addition, be switched off in order to prevent illicit use by means of the boot password.
- In hotel rooms, laptops should be kept out of general view. Locking the computer up in a cabinet will discourage casual thieves.
- Some computers of more recent date additionally offer the choice of the chaining up of the device. Theft could then be effected only with the use of tools.

Additional controls:

- Are laptop users instructed as regards safe keeping of their computers?

S 1.34 Safe keeping of laptop PCs during stationary use

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

In case of temporary stationary use of a laptop in an office, the measures described in Part I, Chapter 4.3.1 Office, must be observed. However, since a laptop is particularly easy to transport and to conceal, the computer should, when not in use, be locked up in a cabinet.

Additional controls:

- How are laptop PCs stored in offices?

S 1.35 Pooled storage of a number of laptop PCs

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

If a large number of laptops are in (mobile) use within an agency/a company or if their users change frequently, it may be advisable to keep those laptops which are temporarily not used in a pool. The room used for this purpose should meet the requirements specified for the *Technical Infrastructure Room* described in Chapter 4.3.4.

In addition, power supply must be ensured for portable PCs so that the batteries of these computers will allow their immediate use. Moreover, the retrieval and issue of laptops must be documented.

Additional controls:

- Who has access to the site for pooled storage of laptop PCs?
- Are the issue and retrieval of such PCs being documented?

S 1.36 Safekeeping of data media before and after dispatch

Initiation responsibility: IT Security Management

Implementation responsibility: IT users, Mailroom

Adequate access control must be ensured prior to the sending of data media for the period between saving and transport of data on a storage medium. Once the data has been saved, it must be kept locked in appropriate containers (cabinet, safe) until transport. The department responsible for transport and delivery (e.g. mailroom) must be instructed on proper and reliable safekeeping and handling of the data carriers.

Additional controls:

- Have employees been instructed to keep data carriers destined for transport in restricted-access areas?

S 1.37 Adequate siting of a fax machine

Initiation responsibility: Head of Site/Bldg Technical Service, IT Security Management

Implementation responsibility: Site/Bldg Technical Service, IT users, Fax Officer

Fax machines should be installed in areas which are not freely accessible. It is advisable to monitor entry into this area and usage of the fax machine.

In this respect, it is expedient to install fax machines in rooms which are constantly occupied (e.g. office, reception room, mailroom). Outside working hours or during the absence of the authorised user, the fax machine should be locked (within the room or inside a cabinet). Here, it is important to prevent incoming fax messages from being viewed or removed by unauthorised persons (c.f. S 2.48 *Designating authorised fax operators*).

Additional controls:

- Who has unrestricted access to the fax machine?
- During which periods is unrestricted access possible (lunch break, shift change, etc.)?
- How is the access to the fax machine controlled?
- How is the device protected outside working hours?

S 1.38 Suitable siting of a modem

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT users, Administrator

To prevent misuse of modems, it must be ensured that only authorised persons have physical access to this equipment. Misuse in this case implies, firstly, unauthorised data transmissions possibly resulting in costs, virus infiltration or the transfer of confidential information outside, and secondly, unauthorised alteration or viewing of the modem configuration possibly resulting in security weaknesses.

To control physical access to an external or PCMCIA modem, it must be ensured, for example, that modems operated continuously are kept inside locked rooms and modems operated temporarily are kept safely inside cabinets when not in use. The provisions in Chapter 4.3.1 Office are to be observed here.

Due to its integration in an IT system, an internal modem has a higher intrinsic degree of physical protection. In this case, it is sufficient to observe the measures in Chapter 4.3.1 *Office* or 4.3.2 *Server Room*.

If access to the internal network is created via a modem or a modem pool, Chapter 7.3 *Firewall* should be consulted. Access to the internal network should not be created via modems whilst bypassing an existing firewall.

If more external accesses to a network protected by a firewall are to be created with a modem pool, this must be set up on the insecure side of the firewall (c.f. S 2.77 *Correct Configuration of Other Components*). The modem pool shouls be set up with the relevant server in a security server room. The safeguards contained in Chapter 4.3.2 Server Room should be observed.

S 1.39 Prevention of transient currents on shielding

Initiation responsibility: Head of IT section

Implementation responsibility: Site/Bldg Technical Service; physical network operator

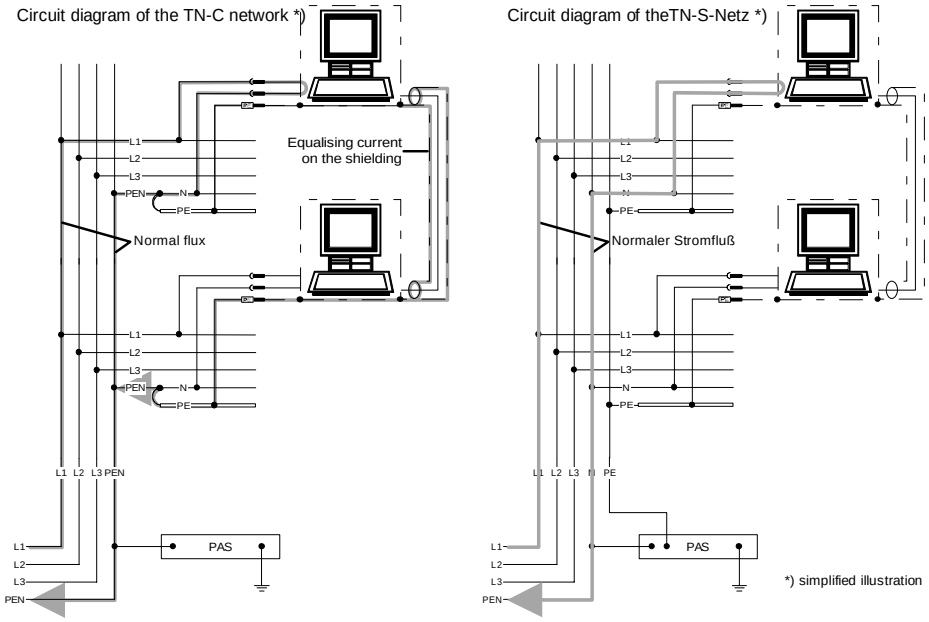
There are various ways of preventing transient currents on the shielding of data lines in buildings:

Transient currents can be avoided in the TN-C network by only linking IT appliances via shielded data lines which are connected to a common electrical distribution system. This must be checked each time the data network is extended.

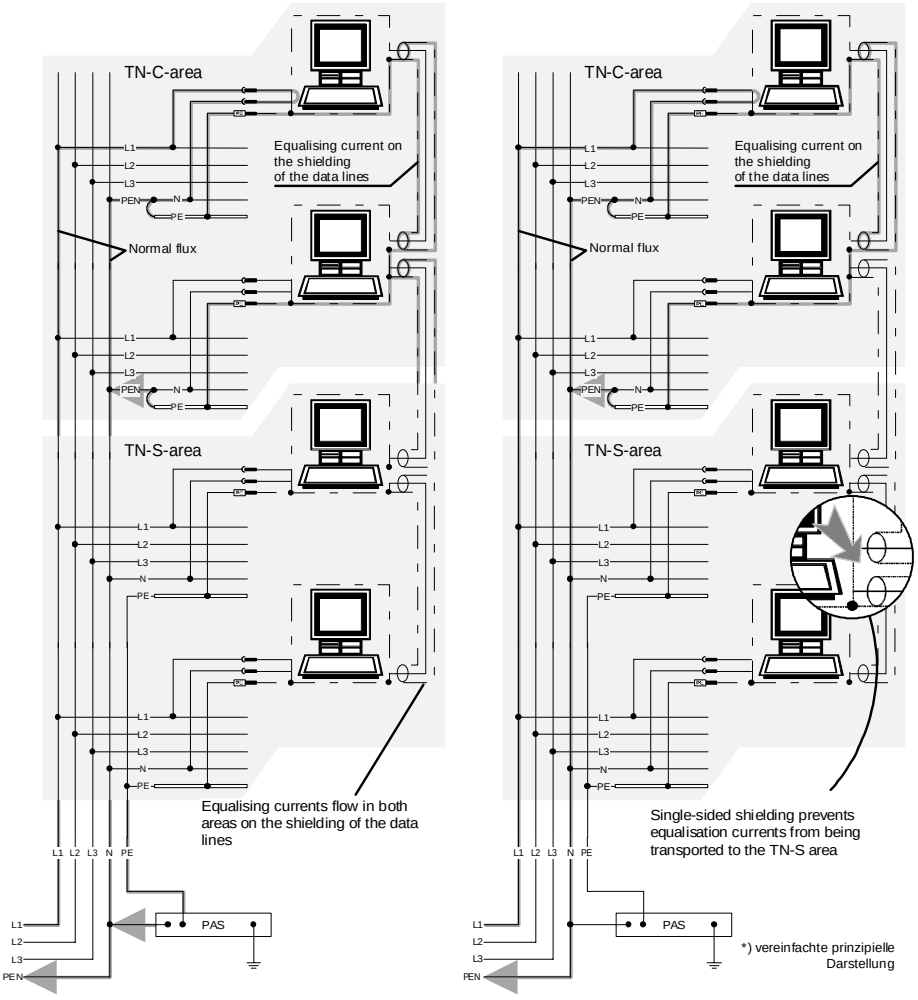
In the event that this is not possible, transient currents can be avoided by only providing shielding on one side of the data line. In case of alteration to the data network, only suitable cables should be used (cables with shielding only on one side).

The optimum and safest method is to design the power distribution network in the entire building as a TN-S network. Here, the PE line and the N line are fed separately after the potential equalisation bar (PEB). Individual safeguards on IT equipment are then generally not necessary. Chapter S 1.28 *Local uninterruptable power supply* should be observed, however, regarding the creation of a new TN-S network for the connected equipment.

The following diagrams show the formation of transient currents on shielding and the possible safeguards:



Circuit diagram of the TN-CS network *)



Additional controls:

- Which type of network is in place?
- How are the protection conditions (a common distribution system or only single-sided shielding) checked and by whom?
- Are alterations to the data network co-ordinated with the site/building technical service?

S 1.40 Appropriate siting of protective cabinets

Initiation responsibility: IT Security Management

Implementation responsibility: Site administration

Due to the generally high weight of protective cabinets, the load-bearing capacity of the floor must be tested before installation at the place of installation.

Protective cabinets which could be carried off relatively easily due to their small size should be permanently fixed to the wall or the floor.

Any existing manufacturer's instructions on suitable installation (e.g. unobstructed ventilation openings, cable routing) should be taken into account.

Additional controls:

- How can the theft of a protective cabinet be prevented?

S 1.41 Protection against electromagnetic irradiation

Initiation responsibility: IT Security Management

Implementation responsibility: Procurer, Company Engineering Department

If IT equipment is housed in a protective cabinet, electromagnetic radiation can be produced by adjacent devices which impairs the functioning of the equipment (particularly in industrial production areas). By retrofitting filters and door seals, irradiation inside the protective cabinet can be reduced. At the same time these safeguards also prevent the spread of compromising emissions from the equipment inside the cabinet.

Additional controls:

- Is there a danger of electromagnetic irradiation?

S 1.42 Secure siting of Novell Netware servers

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

In order to protect the Novell Netware servers against manipulation, it is absolutely necessary to site the server in a secure area. This can either be a server room (refer to Chapter 4.3.2 Server room) or a server cabinet, if a separate server room is not available (refer to Chapter 4.4 Protective cabinets). Unsupervised access to the server should not be available to unauthorised persons. Furthermore, the diskette drives of Novell Netware servers have to be locked with supplementary locks.

With the help of *SYS:SYSTEM\MONITOR.NLM* direct data input into the server console should be prevented with a password. The command *LOAD MONITOR.NLM -L* should already have been added to the file *SYS:SYSTEM\AUTOEXEC.NCF*. The result of this is that whenever the server is started, it protects the server console with a password. However, it must be taken into account that the password of the bindery-user *SUPERVISOR* is needed to unlock the server. When the Netware 4.x server is installed, this password is identical to that of the user who has installed the server in the NDS. As a rule, this is the NDS user *ADMIN*. However, if the password for the user *ADMIN* is changed regularly, this does not mean that the password of the bindery-user *SUPERVISOR* is changed on the NDS servers. This can cause problems, as the *SUPERVISOR* passwords, which are different for each NDS server, are often left unchanged and may with time be forgotten.

Another important command with which the server console can be secured is *SECURE CONSOLE*. This command deactivates the server's debugger. Without this command, for example, it would be possible to reach the debugger, even though the server's console is protected with a password. Other important functions of the command S*ECURE CONSOLE* are:

- Netware Loadable Modules (NLM) can only be loaded from *SYS:SYSTEM* and possibly from other available search paths, whereby the DOS search paths are removed automatically,
- some SET parameters can no longer be changed,
- the time and date can no longer be set on the server console and
- the server's system debugger can no longer be reached.

Additional controls:

- Is authorised access to the Novell Netware server ensured in the case of a substitute supervisor?
- Is every Novell Netware server located in a server room or server cabinet?

S 1.43 Secure siting of ISDN routers

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

To ensure that ISDN routers cannot be manipulated during their operation, it is absolutely necessary to install them in a secure environment. This can either be a server room (refer to Chapter 4.3.2 Server room) or a server cabinet, if a separate server room is not available (refer to Chapter 4.4 Protective cabinets). Unauthorised persons must not be allowed unsupervised access to ISDN routers.

Additional controls:

- Has it been ensured that ISDN routers can only be accessed by authorised persons, also in cases where regular employees have been substituted temporarily?
- Is every ISDN router installed in a server room or server cabinet?

S 1.44 Suitable configuration of a home workplace

Initiation responsibility: Head of Site/Bldg Technical Service, personnel committee/works council, superiors

Implementation responsibility: Site/Bldg Technical Service, staff members

It is advisable to assign a complete room for use as a workplace at home. Such a workplace should at least be separated from the rest of the premises by means of a door.

The workplace should be configured in compliance with ergonomic, security and health requirements including the following:-

These include:

- Sufficient space for furniture and the desktop monitor
- Adjustable room temperature and adequate ventilation
- Sufficient sound-proofing
- Sufficient daylight and electrical illumination
- Visual shielding of the monitor if it could be observed through a window
- Avoidance of glare and reflections at the workstation
- Telephone and electrical connections

IT equipment intended for professional purposes should be provided by the employer, and the use of these services for private purposes should be prevented by official instructions, for example.

Additional controls:

- Are employees who have a workplace at home questioned regularly or periodically as to whether their workplace complies with ergonomic and operational requirements?

S 1.45 Suitable storage of business-related documents and data media

Initiation responsibility: Head of Site/Bldg Technical Service, IT Security Management

Implementation responsibility: Staff members

Also at the workplace at home, business related documents and data media should only be accessible to the authorised staff member. A lockable compartment (cabinet, desk drawer etc.) has to be available for this purpose. When not in use, the business-related documents and data media must remain locked inside this compartment. The degree of protection provided by the compartment should comply with the security requirements of the documents and data media contained therein.

Additional controls:

- Is a lockable compartment available for the workplace at home?
- Has the staff member been informed that the documents and data media need to be stored under lock and key?

S 1.46 Use of anti-theft devices

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section

Anti-theft devices should be used wherever valuable items need to be protected or where other safeguards, such as appropriate control of access to the workstations, cannot be implemented. Anti-theft devices are useful in places to which the public have access or where the fluctuation of users is extremely high.

Not only the object to be protected, but also the monitor, keyboard and other accessories should be fitted with anti-theft devices.

There are now various types of anti-theft devices available on the market. On the one hand, there are anti-theft devices for hardware which protect IT equipment, for example by connecting the IT system to the desk. There are also a number of security mechanisms to prevent thieves from opening the casing and stealing components or manipulating security-related settings, for example by removing security cards.

When new IT equipment is procured, it should be ensured that it has eyes on the casing, so that it can be attached to other objects, and that the casing can be locked.

Additional Controls:

- Have IT systems or IT components been stolen within the last year?
- How are IT systems or IT components protected against theft?

S 2 Safeguard Catalogue - Organisation

S 2.1 Specification of responsibilities and of requirements documents for IT uses

S 2.2 Resource management

S 2.3 Data Media Control

S 2.4 Maintenance/Repair Regulations

S 2.5 Division of responsibilities and separation of functions

S 2.6 Granting of site access authorisations

S 2.7 Granting of (system/network) access rights

S 2.8 Granting of access rights

S 2.9 Ban on Using Non-Approved Software

S 2.10 Survey of the Software Held

S 2.11 Provisions Governing the Use of Passwords

S 2.12 Services and counselling for IT users

S 2.13 Correct disposal of resources requiring protection

S 2.14 Key management

S 2.15 Fire safety inspection

S 2.16 Supervising or escorting outside staff/visitors

S 2.17 Entry regulations and controls

S 3.18 Inspection rounds

S 2.19 Neutral documentation in distributors

S 2.20 Monitoring of existing connections

S 2.21 Ban on smoking

S 2.22 Escrow of Passwords

S 2.23 Issue of PC Use Guidelines

S 2.24 Introduction of a PC Checklist Booklet

S 2.25 Documentation of the System Configuration

S 2.26 Appointment of an administrator and his deputy

S 2.27 Dispensing with remote maintenance of the PBX

S 2.28 Availability of external telecommunications advisory services

S 2.29 PBX operating instructions for users

S 2.30 Provisions governing the configuration of users and of user groups

S 2.31 Documentation on authorised users and on rights profiles

S 2.32 Establishment of a restricted user environment

S 2.33 Division of Administrator roles under UNIX

S 2.34 Documentation of changes made to an existing IT system

S 2.35 Obtaining information on security weaknesses of the system

S 2.36 Orderly issue and retrieval of a portable (laptop) PC

S 2.37 Clean desk policy

S 2.38 Division of administrator roles in PC networks

S 2.39 Response to violations of security policies

S 2.40 Timely involvement of the staff/factory council

S 2.41 Employees' commitment to data backup

S 2.42 Determination of potential communications partners

S 2.43 Adequate labelling of data media for dispatch

S 2.44 Secure packaging of data media

S 2.45 Controlling the exchange of data media

S 2.46 Appropriate key management

S 2.47 Designating a person in charge of the fax system

S 2.48 Designating authorised fax operators

S 2.49 Procurement of suitable fax machines

S 2.50 Appropriate disposal of consumable fax accessories and spare parts

S 2.51 Producing copies of incoming fax messages

S 2.52 Supply and monitoring of consumable fax accessories

S 2.53 Deactivation of fax machines after office hours

S 2.54 Procurement/selection of suitable answering machines

S 2.55 Use of a security code

S 2.56 Avoidance of confidential information on answering machines

S 2.57 Regular playback and deletion of recorded messages

S 2.58 Limitation of message time

S 2.59 Procurement of a suitable modem

S 2.60 Secure administration of a modem

S 2.61 Requirements document for modem usage

S 2.62	Software acceptance and approval Procedure
S 2.63	Establishing access rights
S 2.64	Checking the log files
S 2.65	Checking the efficiency of user separation on an IT System
S 2.66	The importance of certification for procurement
S 2.67	Defining a security strategy for peer-to-peer networks
S 2.68	Implementation of security checks by the peer-to-peer network users
S 2.69	Establishing standard workstations
S 2.70	Developing a firewall concept
S 2.71	Establishing a security policy for a firewall
S 2.72	Requirements on a firewall
S 2.73	Selecting a suitable firewall
S 2.74	Selection of suitable packet filters
S 2.75	Selection of a suitable application gateway
S 2.76	Selection and implementation of suitable filter rules
S 2.77	Secure configuration of other components
S 2.78	Secure operation of a Firewall
S 2.79	Determining responsibilities in the area of standard software
S 2.80	Drawing up a requirements catalogue for standard software
S 2.81	Preselection of a suitable standard software product
S 2.82	Developing a test plan for Standard Software
S 2.83	Testing Standard Software
S 2.84	Deciding on and developing the installation instructions for standard software
S 2.85	Approval of standard software
S 2.86	Guaranteeing the integrity of standard software
S 2.87	Installation and configuration of standard software
S 2.88	Licence management and version control of standard software
S 2.89	De-installation of standard software
S 2.90	Checking delivery
S 2.91	Determining a security strategy for the Windows NT client-server network

S 2.92	Performing security checks in the Windows NT client-server network
S 2.93	Planning of a Windows NT network
S 2.94	Sharing of directories under Windows NT
S 2.95	Obtaining suitable protective cabinets
S 2.96	Locking of protective cabinets
S 2.97	Correct procedure for code locks
S 2.98	Secure installation of Novell Netware servers
S 2.99	Secure set-up of Novell Netware servers
S 2.100	Secure operation of Novell Netware servers
S 2.101	Revision of Novell Netware servers
S 2.102	Relinquishing activation of the remote console
S 2.103	Setting up user profiles under Windows 95
S 2.104	System guidelines for restricting usage of Windows 95
S 2.105	Obtaining PBX-annexes
S 2.106	Purchase of suitable ISDN cards
S 2.107	Documentation of the configuration of ISDN cards
S 2.108	Relinquishment of remote maintenance of ISDN gateways
S 2.109	Assigning rights for remote access
S 2.110	Data privacy guidelines for logging procedures
S 2.111	Keeping manuals at hand
S 2.112	Regulation of the transport of files and data media between home workstations and institutions
S 2.113	Requirements documents concerning telecommuting
S 2.114	Flow of information between the telecommuter and the institution
S 2.115	Care and maintenance of workstations for telecommuting
S 2.116	Regulated use of communications facilities
S 2.117	Regulation of access by telecommuters
S 2.118	Determination of a security policy for the use of e-mail
S 2.119	Regulations concerning the use of e-mail services
S 2.120	Configuration of a mail centre
S 2.121	Regular deletion of e-mails
S 2.122	Standard e-mail addresses

S 2.123 Selection of a mail provider

S 2.124 Selection of suitable database software

S 2.125 Installation and configuration of a database

S 2.126 Creation of a database security concept

S 2.127 Inference prevention

S 2.128 Controlling access to a database system

S 2.129 Controlling access to database information

S 2.130 Ensuring the integrity of a database

S 2.131 Separation of administrative tasks for database systems

S 2.132 Provisions for configuring database users / user groups

S 2.133 Checking the log files of a database system

S 2.134 Guidelines for database queries

S 2.135 Save transfer of data to a database

S 2.136 Observance of rules concerning workstations and working environments

S 2.137 Procurement of a suitable data backup system

S 2.138 Structured data storage

S 2.139 Survey of the existing network environment

S 2.140 Analysis of the existing network environment

S 2.141 Development of a network concept

S 2.142 Development of a network realisation plan

S 2.143 Development of a network management concept

S 2.144 Selection of a suitable network management protocol

S 2.145 Requirements for a network management tool

S 2.146 Secure operation of a network management system

S 2.147 Secure migration of Novell Netware 3.x servers to Novell Netware 4.x networks

S 2.148 Secure configuration of Novell Netware 4.x networks

S 2.149 Secure operation of Novell Netware 4.x networks

S 2.150 Auditing of Novell Netware 4.x networks

S 2.151 Design of an NDS concept

S 2.152 Design of a time synchronisation concept

S 2.153 Documentation of Novell Netware 4.x networks

S 2.154 Creation of a computer virus protection concept

S 2.155	Identification of IT systems potentially threatened by computer viruses
S 2.156	Selection of a suitable computer virus protection strategy
S 2.157	Selection of a suitable computer virus scanning program
S 2.158	Reporting computer virus infections
S 2.159	Updating the computer virus scanning programs used
S 2.160	Regulations on computer virus protection
S 2.161	Development of a cryptographic concept
S 2.162	Determining the need to use cryptographic procedures and products
S 2.163	Determining the factors influencing cryptographic procedures and products
S 2.164	Selection of a suitable cryptographic procedure
S 2.165	Selection of a suitable cryptographic product
S 2.166	Provisions governing the use of crypto modules
S 2.167	Secure deletion of data media
S 2.168	IT system analysis before the introduction of a system management system
S 2.169	Developing a system management strategy
S 2.170	Requirements to be met by a system management system
S 2.171	Selection of a suitable system management product
S 2.172	Developing a concept for using the WWW
S 2.173	Determining a WWW security strategy
S 2.174	Secure operation of a WWW server
S 2.175	Setting up a WWW server
S 2.176	Selection of a suitable Internet service provider
S 2.177	Security during relocation
S 2.178	Creation of security guidelines for the use of faxes
S 2.179	Procedures controlling the use of fax servers
S 2.180	Configuration of a fax mail centre
S 2.181	Selection of a suitable fax server
S 2.182	Regular revision of IT security measures
S 2.183	Performing a RAS requirements analysis
S 2.184	Development of a RAS concept

S 2.185 Selection of a suitable RAS system architecture

S 2.186 Selection of a suitable RAS product

S 2.187 Definition of a set of RAS security guidelines

S 2.188 Security guidelines and rules for the use of mobile phones

S 2.189 Blocking of the mobile phone in the event of its loss

S 2.190 Setting up a mobile phone pool

S 2.191 Establishment of the IT security process

S 2.192 Drawing up of an Information Security Policy

S 2.193 Establishment of a suitable organisational structure for IT security

S 2.194 Drawing up a schedule of existing IT systems

S 2.195 Creation of an IT security concept

S 2.196 Implementation of the IT security concept in accordance with an implementation plan

S 2.197 Drawing up a training concept for IT security

S 2.198 Making staff aware of IT security issues

S 2.199 Maintenance of IT security

S 2.200 Preparation of management reports on IT security

S 2.201 Documentation of the IT security process

S 2.202 Preparation of an IT Security Manual

S 2.203 Establishment of a pool of information on IT security

S 2.204 Prevention of insecure network access

S 2.205 Transmission and Retrieval of Personal Data

S 2.1 Specification of responsibilities and of requirements for the use of IT

Initiation responsibility: Agency/company management

Implementation responsibility: Head of IT Section, Head of organisation

For the functional areas of "IT use" and "IT security", responsibilities as well as authorities must be specified.

For "IT use", the responsibility for substantive tasks and operational responsibility must be laid down. The person responsible for substantive tasks has to develop the specific requirements to be implemented in an IT procedure. On the other hand, operational responsibility covers the following tasks, *inter alia*:

- data acquisition
- work scheduling and preparation;
- data processing
- post-processing of data output;
- data media management and
- monitoring of procedural execution.

Overall regulations governing "IT security", as an aspect of IT use, must be laid down in a binding form. It is advisable to lay down regulations on:

- data backup
- keeping data archives,
- transport of data media
- data transmission
- destruction of data media
- documentation on IT procedures, software, IT configuration;
- use of passwords;
- entry rights
- access rights
- resources control
- resource management
- purchase and leasing of hardware and software;
- maintenance and repair work;
- software: acceptance and approval;
- software: application development;
- data privacy,
- protection against computer viruses;

- auditing
- emergeny precautions and
- approach in case of infringement of the security policy.

. Information regarding the above can be found in the following safeguards descriptions.

These regulations must be made known to the staff concerned in a suitable way (see S 3.2 *Commitment of staff members to compliance with relevant laws, regulations and provisions*). A written record of the announcement of these regulations is recommended. In addition, all regulations, in their current version, must be kept in a given place and be made available to those having a justified interest.

The existing regulations must be kept up to date so as to avoid misunderstanding, uncertain allocation of responsibilities, and inconsistencies.

Additional controls:

- Which provisions are in force?
- Are such regulations revised on a regular basis?
- How are the staff informed of these regulations?

S 2.2 Resource management

Initiation responsibility: Agency/company management

Implementation responsibility: Head of IT Section, Head of organisation

Resources (or non-monetary resources) for IT uses are all necessary articles such as hardware components (computer, keyboard, printer, etc.), software (system software, individual programs, standard programs, and the like), consumables (paper, toner, printer cartridges), data media (magnetic tapes, floppy disks, streamer tapes, hard disks, removable hard disks, CD ROMs, and the like).

Resource management comprises the following tasks:

- procurement of resources,
- pre-use testing;
- marking and
- inventorising,

Procurement of resources is of particular importance in the use of information technology systems. A well-regulated procurement procedure will, in particular, support the objectives to be achieved with the use of information technology: improved performance, economic efficiency, improvement of communication possibilities.

Apart from mere economy aspects, a regulated procurement procedure - which can also be handled centrally - can also provide for greater account being taken of new developments and of improvements in the area of information technology.

Moreover, central procurement will ensure the introduction and observance of an "in-house standard", which simplifies the training of the staff and maintenance activities.

With a regulated **test procedure before the use** of resources, various threats can be averted. Examples are:

- verifying the completeness of deliveries (e.g. manuals) in order to ensure the availability of all components to be delivered;
- testing of new PC software and of new pre-formatted data media by means of a computer virus detection program;
- test runs of new software on specific test systems;
- verification of the compatibility of new hardware and software components with existing components.

It is only by means of an **inventory** of the resources used that consumption requirements can be determined, and replenishment orders be placed. Moreover, inventorising makes it possible to carry out checks for completeness, to check the use of non-approved software or to detect purloining of resources. This calls for clear **marking** of the most important resources with distinct identification features (e.g. grouped serial inventory numbers). In addition, the serial numbers of existing devices such as monitors,

printers, fixed disks, etc. should be documented in order to allow identification after a theft.

For stocktaking purposes, resources must be listed in inventories. Such an inventory must provide information on:

- Identifying characteristics,
- Procurement sources, delivery times,
- final destination/user of the resources,
- stockpiling/provisioning,
- regulations governing issue and
- maintenance contracts, maintenance intervals.

Additional controls:

- Does inventorising provide for checks for completeness?
- What testing procedures have been introduced before actual use? What results have been obtained?
- Have the procurement procedures been regulated, or is it possible to elude resource management during any of the phases of procurement?
- How up-to-date is the inventory?

S 2.3 Data media control

Initiation responsibility: Head of IT section

Implementation responsibility: Archive keeper; IT procedures officer

The role of data media control, as part of resource management, is to ensure access to data media to the necessary extent and within a reasonable period of time. This calls for well-regulated management of data media, including the requirement for consistent labelling and keeping of inventories. Moreover, as part of data media control, proper handling and safe keeping of data media, their orderly use and transport and, finally, deletion and/or destruction of data media must be ensured.

Inventories provide for quick and specific access to data media. Inventories give information on: the storage location, the retention period, authorised users.

The outer **marking** of data media provides for their quick identification. However, to discourage any misuse, marking should not provide any clues as to the contents (e.g. marking a magnetic tape with the index word "*telephone charges*"). A predefined structure of identification characteristics (e.g. date, filing structure, serial number) will facilitate integration within inventories.

For **proper handling** of data media the information usually provided by manufacturers on the packaging is to be consulted. As regards **safe keeping** of data media, the required measures refer both to storage (protection against magnetic fields and dust; air-conditioning protection) and to the prevention of unauthorised access (suitable containers, cabinets, rooms).

Mailing or transport of data media must be carried out in a way which precludes damage to the data media to the extent possible (e.g. mailers for magnetic tapes, padded envelopes). Packaging of data media must be based on the protective requirements of the given media (e.g. lockable conveyance containers). Provisions must be laid down with regard to the types of dispatch or transport (e.g. transportation by courier) as well as in respect of accountability procedures for the mailing/transport of items (e.g. waybill, shipping note) and their arrival at the place of destination (e.g. receipts). The data medium must not contain any "remaining data" other than the data which is to be sent. This can be done by physical deletion. In the event that the necessary tools are not available to achieve this, the data medium must at least be formatted. It should also be ensured that it is not possible to undo the command with the operating system used. Another point to be noted is that, before relevant data media are handed over, backups should be made. Chapter 7.1 *Exchange of Data Media* contains further information on the despatch and transport of data medium.

In the event that data media are to be passed on internally, certain steps can be taken, such as the introduction of a receipt system, an collection entitlement procedure, keeping inventories concerning the location of data media.

If **data media provided by third parties** are used, provisions must be made with regard to their handling before use. If, for instance, data for PCs are conveyed, a computer virus check of the data medium should be made as a

general rule. The same should be done before first use of new data media. It is advisable to make a computer virus check of data media both at the time of receipt and before dispatching.

A regulated procedure for the **deletion** or **destruction** of data media will prevent misuse of stored data. Before reusing data media the stored date have to be deleted, see: S 2.167 Secure deletion of data media

Additional controls:

- Does a current (daily up-date) inventory exist?
- Does the archive keeper check the justification for a request for data media?
- Are the existing data media checked for completeness?

S 2.4 Maintenance/repair regulations

Initiation responsibility: Head of IT section

Implementation responsibility: Head of IT Section, Administrator, IT users

As a precautionary measure to safeguard IT systems against failure, proper performance of maintenance work is of particular importance. **Timely initiation** and monitoring the execution of maintenance work should be ensured by a central unit (e.g. procurement office). Maintenance work should be carried out by trustworthy persons or companies.

In-house maintenance and repair

Supervisory regulations must be laid down for maintenance and repair work, especially if this is carried out by external staff: A competent person should supervise this work in such a way that he/she can assess whether unauthorised actions occur during such maintenance/repair. In addition, it must be verified whether the required maintenance has actually been carried out.

The following measures before and after maintenance/repair work must be planned:

- The relevant staff members must be informed of the measures.
- Maintenance engineers must, upon request, establish their identity.
- Data access by the maintenance engineer must be avoided to the extent possible. If and where required, **data media** should be previously removed or deleted (after complete backup), especially when such work is carried out externally. If deletion is not possible (e.g. because of a defect), such work must be monitored also externally or specific contractual arrangements must be made.
- The entry and access permissions granted to maintenance engineers are to be confined to the absolute minimum and must be revoked or cancelled after such work.
- Upon completion of maintenance or repair work, changes to the passwords will be required depending on the "penetration depth" afforded to maintenance staff. With regard to PCs, it might be expedient to make a computer virus check.
- The maintenance work carried out must be documented (scope, results, time, possibly the name of the maintenance engineer).

External maintenance and repairs

If IT systems are sent away for maintenance or repair, all sensitive data on the data-medium must first be physically deleted. If this is not possible due to a defect preventing access to the data medium, the company responsible for the repairs is obliged to comply with the necessary IT-security measures. The contractual regulations should comply with S 3.2 (Commitment of staff members to compliance with relevant laws, regulations and provisions) regarding the secrecy of data. In particular, data stored externally during maintenance must be erased meticulously after work has been completed. The

obligations and responsibilities of the external maintenance personnel must also be carefully specified.

The execution of external maintenance work must be logged; which IT systems or components have been sent away for repair, when and to whom, who was responsible, when the repair should be finished and when the machine was brought back. For reference, registration of the IT systems or components is necessary. On the one hand, this makes it clear to which organisation these systems belong, and on the other hand it allows straightforward classification within the organisation.

It must be ensured that damages or theft are prevented during transit of the IT components which are to be repaired. If sensitive data is still to be found on the IT systems, they must be transported with the appropriate protection, e.g. via locked containers or couriers. Moreover, proof of dispatch (accompanying documents, dispatch note) and arrival (confirmation of receipt) must be carried out and logged.

In the case of IT systems protected with passwords and depending on the scope of repair work and type of password security, all or some of the passwords must be made known, or settings must be established such as "REPAIR", so that the maintenance technicians can access the machines.

Once the IT systems or components have been handed back, their completeness must be checked. **All** passwords must be changed. PC data-media must be checked for computer viruses with an up-to-date anti-virus program. All files contained in the repaired machine must be checked as regards their integrity.

Remote maintenance

Regulations for remote maintenance are contained in S 5.33 *Secure remote maintenance via modem.*

Additional controls:

- Are the staff encouraged to ensure supervision?
- Are records kept to account for the maintenance work carried out?
- Has a timetable been laid down for maintenance work?

S 2.5 Division of responsibilities and separation of functions

Initiation responsibility: Agency/company management

Implementation responsibility: Head of IT Section; Head of Organisational Section; IT Security Management

The functions to be performed by the agency/company as regards IT uses must be laid down. Here, a distinction must be made between two levels:

- The first level comprises those functions which provide for, or support, IT system uses for data processing purposes, such as work preparation, data post-processing, operating, programming, network administration, administration of permissions, auditing.
- The second level comprises those functions which apply to the IT procedures available for task performance. Examples of such functions are: person responsible for specialised tasks, IT application supervisor, data acquisition operator, desk officer, payment in-charge.

The next step is to lay down and justify **separation of functions**, i.e. functions which are not compatible with each other and thus must not be performed by *one* person at the same time. The relevant requirements may be implied by the tasks themselves or by legal provisions. **Examples** include:

- administration of permissions and auditing;
- network administration and auditing.
- programming and test of self-developed software;
- data acquisition and authority to sign orders to pay;
- auditing and authority to sign orders to pay;

This shows, in particular, that in most cases operational functions are not compatible with controlling functions.

After the separation of functions to be observed has been laid down, the functions can be assigned to persons.

The provisions laid down in this context must be documented and up-dated in case of changes being made to IT uses. If such assignment do result in incompatible functions having to be performed by one person, this fact must be explicitly mentioned in the relevant documentation on the separation of functions.

Additional controls:

- Has an exhaustive list of the relevant functions been established?
- Is completeness of the defined separation of functions ensured?
- Is separation of functions being maintained in staffing terms?
- Is the allocation of persons/functions updated?

S 2.6 Granting of site access authorisations

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of Organisational Section; Head of Site/Bldg Technical Service

Prior to granting access rights to persons, the rooms in a building requiring protection must be defined, e.g. office, data media archive, server room, operating room, machine-room, document archive, computing centre. The protective requirements of a room must be determined on the basis of the IT equipment kept in the given room, and by the need for protection of the IT applications used and their set of information.

Subsequently, it must be defined which person needs what access permissions for the performance of the assigned function. This must be done in compliance with the previously defined separation of functions (S 2.5 *Division of responsibilities and separation of functions*). Granting of unnecessary access permissions must be avoided.

In order to minimise the number of persons authorised to have access to a room, the principle of separation of functions should also be observed in the use of IT facilities. Thus, separate storage of IT spare parts and data media will prevent unauthorised access by a maintenance engineer to data media.

Access rights granted and withdrawn must be documented. In the event that a site access permission is withdrawn, it must be ensured that the means of site access is also withdrawn. In addition, it must be documented which conflicts have arisen when granting access rights to persons. Possible reasons for conflicts are: persons performing functions which, in terms of access authorisations, are opposed to the separation of functions, or which result from spatial requirements.

For the control of entry permissions, either persons (entrance control staff, lock-up service), or technical devices (badge reader, lock) may be used (cf. S 2.14 *Key Management*). Non-authorised persons (e.g. visitors) may be granted access to rooms requiring protection only in the presence of, or when accompanied by, authorised staff.

Regulations concerning the granting/withdrawal of site access authorisations for employees of outside contractors must also be established.

Additional controls:

- Is documentation on the protective requirements of IT rooms in existence?
- Is the documentation on rooms requiring protection, and on persons authorised to have access, being up-dated?

S 2.7 Granting of (system/network) access privileges

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section

This type of access authorisation allows the person concerned to use IT systems, systems components and networks. This must be laid down in detail for every person authorised to use such facilities on the basis of his/her function and with due regard to the separation of functions (cf. S 2.5 *Division of responsibilities and separation of functions*). Access to a computer must be defined depending on the function, e.g. access to the operating system (system administrator), or access to an IT application (application user). Moreover, it must be ensured that staffing and task-related changes are promptly taken into account.

Where feasible in IT-terms, access should only be possible after the identification (e.g. name, user ID or smart card) and the authentication (e.g. password) of the authorised person, and should be logged.

The issue and retrieval of access-granting means such as user IDs or smart cards must be documented. Also, provisions must be laid down as regards the handling of access-granting and authentication means (e.g. use of smart cards, handling of passwords, cf. S 2.11 *Provisions governing the use of passwords*).

Access authorisation should be temporarily blocked in case of long term absence of the authorised person in order to prevent abuse.

It is necessary to make sporadic checks for compliance with the aforementioned requirements.

Additional controls:

- Are the issue and the retrieval of access authorisations and access-granting means documented?
- Is separation of functions being observed in the granting of access rights?
- Are users being trained in the correct handling of access-granting means?
- If use of access-granting means is logged, are such logs also analysed?

S 2.8 Granting of (application/data) access permissions

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators; persons responsible for substantive tasks

Such access permissions determine which person will, on the basis of his/her function, be authorised to use applications or data. The access permissions (e.g. read, write, execute) to IT applications, parts of applications, or data, depend on the function fulfilled by the given person, e.g. application supervisor, scheduler, system program, application developer, system administrator, auditor, data acquisition operator, desk officer. In any case, only so many access permissions as are required for task performance (*need-to-know* principle) should be granted. Enforcement of access rights must be through the administration of rights of the IT system.

A variety of IT systems allow various privileges to be defined as group privileges or as profiles (e.g. data acquisition operators). This definition corresponds to the technical implementation of privileges allocated to a function. It is beneficial for the administration of the privileges of an IT system to compile such groups or profiles, thus considerably simplifying the allocation and updating of privileges.

The person responsible in each given case must arrange for, and document, the assignment of, and changes in, access privileges. Such documentation must show:

- what function, in compliance with the separation of functions (cf. S 2.5 *Division of responsibilities and separation of functions*), is provided with what access privileges;
- which groups or profiles are in place;
- what person performs what function;
- the access privileges granted to a person; and
- the conflicts entailed by the granting of access privileges to persons. Such conflicts may, for instance, result from incompatible functions being performed by one person or from the fact that, depending on the given IT system, it is not possible to separate certain access privileges.

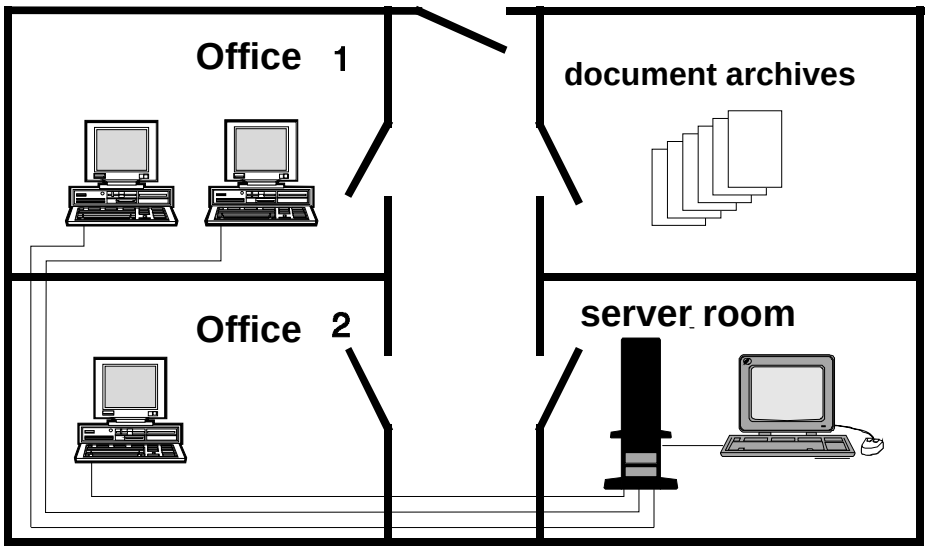
Additional controls:

- Does up-dated documentation on the granted access privileges exist?
- Are requested access privileges or changes to granted access privileges being confirmed or verified by the responsible persons?
- Is there a standard procedure for granting and revoking access privileges?

The approach to the separation of functions and granting of privileges is illustrated in the following example.

The IT application considered here is a system for travel expenses accounting. The relevant rooms are shown in the graph below. The IT system consists of a

LAN to which, in addition to the operator's console, three PCs are connected as workstations.



Step 1: Division of responsibilities and separation of functions

The following functions are required for the travel expenses accounting system considered here:

1. LAN administration
2. Auditing
3. data acquisition
4. casework, including ascertainment of mathematical correctness
5. casework, including ascertainment of factual correctness
6. casework, including authority to issue orders

The following functions are not compatible with each other on account of inherent necessities:

- Function 1 and Function 2 (self-control of administration must be precluded)
- Function 2 and Function 6 (self-control of the person authorised to issue orders must be precluded)
- Functions 4 or 5 with 6 being performed at the same time (the two-person rule would be violated with regard to orders to pay)

These functions are performed by the following persons:

	Mr. Brown	Ms. Smith	Ms.Miller	Ms. White
1. LAN administration	X			
2. Auditing		X		
3. Data acquisition			X	
4. Casework – mathematical accuracy			X	
5. Casework - factual accuracy			X	
6. Authority to issue orders				X

Step 2: Granting of room access permissions

The protection requirement of the various rooms is described below and the granting of room access permissions documented in the table:

- Server room:

  unauthorised access to the server must be prevented because accessibility, integrity and confidentiality of the entire application are dependent on these central components.

- Document archives:

  for invoicing purposes, travel expense documents must be stored. It should archive: be ensured that the documents are stored complete and unchanged.

- Office 1

  this office is used for the input of data in connection with establishing the mathematical accuracy and factual correctness. In order to guarantee the correctness of these processes, unauthorised access to the workstation computers must not be possible.

- Office 2

  The issuing of orders takes place here for the payment of travel expenses on the workstation. This procedure must be carried out by only one authorised person. Unauthorised access should not be possible.

	Server room	Document archives	Office 1	Office 2
1. LAN administration	X			
2. Auditing	X	X	X	X
3. Data acquisition			X	
4. Casework – mathematical accuracy		X	X	
5. Casework - factual accuracy		X	X	
6. Authority to issue orders		X	X	X

Step 3: Granting of (system/network) access privileges

According to functions, the following access privileges are assigned:

	Operating system server	Applica-tion: Analysis of audit trails	Applica-tion: Data acquisition	Applica-tion: document processing
1. LAN administration	X			
2. Auditing	X	X		X
3. Data acquisition			X	
4. Casework – mathematical accuracy				X
5. Casework - factual accuracy				X
6. Authority to issue orders				X

Step 4: Granting of (application/data) access permissions

In the following, the (application/data) access privileges required for the execution of a function are set out. Legend:
E = = right to *Execute* an application/software
R = = right to *Read* data

W = = right to *Write* data, i.e. generate data

M = = right to *Modify* data

D = = right to *Delete* data

S = Right to *Sign* orders to pay

	Operating system server	Protocol evaluation	Application: Data acquisition	Application: document processing
1. LAN administration	E,R,W,M, D			
2. Auditing	E,R	E,R,D		E,R
3. Data acquisition			E,W	
4. Casework – mathematical accuracy				E,R,M
5. Casework - factual accuracy				E,R,M
6. Authority to issue orders				E,R,S

Documentation of this kind facilitates the assignment of privileges. Assuming job changing by Ms. Smith, the vacancy thus having to be filled, the above tables can be used to determine which of Ms. Smith's former privileges must be revoked and assigned to the new staff member. If the latter, *qua* substitute, additionally is to perform the function "casework, including authority to issue orders", the required assignment of privileges elucidates the conflict arising from the fact that the new staff member, when acting as a substitute, can carry out unnoticed manipulations.

S 2.9 Ban on using non-approved software

Initiation responsibility: Agency/company management; Head of IT Section; IT Security Management

Implementation responsibility: Head of IT section

Provisions must be laid down on how software may be accepted, approved, installed and used (c.f. S 2.62 *Software acceptance and approval Procedure* and Chapter 9.1 *Standard Software*). Installation or use of non-approved software must be prohibited and as much as possible prevented via technical means. For example, this can be attained under Windows 95 by restricting the user environment (see S 2.104 *System guidelines for restricting usage of Windows 95*). This is to prevent introduction of programs with undesirable effects. In addition, uncontrolled use of the system beyond the defined range of functions is to be prevented. Where necessary, this ban on use can be extended also to the use of private hardware and private data (floppy disks, removable hard disk, PC, laptop).

Prior approval should be required for any exemptions to be granted.

Additional controls:

- Has a procedure for the authorisation and registration of software been laid down?
- Has the ban on use of non-approved software been laid down in writing?
- Have all staff members been informed of the ban on use?
- Are reminders periodically given of the ban on use?
- What possibilities exist for installing or using unauthorised software?
- What possibilities exist for autonomous development of software on individual computers?
- Do regulations exist concerning the programming and passing on of macros of standard products, e.g. text processing, table calculation and data bases?
- Have any lists been established which show the approved versions of executable files and, in particular, indicate the creation date and the size of the file?
- Are periodic checks being made of whether approved versions of executable files have been altered?
- Is it possible to technically prevent software from being installed?

S 2.10 Survey of the software held

Initiation responsibility: Agency/company management; Head of IT Section; IT Security Management; superiors

Implementation responsibility: IT Security Management

In order to be able to detect any infringements of the ban on the use of non-approved software, regular checks must be made of the software inventory. In case of a large number of IT systems, random checks may be made. The findings of such checks must be documented in order to provide for detection of any recurrences.

If non-approved software is found during such checks, arrangements should be made for its removal. In order to be able to carry out these checks, the reviewing entity must be vested with adequate powers by the company/agency management. In addition, the reviewing entity must be informed of which software is approved for which IT system (software inventory).

Additional controls:

- At what intervals are such checks recommended?
- Have there been cases in which non-approved software was used?
- How are infringements handled?

S 2.11 Provisions governing the use of passwords

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT security management, users

If passwords are used for authentication in an IT system, the safety of the management of access privileges of the system will decisively depend on the correct use of the respective passwords. For this purpose, it is advisable to introduce a set of provisions governing password use and to inform the users accordingly.

The following rules regarding password use should be observed:

- It must not be possible to guess the password as easily as names, motor vehicle licence numbers, birth dates, or the like.
- The password should consist of at least one non-letter character (special character or number).
- The password should consist of at least 6 characters. The number of password characters checked by the computer must be tested.
- Preset passwords (e.g. by the manufacturer at the time of delivery) must be replaced by individually selected passwords.
- Passwords must not be stored on programmable function keys.
- The password must be kept secret and should only be known personally to the user.
- The password should be laid down in writing only for the purpose of ist escrowing whereby it is kept safely in a sealed envelope. If an additional written record is made, the password should be kept at least as safely as a check identification card or a bank note (c.f. S 2.22 *Depositing of passwords*).
- The password must be altered regularly, e.g. every 90 days.
- The password should be altered if it has come to the knowledge of unauthorised persons.
- After any alteration of the password, previous passwords should no longer be used.
- Entry of the password should be made away from general view.

Where feasible in data processing terms, the following complementary rules should be observed:

- The selection of trivial passwords (BBBBBB, 123456) must be prevented.
- Every user must be able to alter his own password at any time.
- For initial log-on of new users, one-time passwords should be assigned, i.e. passwords which must be changed after their first use. In networks in which passwords are transferred in non-encrypted form, the constant use of one-time passwords is recommended (c.f. S 5.34 *Use of one time passwords*).

- After three unsuccessful attempts to enter the correct password, a lockout should be imposed which can only be cancelled by the system administrator.
- During authentication of networked systems, passwords should not be transmitted in an unencrypted form.
- The password must be entered covertly, i.e. the input will not be displayed on the monitor.
- Passwords should be stored in the system in a way preventing unauthorised access, e.g. by means of one-way encryption.
- Password alteration must be initiated by the system on a regular basis.
- Re-use of previous passwords in the case of password alteration should be prevented by the IT system (password history).

Additional controls:

- Have users been informed on how to handle passwords correctly?
- Is the password quality controlled?
- Are password changes mandatory?
- Has every user been provided with a password?

S 2.12 Services and counselling for IT users

Initiation responsibility: Agency/company management; Head of IT Section

Implementation responsibility: Head of IT section

Use of IT systems requires comprehensive training/instruction of IT users. In addition to training enabling the IT users to handle the used information technology properly, IT users must be provided with information and advisory services regarding any problems encountered in current operations. Such problems may result from hardware defects or faulty software installation, but also from operating errors as regards the programs used.

In larger-size agencies/companies, it may therefore be a good policy to charge a central unit with attending to the needs of IT users and to inform all staff members of the designation of that unit. This requirement may be practicable, in particular, in cases where a large number of decentralised systems such as PCs is involved.

Additional controls:

- Who can be contacted by the IT users in case of any problems?

S 2.13 Correct disposal of resources requiring protection

Initiation responsibility: Agency/company management; Head of IT Section; IT Security Management

Implementation responsibility: Head of Site/Bldg Technical Service; staff members

Resources (non-monetary resources) on which sensitive data are stored (printing paper, floppy disks, streamer tapes, magnetic tapes, hard disks, but also special toner cassettes, carbon paper or carbon ribbon) and which are no longer needed or, on account of a defect, are to be discarded, must be disposed of in such a way that no conclusions can be drawn as regards previously stored data. In the case of functioning data media, the data should be physically deleted. Non-functioning data media such as CD-ROMS should be destroyed mechanically (see S 2.167 Secure deletion of data carriers).

The recommended disposal of material requiring protection should be detailed in a specific directive; adequate disposal facilities are to be provided (see also DIN 32757).

If sensitive resources are collected prior to their disposal, the collected material must be kept under lock and be protected against unauthorised access.

If, within the given company/agency, safe and environmentally-sound disposal cannot be ensured, the companies entrusted with this task must be put under obligation to comply with the required IT security measures. A sample contract is enclosed with this manual.

Additional controls:

- Are all types of material requiring protection covered by the aforementioned provisions?
- Is the disposal procedure reliable?
- Are the specified disposal provisions complied with?

S 2.14 Key management

Initiation responsibility: Head of Organisational Section; IT Security Management

Implementation responsibility: Head of Site/Bldg Technical Service

For all keys to the building (of floors, hallways and rooms), a lock-up plan should be drawn up. The manufacture, storage, management and issue of keys must be organised on a centralised basis. Reserve keys are to be provided and have to be stored securely. The same goes for all identification means such as magnetic or smart cards. Attention must be paid to the following:

- Where a lock-up facility is available, either specific lock-up groups must be established for sensitive areas, or individual rooms should be removed from the lock-up group and provided with a single lock-up.
- Keys not issued to personnel and spare keys must be stored in a way affording protection against unauthorised access.
- Issue of keys will be against receipt and must be documented.
- Arrangements must be made with regard to the response required in case of loss of individual keys (reporting, replacement, reimbursement of costs, replacement of the lock, alteration of the lock-up group, etc.).
- When changes are made to the authorities of staff members, the lock-up rights are to be checked; if and where required, the keys will have to be recovered.
- In case of termination of employment, all keys must be retrieved from the persons concerned (inclusion of key management in the inter-office slip (checklist)).
- Locks and keys to particularly sensitive areas (for which only a very restricted number of keys should be issued) may be exchanged as required in order to neutralise the function of counterfeited keys.

Additional controls:

- What rules have been laid down as regards key management?
- Are these rules accepted by the staff members?

S 2.15 Fire safety inspection

Initiation responsibility: Head of Site/Bldg Technical Service

Implementation responsibility: Site fire protection officer

The construction and use of buildings must comply with fire protection regulations. These are laid down in DIN and VDE specifications and are complemented by the requirements imposed by local fire departments (cf. also S 1.6 *Compliance with fire-protection regulations and requirements imposed by the local fire department*).

Experience shows that, after initial use, such regulations are, in the course of daily business, handled with increasing negligence or, in extreme cases, with utter disregard. To give some **examples**:

- escape routes are blocked, e.g. by furniture or paper stocks;
- fire doors are kept open by wedging;
- admissible fire loads are exceeded by increasing quantities of cables or as a result of newly-defined uses;
- fire walls and/or fire seals are damaged during operations or are not properly restored.

Fire safety inspections should be carried out once or twice per year, with and without prior notice.

Since the action of staff members is usually not determined by malevolent intent, but by in-house requirements, or by insolence, or aspects of convenience, fire safety inspections cannot be designed to detect and to punish offenders. Rather, the identified shortcomings and their causes should be remedied immediately.

Additional controls:

- Are fire safety inspections carried out on a regular basis and all deficiencies eliminated?

S 2.16 Supervising or escorting outside staff/visitors

Initiation responsibility: Head of Organisational Section

Implementation responsibility: Staff members

Strangers (visitors, craftsmen, maintenance and cleaning staff) should not be left unattended (cf. also S 2.6 *Granting of site access authorisations*), except in rooms specifically designed for such purposes. Should the need arise to leave a stranger by himself in an office, the occupant of that office should ask a colleague to stay there or should ask the visitor to wait in a colleague's office.

If it is not possible to permanently accompany outsiders (e.g. cleaning staff), the minimum requirement should be to secure the personal work area: desk, cabinet and PC (lock for floppy disk drive, keyboard lock). Cf. also S 2.37 Clean desk policy.

In the case of the work -place at home, family members and visitors should only be allowed inside the work area after all work documents have been locked up and IT access protection has been activated.

The requirement for this measure must be explained to the staff and should possibly be laid down in service instructions. The location of an outsider can be recorded in the visitors' book.

Additional controls:

- Are staff members encouraged to act accordingly?
- What is the actual in-house practice as regards these requirements?

S 2.17 Entry regulations and controls

Initiation responsibility: Head of Organisational Section; Head of Site/Bldg Technical Service

Implementation responsibility: Head of Site/Bldg Technical Service; staff members

Entry into parts of buildings and to rooms requiring protection is to be regulated and controlled (see S 2.6 *Granting of site access authorisations*). The pertinent measures range from the simple issue of keys to intricate identification systems including one-by-one checks of persons; in this respect, use of a physical key with lock also constitutes a form of entry control. For entry regulation and control, it is necessary that:

- The area subject to such regulations must be clearly defined.
- The number of persons with right of access is to be confined to a minimum. These persons should be mutually aware of their permissions in order to be able to recognise unauthorised persons as such.
- Any other persons (visitors) may be allowed to enter only after the need to do so has been previously verified.
- The permissions granted must be documented.

The mere allocation of permissions will not suffice if their observance, or infringement, is not monitored. The detailed design of control mechanisms should be based on the principle that simple and practicable solutions are often just as effective as intricate technology. Examples here are:

- Informing, and raising the awareness of, the authorised persons.
- Full information must be provided on any changes to the permissions granted.
- Visible carrying of premises passes; possibly issue of visitor's passes.
- Escorting of visitors.
- Procedural patterns when any infringement of rights has been detected.
- Unhindered entry for unauthorised persons must be prevented, or at least rendered difficult (e.g. door with a dummy knob; lock for authorised persons provided with a key; bell for visitors).

In addition, the installation of various types of badge readers, of walk-through detectors and of one-by-one checking facilities may be expedient. For key management, cf. S 2.14 *Key Management*.

S 2.18 Inspection rounds

Initiation responsibility: Site/Bldg Technical Service; IT Security Management

Implementation responsibility: Site/Bldg Technical Service; IT Security Management

The effectiveness of any measure will always be commensurate to the enforcement of that measure. Inspection rounds offer the simplest means of monitoring the implementation of measures and the observance of requirements and instructions.

Inspection rounds should not be aimed at the detection of offenders for the purpose of punishing them. Rather, controls should be aimed primarily at remedying perceived negligence at the earliest time possible (closing windows, taking documents into custody, etc.). As a secondary objective, the causes of such carelessness can be identified and possibly avoided in future.

Inspection rounds should indeed also be made during office hours and be used to inform staff members about how and why pertinent regulations are being applied. Thus, they will be perceived by all persons concerned as a help rather than a hinderance.

S 2.19 Neutral documentation in distributors

Initiation responsibility: Head of Site/Bldg Technical Service

Implementation responsibility: Head of Site/Bldg Technical Service; network planner

Each distributor should be provided with documentation showing the current status of strap connections and line assignments. Such documentation must be kept as neutral as possible. Only existing and used connections should be listed in it. Unless expressly required (e.g. for fire-alarm lines), no information should be included as regards the specific uses of such lines. In many instances, line, distributor and room numbers will suffice. Any further information must be provided in a review documentation.

Additional controls:

- How is it ensured that the documentation is always up to date?
- How is it ensured that such documentation does not contain any information that should not be disclosed?

S 2.20 Monitoring of existing connections

Initiation responsibility: Head of Site/Bldg Technical Service, Head of IT Section

Implementation responsibility: Head of Site/Bldg Technical Service; network planner

A visual inspection (at least on a random basis) must be made of all distributors and duct boxes. Attention must be paid to the following aspects:

- traces of attempts to open locked distributors by force;
- up-to-date information provided in the documentation placed in the distributors;
- correspondence of actual line assignments and strap connections with the information provided in the documentation;
- integrity of the short-circuits and grounding of non-required circuits; and
- inadmissible installations/modifications.

A functional check can be made in addition to the mere sight check. For this purpose, existing lines will be reviewed for their necessity and for compliance with technical parameters. Such a review is advisable in the following situations:

- in the case of lines which are very seldom used and where manipulations are not detected at once;
- in the case of lines over which sensitive information is transmitted frequently and regularly.

Additional controls:

- At what intervals are existing connections being checked?
- How are identified irregularities documented and followed up?
- To whom must such irregularities be reported?
- Who will remedy any irregularities, and who will monitor such work?

S 2.21 Ban on smoking

Initiation responsibility: Head of Site/Bldg Technical Service

Implementation responsibility: Staff members

In rooms housing IT systems or data media (server room, data media archives, as well as document archives) where fires or soiling may cause significant damage, a ban on smoking should be imposed. This will serve for both preventive fire protection and for the operational reliability of IT facilities with mechanical functional units.

Additional controls:

- Is the ban on smoking observed in rooms requiring protection?

S 2.22 Escrow of passwords

Initiation responsibility: Head of IT section

Implementation responsibility: IT-user

If access to an IT system is protected by means of a password, provisions must be made to ensure that, in case of absence of a staff member, e.g. vacation or illness, his/her substitute will have access to the IT system. For this purpose, the current password must be deposited by each staff member in an appropriate place (in a sealed envelope) and must be updated whenever the password is altered. If the need arises to use that escrowed password, this should be done according to the two-person rule.

In the case of telecommuters, it should be ensured that their passwords are also deposited at the institution, so that if an emergency arises, a stand-in can access the data stored on the telecommuting computer.

For all systems attended to by administrators, especially for networked systems, regular inspections must ensure that the current system administrator password has been escrowed.

Additional controls:

- Are the escrowed passwords complete and up to date?
- Have provisions been made to ensure proper use of the given escrowed password?
- Is the system of password changes being controlled on the basis of the updating entries for escrowed passwords?

S 2.23 Issue of PC Use Guidelines

Initiation responsibility: Agency/company management; IT Security Management; Head of IT Section

Implementation responsibility: Head of IT Section; IT users

In order to promote the secure and proper use of personal computers in larger-size companies/agencies, PC Use Guidelines should be prepared which lay down mandatory provisions on what general requirements must be met and which IT security measures will have to be taken. As a minimum, such PC Use Guidelines are to regulate the use of non-networked PCs; if PCs are operated within a network or are used as intelligent terminals, these aspects will have to be covered by the Guidelines. The following is to give a broad outline of the items which might expediently be included in such PC Use Guidelines.

The contents of PC Use Guidelines may be structured as follows:

- Objectives and definitions

  This introductory part of the PC Use Guidelines serves to raise the IT security awareness and motivation of PC users. At the same time, the concepts required for shared understanding are defined, such as *PC*, *users*, *objects requiring protection*.

- Scope of application

  In this part, the units of the company/agency to which the PC Use Guidelines are to apply must be laid down in a binding form.

- Legislation and in-house regulations

  Here, information is given on the legal provisions to be complied with, e.g. the *Federal Data Protection Act* and the *Copyright Act*. In addition, all relevant in-house regulations can be listed in this section.

- Distribution of responsibilities

  This section defines what function will be associated with what responsibility in the context of PC use. In particular, a distinction will have to be made between the functions of user, superior, auditing officer, departmental data privacy officer, and IT Security Management.

- IT security measures to be implemented and observed

  In the final section of the PC Use Guidelines, those IT security measures which are to be observed and implemented by the IT user must be laid down. Depending on the required level of protection the measures can exceed the IT base protection.

If telecommuters are employed by an enterprise or agency, the PC usage guidelines should be extended by rules pertaining to telecommuting workstations. Also refer to Chapter 9.3.

Additional controls:

- Have PC Use Guidelines been established?
- How is compliance with the PC Use Guidelines monitored?
- Is it necessary to update the contents, especially as regards IT security measures?
- Does every PC user have a copy of these PC Use Guidelines?
- Are such PC Use Guidelines covered by the curriculum for training in IT security measures?

S 2.24 Introduction of a PC Checklist Booklet

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: IT-user

For documentation of the IT security measures taken with regard to a PC, it is expedient to introduce a PC Checklist Booklet in which the user can record the following:

- name of the PC user;
- site where the PC is installed;
- description of the configuration;
- access-granting means;
- hardware and software used;
- scheduled data backup intervals;
- maintenance work and repairs carried out;
- effected checks regarding computer viruses;
- time of password changes;
- available accessories;
- effected audits;
- point of contact in problematic cases;
- times of data backup.

The *Additional Aids* section of this IT Baseline Protection Manual contains a specimen of such a PC Checklist Booklet.

Where keeping of such a PC Checklist Booklet is mandatory, control activities will definitely be facilitated as all PC-relevant changes and IT security measures carried out will be documented in this booklet. Moreover, keeping of such a checklist provides the PC user with the required self-control for carrying out regular data backup, password changes and virus checks.

S 2.25 Documentation of the system configuration

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: Administrators

Planning, control, monitoring and contingency planning for IT systems depend on up-to-date documentation of those systems. Only if documentation of the system configuration is up-to-date is orderly recovery of the IT system possible following an emergency.

In the case of network operation, the physical network structure (cf. S 5.4 *Documentation on, and marking of, cabling*) and the logical network configuration must be documented, as must the access rights of individual users (cf. S 2.31 *Documentation on authorised users and rights profiles*) and the data backup status. Again, the applications used and their configuration must be documented, also the file structures on all IT systems.

Care should be taken to ensure that documentation is up-to-date and easy to understand so that a deputy could take over the administrative tasks at any time. The system documentation must be kept in such a way that it is available should an emergency occur at any time. If it is maintained in electronic form, it should either be printed out at regular intervals or else it should be stored on a transportable data medium. Access to the documentation should be confined to the responsible Administrators.

The system documentation should cover all the actions to be taken on starting up or shutting down IT systems. This is especially important for networked IT systems. Here, for example, it is often necessary to adhere to a particular sequence when mounting drives or starting up network services.

Additional controls:

- Is the existing documentation up-to-date?
- Is it possible to continue administration on the basis of that documentation?

S 2.26 Appointment of an Administrator and his Deputy

Initiation responsibility: Head of IT Section, IT Security Management, PBX officer

Implementation responsibility: -

To ensure the orderly operation of IT systems, Administrators must be appointed for all IT systems and networks. In addition to general administration work, Administrators are responsible, in particular, for user administration, including the administration of access rights. They are also responsible for the security aspects of all the IT systems they look after.

In larger organisations with a number of different IT systems and subnetworks, it is also necessary to ensure that the work is divided between the different Administrators in such a way that there are no problems regarding who is responsible for what, i.e. so that no two Administrators have overlapping responsibilities and all the tasks which need to be performed are assigned. In addition, communication between the different Administrators should function as smoothly as possible. It can be helpful to hold regular meetings of Administrators at which typical problems and solutions to problems encountered in everyday operations are discussed.

When use is made of logging, steps should be taken to ensure separation of the roles of administration and auditing. The extent to which this objective is supported by the IT systems must be checked in this context.

To ensure continuity of service when an Administrator is absent, a deputy must be appointed. Care must be taken here to ensure that the deputy is given his own Administrator ID (see also S 2.38 *Division of Administrator Roles*). Under no circumstances should the password simply be handed over to the stand-in because that is less trouble.

In order that such deputies can take over these functions, it is necessary to ensure that every Administrator and his deputy have sufficient time to carry out their tasks with due care. Training and further education of Administrators are also required in this regard.

Additional controls:

- Have all Administrators and their deputies been adequately trained?
- If responsibilities for administrative tasks have been changed, have the necessary training measures been initiated?

S 2.27 Dispensing with remote maintenance of the PBX

Initiation responsibility: Head of IT Section; IT Security Management; PBX officer

Implementation responsibility: -

Dispensing with remote maintenance is an effective measure to prevent external persons from manipulating the PBX installation configuration. For individual installations and small networks of interconnected installations with short spatial distances between their individual members, this approach is expedient also for economic reasons.

Advantage: As opposed to all other measures listed in Part I, Chapter 8.1 Telecommunications System (Private Branch Exchange), this approach can ensure that access to the servicing port of the installation will be precluded even in case of direct access to the lines of the *Telekom*. Otherwise, a similar degree of security could only be achieved with the help of cryptological means.

Disadvantage: All maintenance work must be carried out directly on the facility. Failing any additional measures, e.g. removal of the maintenance PC to the adjacent room, the maintenance staff will always have access to the PBX facility as well. The remote interfaces are often not only used for remote maintenance. Remote signalisation needed for the operation of the PBX network is occasionally carried out via the same interfaces. In such cases, dispensing with remote maintenance would mean dispensing with central network management. If a remote interface is only to be used for remote signalisation purposes via modem, this modem should be configured in such a way that calls cannot be received.

Additional controls:

- Which reasons speak for and which reasons speak against the relinquishment of remote maintenance?
- Has a corresponding decision on remote maintenance been made?

S 2.28 Availability of external telecommunications advisory services

Initiation responsibility: Head of IT Section; IT Security Management; PBX officer

Implementation responsibility: -

In order to be able to make quick use of expert assistance, consideration should, already at the time of the purchase or renting of a PBX facility, be given to the provision of appropriate advisory services. An important requirement is for assistance to be rendered promptly in an emergency since failure of a PBX facility can significantly impair the functioning of an entire institution and might be tolerable only for a short period of time.

Additional controls:

- For how long will it be possible to do without the PBX?
- Within which time can assistance be furnished by the manufacturer?
- How much time is needed for a complete restart of the facility on the basis of available data backups?

S 2.29 PBX operating instructions for users

Initiation responsibility: Head of IT Section; IT Security Management; PBX officer

Implementation responsibility: Administrators

The required documents for the operation of the terminal equipment (e.g. telephone operating instructions) must be made available to the PBX (telecommunications) user. In addition to normal operation of his telephone, the user should, above all, also be able to interpret any warning signals (LEDs or icons on the display) and acoustic alarm signals (cf. S 3.12 *Informing all staff members about possible PBX warning notices, warning symbols and acoustic alarm signals*).

Additional controls:

- Has all terminal equipment been furnished with the proper operating instructions?
- Is the user able to make correct use of the user facilities available to him?
- Does the user know the warning signals and acoustic alarms?

S 2.30 Provisions governing the designation of users and of user groups

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Provisions governing the designation of users and of user groups are the prerequisite for adequate allocation of access rights and for ensuring orderly and controlled operations.

A blank form should be in existence so that, as a first step, the required data can be obtained from each user or each user group:

- Surname, first name
- Proposed user name and group ID, if not already allocated by convention,
- Organisational unit
- Reachability (e.g. telephone, room)
- If applicable: project
- where appropriate, information on the planned activity within the system and the rights required for that purpose and on the duration of the activity;
- where appropriate, restriction on times, terminals, disk volumes, access rights (for certain directories, remote access, etc.), restricted user environment;
- If applicable: Approval by superiors

If access rights are provided which go beyond those provided as standard, this must be justified. This can also be done by electronic means, e.g. by a special log-in, the name and password of which will be made known to the designated users. There, a pertinent program will be run which ends with a log-out. A print-out may be made of the recorded data for submission to the superior. A password given to a new user for first-time use of the system must be altered after that use. This should be initiated by the system.

A limited number of authorisation profiles must be specified. A new user will then be assigned to such a profile and thus obtain the exact authorisation required for his activity. In this regard, the system-specific options will have to be taken into account when configuring users and groups. It is advisable to lay down naming conventions for the names of users and groups (e.g. user ID = initials of organisational unit serial number).

Authorisation to have access to files must be confined to users and/or groups having a justified interest. If several persons have to access a given file, a group should be established for these users. As a rule, every user must be assigned his own user ID; no ID must be used by several users. A home directory must be provided for each user.

For user/group configuration within a system, an administrative role should be established: configuration should be effected by means of a special log-in under which an appropriate program or shell script is started. Thus, the responsible administrators can configure users and/or user groups only in a

specified manner, and there is no requirement for granting them rights for other administrative tasks.

This measure is complemented by the following:

- S 4.13 Careful allocation of identifiers
- S 4.19 Restrictive allocation of attributes for UNIX system files and directories
- S 4.20 Restrictive allocation of attributes for UNIX user files and directories

Additional controls:

- Are there any organisational provisions governing the configuration of users or user groups?
- Is there any program for the configuration of users or user groups?

S 2.31 Documentation on Authorised Users and on Rights Profiles

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

Such documentation serves to provide an overview of the authorised users, user groups and rights profiles and is required for effective monitoring.

The following three means of providing documentation should all be used:

- generic administration files provided by the system,
- individual files administered by the responsible Administrator,
- hard copies.

In particular, the following should be documented:

- authorised users together with the following details: assigned rights profile (plus any deviations from the standard rights profile used), reasons for selecting that particular rights profile (plus any deviations, if applicable), user contact details, date and reason for configuring this user, and any time limits;
- authorised groups, together with details of the relevant users, date and reason for configuration, plus any time limits.

The documentation regarding the authorised users and rights profiles should be checked at regular intervals (at least every six months) to see whether it reflects the actual situation regarding the granting of rights and whether the assignment of rights still matches the security requirements and the current tasks of the users.

Additional controls:

- Are there records of the authorised users and groups and their authorisation profiles?
- Are the records up to date?
- When were the records last checked?
- Are the records adequately protected against unauthorised access?

S 2.31 Documentation on authorised users and on rights profiles

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Such documentation is to give a survey of the authorised users, user groups and authorisation profiles and is a prerequisite for controls.

All of the following three means of providing documentation should be used:

- generic administration files provided by the system;
- individual files administered by the responsible administrator;
- hard copies.

In particular, the following are to be documented:

- authorised users, with the following details: assigned authorisation profile (in the given case, deviation from the used standard authorisation profile); reasons for selecting that particular authorisation profile (and any deviations, where appropriate); where the user can be reached; time of, and reason for, the configuration; any time limits;
- authorised groups, with the respective users; time of, and reason for, the configuration, and time limit.

Additional controls:

- Have any records been made of the authorised users and groups and of their authorisation profiles?
- Are the records up to date?

S 2.32 Establishment of a Restricted User Environment

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

Where users only have specific tasks to perform, it often will not be necessary to grant them all the rights associated with their own log-in (possibly even Administrator rights). Examples are certain activities of routine system administration (such as making backups, designating a new user) which are carried out using a menu-driven program, or activities for which the user needs only a single application program. Especial care should be taken where temporary employees are involved, to ensure that they are only allowed to use the services and to access the files which they actually need. When they cease working, their accounts should be deactivated and all other access rights should be revoked (see also S 4.17 *Blocking and Deletion of Unnecessary Accounts and Terminals*).

For these users, a restricted user environment should be established. This can be achieved, for instance, under UNIX with a *restricted shell* (*rsh*) and the restriction of access paths with the UNIX command *chroot*. For a user needing only one application program, this can be entered as a log-in shell so that it is started directly after he logs on, and he is automatically logged off on exiting the program.

The available range of functions of the IT system may be restricted for individual users or user groups. Use of editors or compilers should be prevented unless the user actually needs these to perform his tasks. This can be achieved on stand-alone systems by the removal of such programs and, on networked systems, by the allocation of rights.

Additional controls:

- What user environment and what start-up procedure have been defined for the respective users?
- Are there any procedures regarding user environments in which temporary staff are employed?

S 2.32 Establishment of a restricted user environment

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Where users only have specific tasks to perform, it often will not be necessary to grant them all the rights associated with their own log-in (possibly even Administrator rights). Examples are certain activities of routine system administration (such as making backups, designating a new user) which are carried out using a menu-driven program, or activities for which the user needs only a single application program.

Use *restricted shell* and *chroot*

For these users, a restricted user environment should be established. This can be achieved, for instance, under UNIX with a *restricted shell* (*rsh*) and the restriction of access paths with the UNIX command *chroot*. For a user needing only one application program, this can be entered as a log-in shell so that it is started directly after he logs on, and he is automatically logged off on exiting the program.

Restrict use of editors and compilers

The available range of functions of the IT system may be restricted for individual users or user groups. Use of editors or compilers should be prevented unless the user actually needs these to perfom his tasks. This can be achieved on stand-alone systems by the removal of such programs and, on networked systems, by the allocation of rights.

Additional controls:

- What user environment and what start-up procedure have been defined for the respective users?

S 2.33 Division of Administrator roles under UNIX

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

In most UNIX systems, there is only one Administrator role (the *superuser*, who is known as *root* and has the user ID (UID) *0*). Persons with access to this role have full control over the system. In particular, they can read, modify and delete any file, irrespective of access rights.

The *superuser* password must only be known to the Administrators. Disclosure of that password must be restricted to the cases defined in the pertinent procedures, and must be documented. The superuser log-in *root* can additionally be protected by applying the two-person rule, e.g. through organisational measures such as a split password. In that case, the password must have an extended minimum length (12 characters or more). Steps must be taken to ensure that the password, in its full minimum length, is checked by the system.

For a number of UNIX systems, division of responsibilities can be achieved by making use of existing Administrator roles. In such cases, those roles must be assumed by different persons.

A number of administration activities can also be carried out without access to the *root* log- in. Where Administrators with such special functions exist, use should be made of this option. Especially in those cases where, for large systems, administration functions have to be assigned to several persons, the risks involved can be reduced through appropriate division of responsibilities. This can be done in two ways:

- Introduction of administrative log-ins. While these have the UID *0*, only one program will be started during log-in, with which the administrative function can be executed and which ends with a log-out. Examples: designation of new users, mounting of a drive. In UNIX V.4, for example, the administrative log-in names *setup*, *sysadm*, *powerdown*, *checkfsys*, *mountfsys* and *umountfsys* may be configured with programs of identical names.
- Use of log-ins without the UID *0*: These log-in names (*sys*, *bin*, *adm*, *uucp*, *nuucp*, *daemon* and *lp*) are owners of files and programs which are crucial for the functionality of the system and thus are afforded particular protection. In most UNIX systems, they have been preconfigured for administration of the relevant services.

To determine which log-ins have Administrator rights, auxiliary programs such as USEIT, *cops*, *tiger* should be used regularly to search for log-ins which contain UID *0* in the password file.

Additional controls:

- Who knows the *superuser* password?
- Have Administrator roles been split up?
- Which log-ins have the UID *0*?
- Are there any log-ins with UID *0* and shell access?

S 2.34 Documentation of changes made to an existing IT system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Overview of the system

In order to ensure smooth operation, the Administrator must have, or be able to obtain, an overview of the system. In the event of an unforeseen absence of the Administrator, such an overview must also be available to his deputy. It is also essential to have an overview when making checks of the system (e.g. for problematic settings, consistency in changes).

Therefore, the changes made by Administrators to a system should be documented. If possible this should be automated. This applies, in particular, to changes made to system directories and files.

New operating systems or updates

When installing new operating systems or in case of updates, the changes made should be documented especially carefully. Activation of new, or modification of existing, system parameters may also fundamentally change the behaviour of the IT system (especially security functions).

Approval and documentation of executable files

Under UNIX, executable files to which users other than the owner also have access, or whose owner is *root*, must be approved and documented by the System Administrator (cf. also S 2.9 *Ban on the use of non-approved software*). In particular, lists of the approved versions of these files, which in addition must as a minimum contain the creation date, the size of each file and information on any *s* bit settings, must be kept. They are the prerequisite for regular security checks and for investigations following a loss of integrity.

Additional controls:

- Are log books kept of system changes?
- Are the records up-to-date and complete?
- Can the administration functions be continued on the basis of those records?
- Have the records been protected against unauthorised access?

S 2.35 Obtaining information on security weaknesses of the system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

To counter security flaws that have become known or have been disclosed in publications, the required organisational and administrative measures must be taken and/or additional security hardware or software must be employed.

It is therefore very important to obtain information on vulnerabilities which have recently become known. Sources of such information include:

- Bundesamt für Sicherheit in der Informationstechnik (BSI), P.O.B. 20 03 63, D-53133 Bonn; telephone: 0228-9582-444, fax:-427, E-Mail: *cert@bsi.de*, WWW: *http://www.bsi.bund.de/bsi-cert*
- Manufacturers or distributors of the operating system inform registered customers about security flaws identified on their systems and provide them with updated versions of the system or patches for remedying those security flaws.
- Computer Emergency Response Teams (*CERT*s) are organisations which supply information on operating system flaws identified and on how to remedy them.

  Computer Emergency Response Team / Coordination Center (CERT/CC), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890,

  Tel. ++1+412 268-7090 (24 hour Hotline), E-Mail: *cert@cert.org*, FTP: *ftp://ftp.cert.org*, WWW: *http://www.cert.org*

  CERT messages are published in *News Groups* (*comp.security.announce* and *info.nsfnet. cert*) and through *mailing lists* (inclusion by E-mail for transmission to: *cert-advisory-request@cert.org*).
- CERT in Germany:
  - BSI-CERT, Bundesamt für Sicherheit in der Informationstechnik (BSI), P.O.B. 20 03 63, D-53133 Bonn; telephone: 0228-9582-444, fax: -427, E-Mail: *cert@bsi.de*
  - DFN-CERT, Hamburg University, Computer Science Department, Vogt-Kölln-Strasse 30, D-22527 Hamburg, tel. +49 40-54715-262, fax -241,

    E-mail: *dfncert@cert.dfn.de*,

    FTP: ftp://ftp.cert.dfn.de/pub.security

    WWW: http://www.cert.dfn.de

    gopher: gopher.cert.dfn.de,

    Inclusion in the mailing list for CERT messages by E-mail to: *dfncert-request@cert.dfn.de*

Mailing lists for discussions: *win-sec@cert.dfn.de*

Mailing lists for security information: *win-sec-ssc@cert.dfn.de*

- Micro-BIT Virus Centre/CERT, Karlsruhe University, P.O. Box 6980, D-76128 Karlsruhe, tel. +49 721/-376422; fax +49 721/-32550; e-mail: *cert@rz.uni-karlsruhe.de*

- There are also manufacturer and system-specific news groups and mailing lists, such as the English language BUGTRAQ (to join the mailing list, send an e-mail to *listserv@securityfocus.com).*
- IT trade journals

Additional controls:

- Is the Administrator in regular contact with the manufacturers of the systems in his charge? Have these systems been registered? Have maintenance contracts been concluded?
- Have all known information sources been used?
- Are new information sources identified?
- Are published security flaws remedied as soon as possible?

S 2.36 Orderly issue and retrieval of a portable (laptop) PC

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

When issuing and recovering a portable PC, the following points must be borne in mind:

Issue:

- The requirement for using a portable PC for professional purposes should be verified beforehand.
- A new user will, at the time of issue, be immediately requested to change the previous password of the portable PC or to alter the standard password.
- A new user will be provided with a leaflet on the secure handling of a laptop PC (optional).
- The name, organisational unit, telephone number, operational requirement of the new user will be entered in the issue/retrieval daybook.

Retrieval or passing-on

- The user will communicate his last password, or will set up a standard password such as "LAPTOP".
- The completeness of the equipment, accessories and documentation is to be ensured.
- Before hand-over, users must ensure that the data still required by them are transferred to data media accessible by them (e.g. personal PC). In addition, users must ensure that all files and data generated by them are deleted (preferably physically).
- The recipient must check the laptop PC for infection by computer viruses by means of an up-to-date virus detection program.
- Return of the laptop PC, including the findings of the virus scan, must be documented.
- Returned floppy disks must be re-formatted. When formatting DOS data media, it should be ensured that the parameter */U* is used (contained in DOS 6.2) so that the formatting cannot be undone using the command unformat.

Additional controls:

- Is passing-on of laptop PCs to colleagues being documented?
- Are the pertinent security measures being complied with?

S 2.37 Clean desk policy

Initiation responsibility: Head of Organisational Section; IT Security Management

Implementation responsibility: Staff members

All staff members should be encouraged to leave their desks "neat and tidy". An IT user does not only have to see to it that, when leaving his workplace, the appropriate arrangements have been made to prevent unauthorised persons from having access to IT applications or to data; but he must also just as conscientiously check his workplace and must ensure that no loss of availability, confidentiality or integrity will be entailed by any access of unauthorised persons to data media (diskette, hard disk) or to documents (print-outs). .

For short absences during working hours, it will suffice to lock the room; outside working hours, the workplace must be tidied up so that no media or documents requiring protection that are not locked away, will be left behind at the workplace.

S 2.38 Division of administrator roles in PC networks

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Many networked systems offer the possibility to divide the administrator role and to allocate administrator activities to various users.

Thus, for instance, the following administrator roles can be set up under *Novell Netware 3.11*: Workgroup Manager, User Account Manager, File Server Console Operator, Print Server Operator, Print Queue Operator.

Defined administrator roles can be created under Windows NT for individual users or better for groups by the controlled allocation of user privileges. Besides the administrator group, the following must be mentioned: power users (i.e. administrators with restricted privileges), backup-operators, print-operators, server-operators and replicator-operators. Additionally, further roles can be defined via the explicit allocation of user privileges (see also S 4.50 *Structured system administration under Windows NT*).

Where administrator roles exist for specialised tasks, they should be made use of. Especially when in large systems where administration tasks must be entrusted to a number of persons, the risk of the administrator roles holding excessive powers of control can be reduced by an appropriate division of responsibilities so that administrators will not be able, without being subject to control, to make unauthorised or unintentional changes to the system.

Despite the division of administrator roles, the system will in most cases automatically set up an account for an administrator not subject to any restrictions, i.e. the *supervisor*. The supervisor password may be known only to a small number of people. It must not be known to any of the sub-administrators so as to prevent the latter from expanding their rights in this way. The password must be safely deposited (see S 2.22 *Depositing of passwords*). The supervisor log-in can be additionally protected by the application of the two-person rule, e.g. by means of organisational measures such as a split password. In that case, the password must have an extended minimum length (12 characters or more). It must be ensured that the password, in its full minimum length, will be checked by the system.

Additional controls:

- To which persons is the supervisor password known?
- Have administrator roles been divided up?

S 2.39 Response to violations of security policies

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: IT Security Management

The response to violations of security policies should be laid down so as to ensure a clear and prompt response.

Investigations should be carried out to establish how and where such violation has originated. Subsequently, the appropriate measures must be taken to remedy or minimise the damage caused. If required, additional loss-prevention measures must be taken. The action to be taken will depend both on the nature of the violation and on the offender.

Provisions must be laid down on who is responsible for contacts with other organisations for the purpose of obtaining information on known security flaws (cf. also S 2.35 - *Obtaining information on security weaknesses of the system*) or of passing on information about recently detected security breaches. Care must be taken to inform any other possibly affected units/agencies by the fastest means possible.

Additional controls:

- Has the approach to be taken in case of suspected violations of security policies been clearly defined?

S 2.40 Timely involvement of the staff/factory council

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: IT Security Management

Measures suitable for monitoring the conduct and performance of an employee, e.g. keeping records, also require the approval of the staff council. The precepts of this body are stipulated in state and federal regulations for factory and staff operations. The submission of timely and comprehensive information to the staff/factory council can prevent delays in the implementation of IT security measures.

S 2.41 Employees' commitment to data backup

Initiation responsibility: Agency/company management

Implementation responsibility: IT Security Management

Data backup is an important IT security measure. For this reason, the relevant employees must be committed to adherence to data backup/minimal data backup concepts. Regular refresher and motivation campaigns on data backup must be conducted.

Additional controls:

- Are commitments to data backup documented in writing?
- Is adherence to data backup concepts being checked?

S 2.42 Determination of potential communications partners

Initiation responsibility: Head of IT Section, IT Security Management, Data privacy officer

Implementation responsibility: IT Security Management

If information is to be transferred to a communications partner, it must be ensured that the recipient has the authorisation required for processing this information. If information is exchanged between several communicating points, all participants should be able to identify who received or will receive the information. To meet the above-mentioned criteria, specifications must be made as to which communication partners may receive what information.

In accordance with the Federal Data Protection Act (BDSG), Appendix to § 9, Section 1 (Transfer Control), a list of persons authorised to receive information - particularly personal data - via the exchange of data media should be prepared.

Additional controls:

- Do specifications for communication relations exist?
- Are the above-mentioned lists updated regularly?

S 2.43 Adequate labelling of data media for dispatch

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

In addition to the measures stated in *S 2.3 (Data media control)*, adequate labelling of data media to be exchanged should include clear identification of the sender and (all) recipients. The labelling must allow the recipient to clearly recognise the contents of the data medium. In the case of confidential information, however, it is important that unauthorised persons be unable to interpret the labelling.

In addition, the data media should be labelled with the **parameters necessary** for reading. When transferring magnetic tapes, for instance, the labelling should include the identifier, speed (e.g. 800 bpi), record length, block length and record format (e.g. 132 bytes, 13200 bytes, fixed).

The date of dispatch as well as version numbers or key features can also prove useful.

Additional controls:

- Are there regulations on the labelling of data media destined for transfer?
- Is adherence to labelling regulations checked sporadically?

S 2.44 Secure packaging of data media

Initiation responsibility: IT Security Management

Implementation responsibility: IT users, Mailroom

In addition to the implementations stated in measure *S 2.3 (Data media control)*, the packaging of the data media should be designed to reveal manipulations.

Possible measures in this respect include:

- Sealed envelopes
- Lead-sealed containers or
- Envelopes sealed with an adhesive film and then marked irregularly several times with non-soluble ink.

If the data medium has a write protection facility (slides for disks, rings for tapes), this should be used. If manipulation detection of the information on the data medium are established, encryption or checksum procedures should be implemented (c.f. 4.34 *Using encryption, checksums or digital signatures*).

Additional controls:

- Are appropriate containers stipulated and available for the secure transport of data media?
- Do these containers allow recipients to check whether the contents have been manipulated?

S 2.45 Controlling the exchange of data media

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT users, Mailroom

If data media are to be exchanged between two or more communication partners, the following items should be observed to ensure proper exchange:

- Addressing must be clear so as to preclude incorrect delivery. In this context, the recipient's name should be supplemented by the relevant department and the precise designation of the agency/company. The same applies to the address of the sender.
- The data medium should be accompanied by a slip containing the following information (optional):
  - Sender
  - Recipient
  - Type of data medium
  - Serial number (if present)
  - Identification of the contents of the data medium
  - The date of dispatch and, if applicable, the latest date by which the storage medium should reach the recipient
  - A note that the data medium has been scanned for viruses
  - Parameters required for reading the information, e.g. tape speed

  The following items should not be indicated:
  - Passwords allocated to classified information
  - Encryption keys used for encrypting information
  - Contents of the data medium
- The dispatch of the data medium can be documented optionally. In this case, every file transfer, together with the contents and recipient of the information, is registered in a log. Depending on the protection requirement or importance of the transferred information, its receipt should be acknowledged and an acknowledgement statement added to the aforementioned record.
- Persons responsible for dispatch and receipt should be designated
- The type of dispatch is to be specified

Additional controls:

- Do regulations on the procedure of exchanging data media exist?
- Are the persons responsible for the exchange of data media sufficiently aware of the potential threats involved?

S 2.46 Appropriate key management

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management, IT Procedures Officer

The use of cryptographic security mechanisms (such as encryption or digital signatures) requires that suitable keys must be created, distributed and installed using confidential and authenticated procedures, with integrity ensured. Keys which have become known to unauthorised users, which have been corrupted in the course of distribution or which perhaps even originate from uncontrolled sources (this also applies to the agreement of keys between communication partners) are just as capable of compromising a cryptographic security mechanism as poor quality keys which have been generated in an unsuitable way. Good quality keys are usually created using suitable key generators (see below). Attention must be paid to the following points regarding key management:

Key generation

Key generation should be performed in a secure environment using suitable key generators. Cryptographic keys can either be generated directly at the place where they are used (usually initiated by the user) or they can be generated at a central location. When keys are generated locally, it usually has to be accepted that the security of the environment will be less stringent, whereas when keys are generated centrally it must be ensured that they reach their users authentically and without being compromised.

Suitable key generators must produce controlled, statistically evenly distributed random sequences, making use of the entire possible key space. To do this, for example, a noise source generates random bit sequences, which are post-processed with a logic unit. The quality of the keys obtained in this way is then examined using a variety of test procedures.

Some crypto modules, especially those which do not have an integrated random number generator, make use of user inputs for the generation of keys. For example, these modules may ask for passwords from which a key is subsequently derived, or the user is prompted to type in an arbitrary text in order to obtain random starting values for generating a key. Passwords used in such circumstances should be carefully chosen and as long as possible. If users are requested to make entries that are as random as possible, they should really be random, in other words difficult to predict.

Separation of keys

If possible, cryptographic keys should be employed for only one purpose. In particular, it is important never to use the same keys both for encryption and for the generation of signatures. This makes sense for a number of reasons:

- If one key is disclosed, only some procedures will be affected, not all of them.
- It may sometimes be necessary to divulge encryption keys (when a deputy or substitute is used).

- There may be different cycles for changing keys.

Distribution and exchange of keys

Cryptographic communications relationships can only work if the communicating partners have matched cryptographic keys at their disposal. For this to be possible, all communicating partners must be provided with the necessary keys. Various procedures can be used for distributing keys and for exchanging keys. The differences arise from the use of different cryptographic techniques and mechanisms, or from the combination of such techniques and mechanisms (see S 2.164 *Selection of a suitable cryptographic procedure*). In this case the term key distribution refers to the initial provision of basic keys to communication partners. For this, the keys are transferred to the individual communication partners from a (usually central) key generation point, for example a Trust Center.

The keys should be distributed on suitable data media (e.g. chip cards) or via communications links (e.g. LAN or WAN) in a form which ensures confidentiality (e.g. encrypted with a KEK - key encryption key), integrity (e.g. MAC-secured) and authentication (e.g. with a digital signature in accordance with the signature law). Gaining unauthorised knowledge of the keys or corruption of the keys must be prevented, or it must at least be possible to detect such an event.

The exchange of keys refers to the key agreement procedure between two communication partners to generate a session key. The session key is a key that is used for only a limited time, such as for the duration of a communication connection. This length of time must be specified, because sessions can last a very long time. The time can be specified by relative timing, for example, or by a packet counter. A new session key is negotiated between the communication partners for every new connection.

Advanced systems nowadays make use of asymmetric cryptographic procedures for key distribution and key exchange. A trustworthy certification body can be established to prove the authenticity of the public keys. The communication partners must identify themselves to the certification body and have their public keys certified there by means of a digital signature from the certification body. The digital certificate generated in this way should contain at least the public key and an identification feature specific to the communication partner, the period of validity of the certificate and the digital signature from the certification body. Knowledge of the public signature key of the certification body puts every communication partner in a position to verify the authenticity of the public key of the other party with whom they are communicating.

Installing and storing keys

In the course of key installation it is necessary to check the authentic origin and integrity of the key data. As a general rule, keys should never be stored in the system in plain form but always in encrypted form. When using software encryption products, it must be borne in mind that keys are inevitably present in plain form on the PC system at least temporarily during the encryption/decryption process. If the IT systems on which the cryptographic product is being used do not offer adequate access protection for the keys,

they should not be stored on those systems. In that case, manual entry as needed is the obvious answer. Another possibility would be to transfer the keys to an external data medium, which would then have to be kept securely, however, as described in the section on the archiving of keys. From the security point of view, therefore, preference is to be given to the use of hardware encryption components, where the keys are loaded directly into the encryption component from the data medium (such as a chip card) and never leave the encryption component in unencrypted form.

It must always be ensured that preset keys are changed on installation of the encryption procedure.

Archiving of keys

For the purpose of archiving, it should also be possible to store the cryptographic key material outside the crypto module in an encrypted form, and if necessary reload it. To do this, several keys can be combined in one record, which is then likewise encrypted with the aid of a KEK (key encryption key). Accordingly, the KEK must also be kept securely (for example on a chip card in a safe). If the KEK is split into two partial keys, the two-person rule can be implemented: two different people each have access to a separate data medium (e.g. a chip card or floppy disk) on which only one of the two partial keys is stored. In order to generate the KEK, both data media must be inserted in the crypto module's reading unit at the same time or immediately one after the other.

Access and deputisation arrangements

Matters relating to access rights and deputisation rights should be settled in the security policy. The relevant mechanisms must be supported by key management and by the crypto modules and devices that are to be used (e.g. key escrow in the event that a member of staff leaves the company or is absent for a long period due to illness; see also archiving of keys).

Changing keys

Details of when and how often keys need to be changed must be laid down in the crypto concept, on the basis of the security policy. The larger the quantity of encrypted data that is available to an attacker for analysis, the greater the chance with some algorithms that the analysis process will be successful. Changing keys on a regular basis minimises the opportunities for attacking encrypted data. The frequency of changing is dependent on a variety of factors. The type of encrypted medium (for example long-term data medium or data transmission medium) is just as significant as the cryptographic algorithm, the detection of attacks (such as theft of loss of a key) and the degree to which the data is worth protecting. Other factors playing a part in determining the frequency of change are how often the key is used, the relevant threat potential and the security of the local key storage facility.

Depending on which procedure is used, new keys have to be negotiated for every single communication connection, i.e. session keys have to be used. This should of course be controlled by the procedures, without the user noticing. Changing keys in this case means exchanging the master keys that form the basis on which the session keys are generated, and should of course also be carried out regularly.

If a key being used is suspected of having been disclosed, its use should be discontinued and all participants should be informed. Information already encrypted with this key should be decrypted and encrypted with a different key.

Destroying keys

Keys which are no longer required (for example keys whose period of validity has expired) must be deleted in a secure manner or destroyed (for example by multiple deletion/overwriting and/or mechanical destruction of the data medium). A general rule is that products with a key filing system that cannot be controlled should not be used.

Additional controls:

- Has responsibility for encryption management been designated?
- Is the data that needs to be protected transferred separately from the encryption keys?
- Are the keys in use changed frequently enough?
- Are the keys stored in a secure local environment?

S 2.47 Designating a person in charge of the fax system

Initiation responsibility: Head of Internal Services, Superiors

Implementation responsibility: Internal Services Division

Every fax machine is to be assigned to a person-in-charge who will have the following responsibilities:

- Distribution of incoming fax messages to recipients
- Co-ordinating the supply of consumable accessories required by the fax machine
- Suitable disposal of consumed fax accessories
- Deletion of remaining information in the fax machine prior to service and repair work,
- Monitoring of service and repair works (c.f. S 2.4 *Maintenance and repair regulations*),
- Regular checking of program destination addresses and protocols, particularly after service and repair works,
- Serving as a contact partner for problems occurring during fax usage

Additional controls:

- Has the person in-charge of fax machines been briefed on the duties involved?
- Is the reliability of this person checked from time to time?

S 2.48 Designating authorised fax operators

Initiation responsibility: IT Security Management

Implementation responsibility: Internal Services Division

Authorisation to use a fax machine is to be restricted to a selected group of reliable employees. These employees are to be briefed on the correct usage of the device and the required IT security measures. Every authorised user is to be notified of the other entitled users and the person in-charge of the fax machine. The fax machine should be accompanied by a comprehensive manual.

By restricting the group of fax operators to the minimum number necessary for operation, it is possible to minimise the number of persons who are able to view incoming fax messages.

Additional controls:

- Does the selected number of fax operators restrict operations?
- Is every user notified of the remaining persons authorised to use the fax machine?

S 2.49 Procurement of suitable fax machines

Initiation responsibility: IT Security Management

Implementation responsibility: Procurer

When new fax machines are purchased, it should be ensured that the following standard security features are included:

- Exchange of subscriber ID's
- Transmission report
- Journal keeping

Taking the price/performance ratio into account, the following additional security features are recommended:

- Access protected with a password
- Buffer memory protected with a password
- Configuration of a closed user group
- Exclusion of certain fax connections from sending and receiving

Additional controls:

- Are security features considered as exclusion criteria for the procurement of new fax machines?
- Are additional security features on newly procured fax machines appropriate in terms of the relation between the price and the degree of protection required?

S 2.50 Appropriate disposal of consumable fax accessories and spare parts

Initiation responsibility: Head of Internal Services, IT Security Management

Implementation responsibility: Fax Officer

All fax consumables from which information on fax messages might be derived, e.g. intermediate foils and faulty printouts, must be destroyed before disposal, or disposed of by a reliable and specialised company.

The same applies to the exchange of information-bearing spare parts, e.g. photoelectric drums.

Maintenance companies which periodically maintain or repair the fax machines are to be committed to appropriate handling and checked, if required.

Additional controls:

- How are the fax consumables which are no longer required disposed of?
- Have the persons responsible for the fax machines been briefed on the protection requirements and various possibilities of the material which is to be disposed of?

S 2.51 Producing copies of incoming fax messages

Initiation responsibility: Fax Officer

Implementation responsibility: IT-user

Fax messages printed on thermal paper can fade considerably or turn black after a certain period of time. As a result, copies on normal paper should be made of incoming fax messages whose information content is need for extended periods.

Additional controls:

- Does the company/agency possess fax machines using thermal paper?
- Are important incoming fax messages copied?

S 2.52 Supply and monitoring of consumable fax accessories

Initiation responsibility: IT Security Management, Head of Internal Services

Implementation responsibility: Fax Officer

Users should be instructed to notify the person in-charge of fax machines when fax consumables (e.g. paper, toner) have to be refilled. The person-in-charge should personally carry out such checks at regular intervals (according to requirement, but at least once a month). The person-in-charge should also ensure an adequate supply of fax consumables.

Additional controls:

- Has responsibility for the supply of fax consumables been delegated?
- Are consumables frequently present in insufficient amounts?

S 2.53 Deactivation of fax machines after office hours

Initiation responsibility: IT Security Management, Fire-Protection Officer

Implementation responsibility: Fax Officer

To reduce the perpetual danger of fax machines catching fire, devices not required outside working hours (personal or departmental fax machines) should be turned off after office hours. This also prevents incoming fax messages from remaining inside fax machines for unnecessarily long periods of time. These machines can be turned off easily by means of timers which disconnect the power supply outside normal working hours.

A different (and, if possible, constantly monitored) fax connection can be allocated, or a call-forwarding feature can be activated on modern telecommunications systems for fax messages arriving outside working hours.

Turning off fax machines also prevents them from being overloaded due to technical failure or intentional "flaming" outside working hours.

This type of deactivation should not be allowed for fax machines required for purposes which cannot be fulfilled by the alternative solutions.

Additional controls:

- Which fax machines need to remain active outside office hours?
- Are the remaining devices turned off?
- Is a call-forwarding feature available?

S 2.54 Procurement/selection of suitable answering machines

Initiation responsibility: Agency/company management

Implementation responsibility: Site technical service, purchase department

This measure is to be observed for the procurement of new answering machines. If existing devices do not meet security requirements, their disposal and the procurement of new ones is to be considered.

To reduce threats to a minimum, the following criteria should be observed during the purchase of answering machines, taking their price/performance ratio into consideration:

- The devices must be authorised by the Federal Post in order to ensure trouble-free telecommunication.
- In the case of devices with a fully or partially digital memory, it is recommended to select those which are equipped with an emergency power supply consisting of a battery pack or removable accumulator. Permanently integrated accumulators need to be replaced by a service technician, and this procedure entails longer deactivation periods for the answering machine.
- Due to variations in the quality of message recording (e.g. by analogue or digital units), the performance of answering machines in this context should be checked before purchase.
- Devices with a fully or partially digital memory should be equipped with a display for indicating the battery charge and a distinct warning signal (if possible, acoustic) for timely indication of low battery charges.
- Answering machines which use a single cassette for incoming as well as outgoing messages require longer waiting periods for tape winding. The acceptability of this extra time should be weighed.
- The user-friendliness of answering machines should be evaluated. Ergonomic and clearly arranged buttons, single-function keys and easily understandable manuals are advantageous in this respect.
- If possible, the remote-inquiry unit should have a mechanical or electronic deactivation function, and the security code should consist of at least three or four digits and be freely programmable. Increased security is offered by a disabling circuit which interrupts the connection to the answering machine after three invalid entries of the security code. This at least increases the time required by would-be perpetrators and the telephone charge incurred by them. An even greater advantage is offered by devices which completely disable the remote-inquiry function after three invalid attempts and only allow this function to be restored on the answering machine itself. The prolongation of the disablement periods after each successive invalid entry is also advantageous.

Additional controls:

- Is the purchasing department aware of the above-mentioned instructions?

S 2.55 Use of a security code

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

For answering machines with a remote-inquiry unit and a security code, the remote-inquiry function should preferably be activated only by means of an individually selected, secret code. In particular, any factory codes should be altered. The security code should be deposited in the same way as a password (c.f. S 2.22 *Depositing of passwords*) and altered on a regular basis.

When operating answering machines with a remote-inquiry unit, care should be taken to prevent entry of the code from being heard or viewed by any strangers present in the vicinity.

Additional controls:

- Have users been instructed on correct handling of the remote-inquiry unit?

S 2.56 Avoidance of confidential information on answering machines

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

At present, it is not possible to protect answering machines completely against possible misuse. For this reason, the recording of confidential information should be avoided; moreover, in situations typically involving the regular exchange of confidential information, the use of answering machines should be carefully judged. Consequently, outgoing messages should point out the inexpediency of leaving confidential messages on the answering machine.

Additional controls:

- Are persons leaving confidential messages aware of the associated risks?
- Are answering machines installed in areas where confidential information is often exchanged?

S 2.57 Regular playback and deletion of recorded messages

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

Messages recorded on answering machines should be played back and deleted regularly. If deletion is not possible on analogue recording units, the magnetic tape should be rewound to the beginning so that old messages are overwritten by new ones.

S 2.58 Limitation of message time

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

To prevent premature exhaustion of the storage capacity, the duration of incoming messages should be limited to a maximum of 2-4 minutes, if the device allows such an adjustment.

S 2.59 Procurement of a suitable modem

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT users, Administrator, Purchasing

The following items are to be observed for the purchase of a modem:

- Modem approval

  Modems intended for connection to the public telecommunications network in the Federal Republic of Germany require authorisation by the Federal Post. Note: Contrary to information in many modem manuals, commissioning of an approved modem in the Federal Republic of Germany need no longer be reported to the telephone utility (Telekom).

- Design

  An internal modem is advantageous in that its configuration can only be changed on the computer in which it is integrated. If this computer has access protection features, they can be used to safeguard the modem configuration data. At the same time use of the modem can be restricted to authorised persons. Manipulation of an internal modem is difficult due to its integration in the computer. In networked systems devoid of such protective mechanisms (e.g. some Peer-to-Peer networks), internal modems are disadvantageous due to the possibility of their unregulated operation from all workplaces.

  An external modem can be locked in a safe place after usage. It also offers the advantage of showing its current-status indication capability via various displays and the integrated loudspeaker. By means of the loudspeaker, it can be heard when a connection has been set up from outside or whether an application is trying to transfer information via the installation and the system configuration to the manufacturer without being instructed to do so. A further advantage of an external modem is that it can be switched on solely for the duration of the data transmission independent of the IT system, thus ensuring that the most recent connection has been terminated and that no connection can be established from outside. A disadvantage of external modems is the possibility of connecting them to unprotected IT systems for the purpose of manipulating the configuration data or reading out stored passwords.

  Due to their size, PCMCIA modems offer the advantage of easy storage after use. Secure storage prevents them from being connected to unprotected computers for the purpose of manipulation.

- Transmission rate

  The higher the transmission rate of a modem, the shorter the transmission time, and the lower the cost of transmitting large quantities of data with it.

  First, the transmission rate required for the application should be determined. Sufficient values are, for example, 2400 bits/sec. for ASCII terminal emulation, 9600 bits/sec. for fax transmissions, currently 14400 bits/sec. in the case of Datex-J (T-Online). The highest possible trans-

mission rates should be used for large quantities of data. Transmission rates of more than 2400 bits/sec. make tapping more difficult.

A check must subsequently be made as to whether the interface of the IT system intended for connection to the modem allows operation at speeds above 9600 bits/sec.

When selecting the modem, it should be ensured that performance characteristics, which are of importance for the transmission rate actually attained, are standardised. These are standards for the transmission rate, such as V.32bis for 14400 bits/sec. and protocols for transmission optimisation using data compression and error correction, such as MNP 5 or V.24bis.

- Instruction set

  Most modems today use the manufacturer-dependent Hayes-standard (also termed AT standard). The widespread application of this standard allows largely error-free communication between compatible modems. When purchasing modems of the latest generation, it should be noted that the promised high transmission rates can often only be achieved if machines from the same manufacturer are used on both sides.

- Manual

  A detailed and clearly-written manual is important for rapid installation and the best possible configuration of a modem.

- Security mechanisms

  Modems can incorporate a large variety of security features, e.g. password mechanisms and call-back functions. Some modems even offer the possibility of encrypting data intended for transmission.

  The purchase of a modem with an encryption option is advisable if large quantities of data need to be transmitted within an organisation with scattered premises. This on-line coding requires less organisational effort than the encryption of data by means of auxiliary products. General statements on the security of the algorithms used are not possible. For IT baseline protection, the DES algorithm offers a sufficient degree of security given an appropriate key management.

  As regards security, the widely offered call-back function is advantageous in that it easily allows unauthorised callers to be repudiated (also refer to S 5.30 *Activating an existing call-back option*).

Additional controls:

- Are IT users and the purchasing department aware of these instructions?

S 2.60 Secure administration of a modem

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT users, Administrator

The secure use of a modem requires certain administrative measures:

- The subscriber number of a modem must only be disclosed to the communication partners involved, in order to protect the modem from unauthorised dialling-in attempts. This number must not be listed in the telephone directory of the organisation.
- Modems integrated in a network server can be accessed by users from their respective terminals. In this situation, access to the communications software must only be granted to users who are authorised to transmit data (also refer to S 2.42 *Determination of potential communications partners*).
- The modem settings and communications software must be checked regularly, and a log of the data transmissions must be maintained.
- It must be ensured that the modem interrupts the telephone connection as soon as the user logs-out of the system. For stand-alone systems, this can be realised by leaving the modem connected to the telephone network only for the period of data transmission and then deactivating or disconnecting it from the line. Modems integrated in a network server must be configured accordingly. An external modem can simply be switched off. In addition, all users must be instructed to quit the communications program after completion of data transmission.
- It must be ensured that external users are automatically logged out of the IT system on disruption of a modem link, otherwise the next caller would be able to proceed using the same user ID without having to log-in first. The next caller could then work with the same user ID, without any need to log on to the system

Additional controls:

- Have the modem settings been checked to determine whether they effectively prevent unauthorised use?
- Is the modem disconnected when users log-out?
- Are users logged-out automatically on disconnection of the modem?

S 2.61 Requirements document for modem usage

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

The following must be determined:

- Who is responsible for the secure operation of the modem (e.g. IT users for stand-alone operation, the administrator for networked systems)
- Who is entitled to use the modem
- In which cases must confidential information be encrypted before transmission?
- In which cases must data transmissions be entered in a protocol (e.g. transmission of person related data)? If the communications software includes a protocol feature, it should be used effectively.

All login procedures, successful or not, must be recorded. Correctly entered passwords should not be recorded. But it is worth considering listing unsuccessful login attempts in order to reveal password attacks.

Evidence of password attacks could be, for example, frequent unsuccessful login attempts by one user, unsuccessful login attempts always from the same connection, attempts to login under different user names from one connection or during a connection.

After the connection has been established, a login prompt will appear for the caller. Before the successful login it must be ensured that as little information as possible is given regarding the contacted IT system. Neither the type of installed hardware nor the operating system should be revealed. The login prompt should contain the name of the IT system and/or the organisation, a warning that all connections will be listed and an input requirement for user name and password. The reason for an unsuccessful login attempt may not be shown (false user name, false password).

Separating Dial-In / Dial-Out

For incoming and outgoing connections, separate lines and modems should be deployed. A caller should not have the opportunity to reconnect externally via the dialled IT system. (If this is absolutely necessary for workers with external duties, they must provide strong authentication, e.g. via a chip-card). Otherwise, hackers might abuse access to set up expensive long-distance connections or to cover up any traces they may have left.

When calling back, a different modem or a different line should be used for the call back than the modem used when first calling (see also S 5.44 One-way connection setup).

Additional controls:

- Are all employees authorised for communication aware of the related regulations?

S 2.62 Software acceptance and approval Procedure

Initiation responsibility: Head of IT section

Implementation responsibility: Head of IT section

The use of IT for dealing with certain tasks requires that computerised data processing works as perfectly as possible, as the individual results can in most cases not be checked. In the course of a software acceptance process, therefore, it is checked whether the software works without error, i.e. whether the software works with the desired degree of reliability and whether it creates any undesired side effects. With the subsequent approval of the software by the relevant body, permission is granted to use the software. At the same time, this body assumes the responsibility for the IT process implemented by the software.

In regard to software acceptance, a distinction is made between software which was self-developed or developed by a third party and standard software adapted for special uses.

Acceptance of self-developed software or software developed by third parties

Before the order to develop software is placed internally or externally, the software requirements must be defined. These are then used as the basis for the rough and detailed planning for implementation. Using these documents, the relevant body, not the body responsible for the software development, generally draws up an acceptance plan.

In general, test cases and the expected results for the software are determined. Using these test cases, the software is tested and the difference between the calculated and expected result is used as an indication for the correctness of the software.

In order to develop test cases and to implement these tests, the following should be observed:

- The test cases are developed by the relevant body
- No data of the actual operation should be used for test cases
- Test data, particularly if these are compiled by copying actual data, may not contain any confidential information; person related data should be made anonymous or simulated
- The implementation of the tests should have no effect on the actual operation; if possible, a test computer should be used which is logically or physically separate

Acceptance should be denied if;

- Serious errors are detected in the software
- Test cases occur where the calculated results do not correspond to the estimated results
- User manuals or operating instructions are not available or inadequate
- Documentation of the software is not available or inadequate

The results of the acceptance should be set down in writing. The documentation of the acceptance results should include.

- Name and version number of the software and the IT procedure, where applicable
- Description of the test environment
- Test cases and results
- Acceptance declaration.

Acceptance of Standard Software

If standard software is purchased, this should also be subject to acceptance and approval. The acceptance should include checks of whether

- The software is free of computer viruses
- The software is compatible with other products in use
- The software can operate in the intended working environment and which parameters should be set
- The software was delivered with the relevant manuals
- The required functionality is fulfilled.

Approval Procedure

When the software has been accepted, the software has to be approved for use. It should first be determined who is entitled to approve the software. The approval of software should be in writing and suitably filed.

The approval declaration should include:

- Name and version number of the software and the IT procedure, where applicable
- Confirmation that the acceptance has been correctly carried out
- Limitations for use (parameter setting, user group...)
- Approval date from when the software may be used
- The approval declaration itself.

If possible from the point of view of IT, the software should be prevented from being altered or manipulated after approval. Otherwise, this should be stipulated in a provision.

Even after intensive acceptance tests, it may be the case that errors in the software are detected when running. The procedure for such a case should be determined (contact person, troubleshooting, involvement of the relevant body, repetition of the acceptance and approval, version check).

See Chapter 9.1 *Standard Software* for more details.

Additional controls:

- Is there an acceptance and approval confirmation for all software used?
- Are errors eliminated without the involvement of the relevant body?
- Can software in use be manipulated without being detected?

S 2.63 Establishing Access Rights

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Person-in-charge of the various IT applications, Administrator

If a system is operated by several users, the access rights must be administered in such a way that the users can only operate the IT system in accordance with their tasks.

This assumes that the access authorisations for the various functions have been stipulated by the persons-in-charge (c.f. *S 2.7 Granting of (system/network) access rights* and *S 2.8 Granting of (application/data) access permissions*). The users of the IT system are then allocated to the various functions. The results should be in writing.

The Administrator must then configure the IT system in such a way that these users receive access to the IT system and are only able to conduct their tasks with the access authorisation allocated to them. If the IT system offers no possibility of assigning access rights (e.g. a DOS-PC with multiple users) a supplementary product will have to be used (c.f. S 4.41 Use of a suitable PC security product).

If the IT system permits, the report functions should be activated by the Administrator for the purpose of providing evidence. This may be successful and unsuccessful log-on / log-off processes, system errors, attempts to access the system without authorisation.

In the event of substitution, the Administrator must check that his substitute is authorised by the superior. Only then may he establish the access authorisations in the case of substitution.

Additional controls:

- Are the site authorisations assigned by the administrator randomly checked?
- Does documentation exist which shows the authorisation structure in the IT system?

S 2.64 Checking the Log Files

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Person-in-charge of the various IT applications, Auditor

Keeping records of security-relevant events is only effective as a safeguard if the recorded data is evaluated by an Auditor at regular intervals. If it is not possible either by technical or personnel means to implement the role of an independent Auditor of log files, they can also be evaluated by the Administrator. If this is the case, it should be noted that it is difficult to monitor the Administrator's activities. The result of the evaluation should therefore be passed to the IT Security Officer, the person responsible for IT or another, specifically named person.

Regular checks followed by deletion of the logged data also ensure that the volume of log files does not grow to an inordinate size. Depending on the type of logged data, it may be appropriate to archive it to external data media.

As log files usually contain person-related data, steps must be taken to ensure that this data is only used for the purposes of monitoring adherence to data protection requirements, data backup or ensuring that operations are being carried out in the proper manner (cf. §14. Para 4 of the Federal Data Protection Act (BDSG) and S 2.110 *Data Privacy Guidelines for Logging Procedures*). The scope of logging and the criteria used in evaluating log files should be documented and agreed within the organisation.

There may be either statutory minimum periods for which logged data has to be kept or alternatively there may be statutory upper limits on the length of time for which logged data can be retained. Thus, it might be the case that deletion was required in order to comply with data protection legislation (see also S 2.110 *Data Privacy Guidelines for Logging Procedures* on this point).

On the other hand, for certain types of logged data there may be statutory minimum periods for which the data must be kept, e.g. where it provides information about business processes. These legal stipulations must be adhered to in every case. Prior to deleting any logged data it is therefore necessary to check carefully whether there are any such legal requirements which have to be complied with and, if so, what retention periods result from these. The legal department should be involved here.

The following evaluation criteria are intended as examples to assist detection of any security weaknesses, manipulation attempts or other irregularities:

- Are the log-on and log-off times outside of normal working times (suggesting a tampering attempt)?
- Is the number of incorrect log-on attempts increasing (suggesting an attempt to guess a password)?
- Is the number of unauthorised attempts at access increasing (suggesting tampering attempts)?
- Are there any particularly long periods of time when no protocol data were recorded (suggesting the records could have been deleted)?

- Is too much information recorded (long log files make it more difficult to detect irregularities)?
- Are there any particularly long periods of time when the user has not changed (suggesting that logging-off is not being consistently carried out when a user finishes working)?
- Are there any unusually long periods during which a connection with a public network has been maintained (see T 4.25 *Still Active Connections*)?
- Have unusually high network loads or an interruption in network operations been detected in individual network segments or throughout the network? (suggesting that there have been attempts to obstruct or impair network services or that the network has been inappropriately designed or configured)?

When evaluating the log files, particular attention should be paid to all accesses which have been carried out using an Administrator ID.

If extensive log files are to be evaluated on a regular basis, it is sensible to use an evaluation tool. This tool should allow evaluation criteria to be selected and highlight especially critical entries (e.g. repeated failed attempts at log-on).

The guidelines stated above also apply to the gathering of auditing data, because in principle, this involves the logging of security-critical events.

Additional controls:

- Who analyses the log files? Is the two-person rule applied?
- Can the activities of the Administrator be monitored to a sufficient extent?
- Is the IT Security Management Team notified of irregularities?

S 2.65 Checking the efficiency of User separation on an IT System

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Auditor, Administrator, IT Security Management

By means of report assessment or random testing, it should be checked at appropriate intervals whether the users of the IT system log-off regularly after finishing their task or whether several users work under one ID.

Should it be found that several users work under one ID, then they should be made aware of the duty of logging off after a task is finished. At the same time, it should be pointed out that this is in the interest of the user.

Should it also be determined that the log-on and log-off processes take too much time and are not accepted despite a request to do so, alternative measures should be discussed, such as:

- Allocation of the IT system to a user for certain time periods when other users may not use the IT system. This requires the work process to be flexible from the point of view of time.
- Procurement of additional IT systems, with which quasi-parallel work on one IT system can be avoided. It should be noted that whilst this involves additional costs, the procurement costs for PC security products are no longer required. Instead of the module 5.4 *DOS PC (multi-user)*, the implementation of recommended safeguards of another module e.g. 5.1 *DOS PC (one user)* becomes necessary.
- Should it be possible to separate the data of the various users (e.g. user A processes the data A-L, user B the data M-Z), various authorisations can be granted. When a user wants to work with his data, therefore, he must first log-on to the system as his colleague does not have access to these data.

Additional controls:

- How frequently are logins and logouts checked?
- Is there an acceptance problem regarding login/logoff?
- Can the data be separated?

S 2.66 The importance of certification for procurement

Initiation responsibility: Agency/company management

Implementation responsibility: Procurer

When procuring IT products and IT systems, it must be checked at an earlier stage whether the assurances by the manufacturer or distributor regarding security functions can be considered as sufficient. Particularly with regard to high or very high protection requirements, the trustworthiness of the products concerning IT security can only be guaranteed by having these evaluated by independent testing agencies.

The harmonised European "Criteria for the Evaluation of the Security of IT Systems (ITSEC)" and the evaluation manual ITSEM have offered a generally-accepted basis for these evaluations since 1991 as has the globally-agreed "Common Criteria for the Examination and Evaluation of the Security of IT Systems" / Common Criteria (CC) since 1998. In Germany, the BSI itself and testing bodies acknowledged by the BSI, conduct evaluations of this kind. In the event that the evaluation results are positive and the conditions of ITSEC and ITSEM or the Common Criteria are fulfilled, a safety certificate is issued by BSI as the certifying body for the assessed product or system.

The certification report states at which test level each functionality was investigated and what the result of the evaluation was. The test level ranges from evaluation level E 1 (lowest test level) to evaluation level E 6 (highest test level) for the ITSEC and from evaluation assurance level EAL 1 (lowest test level) to evaluation assurance level EAL 7 (highest test level) for the CC. Evaluation level E 1 of the ITSEC approximately corresponds to evaluation assurance level EAL 2 of the CC and so on.Additionally, the strength of the security functions is stated, which represents the degree of difficulty in overcoming the security functions. The ITSEC and CC differentiate between the strengths low, medium and high. Indications are also given regarding the conditions which must be observed when using the product.

In the event that several products with an acceptable price/performance relationship are available when procuring IT, an existing safety certificate can be considered as a positive criteria for selection. Safety certificates should be particularly considered if the evaluated function (mainly) corresponds with the minimum functionality and the security strength corresponds with the protection requirement (c.f. S 4.41 *Use of a suitable PC security product*). The higher the test level stated in the certificate, the higher the trustworthiness of the effectiveness of the security functions of the product.

The certification bodies regularly issue summaries of which products have a certificate. A summary of the IT products and systems certified by the BSI can be obtained from the BSI: **BSI 7148** - BSI Certificates. The BSI also publishes recently-issued certificates in the magazine KES, a magazine for communication and EDP security. This information can also be obtained from the BSI server.

Additional controls:

- Have the IT procurement bodies been informed of the evaluation / certification system?
- Do the procurement bodies have up-to-date summaries of certified products?
- Does the procurement body request the relevant certification reports?

S 2.67 Defining a security strategy for peer-to-peer networks

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management

Prior to commencement of the configuration and installation of a Peer-to-Peer network on a WfW, Windows 95 and/or Windows NT computer, two basic factors must be considered:

It should first be clarified which service must be performed by the relevant operating system and what is the scope of this service? In particular, it should be clarified whether the Peer-to-Peer functions of the operating system, i.e. shared resources such as printers or directories should be used at all.

This can be illustrated using a number of **examples**:

- The IT-system is used for a working group of typically three to five users, whereby each user should have all rights. The complete Peer-to-Peer functionality should be supported at each workstation.
- The IT-system is used for a large group in which various rights can be allocated. The Peer-to-Peer functionality is to be implemented in a limited manner on the basis of definite requirements.
- The IT-system is used in a server-supported PC network, where Peer-to-Peer functionality for the exchange of data can generally be dispensed with. several printers should be used jointly via peer-to-peer functions.
- The IT-system is to be installed in a server-supported PC network, where Peer-to-Peer functionality is not planned. All Peer-to-Peer functions must then be deactivated. In this case, the consideration of the following points is not necessary. However, the measures described in S 5.37 *Restricting peer-to-peer functions when using WfW, Windows 95 or Windows NT in a server-supported network* should be taken into account.

Note:

security functions offered by server-supported networks are far more extensive than those offered by Peer-to-Peer networks. Moreover, additional security problems may arise when using Peer-to-Peer functions in a server-supported network. **Therefore the use of Peer-to-Peer functions in a server-supported PC network should be avoided.** Peer-to-Peer networks which serve to connect WfW to other computers with WfW, Windows 95 or Windows NT should only be considered as a temporary solution until WfW is replaced by Windows 95 or Windows NT or until a server-supported network operating system is installed.

Given that Peer-to-Peer functions should be used, these considerations must then be transformed into a security strategy.

This demonstrates that the development of a suitable security strategy involves a relatively large amount of time and expense, depending on the system environment and organisation structure already in place, as well as the planned restrictions of Peer-to-Peer functionality.

Below is a methodical approach for the development of a comprehensive security strategy for a Peer-to-Peer network. As a Peer-to-Peer network can be used in various configurations, however, individual decisions regarding the necessary steps have to be taken for each situation.

Defining a Security Strategy for a Peer-to-Peer Network

The security strategy shows how a Peer-to-Peer network can be securely established, administered and operated. The individual development steps of such a strategy are presented below:

1. Definition of the Peer-to-Peer network structure

A Peer-to-Peer network structure is defined by determining the following:

- which computers are to act as file servers (these may share directories)
- which computers are to act as print servers (these may share printers)
- which computers are to act as application servers for certain IT applications, e.g. mail, schedule+, fax (these should continually be available)
- which computers are merely clients (these can only be connected to other computers)

. On the one hand, it should be ensured that the capacity of the servers fulfil the requirements concerning speed and memory. On the other hand, the number of servers should be limited to the amount actually needed. Furthermore, no application should be allocated to servers which constantly involve transmitting large amounts of data through the network, as this can lead to the network overloading.

2. Regulation of responsibilities

A Peer-to-Peer network should be securely operated by trained **administrators** and their substitutes. Only these persons may change security parameters in the Peer-to-Peer network. They are, for example, responsible for providing the relevant persons-in-charge with administration authorisations and tools on application or file servers so that these persons can share the directories and applications needed by others.

Peer-to-Peer administrators must be explicitly named in a server-supported PC network containing additional authorised Peer-to-Peer functions. They may, however be identical to the network administrators.

The responsibilities of the various **users** in a Peer-to-Peer network are described under step 7.

3. Restriction of sharing possibilities

Windows for Workgroups

Using the administration tool ADMINCFG.EXE for WfW, the following can be granted or denied:

- the sharing of directories
- the sharing of printers

- restrictions for the WfW registration password (expiry, minimum length etc.)
- enabling of network DDE (e.g. exchanging data via the output file or making telephone calls via WfW).

The file ADMINCFG.EXE comes with the WfW package but is not installed on the computers as standard. The application is only described in the instructions for systems operators (see S 4.45 *Setting up a secure Peer-to-Peer environment*).

It should be determined on to which computer this administrative tool is to be installed.

This program has a password function to protect the configuration. Anybody who has access to this program can try to find out the password of the configuration file and then change the sharing options.

It is thus sensible to make it available only to the administrator and his substitute. Furthermore, it is also possible using WfW to place the configuration files on one server (either for one user, for groups or for all users jointly; c.f. WfW Resource Kit, Addendum for Operating System Version 3.11"). The advantage of this is that alterations can be made simultaneously for several WfW users, particularly if the password of the configuration file(s) is to be changed.

Note: A configuration protected by a password only offers limited security as it cannot withstand a direct attack. The restriction of the WfW functionality thus primarily protects against user errors.

Windows 95

The option to share directories or printers for individual computers and/or users may be restricted under Windows 95 by appropriate entries in the profile (see also S 4.58 S*haring of directories under Windows 95*).

Windows NT

Under Windows NT the option to share directories is restricted to administrators, thereby preventing misuse by the end user. If applicable, the resources to be approved should be determined in detail when planning the network (see S 2.94 S*haring of directories under Windows NT*).

4. Establishing a name convention

In order to hinder a masquerade under WfW, clear names should be used for the computers, user groups and the users. These names should be known to all users. In the event that a name which is not possible according to the convention is used for registration, e.g. a name similar to an existing one, a masquerade is obvious. Registration under an already registered computer name is denied by WfW. A masquerade under a registered name is possible, however, if the user in question is not currently registered.

By means of the system guidelines under Windows 95, unauthorised persons must be prevented from changing user names and computer names. Access to the system control option "network" should thus be deactivated for standard users (see also S 2.103 *Setting up user profiles under Windows 95*).

Under Windows NT the only authorised users are those defined by the administrator. Only administrators may change computer names. However, users can try to log on under another user name via the option "log on as" under "connect network drive".

In addition, name conventions can be introduced for the sharing of names of directories or printers. In the event that it should not be possible to draw conclusions regarding the contents of the directory, pseudonyms should be used. Should a shared resource not be recognisable as such, the symbol ”$” must be attached to the share name. The latter is recommended if directories are only used for the bilateral exchange of information between two users.

5. Determining directories or printers to be shared and the granting of access rights

For the application server, it should be determined which directories (e.g. the Post Office directory AGPO under *Mail*) are to be shared. For the file server, the directories to which the users are to have access should be selected. Under WfW and Windows 95 any user can share resources for network access; under Windows NT only administrators have permission to do this.

Two access models must be differentiated. *Share Level Security*, in which access to shared resources is controlled by passwords and *User Level Security*, in which access is controlled by the server operating system. WfW supports only the first of these models, Windows NT (as client) only the second whilst Windows 95 allows the choice between both models, via the system control option "network" under the register card "access control". When using Share Level Security, access rights (read and write access) for shared directories must be defined and appropriate passwords selected.

As a result of the allocation of these passwords to individual users, the access authorisations are distributed in the Peer-to-Peer network. These passwords should only be made known as far as is necessary, since the withdrawal of authorisation for one person involves changing the password for all other authorised users.

When using User Level Security under Windows NT and Windows 95 access rights will be explicitly assigned to individual users and/or groups. The clients must be connected in a workgroup or domain with at least one Windows NT system. In this case password entry will be omitted. Use of Share Level Security must be avoided here, since it offers considerably less protection. It should then be decided whether the directories are automatically shared when the server is started and whether it should automatically be connected to the accessing computer upon start-up.

The above comments also apply to the sharing of printers.

6. Changing passwords

Windows for Workgroups

A series of passwords are used in the WfW network - registration passwords, the password for calling up ADMINCFG.EXE and the passwords for the various rights of shared directories, printers and output file. The registration passwords and the password for calling up ADMINCFG.EXE should be changed on a regular basis (see also S 2.11 *Provisions governing the use of*

passwords). The maximum term of validity for these passwords should thus be stipulated. In order to be able to change the ADMINCFG.EXE password efficiently, the relevant configuration files can be stored centrally on one server. As changing the share passwords can involve a high degree of organisation (see No. 5), it should be determined in advance how often these are to be changed and how those persons affected are to be informed of the new passwords.

Windows 95

Under Windows 95, the amount of passwords to be used depends upon which access model is deployed (User Level Security or Share Level Security). In the former case, as with Windows NT, the passwords will only be required for the computers having shared resources for network access. In the latter case, similar to WfW, passwords for the shared resources will also be required. Separate passwords for the administration of Peer-to-Peer functions are not required as these will be controlled via the user profile.

Access protection at the user level is based on the user lists contained in Windows NT or Novell Netware servers, and can thus only be implemented in these networks. If Peer-to-Peer functions must be implemented despite having a Windows NT or Novell Netware server network, then it is preferable to implement this access model since it offers a higher level of protection.

Windows NT

Under Windows NT, the administration of Peer-to-Peer functions takes place under general network and access control, so that no separate passwords are required for these administrative tasks. Regarding administration of access passwords for the users concerned, please refer to the notes contained in safeguard S 2.11 *Provisions governing the use of passwords.*

7. Responsibilities for users in a Peer-to-Peer network

In addition to Peer-to-Peer management tasks (see No. 2), other responsibilities must be determined. It should be determined what the responsibilities of the various Peer-to-Peer network users are to be, such as: These can, for example, be responsibilities for

- the evaluation of the log files on the individual servers or clients,
- the allocation of access rights,
- the escrow and changing of passwords and
- carrying out data backups.

8. Training

It must then be determined which Peer-to-Peer users have to be trained in which points. Effective operation can only begin after adequate training.

The security strategy developed in this way should be documented and announced to the users of the Peer-to-Peer network to the extent required.

Additional controls:

- Is the security strategy adapted to changes in the usage environment?

S 2.68 Implementation of security checks by the peer-to-peer network users

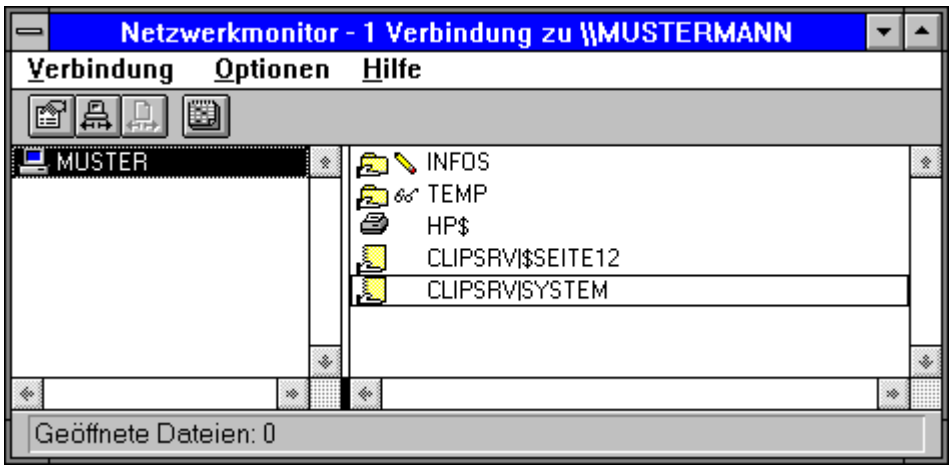
Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

As the major security measures in a Peer-to-Peer network can only be checked on a decentralised basis, the users are responsible for implementing security checks of this kind. The following checks should thus be carried out by the users at appropriate intervals:

- Checking active connections: Using the program Network Monitor (in the program group NETWORK) under WfW, it is possible to check which computer currently has access to the user's own computer and what the nature of this access is. The program can be optionally installed in the program group ACCESSORIES, sub-menu SYSTEM PROGRAMS under Windows 95, or the control panel option "Server" under Windows NT.

For example:



The connections from the computer "MUSTER" are displayed. The icons have the following meaning:

INFOS Access for writing purposes to the directory INFOS

TEMP Access for reading purposes to the directory TEMP

HP$ Access to the printer with the name HP$

CLIPSRV\SYSTEM A connection was created to your output file

CLIPSRV\$SEITE12 Access to the page with the name PAGE12 of your output file

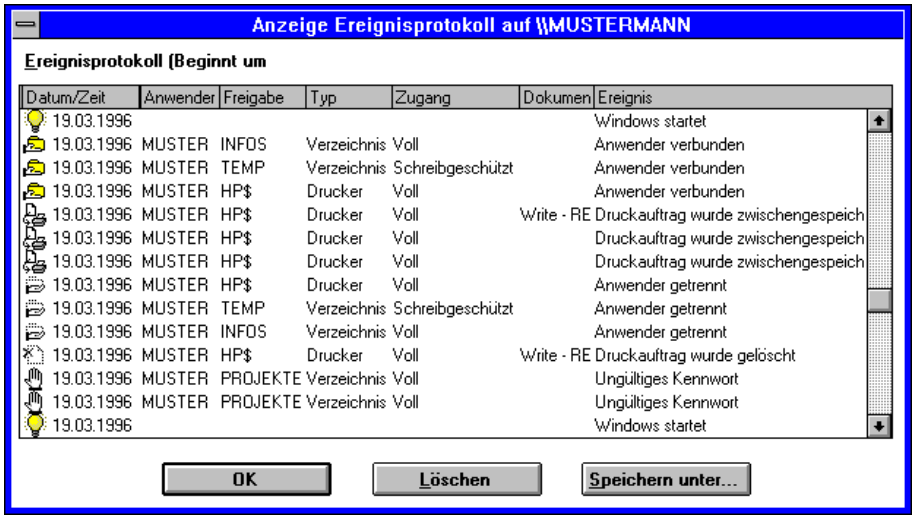
In the event that unauthorised access by a computer to a directory or the printer is displayed, share is to be withdrawn. Any pending printing jobs can be interrupted using the print manager. The various actions are documented in the event protocol (see next illustration). In the event of

unauthorised access to the output file, this should also be interrupted. It is recommended, however, to copy the contents of the window of the Network Monitor to the clipboard with the *Print* key as access to the output file is not documented.

- **Checking the protocol data**: In the event that resources have been shared on a computer, the event protocol should be activated (in the program group CONTROL PANEL under *Network* for WfW, or in the program group ADMINISTRATION under *User-Manager* for Windows NT) and assessed on a regular basis (in the program group NETWORK under *Network Monitor* for WfW or in the program group CONTROL PANEL under *Events* for Windows NT**). Windows 95 offers no standard procedure for logging events.** Therefore, under Windows 95, the Network Monitor absolutely must remain open in case Peer-to-Peer functions need to be carried out despite this weakness.

  It should be checked on a weekly basis, for example, whether unauthorised users accessed shared directories, whether there were errors in accessing shared directories or whether the system was started at unusual times. As these protocol data also contain person-related data, they should be deleted after assessment if storage is no longer required.

Example for a possible incident protocol:



- **Checking automatically shared resources**: WfW and Windows 95 users should check on a random basis which of their resources are automatically shared after start-up of the system without their direct participation (for example, by checking after start-up which directories, printers and pages of the output file are then shared). If necessary, this share should be withdrawn. Inexplicable irregularities, such as the automatic sharing of a directory which the user himself did not share, should be reported to the administrator. These could be indications of Trojan horses which share directories without being detected. Should the user not be sure whether or what was shared, the file *shares.pwl* under WfW should be deleted, which contains the entries for automatic sharing. Under Windows 95, shares can be deleted with the help of the Explorer. This problem will not arise under Windows NT since only administrators can share resources.

A **check of the allocation of rights** is not possible in a Peer-to-Peer network directly as the person who knows the valid password also has the relevant rights. Only by using the complicated password change process can a consistent distribution of rights be ensured.

Additional controls:

- Is the administrator informed of irregularities?

S 2.69 Establishing standard workstations

Initiation responsibility: Head of IT section

Implementation responsibility: Head of IT Section, Administrator

A standard workstation is denoted by standard hardware and software and their configuration. The planning and establishment of a standard workstation is usually performed taking into consideration the task, reliability, ergonomics, speed and serviceability. It is carried out by specialist personnel. The establishment of standard workstations is advantageous in several points:

IT Security:

- Standard workstations are easy to include in security concepts
- The expense for IT documentation is reduced

IT Management:

- The procurement of large numbers of the same components reduces costs
- The use of impermissible software is easier to detect
- The "envy factor" between users is eliminated as a result of standardised IT equipment

IT Users:

- When it is necessary to change workstations, it is not necessary to receive new training. Inoperable time is thus minimised.
- Users can help each other concerning hard and software questions

System administration for installation and maintenance:

- A well-planned and tested installation can be installed without error and with little effort
- The standard working environment facilitates the user service (maintenance and support)

Training:

- The participants are trained in the same environment as at the workplace.

Additional controls:

- Are any differences compared to standard workstation justified?
- Are these reasons reviewed on a regular basis?
- Which factors are taken into consideration when planning and establishing standard workstations?

S 2.70 Developing a firewall concept

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management

The connection of existing sub-networks with global networks, such as the Internet, leads to a new supply of information. At the same time, the increasing amount of local networks leads to the situation where all workstation computers have access to a wide variety of information.

This networking gives rise to new threats, however, as it is not only possible for information to flow into the network requiring protection from outside, but also in the other direction. Furthermore, the possibility of *remote access*, i.e. a remote computer (e.g. through the Internet) can execute commands in the local network, poses a threat to the integrity and availability of the local computers and thus indirectly also to the confidentiality of the local data.

A sub-network requiring protection should thus only be connected to another network if this is essential. This particularly applies to connections to the Internet. It should be checked to what extent the network requiring protection can be divided into parts which cannot be connected, which can be connected and which can be connected with limitations. It should also be checked whether a stand-alone system is not sufficient for the connection to the Internet (see S 5.46 *Installing stand-alone systems for Internet usage*).

In order to guarantee the security of the network requiring protection, a suitable firewall must be used. For the firewall to offer effective protection, the following conditions must be fulfilled. The fire wall must be:

- based on a comprehensive security policy
- incorporated into the IT security concept of the organisation
- installed correctly and
- administered correctly.

The connection to an external network can only take place when it has been checked that all risks can be handled by the firewall concept and the personnel and organisational conditions.

There are several ways to implement a firewall. In order to determine which firewall concept is most suitable for the intended uses, it must first be clarified which security objectives are to be fulfilled by the firewall. Examples of security objectives are:

- Protection of the internal network against unauthorised remote access,
- Protection of the firewall against attacks from the external network, but also against manipulation from the internal network,
- Protection of the locally transmitted and stored data against attacks on their confidentiality or integrity,
- Protection of local network components against attacks on their availability (this particularly applies to information servers which provide information from the internal area for general use),

- Availability of information from the external network in the internal network requiring protection (the availability of this information is secondary to the protection of the local computers and information, however),
- Protection against attacks based on IP spoofing or which abuse the source routing option, the ICMP protocol, or routing protocol,
- Protection against attacks as a result of the leaking of new software weakness relevant to security. (As it must be considered that the number of potential attackers using an Internet connection is very high, as is their expertise, this security objective is of particular importance).

Based on the security objectives, a security policy must be drawn up which stipulates the tasks of, and requirements placed on, the firewall. This security policy must be included in the IT security strategy of the organisation and thus agreed with the IT management.

The firewall security policy is put into effect by the implementation of the firewall, the selection of suitable hardware components, such as packet filters and application gateways, and the careful implementation of filter rules.

Note:

Packet filters are IT systems with special software which filter the information of the lower layers of the OSI model and pass on or intercept packets in accordance with special regulations (see S 2.74 *Selection of a Suitable Packet Filter*).

An application gateway is a computer which filters the information of the application layer and permits or forbids connections in accordance with special regulations (see S 2.75 *Selection of a Suitable Application Gateway*). Whilst packet filters work on layer 3 and 4 of the OSI model, gateways work on layer 7 and are thus considerably more complex. An application gateway is generally implemented on an IT system which is used solely for this purpose and whose command set is reduced to a minimum.

In order for a firewall to offer effective protection of a network against external attacks, several fundamental factors must be fulfilled:

- All communication between the two networks must be carried out via the firewall. To achieve this, it must be ensured that the firewall is the only connection between the two networks. Provisions must be taken so that no other external connections bypassing the firewall are permitted (see also S 2.77 *Secure Configuration of Other Components*).
- A firewall must only be used as a protective connection to the internal network. Only the services required for this purpose must be available on the firewall, therefore, and no other services must be offered, such as remote log-in.
- Administrative access to the firewall must only be possible via a secure route, e.g. via a secure console, an encrypted connection or a separate network. For the establishment of a secure console, see S 1.32

Establishment of the Consoles, Devices with exchangeable data media, and printers.

- A firewall is based on a security policy defined for the network requiring protection and allows only the connections contained herein. It must be possible to permit these connections separately according to IP address, service, time, direction and user.
- Suitable personnel must be available for the planning and operation of a firewall. The time required to operate a firewall must not be underestimated. Experience has shown that an analysis of the accumulated log data alone is very time consuming. A firewall administrator must have a detailed knowledge of the IT components used and be trained accordingly.
- The users of the local network should only be affected by the use of a firewall to the smallest possible extent.

A firewall can protect the internal network against many of the dangers encountered when connecting to the Internet, but not against all of them. Thus, when a firewall is established and a firewall security policy is elaborated, it is necessary to be aware of the firewall's limits.

- Protocols are tested, not the contents. Testing the protocol confirms, for example, that an E-mail was delivered using commands that comply with the rules, but cannot provide any information about the actual content of the E-mail.
- The filtering of active contents may only be partially successful.
- As soon users are allowed to communicate over a firewall, they can create a tunnel from the protocol they are using for any other protocol. An internal perpetrator could thereby enable an external party to access internal computers.
- In reality, it is not possible to restrict Internet access to certain Web servers because too many WWW servers can be used as proxies, making it easy to bypass the blockage of particular IP addresses.
- The filter software is often still immature. For instance, it possible that some forms of address are not included. The following example with the BSI Web server shows which possible forms of address are available. The list is far from complete, as individual letters can also be represented by escape sequences.
  WWW.BSI.BUND.DE
  WWW.BSI.DE
  194.95.176.226
  3261051106
- The filtering of spam mails is not yet fully developed. No firewall can determine beyond doubt whether a user wishes to receive a particular E-mail or not. Spam mails will only disappear when it is possible to be sure who the sender is, and it will take a while before this happens.
- Firewalls do not safeguard systems against all denial of service attacks. For example, if a perpetrator disables the connection to the provider, even the

best firewall cannot help. In addition, protocol implementation errors repeatedly occur in terminal equipment which a firewall cannot intercept.

- Unfortunately, many firewalls do not allow security to be increased by connecting various firewalls in series. This is particularly a problem in large firms if firewalls are also used within the firm, for example to create secure subnetworks.
- Although a firewall can protect a gateway, it has no influence on the security of communication within the networks!

S 2.71 Establishing a security policy for a firewall

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management

The first step in establishing a security policy is to determine which types of communication with the external network are permitted. When **selecting the communication requirements**, the following questions must be answered:

- Which information should the firewall allow out / in?
- Which information should the firewall conceal (e.g. the internal net structure or the user names)?
- Which authentication procedures should be used within the network requiring protection or for the firewall (e.g. one-time passwords or chip cards)?
- Which access possibilites are needed (e.g. only via an Internet service provider or also via a modem pool)?
- What data throughput is to be expected?

Selection of Services

The communication requirements are the basis for determining which services are permitted in the network requiring protection and which must be forbidden.

A distinction must be made between those services permitted for the users in the network requiring protection and those permitted for external users.

If E-mail is to be received, for example, which is generally the minimum requirement, the firewall must allow the SMTP protocol to pass through. If files from external IT systems are to be collected, FTP must be available.

The security policy must clearly state for each service which services are permitted for which user and/or computer and for which services confidentiality and/or integrity must be guaranteed. Only services which are absolutely necessary should be permitted. All other services **must be forbidden**. This must be the basic principle: All services for which there are no explicit rules must be forbidden.

It must be determined whether and which information should be filtered (e.g. checking for computer viruses).

The security policy should be established in such a way that it can meet future requirements, i.e. it should have a sufficient number of connection possibilities. Any alteration at a later date must be strictly monitored and particularly checked for side effects.

Provisions must be made for exceptions, particularly for new services and short-notice alterations (e.g. for tests).

The filters must fulfil certain requirements: the filters using information from the services of layers three and four of the OSI layer model (IP, ICMP, ARP, TCP and UDP) and the filter using information from the services of the application layer (e.g. Telnet, FTP, SMTP, DNS, NNTP, HTTP). An overview

of aspects to be observed for correct operation of the various protocols and services is provided in S 5.39 *Secure Use of Protocols and Services*. Using this as a basis, filter rules must be drawn up (see S 2.76 *Selection and Implementation of Suitable Filter Rules*).

In addition to the establishment and implementation of filter rules, the following **organisational regulations** are required:

- Persons-in-charge should be appointed for the establishment, implementation and testing of the filter rules. It must be clarified who is authorised to alter filter rules, e.g. for testing new services.
- It must be determined which information is logged and who assesses these protocols. All connections which were correctly established and those which were denied must be logged. Logging must comply with the data privacy regulations.
- The users must be informed in detail of their permissions, particularly with regard to the extent of the data filtering.
- Attacks on the firewall should not only be successfully prevented, but also detected at an early stage. Attacks can be detected by assessing the log files. On the basis of predefined events, e.g. repeated entry of an incorrect password on an application gateway, or attempts to establish forbidden connections, the firewall should also be able to issue warnings or even trigger actions.
- It should be clarified which actions are started in the event of an attack, whether the attacker should be traced, for example, or whether the external network connection should be cut off. As this can have a great effect on operation of the network, persons-in-charge must be appointed who are able to decide whether an attack is present and what action should be taken. The tasks and authority for the persons and functions in question must be clearly stipulated.

The following questions must be clarified when determining the security policy:

- What damage can be caused to the network requiring protection if the firewall is passed? As there is no such thing as absolute protection, it must be decided whether the maximum possible damage is acceptable or whether additional measures must be taken.
- What is the remaining risk when the firewall is operating correctly? This may be vulnerabilities in the equipment and operating systems used.
- How quickly is an attack on the firewall detected?
- Which protocol information is still available after a successful attack?
- Are the users willing to accept the limitations caused by the firewall?

S 2.72 Requirements on a firewall

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

Before purchasing a firewall, the following points should be taken into consideration:

- It must be possible to conceal the structure of the network requiring protection (computer number, name and mail addresses) so that no conclusions can be drawn regarding the internal network structure and the internal users. This can be achieved by using an application gateway, for example, and two DNS servers.
- The firewall should be able to protect certain computers against attacks without these computers having to be in the network requiring protection. No user-specific filter rules have to be established for these computers. This can be, for example, information servers connected to a dedicated interface of a packet filter or the application gateway (multi-homed gateway) (see also S 2.77 *Secure Configuration of Other Components*).
- The components must be centrally administered via a trustworthy path (e.g. via a separate network or an encoded connection) and they must be understandable (e.g. via a graphic interface on a separate computer). Administration should be performed on a separate computer, i.e. the required management platform should be on a separate computer so that no complex and thus error-prone software, such as X-Windows, has to be on the firewall.
- A firewall configuration which consists of at least two separate units is recommended. The units must be arranged one after the other so that both units must be passed for a connection between the two networks. The units should work with different operating systems and different formats for the description of filter rules.

  The two units can, for example, be a packet filter and an application gateway. This ensures that errors made during the administration of a component can be intercepted by the other correctly configured component.

S 2.73 Selecting a suitable firewall

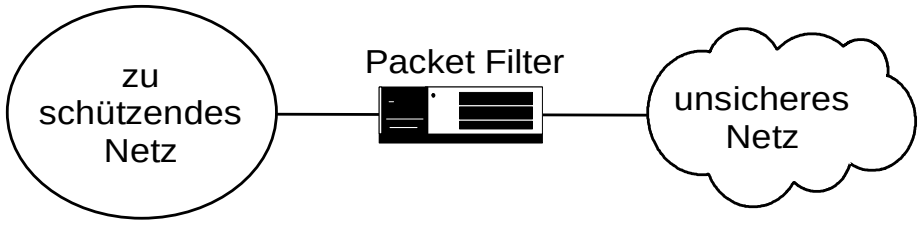
Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

After a security policy has been determined for the firewall, it must be decided which components are to be used for the implementation of the firewall. A suitable configuration is to be selected.

The following are possible configurations:

- Exclusive use of a packet filter



  This configuration consists exclusively of a packet filter which filters the information of the lower layers and either accepts or denies packets according to special regulations.

- dual-homed gateway

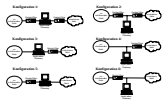
  This configuration consists of an application gateway which is fitted with two network interfaces and which is used as the sole junction between two networks. Application gateways filter information on layer 7 of the OSI layer model. The dual-homed gateway must be configured in such a way that no packets can pass unfiltered, i.e. IP forwarding must be switched off, in particular.

- Screened Sub-net

  A screened sub-net is a sub-network between a network requiring protection and an external network, with firewall components checking connections and packets.

  A screened sub-net consists of an application gateway and one or two packet filters. The packet filters are located in front of and/or behind the gateway and together they form a sub-network. A screened sub-net can, for example, contain a dual-homed gateway. The filter rules are created in such a way that each connection from inside or outside has to pass the gateway.

The following combinations are possible:



The following is a list of the advantages and disadvantages of the various configurations.

Exclusive use of a Packet Filter

Advantages:

- - easy to implement as the functionality is supplied by many routers
- - easy to extend for new services

Disadvantages:

- - IP spoofing might be possible
- - all services to be permitted must be secure on all computers which can be reached
- - complex filter rules
- - no test possibilities. In particular, it is not possible to determine whether the order of filter rules has been changed, which occurs with some routers in order to increase the data throughput
- no sufficient logging possible

This configuration can only be used in small networks where all computers are protected against attacks.

Dual-homed Gateway

Advantages:

- extensive logging possible
- internal network structure is concealed

Disadvantages:

- relatively high price (as a powerful computer with two network interfaces is required)
- problems with new services
- take-over of the application gateway by the attacker leads to total loss of security

Additional protection can be obtained by using a packet filter in front of the gateway, e.g. using an existing router. In this case, the router and gateway must be penetrated in order to gain access to the network.

Screened Sub-net

Advantages:

- no direct access to the gateway possible (with configuration 1 and 2)
- internal network structure is concealed

- simplified rules for the packet filters
- additional security by a second packet filter (configuration 1 and 2)
- availability increases if several gateways are used
- extensive logging possible

Disadvantages:

- high price (as a powerful computer with one or two network interfaces and at least one packet filter is required)
- if the packet filters are manipulated in a screened sub-net with an application gateway with an interface (see configuration 2, 4 and 6), a direct connection is possible bypassing the gateway. This can also be a desired function (e.g. in case of new services)

As a result of the above advantages and disadvantages of the various configurations, only a screened sub-net with a dual-homed gateway (configuration 1) is recommended. In this case, the gateway is between the network requiring protection and the external network and must be passed in any case.

So-called proxy processes run on the application gateway. These set up the connection with the target computer after authentication of the user and filter the data in accordance with the information of the application layer. Connections without proxy processes are not possible.

The more flexible but less secure option consisting of an application gateway with just one interface (configuration 2) should only be used if higher flexibility is absolutely necessary.

The computers involved must be set up in such a way that only the essential programs run on them (minimal system), and that these programs are correctly configured and all known weaknesses are eliminated.

S 2.74 Selection of a suitable packet filter

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Packet filters are routers or computers with special software which use the information in layers three and four of the TCP/IP protocol family (IP, ICMP, ARP, TCP and UDP) for filtering packets. Access and deny lists are used in this regard.

In the event that a packet filter is required for a firewall, the following demands should be made upon purchase:

- The filtering must be possible separately for each interface.
- It must be possible to filter incoming and outgoing packets separately.
- The filtering must be possible separately for individual computers or for complete sub-networks according to source and destination address.
- The filtering must be possible separately according to source and destination port.
- The order in which the filter rules are evaluated should not be automatically changed by the packet filter.
- The order in which the filter rules are evaluated should be easily recognised, i.e. sufficiently documented.
- The entry and control of filter rules must be simple and clear, e.g. by symbolic service and protocol names.
- In case of TCP packets, it should be possible to determine whether an existing connection is being used or a connection is being established, i.e. to distinguish between packets with and without ACK.
- It must be possible to record IP numbers, service, time and date for each packet. Selective logging for certain packets (e.g. only packets with a specific source address) has also to be possible.
- It must be possible to send all logging information to an external host.
- Special, adjustable events must lead to an immediate warning (e.g. repeated incorrect authentication attempts).
- If a router is used as a packet filter, it should be possible to use static routing tables. In general, however, routers should not be used as packet filters as they have a very wide range of functions so that the filter attributes are often just offered as add-ons. This accordingly influences the creation and testing of the related software.
- If a router is used as a packet filter, dynamic routing must be configured in such a way that routing packets (e.g. RIP) which affect the network requiring protection are only permitted on the interface connected to the network requiring protection.
- It must be possible to reject packets with source routing information by default.

- If required, the packet filter should support dynamic packet filtration. This means that during the transmission of UDP packets, for example, the related context is stored for a particular time period and the corresponding response packets are allowed to pass through.

Dynamic filters

Based on the definition of a packet filter as a filter which uses the information of layers three and four as a check, the limits of this procedure soon become apparent. Although it is possible, in the case of TCP (Transmission Control Protocol) to recognise the establishment of a connection and thereby prohibit connections from the Internet to the network requiring protection, this is no longer possible in the case of UDP (User Datagram Protocol). In order to solve this problem, **dynamic packet filters** are used. If a UDP packet is sent from an internal computer to a DNS server in the Internet, the dynamic packet filter stores the data (source and destination address, source and destination port) and produces a new permission rule for the response packets. This rule is only valid for a certain period, which can be adjusted. If no response packets are received, it is deleted.

S 2.75 Selection of a suitable application gateway

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

An application gateway is a computer which uses the information in the application layer to filter connections.

This can, for example, be user names in connection with a strong authentication, special information in the transmitted data (e.g. check for computer viruses) or information of the application layer. An application gateway also offers the possibility of creating a unified access to the sub-network requiring protection and of concealing this network. The filter processes running on the application gateway are called **proxy processes**.

In the event that an application gateway is required for a firewall, the following demands should be made upon purchase:

- All important protocols (such as Telnet, FTP, SMTP, DNS, NNTP, HTTP) of the application layer must be treated.
- Filtering must be possible for each supported protocol according to all information stipulated in measure S 2.76 *Selection and Implementation of Suitable Filter Rules*. In particular, it must be possible to formulate the filter rules dependent on the user and to merge several users into one group.
- Filtering for contents should be supported, so that a central virus scan and the blockage of active contents is possible (see T 5.23 *Computer Viruses*).
- When using an application gateway, no changes should be necessary to the software in the network requiring protection or in the external network.
- The entry and control of filter rules must be simple and clear, e.g. by symbolic service and protocol names.
- The programs used must be well documented.
- It must be easy to add new protocols.
- It must be possible to record IP numbers, service, time and date for established and denied connections, with limitations on certain connections (e.g. for a special user).
- It must be possible to send all logging information to an external host.
- Special, adjustable events must lead to an immediate warning (e.g. repeated incorrect authentication attempts).
- Strong authentication methods must be used for user identification.
- The application gateway must support virtual private networks.

S 2.76 Selection and implementation of suitable filter rules

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Establishing and updating filter rules for a firewall is not a simple matter. The administrator must have an in-depth knowledge of the protocols used and be trained accordingly.

When **establishing the filter rules**, the following points should be observed:

- The rules should be formulated in such a way that all accesses which are not explicitly allowed are forbidden.
- If user-specific authentication is required, it must be clarified which users are in the inner network, which services they may use and which authentication processes are to be used.
- All computers in the inner network must be taken into consideration.
- It must be determined which services are to be available at what times. If an organisation has fixed working times and employees are only present between 7 am and 7 pm, for example, no connection should be established outside the usual working times.

The filter rules should be summarised in a table, with one axis representing the destination computer addresses, and the other axis the source computer addresses. The entries contain the permissible port numbers, the top one being the source port, the lower the destination port. Packet filters can check the packets immediately after receipt or before rerouting them. Here, filtering should be performed for the packets entering the packet filter. Furthermore, the packet filter should be configured in such a way that only the addresses of the computers connected to the interface are permitted as the sender address. Addresses connected with other interfaces are not permitted. This reduces the threat of IP spoofing attacks.

Example:

The following table contains filter rules for the internal interface of a packet filter between an internal network and a screened sub-net i.e. a sub-network located between the internal and the external network and which monitors the connections between them (see Fig. 1 in S 2.77 *Secure Configuration of Other Components*).

The entries contain the permissible connections, the upper entry being the source port, the lower being the destination port.

	Screend-Subnet		
to from	Appl. Gateway	external DNS server	external mail server
internal mail server	Ä	Ä	TCP > 1023 ÄÄÄÄÄÄ TCP: 25
internal DNS server	Ä	UDP: 53 ÄÄÄÄÄÄ UDP: 53	Ä
IT system with IP address 1.2.3.5	TCP > 1023 ÄÄÄÄÄÄ TCP: 20,21	Ä	Ä
IT system with IP address 1.2.30.7	TCP > 1023 ÄÄÄÄÄÄ TCP: 23	Ä	Ä
IT system with IP address 1.2.5.*	TCP > 1023 ÄÄÄÄÄÄ TCP: 23, 80	Ä	Ä
IT system with IP address 1.20.6.*	TCP > 1023 ÄÄÄÄÄÄ TCP: 80	Ä	Ä

This means that the internal mail server with TCP from a port with a port number > 1023 has access to port 25 (SMTP) of the external mail server in the screened sub-net. Ports with a port number > 1023 are also named as non-privileged ports, as opposed to ports with lower port numbers, which are named as privileged, as only privileged users (those with root authorisations) are entitled to establish connections with these ports.

This table must then be transformed into appropriate filter rules. This is frequently not simple and must therefore be checked precisely. On the basis of regular tests, it should be ensured that all filter rules have been correctly implemented. In particular, it must be ensured that only the services set out in the security policy are permitted.

For the rules of an application gateway, similar tables must be established. These tables are to be implemented in rules.

Example:

User name	service	command	Authentication
Mrs. Example	FTP	RETR, STOR	one-time password
Mr. Smith	FTP	RETR	chip card

Mrs Example can use the commands RETR and STOR of the service FTP, i.e. she can load and send files via FTP, whilst Mr. Smith can only load files.

S 2.77 Secure configuration of other components

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

In addition to the installation and operation of the firewall, other components for the communication between the protected and the external network must be correctly configured. These include, for example, information servers for the provision of information to internal or external users, mail servers and DNS servers.

When configuring the components, a distinction should be made as to whether these are to be set up in the protected network, in the screened sub-net or on the external side of the firewall. To allow a clear distinction to be made, the area between the inner packet filter and the application gateway is referred to as internal screened sub-net, the area between the application gateway and the external packet filter is referred to as external screened sub-net.

External Accesses

Other external accesses to the network requiring protection, e.g. with telnet via a modem pool, should be treated as accesses from the insecure network. This can be achieved, for example, by installing a terminal server with connected modems on the external side of the firewall so that access to the internal computer can only be carried out via Telnet. If virtual private networks (VPNs) are in use, it might be advisable to provide the required access via an additional interface on the application gateway.

Clear regulations must be made so that no external accesses can be created bypassing the firewall. These regulations must be made known to all employees. It must be ensured that both the IT Security Management and the firewall Administrator are informed of relevant plans in good time in order to guarantee inclusion in the IT security concept and the firewall security policy.

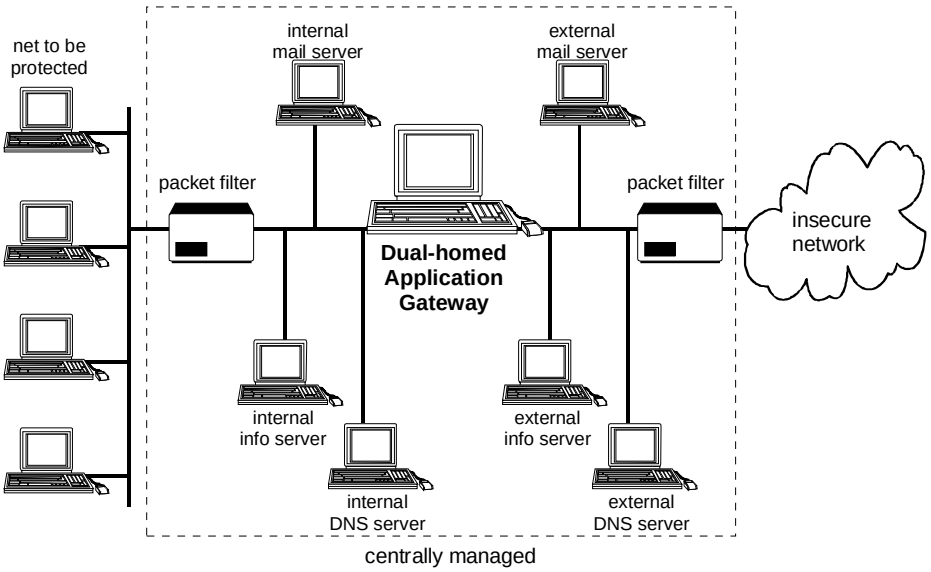


Figure 1: Screened sub-net with dual-homed gateway.

The illustration shows functional units, some of which can be joined together to form one unit (see Fig. 2), although this gives rise to additional security problems. The otherwise secure application gateway can, for example, be open to attack after it assumes the functions of the external DNS server if the DNS software contains an error.

Configuration of information servers

Information servers which provide information to external users must be outside the firewall and be considered in the same way as other servers in the external network. The management of these should either be local or via special time-limited accesses from the protected network. The data should be on write-protected data media.

In the event that some data should only be available for the user of the network to be protected, it is sensible to use further information servers in the internal screened sub-net (see Fig. 1). These data are then not accessible from outside and are protected against internal attacks by the packet filter.

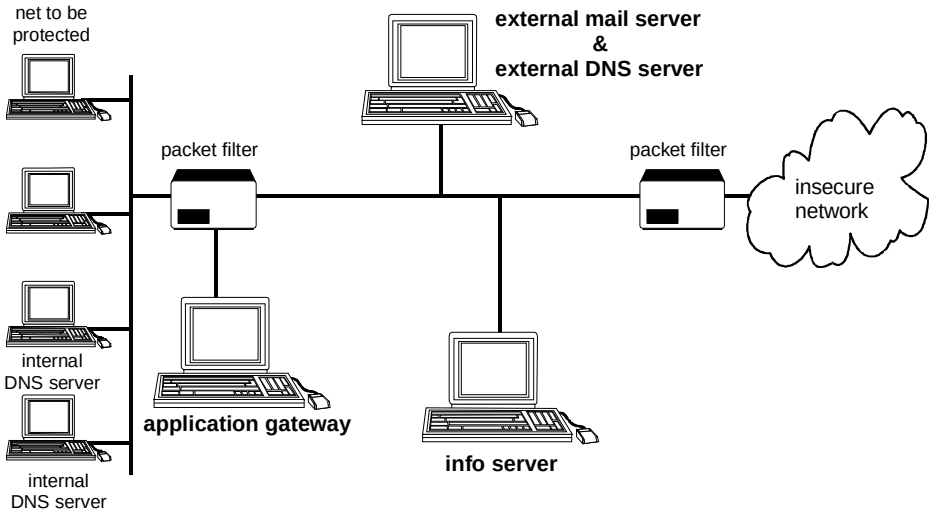


Figure 2: Screened sub-net with application gateway on a separate router interface.

The illustration shows functional units, some of which can be joined together to form one unit. This is shown by the external mail and DNS server.

Configuration of the mail servers

A mail server within the protected network is used for the management of the alias data base, which is for the purpose of transforming user addresses to a unified format, for a POP daemon or as a gateway for the connection to another mail system (e.g. X.400). All internal mail is sent to this server and then passed on to the outside via an external mail server.

The external mail server in the external screened sub-net creates the connection with external computers and accepts the mail from here so that the

internal structure of the protected network is concealed. This function can be assumed by the application gateway.

This configuration ensures that internal mail cannot enter the external network and a unified address structure can be used..

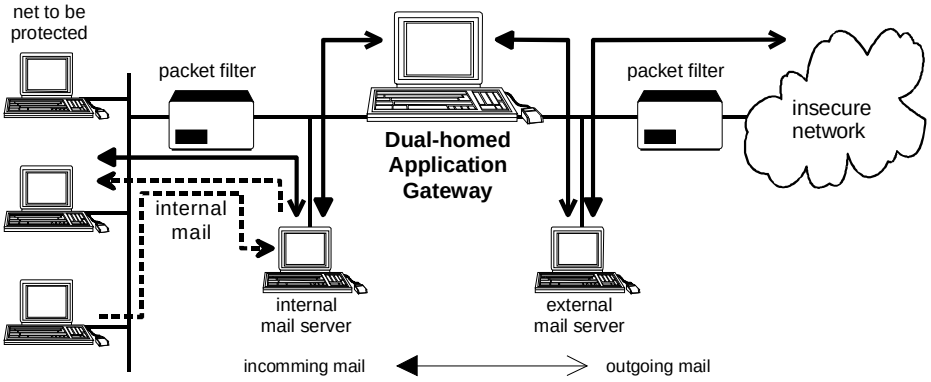


Figure 3: Configuration of the mail servers

Mail between computers in the network to be protected do not leave the network as they are passed on by the internal mail server which also manages the internal alias data base. Mail to external computers is sent via the gateway to the external mail server and then passed on. For mail from external computers, the MX entry (from the external DNS server, see Fig. 4) refers to the external mail server. The external mail server passes the mail to the internal server. It may be possible for the function of the external mail server to be assumed by the gateway.

Configuration of the DNS servers

Domain Name Service (DNS) is used to convert computer names into IP numbers and vice versa and provides information on computer systems using the network. DNS information should be concealed from the outside world, i.e. Internet or other external networks. The most well-known method of doing this is by a special configuration of two DNS servers (name servers). One DNS server in the internal screened sub-net conceals the structure of the network requiring protection and communicates with a DNS server in the external screened sub-net, in order to transform names of external computers. As DNS clients do not necessarily have to communicate with a DNS server on the same computers, it is possible to have both processes run on different computers.

The external DNS server must be configured in such a way that it claims to be the authority for the domain of the protected network (primary server). Of course, this system only knows what is intended to reach the outside world, i.e. names and IP numbers of external mail servers, the application gateway and the external information server. This is then a public DNS server.

The internal DNS server must also be configured in such a way that it claims to be the authority for the domain of the protected network.. Unlike the external DNS server, this private DNS server manages all internal DNS information and passes on search enquiries from internal computers for external hosts to the external DNS server.

All DNS clients, including those on the application gateway, must be configured in such a way that they always use the internal DNS server (e.g. using entries in the file */etc/resolv.conf*).

If an internal client asks for an internal computer, the internal DNS server is used. If an internal client or a client on the application gateway asks for an external computer, the internal DNS server is consulted, which in turn consults the external DNS server, which in turn consults the Internet, which then responds.

An external client which asks for an internal host receives the restricted list from the external DNS server.

The packet filter used must be configured in such a way that only the DNS service is permitted between the servers, i.e. DNS port 53 as the source and destination port. The approval of other ports (> 1023) is thus not necessary.

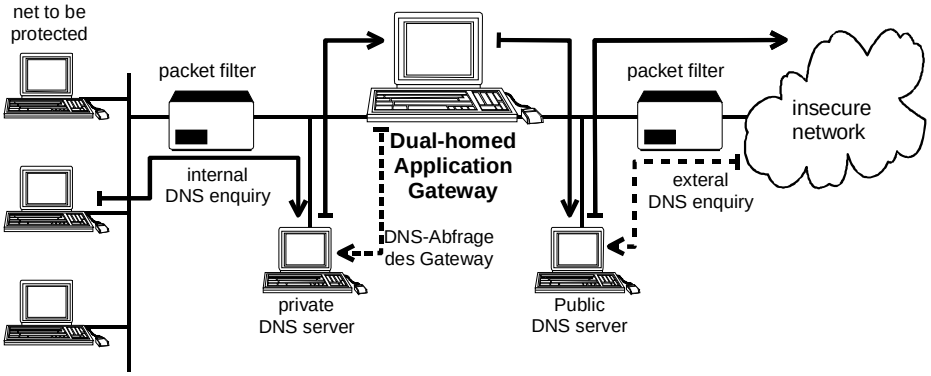


Figure 4: Configuration of the DNS servers

The private DNS server is the primary DNS server for the protected network and passes enquiries about external computers to the public DNS server. The client on the gateway is configured in such a way that the private DNS server is first asked, which then may pass the enquiry on to the public DNS server. For external computers, the public DNS server is the primary DNS server for the protected network. However, it only contains the entries of the computers which are to be made known to the outside world.

S 2.78 Secure operation of a Firewall

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

In order to ensure correct operation of a firewall, the adherence to the required safeguards should be checked on a regular basis. In particular, the organisational provisions for the operation of the firewall should be regularly / randomly checked to ensure that these are being adhered to. Regular checks should be carried out as to whether new accesses have been created bypassing the firewall.

Regular tests should also be carried out to ensure that all filter rules have been correctly implemented. It should be ensured that only those services stated in the security policy are permitted.

In the event that alterations are to be made to the security policy at a later date, these must be closely monitored and checked for side effects, in particular.

The demands placed on packet filters and application gateways when these were purchased should be implemented. They should be updated regularly and checked for completeness.

The default setting of the filter rules and the configuration of the components must ensure that all connections not explicitly allowed are blocked. This must also apply in the event of complete failure of the firewall components.

The following should generally apply: **"Everything is forbidden unless explicitly permitted"**. A user with no entry in an access list, for example, has no way of using the Internet.

The following points should also be observed:

- In order to prevent the eavesdropping of, or alterations to, the authentication information, the Administrator and Auditor may only authenticate themselves via a trustworthy path. This can be directly via the console, for example, an encoded connection or a separate network.
- Integrity tests of the software used must be carried out in regular intervals. The firewall must be switched off in case of errors.
- The firewall must be tested for its behaviour in case of a system crash. In particular, an automatic restart must not be possible and it must be possible to store the access lists on a write-protected medium. The access lists are the main data for the operation of the firewall and must be specially secured so that no old or faulty access lists are used when the unit is restarted as the result of an attack.

  In case of failure of the firewall, it must be ensured that during this time no network connections can be made from, or to, the protected network.
- The components used may only contain programs which are required for the operation of the firewall. The use of these programs must be documented and justified in detail. The software for the graphic user interface, for example, should be removed as well as all superfluous

drivers. These should also be removed from the operating system core. Remaining software must be documented and justified.

- When restoring backup data, it must be ensured that the files for the correct operation of the firewall are up-to-date, such as access lists, password files or filter rules.

S 2.79 Determining responsibilities in the area of standard software

Initiation responsibility: Agency/company management

Implementation responsibility: Head of IT Section, Head of organisation

Prior to the introduction of standard software, a number of responsibilities must be determined, such as for the drawing up of a requirement catalogue, the pre-selection of products, testing and approval, and the installation.

Below is a proposal of how these responsibilities may be sensibly allocated. As titles vary from organisation to organisation, some functions are described according to their tasks:

- The **specialist department** is the user of the standard software. This department states its need for new software and thus initiates procurement. It is involved in the pre-selection and testing stages in order to include the requirements of the user.
- The **agency/company management** is responsible for the approval of the standard software. This responsibility is mostly delegated to the **Head of the Specialist Department**. After approval of the software, responsibility for correct usage of the standard software is transferred to the specialist department.
- The **IT area** has the task of providing IT solutions to fulfil the tasks of the specialist department and of guaranteeing correct and reliable operation of the IT.
- The **procurer** must ensure the interoperability and compatibility of the standard software and the adherence to internal standards and legal stipulations. There are often IT Co-ordinators in the individual departments who assume the tasks of the procurer and co-ordinate the budgetary funds of the departments.
- The **budget** is responsible for accounting, the IT budget management and for the provision of the necessary budgetary funds.
- The **IT Security Officer** must check whether an appropriate security level can be guaranteed with the products used or to be purchased. As part of the IT Security Management (c.f. Chapter 1), he must ensure IT securing during current operation.
- The **Data Privacy Officer** must ensure adherence to the provisions relating to data protection and adequate protection of person-related data.
- The **staff or work council** must in most cases be involved in the selection of new standard software, particularly if this means considerable changes to work processes or if the software is suitable for performance monitoring (see S 2.40 *Timely Involvement of the Staff / Factory Council*).

Throughout the entire process concerning "standard software", it must be determined for each step which of the above are implementation responsibility

and which have to be involved. A sensible proposal for distributing responsibilities is summarised in the following table::

	responsible	**to be involved**
Compiling the requirement catalogue	Specialist Department, IT Area	Procurer, Budget Manager, IT Security Officer, Data Privacy Officer, Staff or Works Council
Selection of a suitable product	Procurer	IT Area, Specialist Department
Testing	Specialist Department and IT Area	IT Security Officer, Data Privacy Officer, Staff or Works Council
Approval	Management of Agency/Company, - maybe delegated to Head of Specialist Department	-
Procurement	Procurer	Budget Department
Ensuring integrity of the software	IT Area	-
Installation and configuration	IT Area	-
Version checking and licence management	IT Area	-
Deinstallation	IT Area	-
Checking IT operation	IT Security officer	-

The allocation of these responsibilities should be set down in writing and it should be checked on a regular basis that the relevant procedures are correctly adhered to.

Additional controls:

- Which provisions are in force?
- Are all employees aware of existing regulations and the monitoring of these regulations?
- Are all relevant bodies (e.g. staff council, budget department, Data Privacy Officer) involved to the appropriate extent?

S 2.80 Drawing up a requirements catalogue for standard software

Initiation responsibility: Head of the Specialist Department

Implementation responsibility: Specialist Department, Head of IT Section

In order to solve a task processed with IT, there are a number of similar standard software products available on the market. These are similar in their basic functions but differ in certain criteria, such as purchase and operating costs, additional functions, compatibility, administration, ergonomics and IT security.

Requirements Catalogue

When selecting a suitable product, a Requirements Catalogue must first be compiled. The Requirements Catalogue should contain information on the following points:

- **Functional requirements** which the product must meet concerning the fulfilment of the task of the relevant department. The individual functions relevant for the specific task should be highlighted.

  Brief examples:

  - Word processing with the additional functions: the inclusion of graphics, macro programming, spell check and syllabification. It must be possible to switch off the macro programming, the spell check must be available in English, French and German. It must be possible to import and export the specified text formats.
  - Data base (front end and back end) for multi-user operation with support of the standard language SQL and graphic user interface.
  - Appointment calendar to co-ordinate and monitor appointments of the members of the department with integrated appointment coordination, automatic despatch of invitations and tasks and priority lists, connection to the internal mail program.

- **IT environment**. On the one hand, this is determined by the requirements of the existing or planned IT environment and on the other hand by the requirements placed on the environment by the product.

  Brief examples:

  - Predetermined IT environment: With Novell 3.11 networked PC, 80486 processor, 8 MB main memory, 500 MB hard disk capacity, disk drive, CD ROM drive, MS DOS 6.0. The product may occupy a maximum of 50 MB on the hard disk, it must run under Windows 3.11 and be compatible for networking.
  - System requirements: The word-processing program X requires 16 MB, it runs on a PC with at least a 80386 processor, 8 MB main memory, Windows 3.11.

- **Compatibility requirements** with other programs or IT systems, i.e. migration support and upward and downward compatibility.

Brief examples:

- Data in the existing data base XYZ must be taken over.
- The functions A, B, C must remain in the event of version exchange.
- The exchange of data with the UNIX system XYZ must be possible.

- **Performance requirements** describe the required performance as regards throughput and running time. Information concerning the maximum permissible processing time should be as precise as possible for the required functions.

  Brief examples:

  - The maximum response time when carrying out function X must not exceed 2 seconds.
  - The encryption rate should be at least 60 KB/sec on a 486 DX 33.
  - Other simultaneously conducted process must not be slowed down by more than 30 % as a result of the product.

- **Interoperability requirements**, i.e. it must be possible to work together with other products despite platform limitations.

  Brief examples:

  - Versions of the word processing program should be available for Windows, UNIX and Macintosh platforms. It should be possible to compile documents on one operating system and processes them on another.
  - The text processing program must be able to work together with the mail program used.

- **Reliability requirements** affect the stability of the products, i.e. the detection of errors and tolerance, failure and operational security.

  Brief examples:

  - Incorrect input by the user must be detected and must not cause the program or system to crash.
  - The data base must have mechanisms which allow all transactions to be reconstructed (roll forward) in the event of a crash with destruction of the data base.

- **Conformity with standards**. These may be international standards, de-facto standards or internal standards.

  Brief examples:

  - The product must comply with the EU monitor guideline 90/270/EEC.
  - The implementation of a token ring LAN must be in conformance with ENV 41110.
  - The product must be in accordance with the X/Open Standard.

- **Adhering to internal regulations and legal stipulations** (e.g. sufficient data protection when processing person-related data)

  Brief examples:

  - The product must comply with the principles of proper EDP-controlled auditing systems.
  - As person-related data are processed, it must be possible to meet the requirements stipulated in the Federal Data Privacy Act.

- **Requirements regarding user-friendliness**, characterised by how easy the system is to operate, understand and learn, i.e. particularly by the quality of the user interface and documentation, and the help functions.

  Brief examples:

  - An on-line help function must be available.
  - The user interface must be designed in such a way that unskilled persons can become familiar with the basic functions within two hours.
  - The documentation should be available in the local language.

- **Requirements concerning serviceability** for the user are mainly based on the handling of errors.

  Brief examples:

  - The amount of administration involved must not be too high.
  - The provider must offer a hotline for questions.
  - The product must be easy to install and configure.
  - The product must be easy to deinstall.

- The **maximum costs** resulting from the purchase of this product are predetermined. Not only the immediate purchase costs should be taken into consideration, but also costs arising at a later date, e.g. for updating hardware, personnel costs or training.

  Brief examples:

  - The product may cost a maximum of DM 15,000.
  - The training costs must not exceed DM 2,000.

- The **requirements concerning documentation** must highlight which documents are required and in which quality (completeness, comprehensibility).

  Brief examples:

  - The user documentation must be easy to understand and suitable for reading without instruction. All functions of the product should be described.
  - The system manager documentation must include troubleshooting information.

- Demands on software can range from the manufacturer's declaration concerning the quality assurance systems used, ISO 9000 etc. certificates to independent software tests according to ISO 12119.

  Brief examples:

  - The software production process of the manufacturer must be certified according to ISO 9000.
  - The functionality of the product must be checked by an independent body according to ISO 12119.

- It the product is to fulfil IT security functions, these are to be set down in security requirements (c.f. S 4.42 Implementation of Security Functions in the IT Application). This is described in detail below.

Security Requirements

Dependent on whether the product must have security features, security functions can be stipulated in the Requirements Catalogue. Typical security functions which are relevant here are briefly explained. Further details are to be found in the ITSEC.

- Identification and authentication

  Many products require that those users who have access to resources controlled by the product should be determined and monitored. Not only the claimed identity of the user should be determined, but it should be checked whether the user really is the person he claims to be. This takes place by the user providing the product with information connected to the user in question.

- Access control

  For many products it will be necessary to ensure that users and processes working for these users are prevented from gaining access to information or resources when they are not entitled to access or when access is not necessary. Further, there will be requirements concerning the unauthorised creation or modification (including deletion) of information.

- Logging

  For many products it will be necessary to ensure that actions taken by users or processes on behalf of such users are recorded. This allows the consequences of such actions to be assigned to the user in question so that the user can be held responsible for his actions.

- Protocol evaluation

  For many products it will be necessary to ensure that sufficient information is recorded concerning both usual and unusual incidents. Checks at a later date can thus determine whether security breaches have taken place and which information or other resources were affected.

- Incorruptibility

  For many products it will be necessary to ensure that certain relations between various data remain correct and that data can be transferred between various processes without alteration.

Furthermore, functions must be available which allow losses, additions or alterations to be detected when transferring data between various processes, users and objects, and which make it impossible to alter the supposed or actual origin or destination of the data transmission.

- Reliability

  For many products it will be necessary to ensure that time-critical tasks are carried out at precisely the required point in time, i.e. not earlier and not later. It is also necessary that tasks which are not time-critical are not transferred into time-critical tasks. Furthermore, it is necessary for many products to ensure that access is possible at the relevant moment and that resources are not unnecessarily called up or withheld.

- Transmission security

  This term comprises all functions designed for the protection of data during transmission via communication channels:

  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - non-repudiation

  Some of these functions are implemented by means of cryptographic processes.

Further security requirements in addition to ITSEC can be placed on standard software.

- Data backup

  Great demands are placed on the availability of data processed with the product. This includes functions integrated in the product which serve to prevent data loss, such as the automatic saving feature or the automatic creation of backups before making major alterations.

- Encryption

  Encryption serves as a preserver of data confidentiality. For many products it will be necessary to encrypt data before transmission or after processing and to decrypt information after receipt or before rerouting. An accepted encryption algorithm should be used for this purpose. It should be ensured that the parameters required for decrypting (e.g. key) are protected in such a way that unauthorised access to this data is not possible.

- Functions for the preservation of data integrity

  In case of data whose loss of integrity could lead to damage, functions can be used which are able to detect or even correct errors by means of redundancy. In most cases, integrity tests are used which can reliably detect intentional manipulation of the product or data and any unauthorised replay of data. These tests are based on cryptographic mechanisms (see S

5.36 *Encryption under UNIX and Windows NT* and S 4.34 *Using Encryption, Checksums or Digital Signatures*)

- Requirements concerning data privacy

  If person-related data are to be processed with the product, additional special technical requirements should be placed beside the stated security functions in order to be able to comply with data privacy stipulations.

Strength of the Mechanisms

Security functions are implemented by mechanisms. Depending on the field of usage, these mechanisms must be of various strengths which provide defence against attacks. The necessary strength of the mechanisms is set forth in the Requirements Catalogue. According to ITSEC, differentiations are made between three mechanism strengths:

- **low**: offers protection against unintentional attacks, e.g. operational errors
- **medium**: offers protection against attackers with limited opportunities or resources.-
- **high**: can only be overcome by attackers with an extensive knowledge, opportunities and resources. A successful attack is generally not considered possible.

Examples of Requirements on Security Features

Below are examples of some important security functions which highlight typical requirements placed on security features.

In the event that the product is to have an **identification and authentication mechanism**, the following requirements could be made, for example:

- Access should only be possible via a defined interface. A log-on mechanism can be used, for instance, which requires unique user identification and a password. In the event that the identity of the user is known when the IT system is accessed, an anonymous password is sufficient. Other possibilities are processes based on certain "tokens", such as a chip card.
- The access procedure itself must correctly handle the critical parameters, such as password, user identification etc. Current passwords should thus never be stored unencrypted on the relevant IT systems.
- The access procedure must react to incorrect entries in a predefined manner. For instance, if an incorrect authentication takes places three times consecutively, the access to the product should be rejected. Alternatively, the time intervals in which further access attempts can be made should be gradually increased.
- The access procedure must allow certain minimum requirements for security-critical parameters to be set. The minimum length of a password, for example, should be 6 characters, the minimum length of a PIN should be 3 digits. The syntax for passwords can also be stated, as necessary.

If the product is to have **access control**, the following requirements can be placed, for instance:

- The product must be able to differentiate between various users.
- The product must be able to assign resources to individual authorised users and to completely deny access to unauthorised parties.
- It should be possible to control access by means of a differentiated rights structure (read, write, execute, change etc.). The data relevant for the management of rights should be managed in such a way that they are protected against manipulation.

In the event that the product is to **keep log records**, the following requirements are recommended:

- The minimum the product must be able to record should be parameterisable. It should be possible to record the following actions, for example:
  - For authentication: User ID, date and time, success, ...
  - For access control: user ID, data and time, success, type of access, what was changed, read, written, ...
  - Implementation of administrative activities
  - Occurrence of operational errors.
- Unauthorised persons must neither be able to deactivate the logging function, nor should they be able to read or edit the actual logs.
- Logs must be clear, complete and correct.

In the event that the product is to have a **protocol evaluation** feature, the following requirements are recommended:

- An evaluation function must be able to distinguish between the various data types contained in a log (e.g. "filtration of all unauthorised attempts at accessing any resource over a specified time period").

  The evaluation function must be capable of generating transparent, readable reports so that no critical security-related activities can be overlooked.

In the event that the product is to have functions concerning **incorruptibility**, the following requirements can be placed, for example:

- A data base management system must be able to describe rules of certain relationships between the stored data (e.g. referential integrity). Furthermore, suitable mechanisms must be in place which prevent these rules being violated by changing data.

In the event that the product is to have functions regarding **data backup**, the following requirements can be placed, for example:

- Specifications can be made as to which data should be backed up when.
- An option for loading any required data backup is available.
- It is possible to backup several generations.

- It is possible to backup instantaneous data at specified intervals while an application is being run.

In the event that the product is to have **encryption components**, the following requirements are recommended:

- Encrypted algorithms used by government agencies should be approved by the BSI. Individual consultation by the BSI is recommended in this case. If not in agencies, the DES is suitable for moderate protection requirements.
- The key management must be in line with the functionality of the product. In particular, fundamental differences between algorithms must be considered here:
  - symmetric algorithms use a key for encrypting and decrypting which is to be kept secret,
  - asymmetric algorithms use a public key for encrypting and a private key (to be kept secret) for decrypting.
- The product must correctly manage security-critical parameters, such as the key. Keys should thus never be stored unprotected (even expired keys), i.e. readable.

In the event that the product is to have an **integrity test** feature, the following requirements are recommended:

- The product carries out an integrity check every time a program is called up.
- Mechanisms should be used which can detect intentional manipulation of address fields and payload data during data transmission. Knowledge of the algorithms alone, without other special knowledge, should not be sufficient to manipulate the above data without detection.

In the event that person-related data are to be processed with the product, the following **requirements concerning data privacy** are placed, for example:

- The product may not permit general requests for data analyses. These analyses of data must be limited to certain criteria.
- It must be possible to parameterise the system in such a way that changes, deletions or print-outs for certain files are only possible according to the two-person principle.
- It must be possible to parameterise the logging feature in such a way that records can be kept of who made which changes to person-related data.
- The transfer of person-related data must be determined and checked with suitable random tests (BDSG, § 10). The type of random test must be individually programmable.
- The product must enable person-related data to be deleted. Alternatively, it must be possible to block person-related data in order to limit or prevent these being processed or used.

Assessment Scale

In order to be able to carry out a comparison of various products, criteria must be available as to what extent the various requirements are fulfilled. To do this, it is necessary to assess the quantitative and qualitative importance of the various requirements for the IT-supported task.

This assessment can take place in three steps, for example. In the first step, it is determined which features stipulated in the Requirements Catalogue are **necessary** and which are **desirable**. If a necessary feature is not fulfilled, the product is rejected (so-called K.O. criterion). In the event that a desirable feature is not fulfilled, this is considered as a negative aspect, but the product is not necessarily rejected as a result.

As a second step, the **importance** of the desirable features is determined. This can be quantitative, for example, with values between 1 for low and 5 for high. Necessary features must not be assessed quantitatively. In the event that this is necessary, however, these features must be of a higher value than the desirable features (in order to highlight the importance of a necessary feature, it can represent a value of 10, for example).

In the third step, a **confidence factor** is determined for the feature with regard to fulfilment of its intended task (e.g. with values between 1 for low and 5 for high). On the basis of this confidence factor, a decision is taken as regards the extent to which feature is to be tested. The confidence factor of the security mechanisms must be determined in accordance with their strengths.

- low mechanism strength with confidence factor 1
- medium mechanism strength with confidence factor 3
- high mechanism strength with confidence factor 5

These guidelines should be checked according to the individual cases.

Examples:

In extracts, security requirements for some typical standard software products are described below:

Word processing programs:

Necessary security features:

- Automatic saving of intermediate data while the program is running

Desirable security features:

- Password protection of individual files
- Encryption of individual files
- It must be possible to switch off the macro programming

File compression program:

Necessary security features:

- With regard to data preservation, files to be deleted after compression must only be deleted by the compression program if compression has been performed successfully.
- Before a file is decompressed, its integrity must be checked so that bit errors in the compressed file can be detected, for example.

Desirable security features:

- Password protection of compressed files

Appointment calendar:

Necessary security features:

- Reliable identification and authentication of the users must take place, e.g. using passwords.
- Access control for the appointment calendars of the various employees is required.
- It must be possible to assign separate access rights for individuals, groups and superiors.
- It must be possible to differentiate between read and write access.

Desirable security features:

- Automatic backup of data in an encrypted form should be possible.

Travel expenses calculation system:

Necessary security features:

- Reliable identification and authentication of the users must take place, e.g. using passwords.
- Access control must be in place and available for individual data records.
- It must be possible to assign separate access rights for the user, administrator, auditor, and data privacy officer. It must be possible to separate the functions of administrator and auditor.
- Data backups must be performed in such a way that they are stored in an encrypted form and can only be accessed by authorised persons.
- Detailed logging functions must be in place.

Desirable security features:

- An optional integrity check for payment-related data should be available.

Example of an assessment scale:

A specialist department intends to purchase a compression program for data backup purposes. After a Requirements Catalogue has been drawn up, the features specified in the catalogue could be assessed as follows:

Feature	necessary	desirable	Significance	Confidence factor
Correct compression and decompression	X		10	5
Detection of bit errors in a compressed file	X		10	2
Deletion of files only after successful compression	X		10	3
DOS-PC, 80486, 8 MB	X		10	5
Windows compatible		X	2	1
Throughput at 50 MHz above 1 MB/s		X	4	3
Compression rate over 40% with text files of the program XYZ		X	4	3
On-line help function		X	3	1
Maximum costs 50 DM per licence	X		10	5
Password protection for compressed files (high mechanism strength)		X	2	5

Additional controls:

- Who is involved in the drawing up of the Requirements Catalogue?
- Who decides whether a product must contain security functions?
- Are there standardised requirements concerning how an analysis should be structured?

S 2.81 Preselection of a suitable standard software product

Initiation responsibility: Procurer

Implementation responsibility: Procurer, Head of IT Section, Specialist Department

The preselection of a standard software product is based on the Requirements Catalogue drawn up by the Specialist Department and the IT Area. First, the body responsible for preselection should conduct a market analysis and draw up a tabular market overview based on the Requirements Catalogue. This table should comment on the products in question with regard to the points stipulated in the Requirements Catalogue.

The market overview should be drawn up by the IT Area. It can be compiled using product descriptions, declarations by the manufacturer, journals or information from retailers. Alternatively, an invitation to tender is possible and occasionally required. The Requirements Catalogue should be the basis of such an invitation to tender so that a market overview can be drawn up using the offers received.

Finally, the products contained in the market overview must be compared with the points contained in the Requirements Catalogue. To do this, the assessment scale in S 2.80 *Drawing up a Requirements Catalogue for Standard Software* can be used. On the basis of this information, it is determined which of the required product features are in place. In the event that certain required features are missing, the product is rejected. A total can be determined using the assessment of the importance of the various features of the products. A list of the most favourable products can then be drawn up based on these totals.

Example:

The features for a compression program as stated in the Requirements Catalogue are weighted as follows:

Feature	Necessary/ desirable	Significance	Product 1	Product 2	Product 3	Product 4
Correct compression and decompression	N	10	Yes	Yes	Yes	Yes
Detection of bit errors in a compressed file	N	10	Yes	Yes	K.O.	Yes
Deletion of files only after successful compression	N	10	Yes	Yes	Yes	Yes
DOS-PC, 80486, 8 MB	N	10	Yes	Yes	Yes	Yes
Windows compatible	D	2	No	Yes	Yes	Yes
Throughput at 50 MHz above 1 MB/s	D	4	Yes	Yes	Yes	No
Compression rate over 40% with text files of the program XYZ	D	4	Yes	Yes	No	No
On-line help function	D	3	No	No	No	Yes
Maximum costs 50 DM per licence	N	10	Yes	Yes	Yes	Yes
Password protection for compressed files (high mechanism strength)	D	2	Yes	Yes	No	Yes
Assessment		**65 (=max)**	**60**	**62**	**K.O.**	**57**

As a result, Product 3 is excluded as a necessary feature is not available. The most favourable product is thus Product 2, followed by Product 1 and 4.

This list and the market overview should then be submitted to the procurer so that he can check how far the products comply with internal and legal

regulations. The procurer must also ensure that the other bodies whose stipulations must be adhered to, such as the Data Privacy Officer, the IT Security Officer or the Staff / Works Council, are involved in good time.

It must be decided how many and which candidates on the list should be tested. For obvious reasons the first two or three product leaders should be selected and tested as to whether they actually fulfil the most important criteria of the Requirements Catalogue. This is particularly important with regard to the necessary requirements. Test licences should be obtained and tests carried out as described in S 2.82 *Developing a test plan for Standard Software* and S 2.83 *Testing Standard Software*.

Besides to the criteria of the Requirements Catalogue, the decision can be based on the following points:

- References

  If the manufacturer or distributor can provide reference installations for his product, the experience of this user can be included in the assessment of the product.

  In the event that external test results or quality assurances are available for the software product (e.g. test results in journals, conformity tests according to accepted standards, tests and certificates according to relevant standards and norms, such as ISO 12119), these results should be taken into consideration during the preselection process.

- Product popularity

  In the event that the product is widely spread, the individual user has little or no influence on the product manufacturer as far as troubleshooting or the implementation of certain functions is concerned. He can assume, however, that the product is further developed. There are often external tests carried out by journals or commissioned by the manufacturer. With popular products, weaknesses are generally more widely known which means that the user can assume that most weaknesses are already known and that the knowledge concerning weaknesses and remedies is distributed quickly, i.e. he can obtain help.

  In case of a low degree of popularity, a user can have more influence on the manufacturer. External tests are generally not available as these are too expensive and time-consuming for products from small manufacturers. Products with a low degree of popularity do not usually contain more errors than those which are widely spread. The disadvantage is that these errors are often not detected as quickly, thus allowing swift elimination. If security breaches are involved, however, these are probably not known to potential attackers or they are not worthwhile targets.

- *Cost-effectiveness / costs for purchase, operation, maintenance and training*

  Before the decision to purchase a certain product is taken, the following question should always be asked: Is the cost of the product proportionate to the benefits of the product? In addition to the initial purchase costs, the costs for operation, maintenance and training should be considered. It should be clarified, for example, whether the existing hardware platform

has to be updated or whether training is needed for installation and operation.

When the decision has been taken to purchase a product, it should obviously be purchased from the least expensive supplier. This may have become clear from the market research.

Additional controls:

- Which provisions are in force?
- Does the selected software offer all functions stated in the Requirements Catalogue?
- Is the product compatible with the current IT infrastructure?
- Which additional costs are to be expected for training and maintenance, for example?
- Can installation and operation be carried out by existing staff, is additional staff necessary or does external advice have to be obtained?

S 2.82 Developing a test plan for Standard Software

Initiation responsibility: Agency/company management

Implementation responsibility: Head of Specialist Department, Head of IT Section

The test procedures described below are based on DIN ISO/IEC 12119 "Software Products, Quality Requirements and Testing Conditions", the Procedural Model for the Planning and Implementation of IT (V Model) and the Information Technology Security Evaluation Handbook (ITSEM), which are recommended as secondary literature.

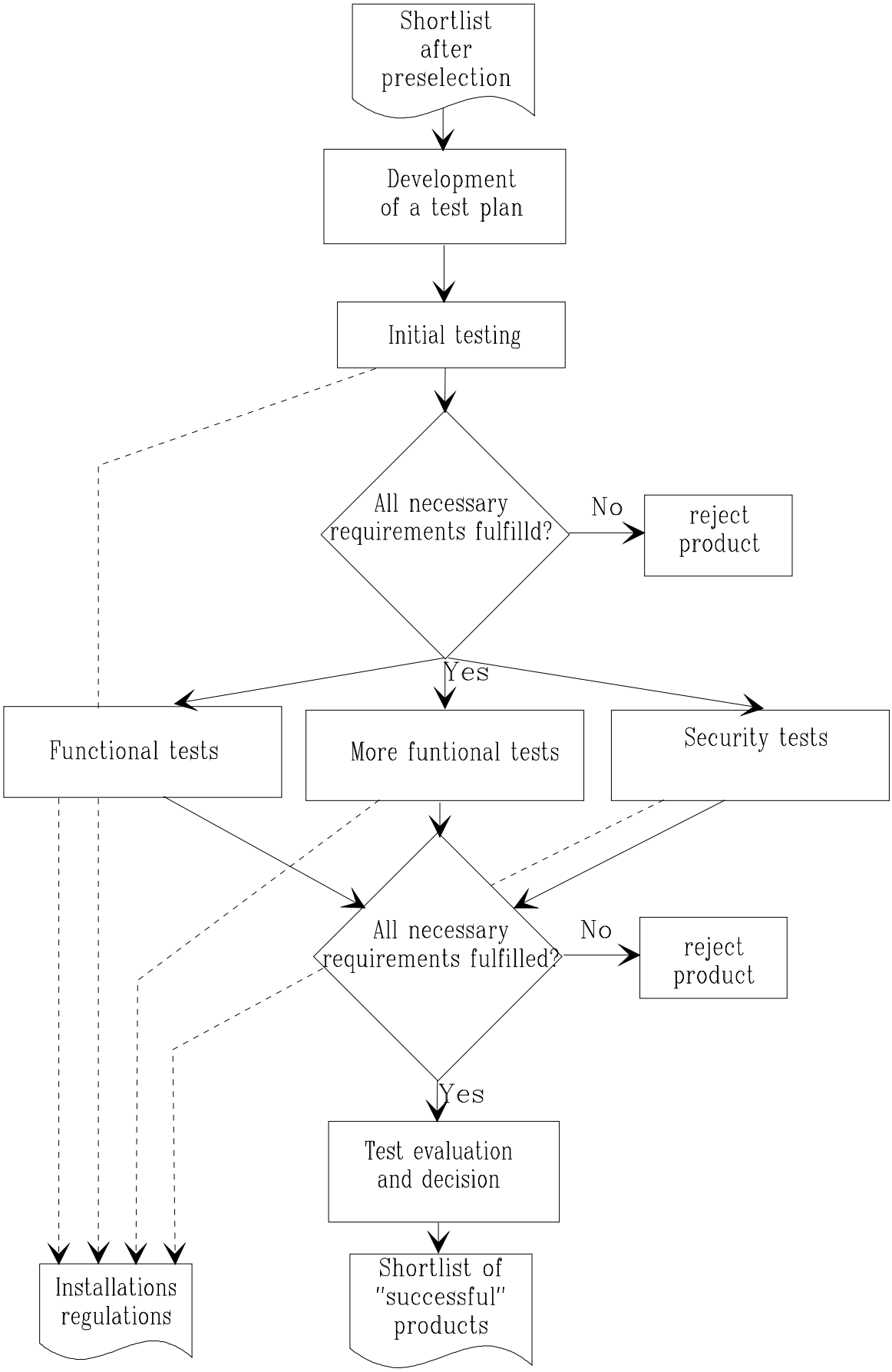
Before deciding on a suitable software product, the products which were shortlisted according to the preselection (see S 2.81 *Preselection of a Suitable Standard Software Product*) must be obtained with a test licence and sufficiently tested. If it was not possible to test the product before purchase due to time limitations, internal procurement recommendations (adherence to internal standards) or any other reasons, tests must be conducted before the product is put into operation. The results of these tests then form the basis for the installation regulations and other approval conditions.

Although the product requirements were checked in the preselection stage on the basis of the manufacturers' declarations, it cannot be assumed that these requirements are met to the desired extent. Systematic testing must be conducted in order to check the suitability and reliability of the product on the basis of the Requirements Catalogue so that the most suitable product can then be selected.

It is recommended to divide these tests into four areas:

- Initial tests (tests for computer viruses, operation in the intended IT environment, ...)
- Functional tests (test of the functional requirements)
- Tests of other functional features (compatibility, performance, interoperability, conformity with regulations or laws, user-friendliness, serviceability, documentation)
- Security tests (check of the security requirements)

The test procedure of standard software is illustrated below.


Shortlist after preselection
Development of a test plan
Initial testing
All necessary requirements fulfilld?
No
reject product
Yes
Functional tests
More funtional tests
Security tests
All necessary requirements fulfilled?
No
reject product
Yes
Test evaluation and decision
Installations regulations
Shortlist of "successful" products

On the basis of the shortlist drawn up during the preselection stage, those products should be selected which are to be tested. A **test plan** is then compiled.

This plan comprises the following:

- Determining the contents of the test on the basis of the Requirements Catalogue
- Checking references
- Determining the total testing time
- Time planning, including time required for each test
- Determining persons-in-charge of testing
- Testing environment
- Contents of the test documentation
- Determining decisive criteria

These points are described in detail below.

Determining the contents of the test on the basis of the Requirements Catalogue

The requirements which are to be tested are selected on the basis of the Requirements Catalogue. In particular, these should be the features which are of great importance or which have a high confidence factor.

Checking references

Initial references were obtained during the preselection stage (see S 2.81 *Preselection of a Suitable Standard Software Product*). These can also be obtained if the external test group gives rise to sufficient confidence.

If a certificate was issued for the product in accordance with the criteria for the evaluation of the security of IT systems (ITSEC) or the Common Criteria (CC), the certification report should be used to check to what extent the test results can be taken into consideration.

An internal test can either be dispensed with or conducted on a small scale. The test capacities this leaves free can be distributed among other tests.

Determining the total testing time

In order to limit the time required for testing, the total time should be determined in advance, e.g. in working days or by setting a deadline.

Time planning, including time required for each test

When testing several products, it is recommended to run comparative tests. This means that all products are tested by one test group or in regard to one requirement of the Requirement Catalogue. The testing time should thus be determined for each requirement of the Requirement Catalogue and is thus automatically distributed evenly among all products to be tested. The testing time results from the testing depth and complexity of the feature. The testing

depth of the various features should be based on the confidence factor, i.e. the amount of confidence placed in the correct operation of this feature. The proneness to error and frequency of use of the feature must also be taken into consideration. More detailed information is to be found in ISO 12119.

Notes:

- For requirements relevant to security, the test depth can also be adapted to the mechanism strength required.
- The testing time for the initial tests should be kept to a minimum in regard to the other tests.

The total testing time should then be distributed to the individual test sections in accordance with the relative testing time of the feature.

Determining persons-in-charge of testing

It should be determined for each test which tasks are to be carried out and who is responsible for these. In particular, it should be ensured that the staff / works council, the Data Privacy Officer and the IT Security Officer are involved in some tests.

Test environment

Testing is always destructive as errors are being looked for. Tests should thus always be conducted in an isolated test environment.

If possible, the test environment should be a precise functional copy of the production environment. It is generally not viable to completely recreate the production environment.

So that the same conditions are present for the selected products, a reference test environment should be defined. This can be further adjusted or limited for individual tests.

The resources required for the various tests (equipment, IT infrastructure) should be specified. It should be described in detail when, and to what extent, these must be available.

It is important that all operating systems in all versions used in production are available in the test environment. The intention is to determine system-based weaknesses of components of the production environment in connection with the standard software production to be installed. In exceptional cases, if aspects can be generalised, individual components can be omitted.

The following aspects should be observed and help to set up a reliable and suitable test environment:

- An up-to-date virus scan program should ensure that the test environment is free of viruses.
- The test environment must be free of side effects on the actual operation. In order to avoid interaction from the outset, the installation of dedicated IT systems is recommended.
- The access rights must be configured in the test environment in the same way as in the production area.

- The access to the test environment must be controlled.
- When taken over into production, it must be ensured that the product is configured in the same way as in the test environment. A suitable integrity protection system (digital signatures, checksums) should thus be used in the test environment.
- The costs for setting up the test environment must be acceptable.

After all planned tests have been concluded, it should be decided whether the test environment is to be dismantled. It may be necessary for more tests to be carried out, i.e. it might be viable to retain the test environment. Before the test environment is dismantled, the test data should be deleted if no longer required (e.g. for installation at a later date). Printer products should be disposed of correctly, programs should be deinstalled. The test licences of the products which were not selected should be returned.

Contents of the test documentation

The test plan should state how detailed the test documentation should be. The aspects of comprehensibility, reproducibility and completeness should be taken into consideration.

The test documentation must contain test plans, targets, processes and results. It must also describe the correspondence between the tests and the specified requirements. All test activities and the test evaluation (including reasons for decisions) should be set down in writing. These include:

- product name and description
- test begin, end, and time
- persons-in-charge
- configuration of the test environment
- description of the test cases
- criteria for decisions, test results and argumentation
- unfulfilled requirements of the Requirement Catalogue

The test group should be able to have access to clear documentation and records of the test activities and results (e.g. recording tool, forms etc.).

In the event that an automatic tool is used for testing, the test documentation must contain sufficient information about this tool and its usage so that the decision can be understood.

Determining criteria for a decision

When evaluating the contents of a test, the following three-point scale can be used, for example:

Grade	Decision criteria
0	- Requirements are not fulfilled. or - Intolerable errors were determined which could not be eliminated.
1	- Requirements are fulfilled, there are still some reservations, however (e.g. function is not entirely suitable). or - Minor errors were detected. These are relatively unimportant as they only have a tolerable effect on production, or as they only occur with a negligible degree of probability.
2	- Requirements are fulfilled completely. and - Errors which may have arisen could either be eliminated or have no effect on production.

In the event that errors have arisen which cannot be reproduced, the tester must decide to which category (grade) the error should be allocated.

If errors have occurred which can be eliminated during testing, these should be tested again after elimination.

Example:

The example of a compression program in S 2.81 *Preselection of a Suitable Standard Software Product* is continued here in order to describe how the testing time can be determined for each requirement of the Requirement Catalogue. The testing time is based on the depth and complexity of the test. The confidence factor represents the amount of confidence in the feature.

The frequency of use, proneness to error and complexity of a feature are assessed as follows:

- 1 means "low"
- 2 means "moderate"
- 3 means "high"

An exception to this is if an unchangeable feature of the product is to be examined which is independent of the proneness to error and frequency of use. In this case, the value 0 is given. This results in the following table for the compression program:

	Confidence factor	Error-proneness	Frequency of use	Test depth	Comp-lexity	Test time	in %
Correct compression and decompression	**5**	**2**	**3**	**10**	**2**	**20**	**23**
Detection of bit errors in a compressed file	**2**	**2**	**1**	**5**	**2**	**10**	**11**
Deletion of files only after successful compression	**3**	**2**	**1**	**6**	**1**	**6**	**7**
DOS-PC, 80486, 8 MB	**5**	**0**	**0**	**5**	**1**	**5**	**6**
Windows compatible	**1**	**0**	**0**	**1**	**1**	**1**	**1**
Throughput at 50 MHz above 1 MB/s	**3**	**1**	**2**	**6**	**1**	**6**	**7**
Compression rate over 40% with text files of the program XYZ	**3**	**2**	**2**	**7**	**1**	**7**	**8**
On-line help function	**1**	**1**	**2**	**4**	**1**	**4**	**5**
Maximum costs 50 DM per licence	**5**	**0**	**0**	**5**	**1**	**5**	**5**
Password protection for compressed files (high mechanism strength)	**5**	**1**	**2**	**8**	**3**	**24**	**27**

In this example, the testing time is defined as follows

test time = complexity * test depth.

and

test depth = confidence factor + proneness to error + frequency of use

(The percentage for the testing time in the last column of the table results from the values calculated for the testing time divided by the total of these values).

An example for another method of calculating the testing time and assessing the test results is described in ISO 12119. Here, the requirements are weighted as follows: *Assessment of each test = (complexity + proneness to error) * (frequency of use + importance).*

In any case, the person responsible for testing must decide on an adequate assessment method for both the product and the institution.

After drawing up a test plan, a tester or test group is appointed for each test specified in the test plan. The test group should be given the test plan and informed of the times for the individual tests.

Additional controls:

- Have all forms and checklists required for the test been compiled?
- Were all tasks allocated?
- Were all tests implemented according to the stipulations of the test cases?

S 2.83 Testing Standard Software

Initiation responsibility: Head of Specialist Department, Head of IT Section

Implementation responsibility: Test group

The testing of standard software can be divided up into the preparation, implementation and evaluation. The following tasks must be carried out in these sections:

Test Preparation

- Determining the test methods for the individual tests (test type, processes and tools)
- Creating test data and test cases
- Establishing the necessary test environment

Performing the test

- Receipt tests
- Functional tests
- Tests of additional functional features
- Security-specific tests
- Pilot application

Test evaluation

The various tasks are described below

Test Preparation

Determining the test methods for the individual tests (test type, processes and tools)

Methods for carrying out tests are, for example, statistical analyses, simulation, proof of correctness, symbolic program execution, review, inspection, failure analysis. It should be noted that some of these test methods can only be carried out if the source coding is available. The suitable test method must be selected and determined in the preparation stage.

It must be clarified which processes and tools will be used for testing programs and checking documents. Typical processes for testing programs are, for example, black box tests, white box tests or penetration tests. Documents can be checked using informal methods, reviews or checklists, for example.

A black box test is a functionality test without knowledge of the internal program sequences. Here, the program is run with all data types for all test cases with troubleshooting and plausibility checks.

A white box test is a functionality test with disclosure of the internal program sequences, e.g. by source code evaluation or tracing. White box tests generally

go beyond IT baseline protection and can not normally be carried out for standard software as the source code is not disclosed by the manufacturer.

Functionality tests are intended to prove that the test is in accordance with the specification. Using penetration tests, it is intended to determine whether known or assumed weaknesses can be exploited in practical operation, for example by attempts to manipulate the security mechanisms or by bypassing security mechanisms by manipulation at the operating system level.

The way the results are to be secured and evaluated should be stipulated, particularly as regards repeating tests. It should be clarified which data should be kept during and after the test.

Creating test data and test cases

The preparation of tests also includes the creation of test data. Methods and procedures should be stipulated and described in advance.

A number of test cases in accordance with the testing time must be created for each test. Each of the following categories should be taken into consideration.

Standard cases are cases which are used to test whether the defined functions are implemented correctly. The incoming data are called **normal values** or **limit values**. Normal values are data within the valid input area, limit values are threshold data.

Error cases are cases where attempts are made to provoke possible program error messages. The input values which should cause a predetermined error message to occur in the program are called **false values**.

Exceptional cases are cases where the program has to react differently than to standard cases. It must therefore be checked whether the program recognises these as such and then processes them correctly.

Examples:

- If the input parameters can be between 1 and 365, tests are to be carried out with false values (e.g. 0 or 1000), the limit values 1 and 365 and with normal values between 1 and 365.
- An appointment planning program should take national holidays into consideration. A special case is when a certain day is a holiday in all states except one. The program must then react appropriately for this state and this day.

In the event that it is too time-consuming or difficult to create test data, anonymous actual values can be used for the test. For reasons of confidentiality, actual data must be made anonymous. It should be ensured that these anonymous data do not cover all limit values and exceptional cases, these having to be created separately.

Beyond the test data, all types of possible user errors should be taken into consideration. Particularly difficult are all user reactions which are not planned in the program sequence and which are thus not correctly rejected.

Establishing the necessary test environment

The test environment described in the test plan must be established and the products to be tested installed. The components used should be identified and their configuration described. In the event that deviations from the described configuration arise when installing the product, this should be documented.

Performing the test

The test must be carried out using the test plan. Each action, together with the test results, must be adequately documented and evaluated. In particular, if errors appear, these must be documented in such a way that they can be reproduced. Operating parameters suited to later production working must be determined and recorded to enable installation instructions to be drawn up later.

If additional functions are detected in the product which are not listed in the Requirements Catalogue but can nevertheless be of use, a short test for them must be carried out at the very least. If it becomes apparent that this function is of particular importance for later operation, they must be tested in full. For the additional test expenditure incurred, application must be made if necessary for an extension of the time limit to the person responsible. The test results must be included in the overall evaluation.

If, when processing individual test contents, it becomes apparent that one or several requirements of the Requirements Catalogue were not sufficiently specific, these must be put in more specific terms if necessary.

Example: In the Requirements Catalogue, encryption is demanded to safeguard the confidentiality of the data to be processed. During testing it has become apparent that off-line encryption is unsuitable for the intended purpose. An addition must therefore be made to the Requirements Catalogue with regard to on-line encryption. (Off-line encryption must be initiated by the user and each of the elements to be encrypted must be specified; on-line encryption is carried out in a transparent way on behalf of the user with pre-set parameters.)

Receipt tests

Before all other tests, the following basic aspects must first be tested, as any failure in these receipt tests will lead to direct actions or the stopping of the test:

- The absence of computer viruses in the product must be checked by a current virus search program.
- It must be established in an installation test whether the product can be installed simply, completely and comprehensibly for the later-intended purpose. Likewise, there must be a check on how the product is completely de-installed.

- The running capabilities of the product must be checked in the planned usage environment; this comprises in particular a check of screen editing, printer output, mouse support, networking capability, etc.
- The completeness of the product (programs and manuals) must be checked, e.g. by comparing with the inventory, the product specification or similar.
- Short tests of program functions should be performed which are not explicitly mentioned in the requirements, with regard to function, plausibility, freedom from error, etc.

Functional tests

The functional requirements which were placed on the product in the Requirements Catalogue must be examined in terms of the following aspects:

- *Existence of the function* by calling up in the program and evaluation of the items of program documentation.
- Freedom from error or correctness of the function

  In order to guarantee the freedom from error or correctness of the function, depending on the test level various test procedures should be used during the check such as black box tests, white box tests or simulated production running.

  The test data and test cases created in the initial phase are used in the functionality test. During the functionality test it is necessary to compare the test results with the specified requirements. In addition, a check should be made on how the program reacts in the case of faulty input parameters or faulty operation. The function must also be tested with the limit values of the intervals of input parameters and with exceptional cases. These must be detected accordingly and correctly handled.
- Suitability of the function

  The suitability of the function is distinguished by the fact that the function

  - actually fulfils the task to the required extent and in an efficient manner and
  - can be integrated easily into normal work processes.

  If the suitability of the function is not obvious, the solution is to test this in a simulated production operation, but still in the test environment.
- Consistency

  The consistency of the separate functions must be checked, in each case between the Requirements Catalogue, the documentation and the program. Any contradictions must be documented. Discrepancies between the documentation and the program must be recorded in such a way that they can be incorporated into the additions to the documentation when the product is used later.

Tests of additional functional features

The additional features itemised in the Requirements Catalogue alongside the security-specific features and the functional features must also be checked:

- Performance

  Running time behaviour should be determined for all planned configurations of the product. In order to test performance adequately, general tests in which production working is simulated, or a pilot application with selected users, are useful. It must be established whether the set performance requirements are being met.

- Reliability

  Behaviour during accidentally or maliciously caused system crashes (crash test) must be analysed and it must be established what damage results from this. A record must be made of whether the product can be properly and correctly restarted following system crashes. A check must also be made as to whether there can be direct access to data bases independent of the regular program function. In many cases such access can lead to loss of data and should be prevented by the product. It should also be recorded whether the program supports possibilities of reversing ”critical actions” (e.g. deleting, formatting).

- User-friendliness

  Whether the product is user-friendly depends, to a particular degree, on the subjective feeling of the tester. However, the following aspects can provide clues when making the assessment:

  - technology of menu surfaces (pull-down menus, scrolling, drag & drop, etc.),
  - design of menu surfaces (e.g. uniformity, comprehensibility, menu-driven operation),
  - keyboard layout,
  - error messages,
  - trouble-free access to interfaces (batch operation, communication, etc.),
  - readability of the user documentation,
  - help functions.

  Analysis of user-friendliness must describe possible modes of operation of the product, including operation following handling- or operating errors, and their consequences and implications for maintaining secure operation.

- Maintainability

  Personnel and financial expenditure on the maintenance and care of the product should be determined during testing. This can be estimated with the aid, for example, of reference factors such as other reference installations, tests in specialist magazines, or using the installation expenditure determined during testing. To do this, the number of manual

interventions which were necessary during installation to arrive at the configuration sought must be documented. If experience with preceding versions of the tested product has already been accumulated, an analysis should be made of how expensive their maintenance was.

Enquiries should be made regarding the extent to which support is offered by the manufacturer or seller and under what conditions. If a hotline is offered by the manufacturer or seller, its ease of access and quality should also be considered.

- Documentation

  The existing documentation must be checked with a view to whether it is complete, correct and consistent. In addition to this it should be understandable, clear, error-free and easy-to-follow.

  It must further be monitored whether it is adequate for secure use and configuration. All security-related functions must be described.

Over and above this, the following additional points of the Requirements Catalogue must be tested:

- compatibility requirements
- interoperability
- conformity to standards
- adherence to internal rules and legal provisions
- software quality

Security-specific tests

If specific security requirements were placed on the product, in addition to the trials mentioned above, the following aspects must be examined:

- effectiveness and correctness of the security functions,
- strength of the security mechanisms and
- absolute necessity and unavoidability of the security mechanisms.

As the basis for a security check the Manual for the Evaluation of the Security of Information Technology Systems (ITSEM) could, for example, be consulted. This describes many of the procedures shown below. The additional comments are an aid to orientation and serve as an introduction to the topic.

At the outset it must first be demonstrated by functional tests that the product supplies the required security functions.

Following this, it must be checked whether all the required security mechanisms were mentioned in the Requirements Catalogue and, if necessary, this must be amended. In order to confirm or reject the minimum strength of the mechanisms, **penetration tests** must be carried out. Penetration tests must be carried out after all other tests, as indications of potential weaknesses can arise out of these tests.

The test object or the test environment can be damaged or impaired by penetration tests. To ensure that such damage does not have any repercussions, backups should be made before penetration tests are carried out.

Penetration tests can be supported by the use of security configuration- and logging tools. These tools examine a system configuration and search for common flaws such as, for example, generally legible files and missing passwords.

Using penetration tests, the product should be examined for design flaws by employing the same methods a potential 'invader' would use to exploit weak points, such as, for example,

- changing the pre-defined command sequence,
- executing an additional function,
- direct or indirect reading, writing or modification of internal data,
- execution of data whose execution is not planned,
- use of a function in an unexpected context or for an unexpected purpose,
- activation of the error recovery,
- use of the delay between the time of checking and the time of use,
- breaking the sequence by interrupts, or
- generating an unexpected input for a function.

The mechanism strengths are defined using the terms specialised knowledge, opportunities and operating resources. These are explained in more detail in ITSEM. For example, the following rules can be used for defining mechanism strength:

- If the mechanism can be mastered by a lay person alone within minutes, it **cannot even be classified as low.**
- If a successful 'invasion' can be carried out by anyone except a lay person, the mechanism must be classified as **low.**
- *If an expert is required for a successful 'invasion' and the expert takes some days with the available equipment, the mechanism must be classified as* ***medium.***
- If the mechanism can only be mastered by an expert with special equipment and the expert takes months to do it and has to come to a secret arrangement with a system manager, it must be classified as **high.**

It must be ensured that the tests carried out cover all specific security functions. It is important to note that only errors or differences from the specifications can ever be determined by testing, never the absence of errors.

Typical aspects of investigation can be shown by a number of **examples:**

Password protection:

- Are there passwords which have been pre-set by the manufacturer? Typical examples of such passwords are the product name, the manufacturer's name, "SUPERVISOR", "ADMINISTRATOR", "USER", "GUEST".
- Which file changes if a password was changed? Can this file be replaced by an old version from a backup to activate old passwords? Are the passwords stored in encrypted form or are they readable in plain text? Is it possible to make changes in this file to activate new passwords?
- Is access actually blocked following several incorrect password entries?
- Are programs offered in magazines or mailboxes which can determine the passwords of the product being examined? Such programs are available for some standard applications.
- If files are protected by passwords, can the position at which the password is stored be determined by a comparison of a file before and after the change in the password? Is it possible to enter changes or old values at this point in order to activate known passwords? Are the passwords stored in encrypted form? How is the position allocated if password protection is deactivated?
- Can the password testing routine be interrupted? Are there key combinations with which password entry can be bypassed?

Access rights:

- In which files are access rights stored and how are they protected?
- Can access rights be altered by unauthorised persons?
- Can files be inserted using old access rights and which rights are needed for this?
- Can the rights of the administrator be restricted such that he does not obtain access to the usage- or protocol data?

Data backup:

- Can backups which have been created be reconstructed without difficulty?
- Can backups be protected by a password? If so, can the password trial attempts described above be used?

Encryption:

- Does the product offer the possibility of encrypting files or backups?
- Are several different encryption algorithms offered? In this connection, generally speaking, the following rule of thumb should be observed: "The quicker an encryption algorithm produced in software is, the more insecure it is."
- Where are the keys used for encryption and decryption stored?

  In the case of local storage there must be an examination of whether these keys are password-protected or are protected by a second encryption with a further key. In the case of **password protection** the above points must be

taken into account. In the case of over-encryption, consideration must be given to how the accompanying key is protected.

In addition, the following points can be considered: which file changes if a key is changed? By comparing this file before and after the change in the code, the point can be determined at which this key is stored. Is it possible to make changes at this point to activate new keys which are then employed by the user, without the latter noticing the illicit change?

- Are there keys which have been pre-set by the manufacturer which have to be changed before the first use of the program?
- What happens if an incorrect key is entered during decryption?
- Following the encryption of a file, is the unencrypted variant deleted? If so, is it reliably overwritten? Is a check made before deletion as to whether the encryption was successful?

Logging:

- Is access to protocol data denied to unauthorised persons?
- Are the activities to be logged fully recorded?
- Does the administrator have the option, by virtue of his privileged rights, of obtaining access to protocol data without authorisation and unobserved, or can he deactivate the logging without being noticed?
- How does the program react if the logging memory overruns?

In addition to this it must be ascertained whether, as a result of the new product, security features will be circumvented elsewhere. **Example:** the product to be tested offers an interface to the operating system environment, previously however, the IT system was configured in such a way that no such interfaces existed.

Pilot application

Following the conclusion of all other tests a pilot application, i.e. use under real conditions, might still be considered necessary.

If the test is carried out in the production environment using actual data, the correct and error-free operating method of the program must have been confirmedto begin with a sufficient number of tests, in order not to jeopardise the availability and integrity of the production environment. For example, the product may be installed at the premises of selected users who will then use it for a set period in actual production conditions.

Test evaluation

Using the decision criteria specified, the test results must be assessed and all results must be assembled and submitted along with the test documentation to the procurer, or the person responsible for the test.

With the aid of the test results a final judgement should be made regarding a product to be procured. If no product has passed the test, consideration must

be given as to whether a new survey of the market should be undertaken, whether the requirements set were too high and must be changed, or whether procurement must be dispensed with at this time.

Example:

Using the example of a compression program, one possibility is now described of evaluating test results. Four products were tested and assessed in accordance with the three-point scale derived from S 2.82 *Developing a Test Plan for Standard Software*.

Feature	Necessary/ desirable	Significance	Product 1	Product 2	Product 3	Product 4
Correct compression and decompression	**N**	**10**	**2**	**2**	**Yes**	**0**
Detection of bit errors in a compressed file	**N**	**10**	**2**	**2**	**No**	**2**
Deletion of files only after successful compression	**N**	**10**	**2**	**2**	**Yes**	**2**
DOS-PC, 80486, 8 MB	**N**	**10**	**2**	**2**	**Yes**	**2**
Windows compatible	**D**	**2**	**0**	**2**	**Yes**	**2**
Throughput at 50 MHz above 1 MB/s	**D**	**4**	**2**	**2**	**Yes**	**2**
Compression rate above 40%	**D**	**4**	**2**	**1**	**No**	**0**
On-line help function	**D**	**3**	**0**	**0**	**No**	**2**
Password protection for compressed files	**D**	**2**	**2**	**1**	**No**	**2**
Assessment			**100**	**98**	**K.O.**	**K.O.**
Pricing (maximum costs DM 50 per licence)			**49,- DM**	**25,- DM**		**39,- DM**

Product 3 had already failed at the pre-selection stage and was therefore not tested.

Product 4 failed in the test section ”correct compression and decompression”, because the performance of the feature was assessed with a 0, although it is a necessary feature.

In calculating the assessment scores for products 1 and 2, the marks were used as multipliers for the respective significance coefficient and the total finally arrived at.

Product 1: 10*2+10*2+10*2+10*2+2*0+4*2+4*2+2*2 = 120

Product 2: 10*2+10*2+10*2+10*2+2*2+4*2+4*1+2*1 = 118

Following the test evaluation product 1 is thus in first place but is closely followed by product 2. The decision in favour of a product now has to be taken by the procurer using the test results and the price-performance ratio resulting from them.

Additional controls:

- Is the hardware- and software configuration used in conformity with the Requirements Catalogue?
- Do manufacturers or sellers offer support or maintenance services in connection with the use of the product?
- Are all functions relevant to the user described fully and comprehensibly in the user documentation?
- Do the existing documentation items contain a table of contents, a key word index and page references?
- Are all required functions executable and correct?
- Is the product reliable and robust in its usage environment? Under limit loads or in the event of faulty operation, can data be corrupted or destroyed?
- Are inadmissible and non-defined entries not processed in the same way as admissible ones?
- Were test documentation items produced in accordance with the standards?

S 2.84 Deciding on and developing the installation instructions for standard software

Initiation responsibility: Agency/company management

Implementation responsibility: Procurer, Head of Specialist Department , Head of IT Section

Following the completion of all tests, the test results must be submitted to the procurer. The decision in favour of a product must now be made by the procurer with the involvement of the Head of the Specialist Department and the Head of IT Sector on the basis of the test results and the price-performance ratio resulting from them. In this connection, the particular aspect to be set in relation to the purchase price is the level of performance of the individual products compared to the Requirements Catalogue. Also, additional functions of the products which were not listed in the Requirements Catalogue but which are nevertheless significant to their use, should be taken into account in reaching the decision.

Drawing up of installation instructions

After a decision is taken in favour of a product, installation instructions must subsequently be drawn up for the selected product. During testing, the configuration of the product was so determined to permit secure and efficient production working. This is the way to guarantee user-friendliness, correctness and security in the workplace.

In order to guarantee the right configuration of the product in actual operation, specific parameters must be specified. Some of these must be accompanied by organisational provisions.

For some features of a product the following section shows, by way of example, what can be specified in the context of installation instructions.

Example:

User-friendliness:

- Drivers X, Y and Z (screen, printer, mouse, network) must be installed with the product to create an acceptable working environment for the user (screen flicker-free, reasonable editing, etc.).
- The settings at which individual functions have the greatest processing speed must be specified if other criteria such as security are not at variance with them (the size of the swapping-out files must be fixed at at least 10 MB, the verification option must be activated for data backup, although verification requires additional time).

Security:

- Security function parameters must be pre-set (e.g. the minimum length of passwords must be 6 characters, backups must be created each day, logging must be activated to its full extent, rights of access to personl-related log files must be arranged only for the data privacy officer, ...).
- If several procedures are being supported which are relevant to security (e.g. encryption algorithm, hash functions), the ones that must be selected

are those which attain an appropriate level of protection (RSA, with a code length of at least 768 bits, must be used as asymmetrical encryption, Triple-DES must be used as a symmetrical encryption function).

Function:

- Only the functions X, Y and Z must be activated, functions which are unwanted or not required must be turned off.
- The automatic data backup function must be activated using the parameter ”every 10 minutes”.

Organisation:

- Installation must be carried out by the administrator.
- Provisions for operation must be made (e.g. the user must be responsible for making his own backups, passwords must be changed after 30 days).

Marginal conditions:

- The configuration of the platform on which the standard software product is to be used must be described and specified, especially if this removes system-related weaknesses in the platform.

Additional controls:

- Are all the particulars for a successful installation contained in the installation instructions?
- Are particulars included of how the product is de-installed again?

S 2.85 Approval of standard software

Initiation responsibility: Agency/company management

Implementation responsibility: Head of Specialist Department, Head of IT Section

Before the acceptance of the standard software into actual operation comes the formal approval. Agency or company management are responsible for the approval of a product; however, they can delegate this to the management of the specialist department or the management of the IT Division. The specialist department can further restrict the approval provision specified by agency or company management by means of its own restrictions. The use of non-approved software must be prohibited (see S 2.9 *Ban on using non-approved software*).

Approval is always preceded by the successful completion of all necessary tests (see S 2.83 *Testing Standard Software*). An approval must not take place if unacceptable errors, e.g. serious deficiencies in security, were detected during the tests.

Installation- and configuration provisions must be drawn up for approval. Their level of detail depends on whether installation is to be undertaken by the system administration or the user. The installation- and configuration provisions are results of the tests carried out in the context of procurement (see S 2.83 *Testing Standard Software*). If different configurations are permissible, the effects of the individual configurations on security must be explained. In particular, it must be stipulated whether restrictions on product functionality or access rights are to be imposed on all, or just a few, users. The staff- or works council, the data privacy officer and the IT security officer must be involved in establishing these marginal conditions at the appropriate time.

Approval should take place in the form of a written **approval notice.** In the approval notice, statements should be made on the following points:

- Program name and version number,
- Designation of the IT procedure in which the product is to be used,
- Confirmation that the IT components used comply with the technical requirements,
- Date of the approval, signature of the person responsible for the approval,
- Certificate of non-objection from the IT security officer, the data privacy officer and the staff- or works council,
- Scheduled time of deployment in actual operation,
- For which users the product is being approved,
- Installation instructions, in particular the workstations at which it is being installed and with what configuration,
- Who is authorised to install it,
- Who has access to the installation data media and

- What training measures have to be undertaken before the product is used.

The approval notice must be brought to the attention of all those involved, in particular copies must be available to the Approval Authority, the IT Division, the Specialist Department and where necessary the IT user.

In addition to this, an organisational arrangement must be made that the approval and any possible tests required will be repeated if basic features, particularly in the area of security functions, have altered as a result of a change of version or patches. Changes of the kind mentioned must be notified to the person responsible for the approval of the product.

Furthermore, it can be specified which standard software products, depending on the place of use and the intended use, will enjoy general approval. It is a prerequisite that they have at least been tested for computer viruses, that the licence questions have been resolved and that they are registered. Examples of this would be:

- Demo versions for test purposes which are made available on special computers,
- Public domain software which is installed on special servers,
- Games programs on special computers which are installed in staff rooms.

Additional controls:

- Where are the approval notices administered and deposited?
- Are installation instructions available?
- Is there a guarantee that all software is subjected to the approval procedure?

S 2.86 Guaranteeing the integrity of standard software

Initiation responsibility: Agency/company management

Implementation responsibility: Head of IT section

It must be guaranteed that the standard software approved can only be installed in an unchanged condition. Accordingly, the possibility of desired or unintentional changes occurring in the interim period, e.g. as a result of computer viruses, bit errors due to technical errors or manipulation in configuration files, should be prevented.

Installation must only be allowed to take place, therefore, using original data media or numbered copies of the original data medium. An alternative to the local installation from data media is the installation via a local network of a version approved specifically for this purpose. It should be guaranteed that only authorised persons have access.

If the data capacity allows (e.g. CD-ROM), backup copies should be produced of the original data media. Original data media and all copies must be kept protected from unauthorised access (see S 6.21 *Backup Copy of Software Used*). The copies produced should be numbered and included in inventory lists. Copies which are no longer needed must be deleted. Before installation, a computer virus test must be carried out.

As an option, a checksum (cf. S 4.34 *Using Encryption, Checksums or Digital Signatures*) can be created using the original data media or using a reference version installed during the test. With the aid of this, before installation the integrity of the data media used for it, or the versions deposited in local networks can be checked, as can correct installation. In addition to this, installed programs can also be provided with checksums for protection against unauthorised changes to the approved configuration. In this way infections by, as yet unknown computer viruses, can be detected. It can also be determined whether a virus infection has occurred before or after installation.

Additional controls:

- In what way is the integrity of the standard software guaranteed?
- Is monitoring carried out periodically to check the integrity of the installed programs?
- Are attempts at manipulation of programs and data detected?

S 2.87 Installation and configuration of standard software

Initiation responsibility: Head of IT section

Implementation responsibility: Head of IT Section, Administrator

The approved software is installed on the IT systems intended for it in accordance with the installation instructions. In addition to the programs to be installed, the installation instructions also contain configuration parameters and the set-up of the hardware- and software environment.

Deviations from the installation instructions require the consent of the Approval Authority.

If the users are to install the software themselves, they must be provided with installation instructions which enable installation to be carried out independently. At the very least, pilot installation by a typical user should be overseen by the IT Department, in order to check the comprehensibility of the installation instructions.

As standard software is developed for a wide variety of application fields, it often contains more functions than are required to perform the specialist task. So that less problems and errors arise when working with the software, only the functions actually required should be installed. Functions which can lead to security problems must not be approved.

Both before and after the installation of software, a complete backup should be made. If there are subsequent problems during installation, the first backup can be used to recreate a consolidated re-run point. Following successful installation, a complete backup should be made again, so that if there are problems later, the situation, following the successful installation of the product, can be restored.

Successful installation is reported in writing to the office responsible for the acceptance of actual operation.

As an option, installation can be accompanied by the use of a so-called ”delta tool” which documents all changes in an IT environment between two definable points in time. This documentation of changes is particularly helpful when it comes to the de-installation of software.

When a new product is used, any databases which were produced with a previous product must be taken over. If it has become apparent from the tests that difficulties may arise in this respect, help positions must be created for the user or acceptance of the old databases must be carried out centrally by trained personnel.

Additional controls:

- Which provisions are in force?
- What provisions exist with respect to possible deviations from the installation instructions?
- How is the success of an installation reviewed?

S 2.88 Licence management and version control of standard software

Initiation responsibility: Agency/company management

Implementation responsibility: Head of IT Section, Head of organisation

Without suitable version control and licence control, experience shows that a wide assortment of versions rapidly comes to be used on an IT system or within an organisational unit, some of which may be used without a licence.

Only licensed software must be used on all IT systems within an institution. This provision must be made known to all employees and the administrators of the various IT systems must ensure that only licensed software is used. To do this they must be equipped with suitable tools for licence control.

Frequently, within an institution, different versions of standard software are used. Within the context of licence control it must also be possible to gain an overview of all versions used. In this way it can be guaranteed that old versions are replaced by newer ones as soon as this is necessary, and that when licences are returned, all versions are deleted.

In addition to this, the various configurations of the installed software must be documented. As a result, it must be possible to acquire an overview of which IT system which settings, relevant to security on a standard software product, were specified by the approval and which were actually installed. Thus, for example, it can be rapidly clarified on which computers macro-programming has been installed on product XYZ and on which it has not.

Additional controls:

- Which provisions are in force?
- Are different versions of a standard software product in use?

S 2.89 De-installation of standard software

Initiation responsibility: Head of IT section

Implementation responsibility: Head of IT Section, Administrator

In the de-installation of software, all files must be removed which have been created for the operation of the software on the IT system, and all entries in system files which were made in relation to the product must be deleted. With many software products, files are created during installation in various directories on the IT system or existing files are altered. Often the user is not even informed of all the changes on the IT system made during installation.

In order to be able to perform a complete de-installation, it is therefore helpful to sustain the system changes made during installation, either manually, or with the aid of special tools. If this is not done, experience shows that a de-installation only takes place in a rudimentary way or that it is not carried out for fear of deleting important files during de-installation.

Additional controls:

- Are random checks carried out to determine whether the previous version is completely de-installed when a version is changed?

S 2.90 Checking delivery

Initiation responsibility: Head of IT Section, Head of organisation

Implementation responsibility: Procurer

Following receipt of a delivery, the following must be checked using the documents available,

- Whether the delivery was ordered,
- For whom it is intended,
- Whether there are any signs of damage in transit,
- Whether it is complete, i.e. whether all the components ordered are there and/or whether all the components included within the scope of supply of the product in accordance with the product specification are there.

The results of these checks must be documented in a goods inwards register, together with:

- Product name and version,
- Type of product, e.g. word processing,
- Scope of supply, i.e. description of the individual components including number and form of delivery (book, diskette, CD-ROM, ...),
- Date of delivery,
- Type of delivery,
- Who took delivery of it,
- Place where it is kept and
- Person to whom it was passed on.

The delivered products must be passed on to the IT Department to enable functional tests and subsequent formal approval, installation and configuration to be carried out.

If the products are only being used or made available temporarily, e.g. for test purposes, as a minimum requirement the serial numbers and other product-specific identifying characteristics must be noted down in appropriate inventory lists. If the delivered products are scheduled to remain permanently, they must be marked with clear identifying characteristics (e.g. grouped consecutive inventory numbers). Following this, they must be included in an inventory list. This must give information on:

- Identifying characteristics,
- Procurement sources, delivery times,
- Whereabouts,
- Approval date,
- Installation date and peculiar configuration features and
- maintenance contracts, maintenance intervals.

Additional controls:

- What provisions are in force for the receipt of information technology products?
- What is the procedure if incomplete deliveries are discovered?
- Have incomplete deliveries ever become noticeable on a fairly frequent basis?

S 2.91 Determining a security strategy for the Windows NT client-server network

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management

Before a start can be made on the actual configuration and installation of Windows NT in a client-server network, two fundamental observations must first be made:

First of all, it must be clarified which services are to be provided by the operating system and in what context it is to be used.

This can be illustrated using a number of **examples**:

- The system is deployed in a server-supported PC network as a server for a fairly large workgroup in which different rights can be assigned. If necessary, due to specific requirements, Peer-to-Peer functions should also be implemented in a limited manner. For example, individual printers should be able to be used jointly via Peer-to-Peer functionality.
- The system is deployed as the client in a server-supported PC network with Windows NT servers which can dispense with Peer-to-Peer functionality for the exchange of data.
- The system is deployed as the client in a server-supported PC network with Novell NetWare servers.
- The system is deployed as the server in a PC network with MS-DOS, MS Windows, WfW or Windows 95 clients.
- The system is deployed as the server in a network in which there are exclusively Windows NT clients.

Extra security problems can arise as a result of the use of Peer-to-Peer functions within a Windows NT network (in this respect see also 6.3 Peer-to-Peer network). **For this reason the use of Peer-to-Peer functions within Windows NT networks should be avoided.** Peer-to-Peer functions should, at best, be allowed as a temporary solution in a restricted way, if, for example, WfW computers or non-networkable printers are to be integrated into the Windows NT network.

Following this, the above considerations must be translated into a security strategy.

Here it can be seen that depending on the already existing system environment and organisational structure, together with the restrictions on possible Peer-to-Peer functions that may have to be allowed for, a greater or lesser effort is necessary in the development of a suitable security strategy.

A methodical procedure is shown below which can be used to develop a comprehensive security strategy for a client-server network. However, as Windows NT can be deployed in various configurations, an individual decision should be taken for the respective characteristic as to which of the steps outlined should be applied.

Determining a security strategy for a client-server network

The security strategy must demonstrate how a client-server network for the respective organisation can be securely constructed, administrated and operated. The individual development steps of such a strategy are presented below:

1. Definition of the client-server network structure

The first step involves determining the logical structure of the client-server network, in particular the allocation of the servers and the network domains (see S 2.93 *Planning of a Windows NT network*). If possible, the use of Peer-to-Peer functions should be dispensed with, as these can adversely affect the security of the client-server network. Provided that this cannot be avoided, however, binding rules must be made for the use of Peer-to-Peer functions (see S 2.67 *Defining a security strategy for Peer-to-Peer networks*).

2. Regulation of responsibilities

A client-server network should be operated securely by a trained **network administrator** together with a substitute. Only these individuals should be allowed to alter security parameters in the network. For example, they are responsible for making administration rights and tools available to the relevant **individuals in charge** on the servers, so that the latter can allocate file and directory rights, share directories and applications required by others, configure user groups and accounts, and set system guidelines for users, access supervision and monitoring.

The responsibilities of the individual users in the client-server network are outlined under Step 11.

3. Determining name conventions

In order to facilitate the management of the client-server network, unambiguous names should be used for the computers, user groups and users.

In addition, naming conventions should be introduced for the share names of directories or printers (see S 2.67 *Defining a security strategy for Peer-to-Peer networks*). Should no conclusions be possible on the contents of a shared directory, appropriate pseudonyms must be used. Should a shared resource not be recognisable as such, the symbol ”$” must be attached to the share name. The latter is always recommended whenever directories are shared only for the bilateral exchange of information between two users or for accessing resources which are only meant to be known to individual users.

4. Determining the rules for user accounts

Before user accounts are set up, the restrictions intended to apply to all, or a certain number, of these accounts should be stipulated. In particular, this concerns the rules for passwords and for the reaction of the system to incorrect log-in procedures. The rules laid down can be implemented with the aid of the "*Policies*" option of the User Manager (see S 4.48 *Password protection under Windows NT*).

5. Configuring groups

To facilitate administration, user accounts which need to fulfil identical requirements should be coalesced into groups. User rights such as file, directory and sharing rights as well as any additional, pre-defined functions are then assigned to these groups instead of individual user accounts. The user accounts inherit the rights and authorisations of the groups to which they belong. For example, all the staff members of a particular department can be coalesced into one group. Rights and authorisations should only be allocated to individual users in exceptional situations.

6. Determining user rights

Rights allow a user to perform certain actions on the system. They refer to the entire system, are not assigned to any special object, and can annul the authorisations to an object, as a right takes precedence over all file and directory authorisations. Whenever a user logs into an account to which the desired rights were granted either directly or via group membership, he can perform the corresponding actions. If a user does not possess the appropriate rights, Windows NT stops all attempts to carry out the actions concerned.

As already mentioned, user rights should be assigned to groups instead of individual users wherever possible.

During installation, Windows NT performs default settings which are generally adequate for secure and efficient operation. However, it is advisable to withdraw the "*Shut down system*" and "*Local login*" rights from the "*Everyone*" group and, if applicable, the "*Local login*" right from the "*Guests*" group (refer to S 4.50 *Structured system administration under Windows NT*).

7. Determining the specifications for logging

Windows NT provides very detailed capabilities for the logging of incidents relevant to security which, when used to the full, are capable of occupying the system to a large extent with auditing and consume large amounts of disk space in the process. A spectrum of incident types can be recorded which extends from system-wide incidents, such as, for example, the log-on of a user through to a user attempting to read a certain file. Both the successful and the failed attempts to perform an action can be recorded. In the configuration of the logging, however, it must be noted that an increase in logging does not necessarily also increase the security of the monitored system. Log files which are not evaluated or which, on account of their size, can only be evaluated with great effort, do not lead to improved supervision of the system sequences; on the contrary, they are ultimately useless. For these reasons, logging should be set in such a way that under normal circumstances it only records the really significant incidents (see S 4.54 *Logging under Windows NT*).

8. Rules concerning data storage

A specification is required as to where user data should be stored (refer to S 2.138 *Structured data storage*). In some cases, for example, it is advisable to store user data only on a server. This model does not permit a storage of data on local hard disks. However, it is also conceivable to store certain user data only on a local hard disk. The strategy to be employed must be ascertained in

accordance with the circumstances applicable in each case. A general recommendation is not possible here.

9. Setting up project directories

In order to achieve a clean separation of user and specific project data from each other and from the programs and data of the operating system, a suitable directory structure should be established to support a project and user-based file system. Thus, for example, two main directories \Projects and \Users can be created, under which the files and directories of the projects and users are each then filed in their own sub-directories.

10. Allocating access rights

For the servers, it must be determined which directories and - if NTFS partitions are used - files should be shared for access, and which access rights should be assigned to them (refer to S 4.53 *Restrictive allocation of access rights to files and directories under Windows NT*). In addition, as far as the use of Peer-to-Peer functions at the level of the clients is concerned, a decision must be taken as to which directories should be shared for network access (see S 2.94 *Sharing of directories under Windows NT*).

The above comments also apply to the sharing of printers.

11. Responsibilities for administrators and users in the client-server network

Besides the discharging of network management tasks (see No. 2), further responsibilities must be determined. It should be laid down which responsibility the individual administrators have to assume in the client-server network. These can, for example, be responsibilities for

- the evaluation of the log files on the individual servers or clients,
- the allocation of access rights,
- the escrow and changing of passwords and
- carrying out data backups.

In a client-server network the end-users must also take on certain responsibilities, provided that they are given rights to perform administrative functions. In general, these responsibilities are restricted however to the allocation of access rights to their own files, provided that these are explicitly stipulated and not assumed by the presets of the superior directory.

12. Training

Finally it must be determined which users have to be trained on which topics. Effective operation can only begin after adequate training. In particular, the administrators must be thoroughly trained with regard to the management and security of Windows NT.

The security strategy developed in this way must be documented and communicated to the required extent to the users of the client-server network.

Additional controls:

- Is the security strategy adapted to changes in the usage environment?

S 2.92 Performing security checks in the Windows NT client-server network

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The following points should be checked regularly at the level of the servers in a Windows NT client-server network in terms of whether they are being followed and their effectiveness (see also S 4.54 *Logging under Windows NT*):

- System security settings

  The correct setting of the entries relevant to security in the registry, i.e. essentially the entries in the sector *HKEY_LOCAL_MACHINE*, must be checked regularly by checking the entries of the security logs which refer to the registry.

- Use of privileged user accounts

  The use of privileged user accounts, i.e. of accounts with extended rights and authorisations e.g. for administrators, must be checked regularly by checking the entries in the security log. Likewise the log must be checked for log-on attempts to the guest user account.

- Failed access attempts (authorisation violations)

  If access to files and/or the registry is recorded, the security log must be checked weekly, or more often when required, for the occurrence of failed log-on attempts. If authorisation violations are discovered, the cause must be established.

- System integrity

  System integrity must be checked regularly; in particular, the data relating to the last modification and the rights to access important system files must be checked and compared with the values obtained directly after installation of the system and at each previous check. Since this check, with the aid of the capabilities offered by Windows NT, is relatively expensive, suitable ancillary tools should be used here, for example the shareware program DumpACL, or the service program WinDiff supplied with the Technical Reference (the "resource kit") for Windows NT, with which the contents of directories and files can be compared.

- Unused user accounts

  It must be ensured that the accounts of former employees are immediately deactivated and deleted from the system after a suitable transitional period (approx. ½ year). As the time of the last log-on to the system is not indicated, then, for this purpose, all user accounts should, if, possible, be supplied with an expiry date which has to be updated at certain intervals (e.g. annually) at the request of the user. Inactive, i.e. expired user accounts must be deleted. The owners must first be informed. The list of defined users must be checked regularly to ensure that only active employees are working on the system.

- Group membership

  A structured system administration requires an allocation of system and object rights to user groups instead of individual users wherever possible. It must be ensured that individual memberships in user groups are matched with organisational specifications following any change in the employment profile. Consequently, regular checks are required as to whether the memberships of individual employees in the various user groups have been updated to comply with the current environment. Checks are also required as to whether any changes in a user's group membership result in an accumulation of user rights. In particular, regular checks are needed as to whether the allocation of special rights to groups and individual users corresponds with currently applicable organisational specifications.

- Authorisation control

  It must be ensured that the owners of files and directories understand their obligation that other users should only be granted access if this is required. File Manager and Explorer must be used to regularly ensure that excessively wide-ranging authorisation has not been granted for sensitive data. Authorisations for the group "*Everyone*" and "*Guests*" as well as "*Domain Guests*" are particularly critical. As far as temporary authorisations are used, there must be a guarantee that this only occurs if it is required and that such authorisations are carefully monitored.

Procedures and methods should be developed for the eventuality that deviations from the fixed settings occur. These procedures must include the following points:

- who is informed and when,
- reasons for the possible choice of differing settings and a statement as to whether these might result in a security weakness,
- steps to remove the security weakness,
- steps to identify the cause of the security weakness.

Performing the checks described here at the level of clients should only be carried out if it is ensured that no improper performance controls of the users of these clients are associated with them, and if a guarantee can be given that the logging details will be handled correctly in relation to the data privacy act.

Additional controls:

- Is the network administrator informed of irregularities?
- Are deviations of the security settings from the permissible value corrected without delay?
- Are the possible consequences of such deviations analysed?

S 2.93 Planning of a Windows NT network

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

Windows NT can be implemented in various configurations in a network. To allow an appraisal and understanding of the advantages and disadvantages of the individual types of implementation, the security system of Windows NT needs to be described briefly to start with. In principle, this operating system retains control of all resources. Users can only access the resources if they have been granted the corresponding rights and authorisations. Access to the system is only possible via a valid user account, which can be protected by means of a password. The security account manager (SAM) is used to administer information on user and group accounts in the security account database, often termed SAM database. When a user logs in, the operating system generates an access token for the user, in accordance with the entries in the SAM database. The security reference monitor uses this token to check whether the user is authorised to access certain objects and perform the required actions (e.g. delete a file or shutdown the system).

Windows NT supports network operations with the following concepts:

1. Workgroups

Computers can be assigned to workgroups and jointly use resources via the network as part of the peer-to-peer concept (also refer to Module 6.3 Peer-to-Peer Networks).

Every computer in such a network can be used as a server as well as a workstation. This is done by sharing resources on the individual computers. Every Windows NT workstation employed in a workgroup manages its own SAM database and, thus, its own user and group accounts. The entries in this database cannot be used by any other computer in the same workgroup. As a result, central administration is not possible. A password is generally required to access resources which have been shared.

The main disadvantage of this concept is that it does not allow adequate control of the rights of individual users. For this reason, the configuration of workgroups should be avoided wherever possible.

2. Network with a dedicated server

This type of network incorporates a client-server structure. In this case, a specification is made as to which computers should act as servers and clients respectively. Servers can share directories and / or printers, and supply applications such as *Mail, Schedule+, Fax* on a global basis. In contrast, clients can only use the resources made available by the servers.

An NT computer can be run on the "Windows NT Server" or "Windows NT Workstation" operating system. In small networks, a licensed version of "Windows NT Workstation" can also be operated as a server. Due to licensing regulations, however, no more than 10 users are allowed to simultaneously log into this computer via the network. If this limit proves too low, Windows NT Server needs to be installed. In general, standard users should not be allowed

to work on a server running under the Windows NT operating system. The operation of clients under Windows NT is not absolutely necessary.

The main advantage of this concept is central data storage and management. If only one server is employed in a network like this, then only this server is used to configure and hold an account for every user of the network. To be able to use resources and services on this server via the network, a user simply needs to log into the server. The employment of this concept can by all means prove economically feasible in small networks.

However, if the server capacity no longer proves sufficient for fulfilling requirements concerning processing speed and disk space, a great deal of extra management is required when one or more servers are subsequently added to the network. If all users are to receive the right to access all servers via the network, corresponding user accounts must be configured and maintained on each of the servers.

3. Domain concept

Under Windows NT, a domain is a group of computers having access to a common security and user-account database (SAM database). This means that users only need to log into the domain once. After that, they are able to access all resources released for them, irrespective of which server these resources are located on.

One domain server under the Windows NT Server operating system acts as a primary domain controller (PDC). In addition, the domain can contain one or more backup domain controllers (BDC), member servers - i.e. those without a domain control functionality (also refer to the information provided further below) - and Windows NT workstations. The domain can also contain workstations running on other operating systems, such as Windows for Workgroups, Windows 95 and MS-DOS.

A decision as to whether a server is to act as a primary domain controller, backup domain controller or member server should be made before installation, as subsequent changes are only possible if a re-installation is performed. To provide a clearer understanding, the various types of servers which can be found in a domain are described in more detail below:

a) Primary domain controller (PDC)

One server of a Windows NT domain must always be configured as a primary domain controller. Use of the Windows NT Server operating system is absolutely necessary here, as the Workstation version does not provide this functionality. The central user-account database (SAM database) for the domains is managed on the PDC. All changes can only be performed on this database with the help of the user manager for domains. The primary domain controller also processes user logins.

b) Backup domain controller (BDC)

Other servers of the domain can be configured as backup domain controllers. Use of the Windows NT Server operating system is also absolutely necessary here. A read-only copy of the user database of the domain is replicated automatically on every backup domain controller. Synchronisation is performed regularly. Backup domain controllers can also process user logins

for the domain. Particularly when a large number of users are involved, this feature can be used to distribute the load generated by the user logins among several servers.

If possible, every domain should have at least one backup domain controller, to ensure that management of the domain continues even after a failure of the primary domain controller. In such cases, it is possible to upgrade the backup domain controller to a primary domain controller. If no backup domain controller has been configured, it is not possible to install a new primary domain controller in a domain.

If the domain servers are distributed among several estates linked together via a WAN, at least one backup domain controller should be installed in each estate.

c) Member server

Member servers are not configured as primary or backup domain controllers. These servers do not have copies of the user-account database of the domain. Consequently, they cannot process user logins for the domain.

The addition of a member server to a domain proves beneficial in the following situations:

- If a server needs to perform time-critical tasks, or large applications need to be executed on this computer, so that user logins constitute an unacceptable load.
- If a server is to be added to another domain in the near future. Such an addition proves easier in this case, compared with a server which has been configured as a backup domain controller.

One essential aspect of the domain concept is that all user accounts for each domain only need to be defined once. Management is performed in the central user database on the primary domain controller. This means that users only need to authenticate themselves to this database when logging in. After that, they can access all objects and resources which have been shared for them, regardless of which server these objects and resources are located on. If a user needs to work on a computer running under Windows NT Workstation, authenticating against the central user database is sufficient for gaining access to this computer.

Organisation of domains

Although several domains can be configured in a network, each of these domains must have a unique name. Every domain manages its own central SAM database. For this reason, user and group accounts are only valid in the domain in which they were defined.

Within a network however, a requirement might arise for users of one domain to access resources in another domain. This requirement can be fulfilled by the trust relationships between domains.

In this respect, a distinction is made between two types of domain: the trusted domain and the trusting domain. User accounts and global groups of the trusted domain can be assigned rights and authorisations in the trusting domain, thus allowing access to the resources shared in the latter.

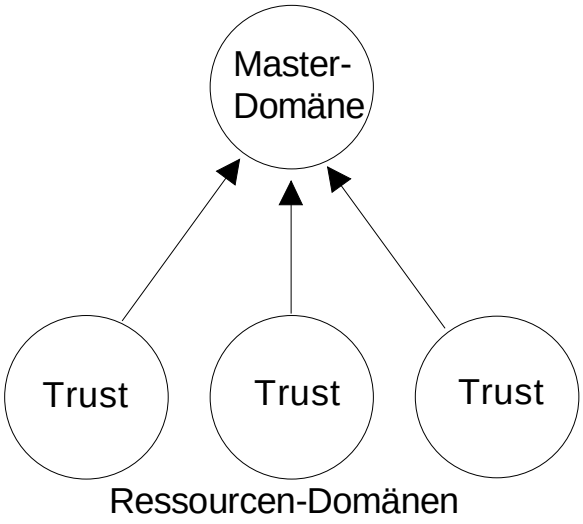
The following domain models can be implemented:

a) Single-domain model

This is the simplest domain model, as it only involves the existence of one domain in a network. Consequently, it is not necessary to manage trust relationships. In this case, only one SAM database exists for management purposes in the entire network. One variant of this model consists of a configuration of several individual domains in a network, between which no trust relationships are defined. In this case, each domain manages its own SAM database as well as user and group accounts. The single-domain model is particularly suitable for networks with a low number of users (approx. 200 to 300) and computer nodes. A disadvantage of this model is the decrease in performance which occurs as the number of users and user groups rises. Furthermore, it is not possible to group resources into organisational units, for example, in order to reserve a server for a particular department.

b) Master-domain model

The main characteristic of this model is that it divides a network into several domains, one of which centrally manages all user accounts and group accounts. This domain is termed master domain. The other domains hold the resources. These resource domains trust the domain holding the user accounts.



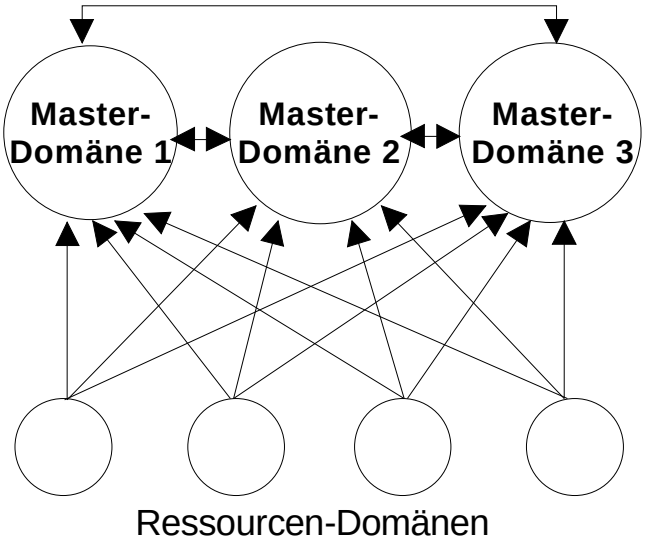
The master-domain model is illustrated in the following diagram:

According to Microsoft, this domain model can handle up to 15,000 users. It is particularly suitable for organisations which consist of several departments, each needing to manage its own resources, and in which user administration is performed centrally. This domain model allows a separate person to be appointed for the administration of each of the resource domains, and also permits central security management.

c) Multiple-master domains

This model consists of several master domains which trust each other. The user and group accounts are managed in these master domains. In addition, there are resource domains which unilaterally trust all master domains. A multiple-master domain is illustrated in the following diagram:

The explicit trust relationship between domain 1 and domain 3 is necessary, as



positions of trust are not transitive, i.e. mutual trust between domains 1 and 2, as well as between domains 2 and 3, does not automatically imply mutual trust between domains 1 and 3.

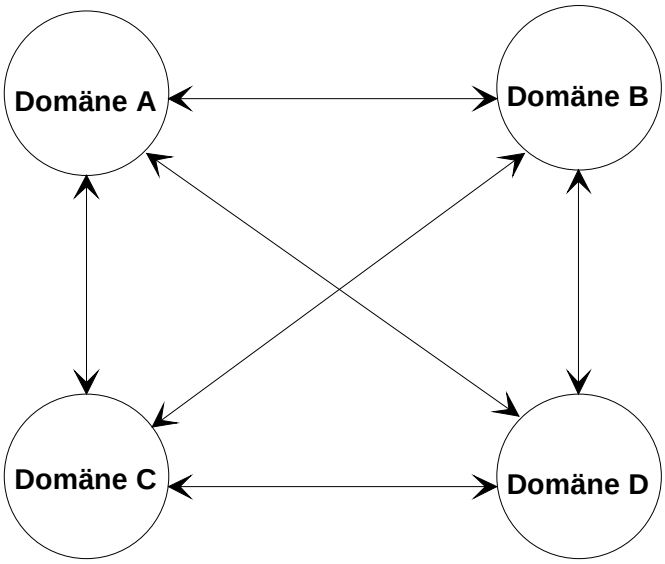
The master domain concepts are often used in networks where more than 15,000 users are present. This concept also allows a network to be partitioned among main departments, and the resources to be managed by these individual departments. For this purpose, a master domain is configured for each main department. The users of a main department are assigned user accounts in the master domain. The resources are managed by the departments in the resource domains. It is also possible to organise a network by location. This involves the configuration of a master domain for each location, and a resource domain for each department. This domain model is scaleable, and no limits are imposed on the size of the organisation. Central security management is possible here, and global groups and user accounts only need to be configured once throughout the organisation.

Finally, it must be noted that this module requires a high degree of administrative discipline and careful planning. Particular care must be exercised when defining the trust relationships. In addition, it is absolutely necessary to prevent a configuration of user accounts in the resource domains.

d) Complete-trust model

This model involves relationships of mutual trust between all the domains of a network. Resources as well as user and group accounts are managed in each domain. A complete-trust model is shown in the following diagram:

This model allows the departments of an organisation to manage user accounts



as well as resources. No central department is required for management. This model can be scaled to any required number of users. However, it also has major disadvantages. For example, it is hard to check compliance with the applicable security policy. This makes it difficult not only to set up a central security management, but also to co-ordinate the activities of the individual administrators. Many trust relationships need to be managed in a network containing a large number of domains, so that a clear overview is ultimately lost.

No general recommendations can be made as to which of the domain models described should be used in an organisation. This can only be ascertained individually, on the basis of the physical and logical network structure, as well as the distribution of data, applications and users in the network. For this reason, a determination of the ideal domain structure requires a detailed analysis, which can prove quite elaborate for extensive networks and might need to be supported with planning software.

Additional controls:

- Have the selected network structure and any trust relationships existing between domains been documented?
- Is the structure adapted to changes in the operational environment

S 2.94 Sharing of directories under Windows NT

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Under Windows NT there is a distinction between various levels of access control to resources. There are access rights at the share level and at the directory and file level (known as NTFS permissions). The access rights at the directory and file level are only available on data media with an NTFS file system, and are dealt with in detail in S 4.53 *Restrictive allocation of access rights to files and directories under Windows NT*.

Sharing directories on servers is necessary in order to enable users to obtain access to the resources via the network. Network access to a directory is not possible unless a share is created in the appropriate way. This is the case even if corresponding NTFS permissions have been granted.

It is possible to share directories on all computers running under the Windows NT operating system, i.e. both on domain controllers and on servers and workstations (clients). Usually, however, directories should only be shared on domain controllers and servers. The sharing of directories or sharing of individual drives on workstations (clients) is implemented as part of peer-to-peer functionality (see S 5.37 *Restricting peer-to-peer functions when using WfW, Windows 95 or Windows NT in a server-supported network*) and should remain very much the exception, because it is liable to lead to the creation of unclear rights structures and even in some cases to undermining of the general security specifications.

A directory can be shared in different ways under the Windows NT operating system, including with Windows NT Explorer, via the "My Computer" desktop icon or with the "NET SHARE" command. The process of sharing a directory is also referred to as creating a share. In Windows NT Explorer or when using the "My Computer" desktop icon, sharing a directory is carried out on the "Share" tab. This is accessible via the "Properties" menu option on the pop-up menu. The share is created by clicking on the "Shared as" option. A share name with a maximum length of 12 characters can then be entered. By default, Windows NT assigns the name of the directory as the share name. To help with administration, a short, succinct description of the share can be entered in the "Comment" box. The number of users who are allowed to access the share at the same time can be specified under the "User Limit" option. The default setting is "Maximum Allowed", i.e. the number is not limited, and this should be retained. This feature is only partially suitable for licence control, because only the number of clients who have connected to the share are counted. Users who are supposed to be able to access the share via the network must be granted an appropriate share permission. This is done using the access control list, which the system opens after the "Permissions" box is selected. The icon for the shared directory is shown with a hand beneath it in Windows NT Explorer and in the "My Computer" desktop icon to indicate that it is shared.

Only members of the "Administrators" and "Server Operators" groups on domain controllers or members of the "Administrators" and "Power Users"

groups on Windows NT workstations and member servers have the right to share directories and to manage share permissions.

The following share permissions are available under Windows NT: "No Access", "Read", "Change" and "Full Access". The actions which the various share permissions allow are shown in the table below:

	No access	Read	Change	Full access
Display subdirectories and file names		X	X	X
Display file contents and file attributes		X	X	X
Run program		X	X	X
Switch to a subdirectory		X	X	X
Create subdirectories and add files			X	X
Modify file attributes			X	X
Delete subdirectories and files			X	X
Change access rights (only relevant for directories that are located on NTFS data media)				X
Transfer ownership (only relevant for directories that are located on NTFS data media)				X

Shares can only be defined for directories, however, not for files. Share permissions apply only to accesses made via the network, i.e. they are of no significance to users who are allowed to work locally on the computer on which a directory has been shared. Also, share permissions apply only in a standardised form for all files and subdirectories in a shared directory. Although it is also possible to share a subdirectory within a shared directory and in so doing also to set different share permissions, this is a new share and brings with it the following consequences: when a user is linked to the shared directory, the share permissions specified for that directory apply to that user with respect to all files and subdirectories. This is not changed in any way even if a subdirectory is shared separately. If the user is linked directly to the subdirectory, however, the share permissions set for the subdirectory apply.

Example: Let us assume the following directory structure: *D:\DEPARTMENT\SECTION*. One share is set up with the *DEPARTMENT* directory with "Full Access" authorisation and another share with the *SECTION* subdirectory with "Read" authorisation. If the user is now connected to the *D:\DEPARTMENT* directory, he can read, write to and delete (among other things) files in that directory but also files in the *D:\DEPARTMENT\SECTION* subdirectory. However, if the user sets up a direct link to the *D:\DEPARTMENT\SECTION* directory, he can only read the

directories contained in that directory. If restrictions on a subdirectory are required, as in the above example, this cannot be achieved by means of share permissions but only with the aid of the NTFS permissions (see S 4.53 *Restrictive allocation of access rights to files and directories under Windows NT*).

When a directory located on an NTFS data medium is shared, in addition to the share permission the NTFS permissions also apply to that directory and to the files and subdirectories that it contains. In each case, the most restrictive permission is the one that applies. If, for example, a user possesses the "Read" share permission for the shared directory, but on the other hand only the "Display" NTFS permission for the same directory, his access right is restricted to "Display". Using the NTFS permission it is therefore also possible to assign access rights individually to files and subdirectories (for more details see also S 4.53).

Share permissions obtained by belonging to groups are cumulative; this means that if a user is a member of various groups to which different share permissions have been granted in relation to a particular directory, the furthest-ranging permission applies for that user. There is an exception to this rule, however: the "No Access" share permission is dominant over all other share permissions.

Example: Let us assume that *D:\RESULTS* is shared. User Smith is a member of group A and of group B. Group A is assigned "Read" permission and group B "Full Access" permission to the above shared directory. In this case the "Full Access" permission is the decisive permission for user Smith. If user Smith is now also made a member of group C, for which the "No Access" share permission has been assigned for the shared directory *D:\RESULTS*, user Smith is denied access to this directory via the network. If this is not the desired effect, all the administrator can do is check which groups have been assigned the "No Access" share permission to the resource and find out to which of these groups the user concerned belongs. The user must then be removed from the relevant group.

Furthermore, it should be noted that Windows NT always shares the root directories of all disks together with the Windows directory *%SystemRoot%* (generally *C:\WINNT*) for administrative accesses. The access rights to these special releases cannot be changed and are restricted to the user group "Administrators". These releases are not directly visible, as they have release names along the lines of "*Disk name*$", thus for example "C$" or the name "ADMIN$".

As a result there is a danger that

- someone can try out the administrator user name and password, or
- an administrator can secretly access users’ computers at any time.

If this feature for facilitating workstation management is required, a decision must be made as to whether administrators should use the same password for all workstations under their jurisdiction. A single password is easier to remember but, if detected, would allow intruders to access all workstations.

If this access capability is not required, e.g. because the administrator is not supposed to be able to access local user data, the right ”Access to this computer from the network ” should be blocked for administrators via User Manager, under Guidelines - User Rights.

By default, Windows NT assigns the "Full Access" share permission for the "Everyone" group every time a share is created. In particular for directories located on data media without the NTFS file system, this is unacceptable, because in this case apart from the share permissions there are no other means of assigning rights and hence of access control. The "Everyone" group therefore has to be removed from the access control list and replaced by the groups and if appropriate individual users who are intended to have access to the shared directory. Corresponding share permissions should then also be assigned.

Even where directories are in fact located on NTFS data media, the "Everyone" group should be removed from the access control list in the event of a share being created. It would be conceivable in this case, however, to include the "User" group with assignment of the "Full Access" access right. The individual assignment of access rights to the directory or the files and subdirectories that it contains is then carried out at the level of NTFS permissions (see S 4.53).

Additional controls:

- Is there any documentation indicating which directories on which computers have been shared for network access?
- Has the "Everyone" group in the shared directories located on data media without an NTFS file system been removed and replaced by the groups and, if appropriate, individual users who are allowed to access the relevant shared directory via the network?
- Is the existing share profile adapted to changes in operational conditions?

S 2.95 Obtaining suitable protective cabinets

Initiation responsibility: IT Security Management

Implementation responsibility: Procurer

Protective cabinets can protect their contents from the effects of fire and from unauthorised access. Depending on the protective effect sought, the following guidelines should be observed when selecting a suitable protective cabinet:

- Protection against the effects of fire:

  Where protective cabinets are concerned, in terms of protection against the effects of fire, there is a distinction between quality categories S60 and S120 complying with VDMA 24991 Part 1. Within these quality categories protective cabinets are tested to see whether, up to a combustion time of 60 or 120 minutes during a standard test for the protected data media, compatible temperatures are maintained within them. The data media to be protected are designated by suffixes in the classification. Specifically, the symbols have the following meanings:

  P = all kinds of paper

  D = Data media (e.g. magnetic tapes, films)

  DIS = Floppy disks, magnetic tape cassettes including all other data media.

  The differences between the categories lie in their insulation performance, which is greatest in the case of DIS cabinets.

  For IT baseline protection, in terms of protection against fire, protective cabinets of quality category S60 should be adequate. It should nevertheless be noted that server cabinets dooffer protection against fire for a certain period of time, so that data media are not destroyed. However, in the event of fire, it should be assumed that operation of the server cannot be maintained.

  Where protective cabinets used for protection against fire and smoke are concerned, provision should be made for a device designed to close the doors automatically in the event of fire. Closure should be able to be triggered locally by smoke gas detectors and/or externally by a signal from a fire alarm system (where one exists).

- Protection against unauthorised access:

  Along with the mechanical strength of the protective cabinet, protection value against unauthorised access is influenced crucially by the quality of the lock. For IT baseline protection, high-performance cabinets complying with RAL-RG 627 should be suitable.

  If access protection and fire protection are required in combination, data security cabinets complying with RAL-RG 626/9 can be used.

Further relevant standards and guidance notes are VDMA 24992 for steel cabinets and RAL-RG 627 for high-performance cabinets. Help in evaluating the resistance value of various protective cabinets is provided by VDMA

Standard Form 24990, which briefly outlines the safety characteristics of protective cabinets.

In choosing protective cabinets, the permissible floor load at the place of installation must also be taken into account.

After these selection criteria for the protection value of the cabinet, the next item to be determined is the equipment for the cabinet in line with known requirements. With this in mind, and before purchasing a protective cabinet, it should be stipulated which equipment and which types of data media are to be kept in it. The internal fittings of the protective cabinet must be selected in line with what is decided. Generally speaking, retrofitting is difficult, as the protection value of the cabinet and its specific certification can be adversely affected. Room for future expansion should also be allowed for in planning.

In server cabinets, as well as for the server and a keyboard, space should also be provided for a monitor and additional peripheral equipment, such as, for example, tape drives, so that administrative work can be carried out on the spot. Here, attention should be paid to choosing equipment which is ergonomically suitable, so that administrative work can be carried out on the server unhindered. Thus, for example, a pull-out base is desirable for the keyboard, fitted at a height which enables the administrator to perform his work while seated. Depending on the use to which the cabinet is being put, air conditioning and/or an uninterruptible power supply (UPS) may be required. The appropriate equipment must then be placed in the cabinet. Otherwise there must at least be some form of ventilation. It is recommendable to equip the cabinet with a locally operating fire early warning system which interrupts the power supply to the equipment in the event of fire (on the input **and** the output side of the UPS, provided there is one).

Back-up data media and log printers should **not** be housed in the same cabinet. In the event of damage to the server, back-up data media would presumably also be damaged. Logging of the actions on the server also acts as a check on the administrator. It is therefore not sensible to grant him access to the log print-outs even where he is the sole recipient.

Additional controls:

- Which protective functions is the cabinet meant to fulfil?
- Are these fulfilled by the cabinet chosen?
- **With which of the above-mentioned quality categories does the protective cabinet comply?**
- Is the console of the server only accessible to the administrator?
- Are the dimensions of the protective cabinet adequate?
- Were unauthorised changes carried out on the protective cabinet?

S 2.96 Locking of protective cabinets

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

In general, protective cabinets should be locked when not in use. If work requiring the protective cabinet to be open is interrupted, even if the room is vacated for a short period, the protective cabinet should be locked. When code locks are used they must be wiped on each occasion.

Additional controls:

- Are sporadic checks carried out to ensure that unused protective cabinets are locked?

S 2.97 Correct procedure for code locks

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

If protective cabinets with mechanical or electronic code locks are used, the code for these locks must be changed:

- after purchase,
- when there is a change of user,
- after opening in the absence of the user,
- if it is suspected that the code was made known to an unauthorised person and
- at least once every twelve months.

The code cannot consist of numbers which are easy to determine (e.g. personal data, arithmetical sequences).

Each valid code of a code lock must be recorded and escrowed in a secure place (see *S 2.22 Depositing of passwords* in a similar application). It should be noted that escrowing of the code in the associated protective cabinet is pointless.

If the protective cabinet has a further lock in addition to a code lock, a judgement should be made as to whether the code and the key are deposited together, which would allow quicker access in an emergency, or separately, so that it is more difficult for an ‘attacker’ to gain access.

Additional controls:

- Is the lock code changed following the occurrences outlined above?
- When was the last time the lock code was changed?
- Is the code for the code locks escrowed safely?
- Where and how is it escrowed?
- Where are any existing spare keys to the cabinet kept?

S 2.98 Secure installation of Novell Netware servers

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

To ensure a fault-free, secure installation of a Novell Netware server, the following aspects should be observed before installation and set-up:

Installation documentation:

The installation of Novell Netware servers should be comprehensively documented so that substitute supervisors, outsiders or newcomers can understand this material after brief viewing.

In particular, the documentation should contain parameterisation of the server (network connection, driver), additional NLMs (Netware Loadable modules, e.g. for data backup) and their configuration, and installed patches. Furthermore, the installation and integration of additional hardware (e.g. network printers, tape drives) should be comprehensively documented.

The documentation should also contain a detailed description of the server hardware and the installed peripheral equipment (e.g. network printer). Depending on the complexity of the Novell network the deployment of administration tools for documentation and revision purposes is desirable.

All the necessary software for installation and configuration of a Novell Netware server should be stored in a secured area, so that unnecessary delays can be avoided. Particular attention should be paid to the patches of the operating system, additional NLMs and drivers.

When loading NLM-Utility *SYS:SYSTEM\CONLOG.NLM* all messages that appear on the server monitor are simultaneously routed to the file *SYS:ETC\CONSOLE.LOG*. This NLM should already be loaded in the start file *AUTOEXEC.NCF*, so that problems reported in the start phase of the server can be detected.

Hardware equipment

When determining the necessary memory capacity (RAM) for Novell Netware servers along with the capacity of the hard drive and the installed operating systems of Novell Netware clients, the RAM utilisation must be taken into account, when loading additional NLMs.

Regarding the capacity of the hard disk when setting up individual volumes on a Novell Netware server, in particular the SYS: volume must have sufficient dimensions, since all Netware processes are carried out in this volume as standard. If the dimensions of the SYS: volume are insufficient, temporary processes such as print commands may, after certain operation time, exhaust the capacity of the volume, thereby causing an avoidable ABEND (abnormal end - server crash).

Hardware requirements:

To increase the availability of Novell Netware servers, i.e. of stored data, Novell Netware 3.x provides three hierarchical System Fault Tolerance

Levels, which are listed below. Each level contains the functionalities of the previous levels.

- SFT I (System Fault Tolerance I)

  Novell Netware 3.x supports SFT I as standard. This level prevents loss of data due to physical hard disk problems. After a write access to a file, the stored data on the disk is compared to the still available memory image on the Netware server. If the data do not compare, the sector of the hard disk will be marked as faulty and will be locked for future access.

  The data is then stored in a ”Hot Fox Area” on the hard disk. Within Novell Netware this area occupies two percent of the disk as a standard.

- SFT II (System Fault Tolerance II)

  SFT II can be implemented in two different ways.

  - Disk Mirroring (System Fault Tolerance II)

    For disk mirroring two identical hard disks are connected to the same controller of a server. The data is stored simultaneously on both hard disks. If one disk fails, the second disk will be used without a loss in availability.

  - Disk Duplexing (System Fault Tolerance II)

    Disk Duplexing means the installation of two hard disks and their controllers. With this mechanism not only a hard disk failure can be remedied, but also the failure of a hard disk controller can be recovered.

- SFT III (System Fault Tolerance III)

  SFT III is the highest level of tolerance for hardware faults that arise during operation. Two identical Novell Netware servers operate simultaneously and parallel to one another within the network.

  The servers are connected via their own high speed network. If one server breaks down, operation of the network can be continued with the second server almost without loss of time and data.

The decision as to whether or not additional measures will be needed besides level I is dependent upon the required level of availability in the network.

Uninterruptible Power Supply (USP)

By using an uninterruptible power supply (UPS), the consequences of a power failure can be remedied. Netware supports the utilisation of devices supporting UPS-Monitoring. In case of a power failure the server will be shut down at the end of the lifetime of the UPS in an orderly manner. All data residing in caches are written to hard disks. Connections to servers are terminated, as are server processes.

Additional controls:

- Is the documentation sufficient for a substitute administrator?
- How has the choice of SFT level been justified?

S 2.99 Secure set-up of Novell Netware servers

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The security features within Novell Netware 3.x are not automatically activated after initial start of the *SERVER.EXE* file. They must be individually installed and configured via the system administration.

By using the program *SYS:PUBLIC\SETPASS.EXE,* the supervisor should allocate a password to this account immediately after the first login. A password should also be provided for the Guest account available as standard. If the guest account is not needed during later use, it should be deleted.

Unauthorised login attempts should be prevented during the set-up phase via DISABLE LOGIN (server console).

With the help of Novell Utilities *SYS:PUBLIC\SYSCON.EXE* under the menu **Supervisor Options** most of the Novell security mechanisms can be installed and configured. It should be considered that the settings made in the **Default Time Restrictions** menu are only valid for all Novell Netware accounts on the server, if these settings are made before the setting up of users and groups.

Relevant security menu points are listed below:

Default Account Balance/Restrictions

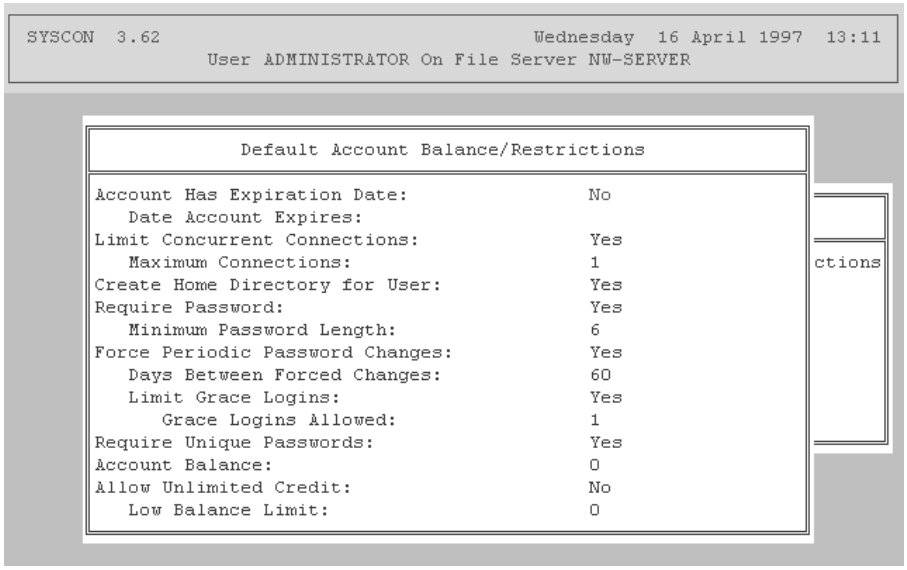
With the help of this menu item the following security settings for the Novell Netware server are activated.

- **Account has Expiration Date**: With this function the validity of an account can be limited to a certain time. Since an account is normally set-up on a long-term basis this feature will generally be activated only for a guest account.
- **Limit Concurrent Connections**: With this function it is possible to limit the number of simultaneous connections from one account to the Novell Netware server. Generally, the number "One" should be selected here.
- **Create Home Directory for User:** An option to create a personal directory for every user. The option "Yes" should be selected here.
- **Require Password: Require Password installs the password entry requirement for every user and, upon activation, rules for password entry can be set. The option "yes" should be selected here.**
- **Minimum Password Length: With this function the required minimum length of a password can be set. The minimum length should be set to six characters (see below S 2.11 *Provisions governing the use of passwords*). If the minimum length is set to less than five characters, this will be shown when activating *SYS:\SYSTEM\SECURITY.EXE* (see S 2.101 *Revision of Novell Netware servers*).**
- **Force Periodic Password Changes: With the setting "Yes" users will be forced to change their passwords regularly. As a rule, this option should be left active.**

- **Days Between Password Changes:** Under this menu the general duration of password validity is determined. Length of password validity must be determined for each system.

  Note: If the duration of password validity is set for more than 60 days, this will be "noted" by the Novell Utility *SYS:SYSTEM\SECURITY.EXE*.

- **Limit Grace Logins: Grace Logins are logins occurring once the duration of password validity has expired. In principal, the number of Grace Logins should be limited by selecting "Yes".**
- **Grace Logins Allowed: The number of permissible grace logins should be set to a value of 1, so that when a password expires, it needs to be changed immediately by the user.**
- ***Require Unique Passwords:*** *Activation of password history (REQUIRE UNIQUE PASSWORDS) results in the last nine passwords of an account being compared with the new password. If any of the passwords match, the new one will be rejected by the Novell Netware server.*
- **Account Balance: Novell Netware accounting function**
- **Allow Unlimited Credit: Novell Netware accounting function**
- **Low Balance Limit:** Novell Netware accounting function



To be added to the illustration: Menu *SYS:PUBLIC\SYSCON.EXE* "Default Account Balance/Restrictions"

Default time restrictions

With the help of Time Restrictions, the allowed working hours on a Novell Netware server can be defined. Outside these times, which generally correspond to normal working hours, no user will be permitted to login to the Novell Netware server.

Note: For guest and supervisor accounts installed as standard, the Netware default setting will be used (no time limit). As far as access times are

concerned, it is recommended that at least the guest-account be restricted by using *SYS:PUBLIC\SYSCON.EXE* (User Information - Time Restrictions).

Additional changes to "Default Time Restrictions" when setting up or maintaining user accounts have no effect on the access times of users already defined. Differing access times for individual users must be set up with the help of *SYS:\PUBLIC\SYSCON.EXE* (User Information - Time Restrictions).

Edit System AUTOEXEC File

The parameters of a Novell Netware server are configured in the start file *AUTOEXEC.NCF* (e.g. volumes, NLMs, additional protocols etc.).

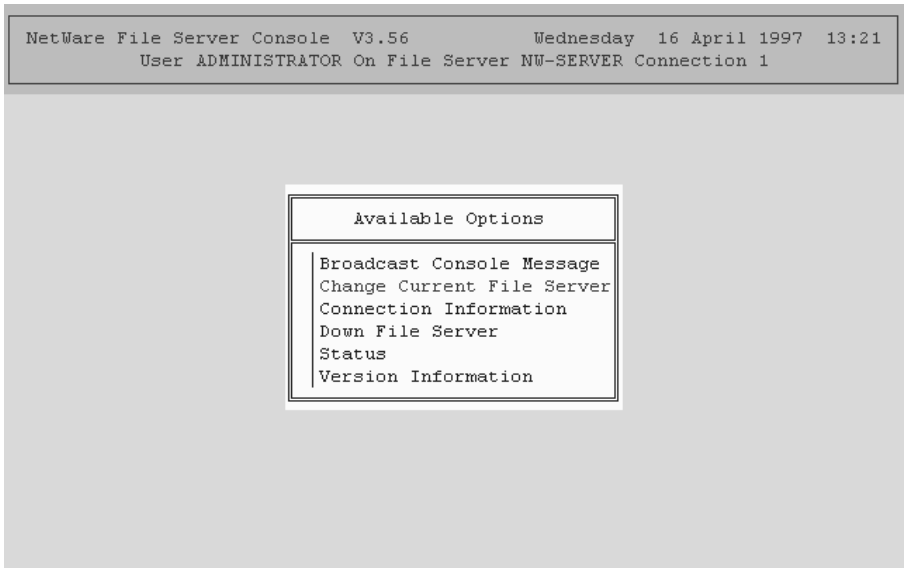
Furthermore, additional security settings can be carried out in the *AUTOEXEC.NCF* file.

The Novell Netware console command SECURE CONSOLE which should be included in the *AUTOEXEC.NCF*, ensures that NLMs can only be started from the server directory *SYS:SYSTEM*. The same applies for the deactivation of Novell Netware Debuggers. Via SECURE CONSOLE, DOS will be removed from the main memory of the Novell Netware server and the defined search paths will be deactivated and cannot be redefined.

File Server Console Operators

It is possible to have restricted control of a Novell Netware server from a workstation with the help of the menu utilities *SYS:\PUBLIC\FCONSOLE.EXE*.

The File Server Operator requiring no further privileges besides explicit entitlement to use *SYS:\PUBLIC\FCONSOLE.EXE*, can send messages to the user, change the Novell Netware server, or shut the server down. Also, the status of the Novell Netware server can be observed and changed (date, time, etc.) and information regarding current connections may be observed. The program *SYS:\PUBLIC\FCONSOLE.EXE* can be activated as standard by a supervisor or supervisor-equivalent account. Other users should not have access to these files



To be added to the illustration: Menu *SYS:PUBLIC\FCONSOLE.EXE*

Intruder Detection/Lockout

By activating "Detect Intruders" unauthorised login attempts to the Novell Netware server will be recognised and the accounts concerned will be frozen, if need be.

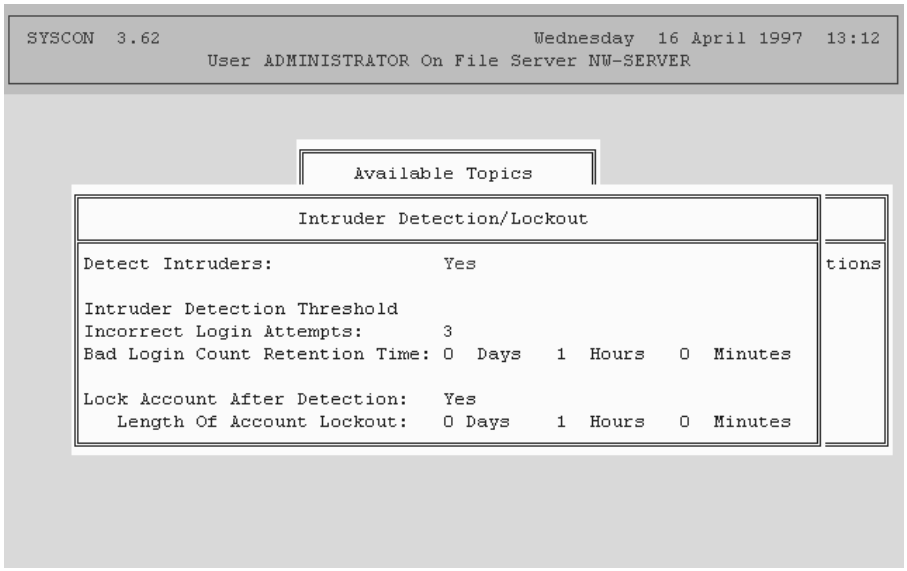
By activating "Detect Intruders" along with further parameterisation of this menu point, a "Brute Force Attack" under Novell Netware will be prevented.

Incorrect Login Attempts indicates the number of permitted failed login attempts. Generally, the number "three" should be selected here.

With the help of **Bad Login Count Retention Time** the time of the failed login attempts to an account can be traced back. If the number of failed login attempts exceeds the number set under **Incorrect Login Attempts**, within the time allowed, the user account will be frozen on the Novell Netware server.

The menu item **Lock Account After Detection** should be set to "Yes", so that an account which exceeds the number of invalid login attempts is frozen.

The time set for **Length of Account Lockout** should under no circumstances be too small (> 1 hour), to assure that the reason for an Intruder Lockout can be resolved by the System-administrator and the user concerned.



To be added to the illustration: Menu *SYS:PUBLIC\SYSCON.EXE* "Supervisor Options - Intruder Detection Logout"

System Login Script

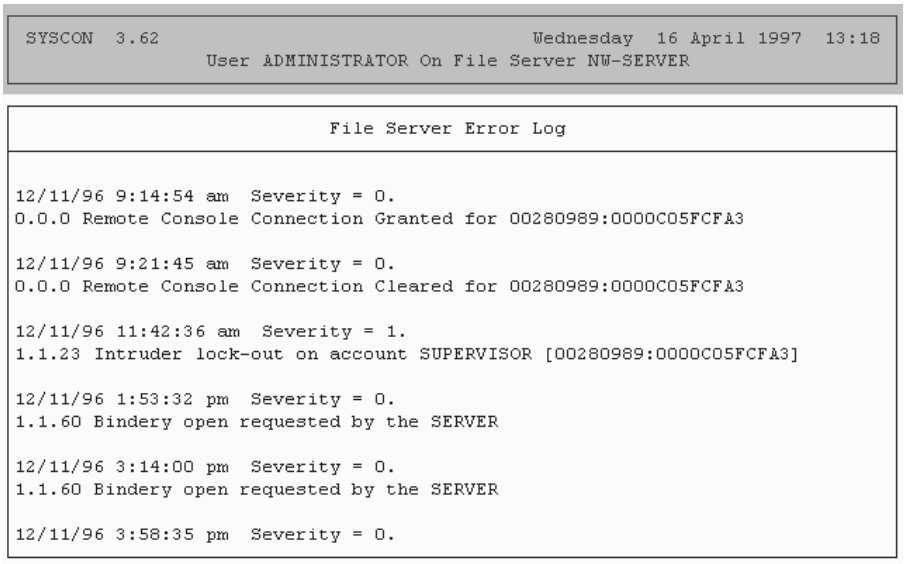
In the System Login Script, settings will be made which should exist for all users once logged on to the Novell Netware server. In contrast to the User Login Script, the System Login Script will be executed for every user. Therefore, settings applying to all users of the Novell Netware server e.g. assignment of disks or activation of external programs, should be made in the System Login Script.

To prevent a user changing the standard settings via use of his own USER-Login-Script the command EXIT must be given when closing the System-Login-Script.

Note: Furthermore, a User-Login-Script must be created for every user. This is necessary since every user possesses the access right "create" in the *SYS:MAIL* directory. Therefore, a *LOGIN* file, which can carry out harmful functions, can be created in the *SYS:MAIL* directory of a user without a User-Login-Script.

View File Server Error Log

The File Server Error Log is the error protocol of a Novell Netware server. All error and warning messages will be saved here and can be analysed by the supervisor



To be added to the illustration: Menu *SYS:PUBLIC\SYSCON.EXE* "Supervisor Options - File Server Error Log"

Workgroup Managers

A workgroup manager is a restricted supervisor account. Like an administrator, it has the right to create or delete bindery objects (users, user groups, printer queues). The rights used by a workgroup manager, which can be passed on to users or user groups must comply with the rights granted by a supervisor.

Workgroup managers may not set up new workgroup managers or users with a supervisor-equivalent security level, unless the workgroup manager already possesses rights equivalent to a supervisor.

Station Restrictions

With the help of the menu point Station Restrictions, the network addresses from which a user can log on to the Novell Netware server can be determined. Information regarding the respective address of a workstation in the network can be found out, for example, by use of *SYS:PUBLIC\USERLIST.EXE /A*. Determining permitted network addresses is particularly recommended for supervisor or supervisor-equivalent accounts. These should be decided on the spot and as conditions require.

Standardised Set-up of Users and User Groups

Besides using menu utilities *SYS:PUBLIC\SYSCON.EXE*, it is also possible to set up users with the help of *SYS:\PUBLIC\MAKEUSER.EXE* and *SYS:\PUBLIC\USERDEF.EXE* .

These programs are particularly suited to the simultaneous set-up of large numbers of users.

With the help of *SYS:\PUBLIC\MAKEUSER.EXE* a type of Batch-file is created, with can be used t set up many users with various privileges.

The purpose of *SYS:\PUBLIC\USERDEF.EXE* is to set up many users with the same privileges. For this purpose, a template will be drawn up which indicates the criteria for the users.

These menu-utilities should be used particularly for larger networks to make administration easier and more consistent.

S 2.100 Secure operation of Novell Netware servers

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Secure operation of a Novell Netware network requires various actions which are listed below:

Allocation of access rights to directories and files

The allocation of access rights (Trustee Assignments) to files and directories on Novell Netware servers plays a central role in the security of Novell Netware servers.

In contrast to the assignment of attributes, Trustee Assignments are assigned to individual users or user groups.

Directories and files can be assigned to specific tasks via the access rights. This ensures that user groups and users are only granted access to the directories and files which they require for performing their respective tasks.

For a clearer overview, easier administration and improved auditing capability, access rights should be assigned primarily to user groups.

To prevent accidental release of directories by users, system administration should ensure that the directories allocated to users and user groups do not contain "Supervisory" (S) and "Access Control" (A) privileges.

If certain properties (e.g. write-protected files) are allocated to files or directories with the help of Netware Attributes, attention should be paid to the fact that users possessing the "Modify" (M) privilege for the corresponding files and directories are able to change these attributes. The number of users with this access right should thus be restricted (see below Allocation of Netware Attributes to files and directories).

Allocation of access rights to directories and files

Besides granting access rights to users and groups for files and directories, the allocation of Netware-Attributes to files and directories can increase data security. Attributes always concern files or directories, i.e. they are independent of the allocated access rights and are valid for all users including the supervisor.

Users, who have been granted the "Modify (M)" privilege for the files and directories concerned, can change the Netware-Attributes and thereby carry out every action permitted by their effective privileges.

By installing Netware-Attributes, security will take the form of a subsystem in file and directory security.

When allocating Netware-Attributes to files and directories, the following properties of Netware-Attributes should be taken into account.

- **Directory Attributes:**

  Hidden (H): The directory will be labelled as hidden; it will not show up in a contents list under DOS, neither can it be copied or deleted.

System (Sy): The directory (e.g. *SYS:SYSTEM\DELETED.SAV)* is used by the system; it will not show up in a contents list under DOS, it can neither be copied nor deleted.

Rename Inhibit (R): The directory cannot be renamed.

Delete Inhibit (D): The directory cannot be deleted.

Purge (P): When deleting, the directory and the files contained therein will immediately be physically deleted. Restoring the directory with the help of *SYS:\PUBLIC\SALVAGE.EXE* is not possible.

- **File Attributes:**

Read write (Rw): Read and write access to the file is possible.

Read only (Ro): The file may only be read. Write access is not possible. To avoid data loss during simultaneous use, these files should also possess the "Shareable" (S) Attribute.

Executable program files (*.exe, *.com) should be given the ”Read only” Attribute to prevent a possible computer-virus attack.

Shareable (S): These files can simultaneously be used by many users. Files that have been given the ”Shareable” Attribute should also possess the ”Read Only” Attribute. The "Shareable" Attribute is only relevant for programs that open files in a non-networkable mode.

Purge (P): Files with the ”Purge” Attribute will, when deleted, not only be immediately logically deleted, but also physically. The consequence being that the file cannot be restored. (*SYS:PUBLIC\SALVAGE.EXE*).

In this context, it must be noted that the physical deletion of a file can be brought about not only by the "Purge" Attribute. If secure deletion of directories and files is required, the Netware program *SYS:PUBLIC\PURGE.EXE* can be installed for this purpose.

Transactional (T): Files with this attribute are subject to transaction control from Novell Netware. Transaction, in this context, means a series of changes in one or more files. Installing this attribute causes only completely executed transactions to be taken over by the data contained in the file. Transactions that have been improperly interrupted will be undone by Novell Netware.

Archive needed (A): The contents of files labelled thus by Novell Netware have been changed or reinstalled since the last backup. With a sequential backup, data backup software can recognise that the file must be backed up again.

Copy Inhibit (C): Files of this type cannot be copied. However, this Netware Attribute is only designed for APPLE Macintosh workstations.

Delete Inhibit (D): The file cannot be deleted.

Rename Inhibit (R): The file cannot be renamed.

Execute Only (X): Executable program files (*.*EXE*, *.*COM*) which have been allocated with this attribute may only be executed or deleted. Copying of the file is not possible.

Hidden (H): The file will be labelled as hidden; it will not show up in a contents list under DOS, neither can it be copied or deleted. I

System (S): This file (e.g. bindery Files -*NET$OBJ.SYS, NET$PROP.SYS, NET$VAL.SYS)* is used by the network operating system; it will not show up in a contents list under DOS, it can neither be copied nor deleted.

Backup of important system files

The server start files *AUTOEXEC.NCF* and *STARTUP.NCF* should be saved by the system administrator in their respective present versions on secured and stored in a safe place secured against unauthorised access. It is wise to supplement these files with comments so that the respective set parameters can be understood when problems arise.

Furthermore, the bindery (*NET$OBJ.SYS*, *NET$PROP.SYS*, *NET$VAL.SYS*) of a Novell Netware server should be regularly backed up with the help of the *SYS:SYSTEM\BINDFIX.EXE* program. The backed up bindery (*SYS:SYSTEM*.OLD*) should then be saved on a data medium and stored in a safe place secured against unauthorised access.

In any case, after executing *SYS:SYSTEM\BINDFIX.EXE* the integrity of the new bindery should be tested. If in doubt, the old bindery can be restored with the help of *SYS:SYSTEM\BINDREST.EXE*.

User access to the present bindery is withdrawn during execution of *SYS:SYSTEM\BINDFIX.EXE*. For reasons of operational security, no user, apart from a supervisor or an equivalent-to-a-supervisor user, should be logged on to the Novell Netware server when backing up the server bindery.

Restricted use of a supervisor or an-equivalent-to-a-supervisor account

The supervisor account should not be used for daily administrative tasks. Rather, it should only be used in case of emergency. Nonetheless, to ensure system administration, an equivalent-to-a -supervisor account should be set up for every user with the "supervisor" network security level, with which the system administration is normally be carried out. If administrative tasks are not performed on a full-time basis, additional accounts need to be created specifically for each non-administrative activity.

Furthermore, a supervisor or an equivalent-to-a-supervisor account should only be used on the workstations defined for that purpose, since under some circumstances the integrity of other workstations can be manipulated by users.

Delegation of system administration

In larger networks (many Novell Netware servers or various locations) or with a large number of users, delegation of certain system administration tasks is recommended. For this purpose Novell Netware 3.x offers the possibility of assigning users with user-account-manager or workgroup-manager accounts.

User-account-managers can administrate users and groups which have been allocated to them by the system administrator. Thus, besides being able to alter user-data (password, operating time, etc.) they can pass on all the privileges which they themselves possess. Furthermore, user-account managers may allocate individual users to a group. In this case, the groups as well as the users must be administrated by the respective user-account-

manager. The user-account manager cannot set up new users or groups. He may, however, delete users or groups which have been allocated to him.

A workgroup-manager has all the privileges of a user-account-manager. Moreover, he can set up new users and groups. An additional task of the workgroup manager is the setting-up of printing queues.

Use of the NCP-Packet-Signature

Communication between Novell Netware clients and a Novell Netware-server is controlled by the Netware Core Protocol (NCP). Client and Server exchange individual packets which contain data. A potential attacker can monitor these packets by using special programs (see T 5.58 *"Hacking Novell Netware"*) and can manipulate packets belonging to highly privileged users.

The Packet-Signature has been developed to counteract this threat. When a user logs on to the server, a secret key will be established. If a workstation then sends an inquiry to the server via NCP, it will be provided with a signature formed from the secret key and the signature of the previous packet. This signature will be attached to the relevant packet and sent to the server. The server will verify the packet signature before dealing with the actual inquiry.

With the option *Set NCP Packet Signature* -value-, the packet signature can be activated on the server.

The possible levels of NCP-Packet signature are as follows:

Value "0": There are no NCP-Packet-signatures.

Value "1": The Novell Netware Server is using NCP-Packet-signatures at the request of the client.

Value "2": The Novell Netware server requires an NCP-Packet-signature from the client. If the client cannot supply one, communication between client and server will nonetheless be granted.

Value "3": The NCP-Packet-signature is mandatory.

To ensure IT-security, the value "3" should be selected for NCP-Packet-signature. Since installation of the NCP-Packet-signature increases network demands by 30%, it should be clarified beforehand whether the performance will be unreasonably reduced.

Restriction of available hard disk memory

With the help of the program *SYS:PUBLIC\DSPACE.EXE* the available hard disk memory of a volume or directory should be limited, as experience shows that use of available hard disk memory increases with the capacity of the hard disk memory.

Alternatively, once set up, the capacity of each user's personal directory can be restricted if single directories have been set up for work data.

Blocking programs that are not required

Most of the Novell Netware programs available under *SYS:PUBLIC* will generally not be required by Netware users, since many of the functions (printer configuration, password change, allocation of disks) can be carried out

with the client software. For this reason, and due to the unfamiliar handling of Novell Netware service programs, it is recommended that programs not required be moved into the *SYS:SYSTEM* directory. In particular the program *SYS:PUBLIC\RENDIR.EXE*, should not be available to users due to the recognised threat (T 5.54 *Deliberately Causing an Abnormal End*).

Under no circumstances should the programs stored in the *SYS:SYSTEM* directory be moved into the *SYS:PUBLIC* directory, as has often been the case.

Information on Novell Netware patches

In the course of developing the network operating system Novell Netware 3.x, various weaknesses and shortcomings have come to light, most of which have been eliminated by the producer with the help of so-called patches. These patches can also be obtained from the manufacturer via the Internet (www.novell.com, ftp.novell.com and www.novell.de, ftp.novell.de). Shortcomings identified during operation of the network can thus be fixed by obtaining information on the network's functionality and, if necessary, loading the patches which have been made available. In particular, additionally installed software products, e.g. for the purpose of performing data backups, often require a certain patch level of the network operating system. Here though, it must be noted that the offered patches should by no means be loaded "blindly", but only after a thorough research if a concrete requirement for them has arisen ("never change a running system").

As not all patches are error-free, they should first be checked in a test configuration.

Apart from the international discussion forums in the Internet (Usenet) regarding Novell Netware (at present, comp.os.netware.announce, comp.os.netware.misc, comp.os.netware.security, bit.listserv.novell), there exists a german-speaking Novell forum for german users (at present, de.comp.sys.novell). A number of experienced Novell administrators are present, who can help solve even the most complicated problems. In addition, files are available over the Internet to answer the most frequently asked questions (FAQs). The most frequent problems are dealt with and solutions are offered.

Furthermore, patches and information regarding Novell Netware are made available by other service providers such as Compuserve, Fidonet and Mailboxes.

However, no guarantee can be given as to the correctness and comprehensiveness of the respective information in the usenet discussion forums or in the FAQs. It should be noted that a complete description of the problems arising, as well as a description of the respective network configuration (Client, Server), is highly advantageous when searching in the Internet (Usenet).

Furthermore, difficulties in network operation can often be remedied by making enquiries with the network operating system salesperson or by exchanging information with colleagues. As before, solving problems will be made considerably easier with a complete description of the configuration.

Testing for Computer-Viruses

Computer-Viruses located in the saved files and programs of a Novell Netware server can cause considerable damage to the network, due to their central position.

For this reason, the programs and files on a Novell Netware server should regularly be checked for the presence of computer viruses using a recent virus scanning program.

For this purpose, it is recommended to set up a special user-account on the Novell Netware server which contains "Read" (R) and "File Scan" (F) privileges for all server files. Under no circumstances should the anti-virus test be carried out with supervisor or equivalent-to-a-supervisor privileges, since an anti-virus program which is itself infected will then transfer this virus to all programs and files on the Novell Netware server.

For files and directories with an executable program code, users and user groups should only receive the effective "Read" (R) and "File scan" (F) privileges. Furthermore, executable programs should be provided with the "Read only" (RO) Netware Attribute.

S 2.101 Revision of Novell Netware servers

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

In practice, complete revision of a Novell Netware 3.x server within the framework of IT-baseline protection will hardly be possible. Nonetheless, the following approaches to revision should be observed.

With the program *SYS:SYSTEM\SECURITY.EXE* the bindery-files of a Novell Netware server will be examined for the following security weaknesses. Recognised weaknesses will be listed.

No password assigned

Users not requiring a password to login to the Novell Netware server will be listed.

Insecure passwords

Here, many aspects of the bindery of a Novell Netware server will be examined.

Firstly, all users whose login name is equivalent to their password will be listed, as will users whose password may be less than five characters. Furthermore, it will be examined for every user if the duration of password validity amounts to less than 60 days and if an unlimited number of Grace Logins is permitted.

Supervisor equivalence

SYS:SYSTEM\SECURITY.EXE checks the bindery of a Novell Netware server in order to list those users who have the "supervisor" security level (Supervisor equivalence).

Root directory privileges

Due to access rights being passed "down" all users of the Novell Netware server will be examined to see if they have access to the main directory (at volume level).

Login scripts

All the users not having their own login-script (User Login Script) will be determined.

In order to exchange electronic messages, all users have the "Create" privilege in the SYS:MAIL directory as standard. An "attacker" could copy a *LOGIN* file (User-Login-Script) into the SYS:MAIL directory of a user not possessing a User Login Script, thus changing the user's Novell Netware environment.

Excessive rights

Within the installation framework, Novell Netware 3.x makes many directories available as standard (*SYS:SYSTEM, SYS:PUBLIC, SYS:LOGIN*). SYS:SYSTEM*SECURITY.EXE* examines the bindery of a Novell Netware server to check if users have more privileges than provided as standard in

these directories. Furthermore, the right of every user to possess a *SYS:MAIL* directory will be examined (exception "Create" for the group "Everyone").

Additional controls:

- When was the last revision carried out?
- How often is a revision carried out?

S 2.102 Relinquishing activation of the remote console

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

With the help of the program *SYS:\SYSTEM\RCONSOLE.EXE*, the Novell Netware network operating system allows remote control of the Novell Netware server console from a workstation. The Novell Netware server is set up in the *AUTOEXEC.NCF* file by loading *RSPX.NLM* and *REMOTE.NLM* with the corresponding password. It should be ensured that the password is not contained in the *AUTOEXEC.NCF* file in plain text. This can be done by entering the command *REMOTE ENCRYPT* on the server console after running the *REMOTE.NLM* program. The password that has been called up is then encrypted and, if required, can be stored in the *LDREMOTE.NCF* file using the necessary command. The command in the *LDREMOTE.NCF* file is as follows:

LOAD REMOTE -E 0613BB68060099

Network analysis tools, so-called Sniffers, can pick up and save data exchanged between the workstation and the Novell Netware server. This includes the encrypted password which must also be entered in order to remotely control the Novell Netware server. Special software can be used to decrypt the encrypted password. Therefore, unauthorised personnel could be in a position to gain access to the Novell Netware server console via remote control.

In order to prevent remote sessions from being recorded with network analysis tools then simply replayed into the network, it should be ensured that signatures for the RSPX packets are activated. This can be checked using the command RSPX on the console of the server. The response should be as follows:

RSPX Packet Signatures:

All packets must contain signatures.

If no signatures are active, use the command *RSPX SIGNATURES ON*. As these functions are not supported by Netware versions prior to Netware 3.12, it is essential that the current version is used.

For security reasons, the option to remotely control Novell Netware servers should be avoided if prevailing conditions and operating procedures allow.

In general, however, the *SYS:\SYSTEM\RCONSOLE.EXE* program should not be used if C2 security is to be achieved (see also S 4.102 *C2 Security under Novell 4.11*)

S 2.103 Setting up user profiles under Windows 95

Initiation responsibility: IT Security Management

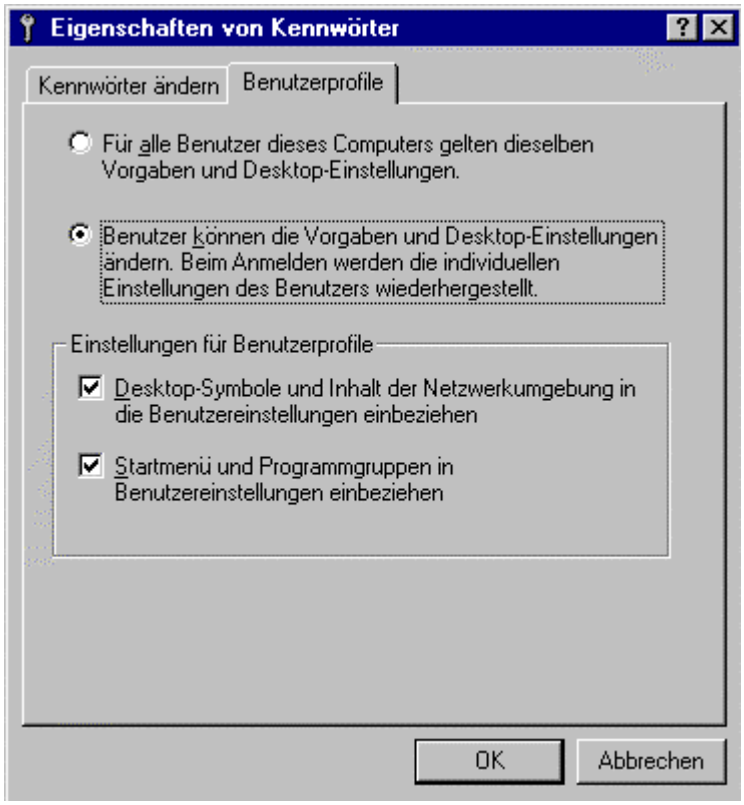
Implementation responsibility: Administrators

Under Windows 95 it is possible to carry out user separation by setting up user profiles. This separation serves, however (if system guidelines do not carry out a restriction, see S 2.104 *System Guidelines for Restricting Usage of Windows 95*) only to retain user-specific settings and thereby contains an individual work environment for each user, which he can adjust according to his needs and requirements. A log-on password for Windows 95 will be compulsory once the user profile has been activated. The same considerations apply for this password as for WfW log-on passwords (see S 4.46 *Use of the Log-On Password under WfW and Windows 95*).

Settings concerning the user will be saved in the following directory: *C:\WINDOWS\PROFILES\Username*.

On a non-networked Windows 95 computer, user profiles should always be activated if navigation under Windows 95 needs to be eased for inexperienced users. This is also sensible if user separation is desired not from the point of view of security, but for organisational or principal reasons.

For this purpose, the program group *CONTROL PANEL* should be opened, then the option *PASSWORDS* and the user profile can then be activated or deactivated.



Note: In Netware or NT networks, compulsory user profiles can be established by saving the appropriate profile with write-protection in a directory allocated to the user. This profile has the name *USER.MAN* and is loaded from the server every time the user logs on (see S 4.51 User Profiles to Restrict the Usage Possibilities *of Windows NT*).

Additional controls:

- Should several users work on a Windows 95 computer?
- Is user separation sensible from the point of view of security or for organisational/principal reasons?

S 2.104 System guidelines for restricting usage of Windows 95

Initiation responsibility: IT Security Management

Implementation responsibility: Administrators

If navigation under Windows 95 needs to be eased for inexperienced users, or if certain resources need to be restricted for operational reasons, certain restrictions can be provided for the user environment via the system guidelines under Windows 95. However, it must be noted that users might take a cold attitude towards an IT system, if restrictions are not immediately comprehensible. Thus a restriction should only occur when absolutely necessary or if this will go unnoticed by the user.

As soon as system guidelines are activated, Windows 95 will check upon starting whether user-specific restrictions have been set up for the present user. If this is the case, they will be loaded. If it is not the case, restrictions for standard users will be applied. In the following, the principal restrictions that can be set via the **system guidelines** are described. It is then listed how these restrictions can be established and activated via the system guideline editor (*POLEDIT.EXE*).

The essential restrictions to be set via system guidelines for a non-networked Windows 95 computer are as follows:

- Access to the control panel can be restricted via the options *DISPLAY*, *NETWORK*, *PASSWORDS*, *PRINTER SETTINGS* and *SYSTEM PROPERTIES*. Each option can be completely deactivated or restricted to single register cards.

  For these options the following points are essential:

  - Entries for screen colours can be made from an ergonomic point of view.
  - It is possible to allow users to change their own passwords.
  - Printer configurations and hardware settings can be securely set.
- Access to single functions of the user interface can be restricted. For example, the commands *RUN*, *SEARCH* and *END* can be removed. This will prevent users from searching for relevant security files or programs and, if possible, executing them. Drives can be removed from the *DESKTOP* and the *EXPLORER* (previously *FILE-MANAGER*). As only the start drive (e.g. *C:*) is available when booting, partitions (drives) can only be switched by using applications.
- The **Program start** of executable files can be restricted and the DOS prompt can be deactivated. Applications available to single users can be explicitly provided (e.g. *WINWORD.EXE, EXCEL.EXE* and the *EXPLORER.EXE*)

Additionally, the computer can be arranged so that Windows 95 log-on passwords must consist of letters as well as numbers or symbols and must

have a minimum length. Programs that should be executed at the system start can also be set.

The following shows in single steps how the system guidelines can be established and activated and which restrictions offer security for a non-networked Windows 95 computer.

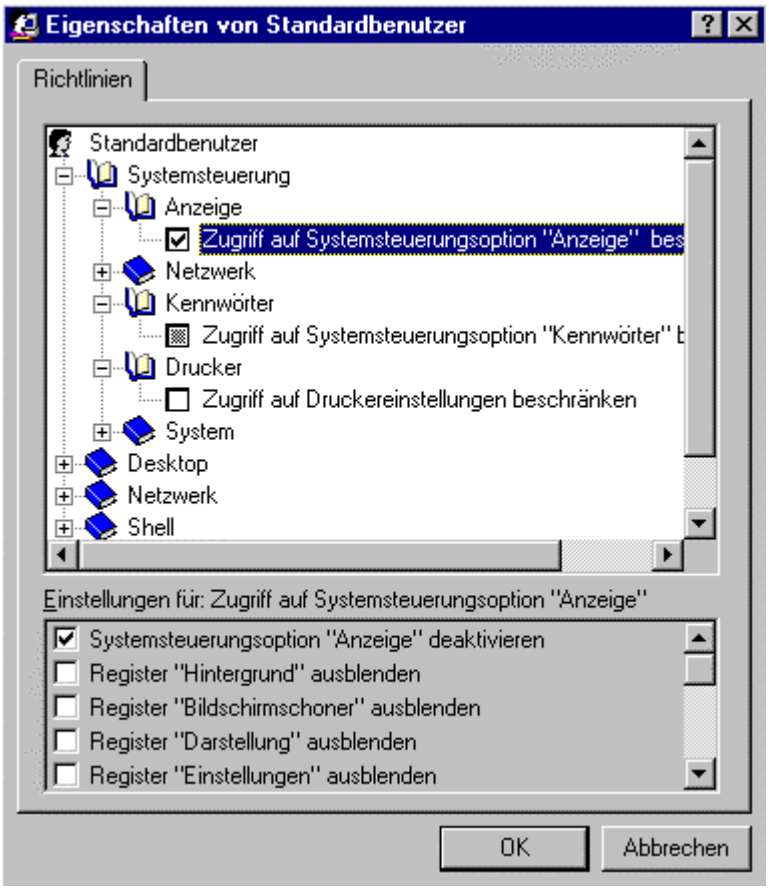
1. Establishing a system guideline file

With the help of the system guideline editor a system guideline file can be created. Any name is possible. However, for reasons of simplicity, the name *CONFIG.POL* will be selected here. The program *POLEDIT.EXE* should then be started, a new file created and saved under the name *CONFIG.POL*. This file automatically contains entries for the standard user and the standard computer which, if applicable, must be restricted in the next step. Entries for computer and user must also be established for the administrator (in the menu point *EDIT* with *ADD USER* and *ADD COMPUTER*). The setting must be specified in the third step.

2. Defining a guideline for a standard user and a standard computer

By opening settings for the standard user with the system guideline editor, the appropriate relevant security entries can be made via the menu.

For example:



The following restrictions should be set for a **Standard user**:

CONTROL PANEL

- Access to the register card *SCREEN SAVER* should be deactivated if the user should not be able to deactivate the screen lock. In this case, however, he must be given the option to change the screen password. The *CONTROL PANEL* (see below) may therefore not be completely deactivated. The same applies for the register card *PASSWORD CHANGE* under the option *PASSWORDS*.
- The register card *USER PROFILE* under the control panel option *PASSWORDS* must definitely be removed, thus preventing the user from deactivating the system guidelines.
- The settings for hardware configuration must be carried out, and access to the register cards and interfaces for the control panel option *SYSTEM PROPERTIES* requires maximum restriction. This prevents faulty configuration by the user, which could restrict the availability or performance of the computer.

Shell-Access Restrictions

- The command *EXECUTE* should be deactivated, if the start-up of certain programs with command line options should be prevented.
- The *CONTROL PANEL* and *PRINTER SETTINGS* can be completely deactivated by activating the option *"REMOVE FOLDER"* under *"SETTINGS"* in *"START MENU"*. This is always necessary when the option to change system or printer settings should be denied for the user. The register card *SCREEN SAVER* (see above) under the control panel option *DISPLAY* must be released so that the user can change his screen password. The user can then access the screen lock by clicking on the desktop with the right mouse button and choosing *PROPERTIES*.
- If use of the *EXPLORER* is not to be permitted, the option *REMOVE DRIVES IN "DESKTOP" WINDOW* must be activated, as the *EXPLORER* can be started from the desktop even if use of this program has been explicitly prohibited.

System-access restriction

- The option *DEACTIVATE PROGRAMS FOR REGISTRY EDITING* must be selected.
  Note: This option only concerns the registry editor (*REGEDIT.EXE*). With the system guideline editor (*POLEDIT.EXE*) the local registry can be edited as before. This program should therefore be deleted from the hard disk.
- Only approved applications should be executable.
  The applications, which the user should be able to execute, must be listed, such as *WINWORD.EXE*, *ACCESS.EXE*, *EXPLORER.EXE*.
- MS-DOS prompt must be deactivated.
- If applicable, single-mode applications for MS-DOS must be deactivated.
  If some DOS applications must be started under Windows 95, but the user should not be able to go to the DOS prompt, the DOS entry prompt must be **activated**. However, only the required authorised applications for Windows should be named. The *COMMAND.COM* may not be named there.

The following restrictions should be set for a **standard computer**:

Network

- Under *PASSWORDS*, an alphanumerical Windows log-on password with a minimum required length of six characters is required.
- *REMOTE-UPDATE* under *UPDATE* must not be deactivated, otherwise the system guidelines will not be loaded.

System

- *USER PROFILES* must be activated.

3. Defining a guideline for the administrator

None of the restrictions listed above should be implemented for an administrator guideline. For this, an own user must be set up under Windows

95 along with a user and a computer via the system guidelines, otherwise the same restrictions will apply as for a standard user. The password may only be made known to the administrator and his substitute.

In any case, this guideline must be saved in the *CONFIG.POL* file.

4. Defining guidelines for single users based on a standard user and a standard computer

If users are required whose restrictions should differ from those specified under 1., the guidelines are the same as for 1. but must additionally be set up in the *CONFIG.POL* file. The standard profile is copied, the name of the user concerned will then be given to the profile and the restrictions are set as described under 1.

5. Activating the guidelines

When the administrator sets up the system guidelines, particular care and attention must be given as inconsistent system conditions can easily be set which hinder work with the computer. The operating system would have to be re-installed. Therefore the system guidelines should only be activated once they have been defined with utmost care.

For this purpose, the administrator must open the local registry with the system guideline editor (*POLEDIT.EXE*) and the switch *REMOTE-UPDATE* for the *LOCAL COMPUTER* under the option *NETWORK-UPDATE* must be switched on. INTERACTIVE must be selected as update-mode. The path for the CONFIG.POL as described above must also be defined.

Highly experienced administrators can carry out the necessary settings with the registry editor (program *REGEDIT.EXE*).

Furthermore, the user profiles must be activated under the option PASSWORDS in the program group CONTROL PANEL.

Additional controls:

- From operational point of view, is restriction of the user environment necessary?
- Is it necessary to restrict certain resources?

S 2.105 Obtaining PBX-annexes

Initiation responsibility: Agency/company management

Implementation responsibility: Site technical service, purchase department

When obtaining a new PBX unit, at the outset it is possible to arrange this in such a way that at a later stage a higher amount of security can be attained with few personnel and little additional organisational effort. Primarily, attention must be paid to:

- the availability of suitable functions for administration of the unit,
- sufficient logging mechanisms and analysis tools and
- the ability of the PBX unit to carry out revision.

The relevant requirements of the federal authorities have been elaborated by the German Information Security Agency (BSI) together with the Central Association for Electronic Technology and Electronic Industry and summarised in the brochure:

Security requirements for PBX-annexes

- Recommendations for federal authorities -

From the point of view of the BSI, these recommendations can be passed on to other administrative areas and to private industry.

The brochure can be found on the IT-baseline protection manual CD-ROM (see appendix: Auxiliary Materials).

S 2.106 Purchase of suitable ISDN cards

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, Purchase Department

ISDN cards which have been selected for purchase should offer all security functions which might be required, so as to prevent unnecessary expenses in future. These security functions should either be an integral part of the card, or realisable with the help of the accompanying communications software and driver programs.

Possible criteria for selecting a suitable ISDN card include:

- Capability to perform authentication via PAP and CHAP (Password Authentication Protocol and Challenge Handshake Authentication Protocol, RFC 1994)
- Availability of a hardware-based or software-based encryption procedure (symmetric/asymmetric)
- Possibility of evaluating CLIP call numbers (Calling Line Identification Presentation) for the purpose of authentication
- Possibility of maintaining a table of call-numbers for performing callbacks
- Possibility of logging unsuccessful attempts to establish a link (refusal due to incorrect authentication of call numbers or PAP/CHAP).

Furthermore, the ISDN cards must be checked for functions which would impair operational security. If any such functions are found to exist, they should at least be deactivated through appropriate configuration. This includes, for example, the remote control functionality which allows an establishment of direct communications with the IT system via the public network.

ISDN cards with the greatest possible number of identical security functions should be used on the IT systems requiring such cards as well as the network gateways (e.g. ISDN routers). If a particular security function exists on one side but is absent on the other, the desired effect will not be achieved.

Additional controls:

- Is the purchase department aware of the additional requirements which ISDN cards need to fulfil?

S 2.107 Documentation of the configuration of ISDN cards

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The possibilities of configuring an ISDN card in accordance with the area of application involved are almost endless. To ensure proper re-starting (e.g. following a replacement of the ISDN card or the related communications software), it is advisable to document at least the following settings:

- Type and serial number of the card in use
- Call number(s) for establishing communications links and performing any authentication required
- D-channel protocol in use (1TR6, EDSS-1 etc.)
- B-channel protocol in use (X.25, PPP, TCP/IP, bit transparent etc.),
- CAPI version in use
- Version of the driver software in use
- Type of data compression, if used
- Type of authentication (e.g. PAP/CHAP), if used

In the case of authentication procedures which involve a mutual maintenance of secrecy (e.g. through the use of a password), the secret can also be documented. However, this documentation must only be made available to a small circle of persons, to avoid unwanted disclosure of the secret.

Additional controls:

- Are passwords described in the documentation? Is the documentation kept in a secure place?

S 2.108 Relinquishment of remote maintenance of ISDN gateways

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Relinquishment of remote maintenance is a useful way of preventing external parties from manipulating ISDN routers and IT systems equipped with ISDN cards.

In the case of IT systems equipped with an ISDN card, a check is required as to whether the communications software in use offers a "remote control" function. This function allows the IT system to be called via a public network: The ISDN card accepts the call, and the caller can then operate the IT system as though he/she were present on-location. If this function is present, it must be deactivated.

In the case of ISDN routers, the remote maintenance via reserved bandwidths (or reserved ISDN call numbers) function should be deactivated because, in this case, links established with the management information base of the router are usually just protected by a password, and allow almost all configuration settings to be modified.

Additional controls:

- Which reasons speak for and which reasons speak against the relinquishment of remote maintenance?
- Has a corresponding decision on remote maintenance been made?

S 2.109 Assigning rights for remote access

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Rights to access a corporate network from external points need to be restricted appropriately. In addition to the requirements stipulated in S 2.8 *Granting of access permissions*, further restrictions need to be imposed on remote access.

Access rights for directories with software may not necessarily exist in the case of a remote workstation, for example (refer to T 5.62 *Misuse of resources via remote IT systems*).

Additional controls:

- When were the rights for remote access reviewed last?

S 2.110 Data privacy guidelines for logging procedures

Initiation responsibility: Head of IT Section, data privacy officer

Implementation responsibility: Administrators, data privacy officer

In terms of data security, logging as part of IT-systems operation constitutes the manual or automatic generation of records which make it possible to determine ”who accessed or performed what, when, using which resources.” These records should also indicate system states, i.e. ”who had which access rights for which period of time.”

The nature and scope of logging depends on general data privacy laws as well as locally applicable guidelines.

The logging of administrative activities is equivalent to system monitoring, while the logging of user activities serves essentially as process monitoring. Accordingly, requirements concerning the nature and scope of system-oriented logging originate primarily from general data privacy laws, while process-oriented logging is defined mainly by locally applicable guidelines. Examples of process-oriented logging guidelines are registration laws, police laws and constitutional laws.

Minimum requirements for logging

The following activities must be logged fully during the administration of IT systems:

- System generation and modification of system parameters

  As system-controlled logs are usually not generated on this level, detailed manual records corresponding to the system documentation are required here.

- Configuration of users

  Complete records must be maintained as to which rights to use an IT system were granted by whom to which people for which periods of time. Long-term retention periods must be specified for these logs, as they form the basis for practically every method of review.

- Preparing rights profiles

  One important logging task as part of user administration is to maintain a record of the people who issued instructions to configure individual user rights (also refer to S 2.31 *Documentation on authorised users and on rights profiles*).

- Installation and modification of application software

  Logs in this context indicate the outcome of releasing programs and processes.

- Modifications to file organisation

  In view of the numerous possibilities of manipulation during the use of standard file management systems, complete logging is of particular importance here (for example, as regards database management).

- Implementation of data backup measures

  As such measures (backup, restore) are related to the copying and overwriting of data stocks, and are mainly required in exceptional cases, logging is of special importance in this context.

- Use of administration tools

  The usage of all administration tools must be protocoled to help ascertain whether unauthorised people have subversively acquired system administration rights.

- Attempts at unauthorised login and transgressions of rights

  Given effective authentication procedures and an appropriate allocation of rights, particular emphasis must be laid on maintaining a complete record of all ”abnormalities” occurring during login and the use of hardware/software components. System administrators are also to be considered as users in this context.

During the processing of person related data, the following user activities must be logged selectively or fully in accordance with the sensitivity of the processes and information involved:

- Input of data

  Input monitoring is always process-oriented (e.g. logging in files if these are used, direct logging in the data stock if no files are used). Even if transgressions of rights are assumed to be logged using a different technique, complete logging of data inputs should be considered as a standard procedure.

- Data transfer

  Selective logging of data transfer can be considered sufficient only if complete logging is not legally specified.

- Use of automatic retrieval procedures

  Complete logging of retrieval and the reasons underlying them (procedure, reference, etc.) is generally necessary to detect unauthorised handling outside the scope of the access rights granted.

- Deletion of data

  The deletion of data must be logged.

- Invocation of programs

  It might be necessary to log the invocation of especially sensitive programs which, for example, must only be used during certain periods or on certain occasions. Complete logging is recommended in such cases. This also makes it possible to exonerate authorised users (proof of exclusive right to invoke a program).

Appropriation of log data

In accordance with the almost fully identical data privacy regulations applicable on the federal and state levels, log data are largely immune to appropriation (e.g. § 14 Sec. 4 and § 31 BDSG, § 13 Abs. 5 HDSG). Such data must only be used for the purposes for which they were originally saved. These purposes usually consist of general monitoring tasks specified in a security concept, "checks for the proper usage of programs for processing person related data" stipulated by most data security laws (for example, refer to § 18 Sec. 2 BDSG, § 8 Abs. 3 LDSG-SH) and monitoring by internal or external data security officers. Only in exceptional cases do locally applicable regulations allow the appropriation of such data for other purposes such as criminal prosecution.

Storage period

Unless specified otherwise by locally applicable regulations, the storage period for logs is defined by the deletion guidelines forming part of generally applicable data privacy laws. The "fulfilment of responsibilities" is used as a yardstick here. If no compelling reasons exist for the further retention of log data, these must be deleted by law (for example, refer to § 20 Sec. 2 BDSG).

The following factors serve as orientation here:

- The probability that irregularities might still be detected
- The possibility of ascertaining the reasons for such irregularities using the logs and other documents

Empirical results have shown that a retention period of one year is sufficient here.

Shorter retention periods should be considered for logs which are prepared for the purpose of selective checks. Storage up to the point of actual checking is usually adequate. Here, too, locally applicable regulations must be observed.

Basic technical and organisational requirements

The effectiveness of logging and its evaluation as part of monitoring depends decisively on technical and organisational conditions. In this context, the following aspects should be considered:

- A review concept should be prepared for the purpose of clearly defining the purpose of the logs and their monitoring functions, as well as security mechanisms for the rights of users and other people involved.
- Measures must be taken to ensure the inevitability and completeness of the logging functions, and to safeguard entries in the log files against manipulation.
- In accordance with the degree of appropriation applicable to the data stock, effective access restrictions must be implemented.
- The logs must be designed to allow effective checking. This also includes IT-supported evaluations.
- Possibilities of evaluation should be ascertained and stipulated at the start.

- Checks must be performed sufficiently often to prevent damage and allow the initiation of appropriate measures following the discovery of violations. Timely checks must be carried out before the expiry of retention periods for log files.
- Checks must be performed in accordance with the two person rule.
- Responses to violations detected through the monitoring of logs should be defined at the start.
- Employees should be made aware of the fact that checks are performed routinely and, if necessary, without prior notice.
- Automatic procedures (e.g. watch dogs) should be used for routine checks.
- The staff and works councils should be involved in the preparation of the review concept and the stipulation of log evaluation techniques.

S 2.111 Keeping manuals at hand

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section, IT Security Management

When procuring information technology - regardless of whether it is hardware or software - the related manuals and technical reference literature must also be procured in sufficient numbers.

In an increasing number of cases, physical documentation related to IT products now only consists of an installation guide and introductory text, the rest being replaced by online help systems. The scope of this documentation proves inadequate and limited, particularly on the occurrence of errors which need to be evaluated. Steps must be taken to ensure that the required manuals, technical reference literature and error catalogues are procured with the IT system. In this context, it is not necessary to refer exclusively to literature provided by the manufacturer of the IT system.

All manuals concerning an IT application must remain available at all times in the application's environment. For example, manuals concerning a server operating system must be stored in the immediate vicinity of the server, not in a library which might be locked. Access to this literature must be ensured as part of contingency planning (refer to S 6.3 *Development of an Emergency Procedure Manual*).

Additional controls:

- Which manuals are available concerning the IT products in use?
- Where are these manuals stored? Are they available at all times?

S 2.112 Regulation of the transport of files and data media between home workstations and institutions

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: Staff members

To allow the safe and reliable transport of files and data media between the workstation at home and the institution, regulations concerning the nature of this exchange need to be drawn up. At least the following issues should be settled here:

- Determination of which files and data media may be transported using which means (mail, courier, parcel service etc.). (In this context, refer to S 5.23 *Selecting Suitable Types of Dispatch for Data Media*.)
- Determination of the security measures required during transport, including:
  - Locked container
  - Padded envelope
  - Registered mail
  - Certified mail
  - Covering letter
  - Seals
- Determination of the files and data media which must only be transported on one's person

As papers, documents and portfolio files are often unique - i.e. no copies of them exist - the selection of a suitable means of exchanging these items must include a consideration of the consequential damage which would arise from their loss. In contrast, data media can be backed up before dispatch.

Additional controls:

- Have the concerned employees been informed about how files and data media are to be transported?

S 2.113 Requirements documents concerning telecommuting

Initiation responsibility: Agency/company management; Head of Personnel Section

Implementation responsibility: Personnel Section; superiors

As official legislation specifically concerning telecommuting does not yet exist, certain issues need to be clarified through wage settlements, corporate resolutions, or individual agreements - as supplements to work contracts - between telecommuters and employers. This should include a clarification and settlement of a voluntary participation in telecommuting, overtime and surcharges, expenses for travelling between home and the institution, electricity and heating costs, liability (in the case of theft or damage to IT equipment, as well as work-related accidents and illnesses) and the duration of telecommuting terms.

Furthermore, the following issues should be clarified from the point of view of IT security:

- **Work periods:** The allocation of working times to activities at the institution and at the home workstation needs to be regulated, in addition to the specification of fixed periods during which telecommuters should remain accessible at their home workstation.
- **Reaction times:** Specifications should be made as regards the intervals at which information (e.g. e-mail) is to be fetched, and the time taken to respond to such information.
- **Work resources:** Specifications can be made as regards work resources which may and may not be used by telecommuters (e.g. software which has not been approved). For example, an e-mail link can be maintained while prohibiting the use of other Internet services. Furthermore, the use of diskettes (danger of computer viruses) can be prohibited if this is not required by the home workstation.
- **Data backup:** Telecommuters must be instructed to regularly perform data backups. In addition, one generation of each backup should be kept at the institution to improve availability.
- **IT security measures:** Telecommuters must be instructed to observe and implement the security measures required for telecommuting. These IT security measures must be specified in writing to the telecommuters.
- **Privacy protection:** Telecommuters must be instructed to observe regulations applying to privacy protection as well as the processing of person related data at the home workstation.
- **Data communications:** Specifications must be made as to which data are to be transmitted using which means. This includes a stipulation of the data which are to be transmitted in encrypted form, or not at all.
- **Transport of folders:** Specifications must be made as to the nature and safeguarding of the transport of folders between the home workstation and the institution.

- **Reporting routines:** Telecommuters must be instructed to immediately inform a particular department at the institution on the occurrence of events relevant to IT security.
- **Rights to access a home workstation:** Rights to access a home working place (with prior notice, if required) can be assigned for the purpose of monitoring and ensuring the availability of files and data if a telecommuter needs to be replaced by stand-in.

Additional controls:

- Are telecommuters aware of the scope of their responsibilities?
- Have telecommuters received written information concerning the scope of their responsibilities?
- Have telecommuters received written instructions on observing IT security measures? When were these instructions last updated?

S 2.114 Flow of information between the telecommuter and the institution

Initiation responsibility: Superiors, telecommuters

Implementation responsibility: Superiors, telecommuters

To keep telecommuters aware of internal affairs, superiors should ensure a regular exchange of information between telecommuters and their colleagues. Keeping telecommuters aware of plans and objectives in their areas of activity is important, in order to prevent frustration and create and maintain a positive telecommuting atmosphere.

The involvement of telecommuters in the distribution of internal circulars, pertinent information and periodicals should be regulated. This might prove problematic in the case of telecommuters who work exclusively from home. One possible solution here would be to scan important documents and then transmit them to the telecommuter via e-mail. Telecommuters also need to be informed about changes to IT security measures.

Furthermore, colleagues of telecommuters need to be notified of their periods of availability, e-mail address, and telephone number.

In addition, the following issues concerning telecommuting need to be clarified:

- Who is to be contacted on the occurrence of a problem during telecommuting?
- Who needs to be notified of security-relatedincidents?
- How are tasks to be allocated?
- How are the results of completed tasks to be transferred?

If technical or organisational problems occur, they must be reported immediately by the telecommuter to the institution.

Additional controls:

- How is the telecommuter informed about business-related affairs?
- To whom does the telecommuter report security-related incidents?
- Who is the contact person (independent of the superior) for the telecommuter?

S 2.115 Care and maintenance of workstations for telecommuting

Initiation responsibility: Head of IT section

Implementation responsibility: Head of IT Section, administrators, telecommuters

A special concept geared towards the care and maintenance of telecommuting workstations and encompassing the following points needs to be prepared:

- **Designation of a contact person for user service:** This is the person with whom telecommuters establish contact on the occurrence of software or hardware-related problems. The user service is intended to provide quick assistance (also via telephone) and initiate maintenance as well as repairwork.
- **Maintenance appointments:** Appointments for on-site maintenance should be announced well in time so that telecommuters can guarantee access to their home workstations at the arranged times.
- **Introduction of standard telecommuting computers:** All telecommuters working for an institution should use defined, standard computers to facilitate problem-solving for the user service department.
- **Remote maintenance:** If telecommuting computers are to be administered and maintained from a remote location, the necessary security measures and online access periods should be agreed upon. In particular, a security routine must be specified in order to prevent misuse of remote maintenance ports (refer to S 5.33 *Secure Remote Maintenance Via Modem*).
- **Transport of IT:** For reasons of liability, specific persons should be made responsible for the transport of IT between the institution and home workstations.

Additional rules are specified in S 2.4 *Maintenance/repair regulations*.

Additional controls:

- Does the telecommuter know who the contact persons for hardware and software-related problems are?
- Is the user service familiar with the configuration of standard telecommuting computers?
- Does the user service have the addresses of telecommuters to be able to provide quick assistance on location?

S 2.116 Regulated use of communications facilities

Initiation responsibility: IT Security Management

Implementation responsibility: Administrators , Telecommuters

All telecommuting computers are equipped with electronic communications facilities. From the point of view of IT security, guidelines concerning the use of these communications facilities need to be prepared. The use of these facilities for private purposes should generally be prohibited.

At least the following issues should be clarified:

- Monitoring of data flow:
  - Which services may be used for data transmission?
  - Which services must be barred explicitly from use?
  - Which information may be sent to which persons?
  - Which written correspondence may take place via E-mail?
  - If the telecommuting computer possesses a fax modem, or if a fax machine is available at the telecommuting workstation, clarification is required as to which information may be transferred to whom via fax.
  - Which information must be approved by the institution before it can be transmitted electronically?
- Information acquisition:
  - Which electronic services (database queries, electronic searches) may be made use of from telecommuting computers? For example, query patterns can serve as a basis for inferring corporate strategy.
  - Which budget is available for electronic services?
- IT security measures:
  - Which data require which type of encryption?
  - Which data should be deleted after successful transmission. This might apply to person- related data, for example.
  - Which data should be backed up on the telecommuting computer even after it has been transmitted successfully?
  - Are data scanned for viruses before dispatch or after receipt?
  - Which data transmissions should be registered in a log? If automatic logging is not possible, a clarification is required as to whether and to what extent manual logging must be performed.
- Internet usage:
  - Is the usage of Internet services prohibited in general?
  - Which type of data may be downloaded from the Internet? Data downloaded from extraneous servers might harbour the threat of computer viruses.

  - Which options may be activated in the Internet browser?
  - Which security mechanisms of the Internet browser should be activated?
  - Is approval by the institution required if a telecommuter intends to exchange information via news groups? Anonymous usage might be required in certain cases.
- Guidelines concerning signatures:
  - Do guidelines concerning signatures for communications exist?
  - Do the digital signatures in use conform with legal regulations?
  - Are other authentication processes used for written correspondence?

Additional controls:

- Are telecommuters aware of regulations concerning the use of communications facilities?
- Do telecommuters provide their signature to acknowledge instructions concerning the use of communications facilities?

S 2.117 Regulation of access by telecommuters

Initiation responsibility: IT Security Management, Head of IT Section

Implementation responsibility: Administrator, Superiors

If telecommuting requires access to the IT of the institution (for example, on a server), clarification is required beforehand as to which objects (data, IT) telecommuters actually require to perform their tasks. Rights such as read and write access need to be allocated accordingly for these objects. Telecommuters should not be allowed to access objects which they do not actually require. This applies to access to data as well as the IT available at the institution. This safeguard is intended to minimise the potential damage caused by hacker intrusions into the communications computer. For the allocation of access rights, refer to S 2.7 *Granting of system/network access rights* and S 2.8 *Granting of application/data access permissions*.

Additional controls:

- Does the administrator know which objects the telecommuter is allowed to access?
- Which requirements must be fulfilled before access rights can be allocated or modified?
- Is the server administered such that telecommuters are only able to access permissible objects?

S 2.118 Determination of a security policy for the use of e-mail

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Before e-mail systems can be approved for use, their intended purpose must be determined. This purpose, in turn, shapes requirements concerning the confidentiality, availability, integrity and non-repudiation of the data to be transmitted as well as the e-mail program to be employed. Clarification is required as to whether e-mail is to be used exclusively for the transmission of non-binding and informal information, or whether some or all of the business transactions processed previously in writing are now to be carried out via e-mail. If the latter is true, clarification is required as to how previously hand-written remarks concerning procedures and orders, signatures and initials should now be placed electronically.

The institution must specify a security policy which describes the following items:

- The persons who are to receive e-mail connections
- The rules to be observed by e-mail administrators and e-mail users
- The degree of confidentiality and integrity up to which information may be dispatched via e-mail
- The manuals which need to be procured
- How users should be trained
- How to ensure a constant availability of technical assistance for users

Organisational rules and technical measures are required to meet, in particular, the following conditions for the proper transfer of files:

- E-mail programs intended for users should be pre-configured by the administrator so as to automatically achieve the highest possible level of security for the users (also refer to S 5.57 *Secure Configuration of Mail Clients*).
- Data should only be transferred following successful identification and authentication of the sender by the transmission system.
- Before making use of e-mail services for the first time, users must be briefed on how to handle the related applications. Users must be familiar with internal organisational rules concerning file transfer.
- To identify the sender of an e-mail, a signature is appended to the end of the e-mail. The contents of this signature should resemble those of a letterhead, i.e. include the user name, organisation name, telephone number etc. A signature should not be too large, as this would take up unnecessary transmission time and storage space. The agency / company should determine a standard for signature design.
- The security mechanisms in use determine the degree of confidentiality and integrity up to which files may be sent via e-mail. Clarification is required

as to whether and when data to be transmitted should be encrypted and signed digitally (also refer to S 4.34 *Using Encryption, Checksums or Digital Signatures*). A central body must determine the applications to be employed by users for the encryption and use of digital signatures. These applications must be made available to the users, who should be briefed beforehand on how to handle the applications.

- Before the introduction of electronic communications systems, clarification is required as to the circumstances under which incoming and outgoing e-mails also need to be printed out.
- File transfer can be documented (optionally). In this case, every file transfer, together with the contents and recipient of the information, is registered in a log. Legal regulations concerning logging must be observed during the transfer of person related data.

E-mail intended for internal dispatch must not be allowed to leave the internal network. This must be ensured by appropriate administrative measures. For example, the transfer of e-mail between the various departments of an organisation should take place via internal, dedicated lines and not via the Internet.

In principle, messages intended for internal addresses must not be forwarded to external addresses. If an exception needs to be made, all employees must be informed duly. For example, e-mails might need to be forwarded to external points where they can be accessed by staff on external duty or other employees on business trips.

Additional controls:

- Does a security policy governing the use of e-mail exist?
- Who is responsible for answering users' queries concerning e-mail?

S 2.119 Regulations concerning the use of e-mail services

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

If data are to be exchanged electronically between two or more communications partners, they must observe the following guidelines to ensure proper exchange:

- E-mails must bear unique addresses to prevent dispatch to the wrong party. Within an organisation, address books and distribution lists should be maintained to ensure that the most commonly used addresses are always correct. Test messages should be sent to newly configured e-mail addresses in order to ensure that the data is transferred correctly.
- If e-mail is sent to several recipients, the "CC" option should not be used as every recipient can then see who else has received the message. Instead, distribution lists or the "BCC" option should be used. BCC stands for blind carbon copy and recipients entered here are not told who else has received the message.
- All e-mails sent to external locations must be appended with a signature file containing the complete sender address.
- The subject of communication must always be indicated, similar to the mention of subjects in written correspondence.
- Data transmissions which have been completed should be checked for correctness. The recipient should check whether data have been received properly, and issue a confirmation to the transmitting party.
- A memory-resident virus scanner should be employed for incoming and outgoing files. Prior to their dispatch, outgoing files should be checked explicitly for computer viruses.
- If a file has been attached to an e-mail, the following information should also be submitted to the recipient:
  - The type of file (e.g. Word Perfect 5.0),
  - A brief description of the file contents
  - A note that the file has been scanned for computer viruses
  - If applicable, the type of compression program (e.g. PKZIP)
  - If applicable, the type of encryption software or digital signature

  The following items should not be indicated:
  - Passwords allocated to classified information
  - Keys used for encrypting information

In the case of most e-mail systems, information is sent in unencrypted form via open lines, and might be stored on a number of computers until it reaches the recipient. The information can be easily manipulated during its journey. In

addition, senders of e-mail are in most cases able to freely enter the origin of the e-mail (From:) so that their authenticity can only be verified through double checking or the use of digital signatures. In case of doubt, the authenticity of the sender should therefore be verified through a corresponding check or - better still - through the use of encryption and/or digital signatures. In principle, the authenticity of sender details should not be taken for granted.

E-mail systems should be checked several times daily to determine whether new e-mails have arrived. Rules should be drawn up to govern the substitution of users during their prolonged absence, for example, in order to forward incoming e-mail to a stand-in.

As in most cases, it is not possible to ascertain which type of e-mail client is used by a mail recipient and which software / operating systems are used on the transmission route, users should be instructed to employ 7-bit ASCII representation for mail bodies as well as attachments. Locally applicable special characters such as mutated vowels and Greek symbols should therefore not be included in the message text. In case of doubt, attachments should be converted into 7-bit ASCII form using *uuencode*, for example.

All rules and instructions concerning the use of e-mail should be specified in writing and remain constantly available to employees. An appropriate draft is provided on the accompanying IT Baseline Protection Manual CD-ROM.

Personnel must be briefed before using communications services such as e-mail in order to avoid incorrect handling and ensure that internal organisational guidelines are adhered to. In particular, users should be made aware of possible threats and the related security measures to be observed during the transmission and reception of e-mail.

To prevent overloading through e-mail, employees should be briefed about the types of action which should be avoided in this context. They should be warned against participation in electronic chain-letter mailings as well as subscription to high volume mailing lists.

Users must be informed that files whose contents might cause offence should not be dispatched to others, stored on information servers, or requested from them. Furthermore, users should be instructed to observe the following rules during the use of communications services:

- Negligent or even intentional interruption of operations in progress should be avoided at all costs. Actions which should be avoided in particular include unauthorised attempts to access network services regardless of their nature, modification of information available via networks, intervention in the operating environments of other network users, and forwarding of inadvertently received details on computers and staff members to third parties.
- Information of no public relevance should not be disseminated. The overloading of networks through an arbitrary and excessive distribution of information should be avoided.
- The distribution of redundant information should be avoided.

Additional controls:

- Have regulations governing file transfer and exchange of messages with external parties been established?

S 2.120 Configuration of a mail centre

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

To allow smooth operation of the e-mail service, a postmaster must be appointed to fulfil the following responsibilities:

- Availability of mail services on a local level
- Maintenance of address tables
- Checking external communications links for proper functionality
- Providing assistance in solving mail-related problems experienced by end-users as well as the operators of gateway and relay services.

All e-mails which did not reach their destination and all related error messages must be reported to the postmaster, who must then try to remedy the faults. E-mail which does not reach the intended recipients after a specified period has elapsed must be returned to the sender together with a corresponding error description.

Furthermore, depending on the size and structure of the organisation involved, one or more persons should be put in charge of maintaining the available communications services. In addition to server operations involving, for example, the mail, news and FTP servers, users' communications clients also need to be maintained.

All persons in charge (or their stand-ins) should remain constantly accessible by telephone to users.

Additional controls:

- Who is the responsible postmaster?
- Where are incorrectly addressed e-mails collected?

S 2.121 Regular deletion of e-mails

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

E-mail should not remain stored on the stack of incoming mail for an unnecessarily long period of time. E-mail should either be deleted after it has been read, or relocated to a corresponding user directory if it is to be retained. If too much e-mail is archived on the incoming stack, the IT system (mail server or mail client) managing this stack will reject new incoming e-mail if the storage space becomes insufficient.

Users must be informed that e-mail which they have deleted via their mail application is usually not erased irrevocably. Instead of deleting e-mail immediately, many programs transfer it to a special folder. Users must be briefed on how to completely delete e-mail on their clients.

Even after having been deleted completely on a client, e-mail may still be present on a mail server. Many Internet providers and administrators archive incoming and outgoing e-mail. Instead of deleting e-mail, many mail applications transfer it to a cybernetic rubbish bin which is emptied every now and then.

Users must be made aware of the fact that the confidentiality of e-mail can only be ensured by encryption, and not necessarily by quick deletion following receipt.

Additional controls:

- Do users know how to delete their e-mail?

S 2.122 Standard e-mail addresses

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

E-mail addresses should be allocated on the basis of clearly defined rules. In this context, it is advisable to base the nomenclature for personal e-mail addresses on the names of the users of the IT systems (e.g. e-mail address = first eight characters of the surname). User names on IT systems which can be accessed outside the protected network should not be directly derivable from the e-mail addresses, in order to prevent intrusions into user accounts. It is important not to change addresses too frequently or make them too long and complicated. In particular, it must be ensured that non-ASCII characters such as mutated vowels are not used as part of e-mail addresses.

To impede intrusions, avoid e-mail advertisements and release as little information as possible outside the protected network, it might be advisable to assign e-mail addresses which are difficult to guess instead of addresses related directly to users and organisations, for example, surname@organization.com. However this also makes the forwarding of addresses less convenient, and can render communications with external parties more difficult.

If e-mail addresses are modified or no longer applicable, it must be ensured that e-mail bearing the old address is transferred to the new address at least for a transitional period.

In addition to personal e-mail addresses, specific organisational and specific functional e-mail addresses can also be configured in order to guarantee proper delivery to the right department, regardless of the persons involved. This is of particular importance in the case of central gathering points.

Additional controls:

- According to which rules are e-mail addresses assigned?

S 2.123 Selection of a mail provider

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT section

Before selecting a mail provider, the responsible persons should inform themselves about the regulations laid down by the prospective provider, for example, whether upper limits have been set for the volume of incoming and outgoing e-mail, whether e-mail is filtered and, if so, according to which rules.

Confirmation of reliable operation of the provider's mail server must be obtained, i.e. the conditions specified in S 5.56 *Secure Operation of a Mail Server* must be fulfilled.

The mail provider stores user data for invoicing purposes (name, address, user-ID, bank account) as well as connection data and transmitted contents (over a period of time which varies from one provider to another).

Users should ask their mail provider for how long which items of data concerning them remain stored. When selecting a provider, it should be taken into account that German providers must comply with data privacy regulations applying to the processing of this information.

Through the use of encryption, users can prevent providers from being able to read the contents of the transferred data.

Large providers with their own large network have an advantage in that e-mail exchanged exclusively within this network is less susceptible to manipulation than if it were forwarded via the Internet.

Many providers whose headquarters are situated abroad route all e-mail via that country. For example, AOL (and Compuserve) route all e-mail via the US. This fact should be taken into account when determining the number of gateways via which e-mail is distributed, i.e. the number of parties who might be able to monitor the e-mail.

Additional controls:

- According to which criteria has the mail provider been selected?
- Which security measures does the mail provider implement?
- According to which criteria is e-mail filtered by the mail provider?

S 2.124 Selection of suitable database software

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

During the procurement of a new database software, it should be selected so as to achieve the highest possible degree of security with a minimum of personnel and organisational resources during future operation.

To start with, the area of application and the purpose of the database system needs to be ascertained in order to formulate requirements concerning availability, integrity and confidentiality. Furthermore, the requirements regarding processed data volumes, processing rate and throughput need to be quantified. This will shape the features required of the database software, such as portability to particular hardware platforms and operating systems, or the scope of necessary security mechanisms. At this stage of planning, it is already possible to determine whether and to what extent hardware will need to be extended and upgraded for future operation of the database system. The required monitoring functions must also be defined on the basis of the availability requirements, i.e. it must be decided which various database states should be identified and in which form (e.g. by means of a log file) as well as the method of notifying responsible persons or groups of persons about critical states of the database (for example, through the output of messages to the console).

Particular note must be made of the following items when procuring database software:

- The database software itself must possess suitable mechanisms for the identification and authentication of users (refer to S 2.128 *Controlling Access to a Database System*).
- The database software must possess suitable mechanisms for limiting resources (refer to S 4.73 *Specifying upper limits*).
- If the database is used to manage confidential data, it must be protected against access by unauthorised persons. In this case, the selected database software must possess appropriate mechanisms for access control (refer to S 2.129 *Controlling Access to Database Information*).

  It should be possible to put several users with identical access rights into groups. In this case, it is necessary to distinguish between administrator groups and user groups. Distinction between various administrative roles should also be supported (refer to S 2.131 *Separation of Administrative Tasks for Database Systems*).
- Different databases are equipped with mechanisms providing different scopes of access control; they might even be equipped with similar security mechanisms providing different degrees of resolution. Clarification is required in advance as to which type of access control is needed, and which database software fulfils the defined security requirements. Of key importance here are techniques of restricting access rights to database objects and data itself.

Examples:

- Users can be denied the rights to create or modify database objects (e.g. tables).
- Users can be granted read-only access to a table, but denied write-access to it.
- Individual users can be denied access to particular tables or table fields.
- Some users can be denied access to data records with certain attributes (e.g. an official in Bonn can be denied access to the data of an official in Cologne).

- Some manufacturers offer the possibility of defining groups as well as roles. This allows differentiated access control to database objects. Related requirements must be clarified in advance and taken into consideration when selecting the database software.
- The database software must also be examined with respect to the monitoring and control mechanisms it offers. Related requirements must be defined and compared with the features of the products (examples are provided in S 2.133 *Checking the Log Files of a Database System* and S 2.126 Creation of *a Database Security Concept*).
- It must be checked as to whether the database software supports distinction between the roles of administrator and auditor. It should be possible to configure the role of an auditor who is solely authorised to analyse and delete log files. This prevents potential manipulations by the database administrator.
- To protect the integrity of the database, the database software must be equipped with a complete transaction system in compliance with the ACID principle. Nowadays, this requirement is fulfilled by all major relational database management systems.
- Mechanisms for backing up the database must be available (refer to S 6.49 *Data Backup in a Database*).

  Clarification is required in advance as to which data backup features the database software needs to provide. For example, a partial database backup is not possible with all commercially available products. In individual cases, a check is therefore required as to whether the prepared database backup policy can be implemented with the available mechanisms.

These criteria must be used as a basis for testing and evaluating the available database systems. The software finally selected should fulfil the specified requirements to the greatest possible extent. Any remaining requirements should be covered using externally or internally developed add-ons. Before procurement, clarification is required as to which external add-ons are available for which database software, in order to avoid costly internal development.

Most commercial database management systems are available in different versions. Versions of the same database management system can differ in terms of their functionality, also as regards data security. Due to intense

competition between manufacturers, some of the software programs supplied by them are not yet fully developed, and are thus potentially restricted in their functionality and reliability.

In view of this, a test phase should be implemented in order to check whether the selected database software actually performs the required functions in the stipulated operating environment. This applies particularly to performance specifications and contingency planning mechanisms.

Experience gathered from comparable installations should also be taken into consideration before procurement of the database software.

Additional controls:

- Have the requirements for the database software been formulated and documented?
- Have relevant database systems been evaluated on the basis of these requirements?

S 2.125 Installation and configuration of a database

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

In principle, a distinction needs to be made between an initial installation of database software and installation in existing database systems.

When database software is installed initially, no users have yet been configured for accessing the database and no data is already in existence (except for any data which forms part of other database systems). Consequently, initial installation is relatively simple and hardly disrupts the normal IT operation.

In contrast, installation in existing systems should, if possible, be performed outside regular working hours in order to minimise disruption of normal IT operation. Users should, at least, be informed about all impending activities so that they can prepare themselves for potential disruptions and delays in operation.

The installation and configuration of a database comprise the following activities:

1. Installation of the database software

Before database software is installed, a check is required as to whether the IT system has been prepared accordingly, e.g. if sufficient memory is available and if the operating system has been configured appropriately.

The database software must be installed in compliance with the manufacturer's instructions. If possible, the default settings recommended by the manufacturer should be accepted. This applies particularly to technical parameters which control the size of various internal tables of the database management system, for example. In the case of security-related parameters, it might be necessary to deviate from the default settings.

The installation of the database software must be documented adequately. This includes, in particular, a detailed explanation of parameters which deviate from the default settings recommended by the manufacturer.

If optional features offered by the manufacturer need to be used, they should be configured appropriately during installation.

All activities in this phase are to be performed by the general database administrator.

2. Creating the database

The process of creating a database includes a specification of parameters which can no longer be changed after the database has been put into operation. The meanings of these parameters and suitable values to which they can be assigned are explained in detail in the manufacturer's installation documents and appropriate manuals, which should be referred to for this purpose.

In case any post installation work is required following the creation of the database, the related instructions must also be looked up in the installation and administration manuals.

Such procedures must also be documented.

All activities in this phase are to be performed by the general database administrator in consultation with the application-specific administrators (in order to specify the size of the database, for example).

3. Configuring the database

The third phase consists of implementing the user and group concepts and - if required - the role concept. For this purpose, the general database administrator configures the individual authorisation profiles, and creates all the groups and administrative user IDs (for the application-specific administrators). In this process, the instructions specified in S 2.132 *Provisions forCconfiguring Database Isers / User Groups* should be observed. Naturally, access rights pertaining to individual database objects can only be defined if these objects are already in existence (refer to step 4).

If the database software supports a distribution of data among several files or hard disks, it is necessary to specify additional parameters assigning the creation of these files as well as the corresponding memory sectors.

All the performed settings must be documented in detail (refer to S 2.25 *Documentation on the System Configuration*).

All activities in this phase are to be performed by the general database administrator.

4. Creating and configuring database objects

In this last phase, the database objects of the individual applications are created in accordance with the database security concept (refer to S 2.126 *Creation of a Database Security Concept*). If possible, this procedure should be automated and logged using scripts. After the database objects have been created, the related access rights for roles, groups and users are to be assigned. Specific users can now also be configured on the basis of the existing authorisation profiles.

All activities in this phase are to be performed by the application-specific administrators.

Additional controls:

- Have users been informed about an impending installation?
- Are all the parameters and related values required during installation known before the database is created?
- Are all post installation tasks required after the creation of the database known?
- Have the installation, creation and configuration of the database and its objects been documented?

S 2.126 Creation of a database security concept

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management

The long-term keeping of centralised data is of crucial importance for the information management at authorities and corporations. For this reason, it is essential to create a database concept. Such a concept defines the preparations necessary for putting the database into operation, and should always include a database security concept which focuses on the operation of the database.

Inadequate protection of data might result in a loss of confidentiality, availability or integrity. To prevent this, it is absolutely necessary to prepare a detailed database security concept.

To ensure the security of a database, a suitable database management system (DBMS) needs to be employed. To offer effective protection, the database management system needs to meet the following requirements: The DBMS must be

- based on a comprehensive security policy
- incorporated into the IT security concept of the organisation
- installed correctly and
- administered correctly.

Direct access to the database (e.g. via SQL interpreters such as SQL*Plus) must only be possible for administrative users, in order to prevent manipulation of the data and database objects (e.g. tables and indices). Modifications to database objects must always be controlled via special IDs. For this purpose, the database management system must incorporate a suitable access control and login concept (refer to S 2.129 *Controlling Access to Database Information* and S 2.128 *Controlling Access to a Database System*). User IDs which can only perform data modifications via an application must not be granted direct access to the database, while IDs for managing database objects must be granted direct, controlled access.

A database security concept must also settle the following important issues:

- The physical storage or mirroring of database files (e.g. the database management software, the database itself, or the log files) as well as their distribution must be specified in order to increase availability and reliability, for example. For security reasons, mirrored control files should be stored on different hard disks. This would prevent a loss of all the control files in case of a failure on one hard disk. If the database objects of an application are stored in separate data files, these files should be distributed so as to prevent a failure on a hard disk from affecting all applications.

  Example:

  A database manages the data of two applications, using one data file each for the tables and indices. These data files can be distributed as required among four hard disks.

An unfavourable distribution of data files is:

Hard disk 1: Storage of the data files for the indices of both applications

Hard disk 2: Storage of the data files for the tables of the first application

Hard disk 3: Storage of the data files for the tables of the second application

Hard disk 4: -

A failure on the first hard disk would affect both applications, rendering them unusable.

A more favourable distribution of data files is:

Hard disk 1: Storage of the data files for the indexes of the first application

Hard disk 2: Storage of the data files for the tables of the first application

Hard disk 3: Storage of the data files for the indexes of the second application

Hard disk 4: Storage of the data files for the tables of the second application

In this case, only one application would be affected by a failure on any of the hard disks.

- Once the database has been put into operation, the generated data volumes must be checked regularly in order to plan sufficient increases in storage capacity for future necessities.
- Suitable data backup mechanisms must be employed (refer to S 6.49 *Database backups*).
- The use of monitoring and control mechanisms must be specified, i.e. whether and to what extent database activities need to be logged. This also includes specifying whether only the times of data modifications should be recorded, or whether the modifications themselves should also be logged (refer to S 2.133 *Checking the log files of a database system*).

Suitable personnel must be available for planning and operating the database system. The time required to run a database system is not to be underestimated. Experience has shown that an analysis of the accumulated log data alone is very time consuming. The database administrator must possess a detailed knowledge of the installed database management software and must be trained appropriately to use it.

Additional controls:

- Have security objectives related to the use of a database system been formulated and documented?
- Has direct access to the databases via an interactive query language been precluded?

S 2.127 Inference prevention

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

To protect person related data and other confidential information stored in a database system, each user should only be allowed to access the data required for performing the tasks assigned to that particular user. All the other information in the database must be concealed from the user.

For this purpose, it must be possible to define the access rights on tables up to their individual fields. This can be done using Views and Grants (refer to S 2.129 *Controlling access to database information*). In this manner, users are only allowed to view and process the data intended specifically for them. Database queries issued by a user to access other information are rejected by the DBMS.

Different security requirements arise for statistical databases containing data on groups of persons, social strata etc. In a statistical database, entries related to individual persons are protected as private data, although the statistical information based on these entries is accessible by all users.

Here, measures are required to prevent information on a group of persons from being used to make inferences on individual members of the group. Steps must also be taken to prevent the anonymity of the information in the database from being circumvented through the use of database queries formulated in accordance with the data storage patterns (e.g. if the result set of a database query only contains one data record). This situation is termed "inference problem", and measures to preclude its occurrence constitute "inference prevention."

Even if the data in a statistical database is technically anonymous, methods of inference can be used to restore associations between persons and certain data records. The rejection of specific queries (e.g. queries with only one or very few result tupels) does not generally prove sufficient, as even a refusal issued by the database management system as a response to a query can contain relevant information.

The anonymity of data can also be impaired through the collection of different statistics. Such techniques of indirect attack use several statistics as a basis for drawing conclusions on the personal data of an individual. A protective measure in this case is to prohibit the release of "sensitive" statistics - this is termed "suppressed inference prevention". Another possibility is to distort such statistics through controlled rounding (identical rounding of identical statistics) or restrict queries to statistically relevant subsets with the prerequisite that identical queries must always refer to the same subsets. This technique is termed "inference prevention through distortion".

If additional demands concerning the confidentiality of data are to be met, the data must be encrypted (refer to S 4.72 *Database encryption*).

Additional controls:

- Have confidentiality requirements for the database system been formulated and documented?
- Are confidential data protected adequately against unauthorised access?

S 2.128 Controlling access to a database system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The database software must possess suitable mechanisms for user identification and authentication in order to ensure effective access control (refer to S 2.132 *Provisions for configuring database users / user groups*).

In general, standard users must be denied access to production databases via an interactive SQL interpreter. It should only be possible to access such databases indirectly via the corresponding applications. Database IDs for administrative purposes constitute the only exception here.

Remote access to databases must be severely restricted. Unless remote access is absolutely necessary, it must be prohibited. Otherwise, remote access should only be granted to users who actually require it. Other users must not be allowed to obtain remote access independently. On no account must remote access be possible without the entry of a valid user ID and password.

Additional controls:

- Are the accounts of individual users managed directly? If so, for which reasons was group management not chosen?
- Are there any user IDs with direct access to a database? If so, what are the reasons for this direct access?
- Have the possibilities of remote access to the database currently in use been investigated and, if applicable, disabled?

S 2.129 Controlling access to database information

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

A number of measures are required to effectively protect the confidentiality and integrity of data in a database. In addition to measures for controlling access to a database system, described in S 2.128 *Controlling access to a database system*, the following measures are essentially needed for controlling access to database information:

- Protection of database objects

  The database objects, i.e. tables, indices, database procedures etc. should be assigned logically to the applications using these objects. The resulting groups of database objects pertaining to each application are each assigned an account configured specially for this purpose. This allows the access rights on the database objects to be defined such that the objects can only be modified via these special IDs. If several applications access the same database objects, these should be put into a separate group.

  For example, if the data of two applications A and B are to be managed in the database, two database accounts - apnA and apnB - need to be created. All database objects which can be allocated uniquely to application A are configured and managed with database account apnA. The database objects of application B are handled similarly.

  One example of a central database object used by both applications is a table which lists all the printers installed. Database objects in this category should not be assigned one of the existing accounts (apnA or apnB); instead, such database objects should be grouped and managed centrally under a separate account (e.g. print).

  Such special IDs are not related to persons. Instead, staff members authorised specifically for this purpose (e.g. the administrator of the database or the corresponding application) receive the password of the required account if the database objects need to be modified.

- Data security

  Special *views* can be configured for users, allowing data to be rendered visible or kept concealed in accordance with specified criteria. A view is used to explicitly define the fields of one or more tables which can be viewed by a user. A restrictive allocation of access rights (or *grants*, as described below) for such views allows confidential data to be protected against unauthorised access.

  Access rights (*grants*) need to be allocated for tables, views and even individual fields of a table. These rights generally pertain to individual users, roles or user groups. However, such access rights should always be granted to user groups or roles, not to individual users, as a high number of users would require a great deal of administrative effort in this case. The following types of access rights are available: *read*, *update*, *delete* and *insert*. Access rights should be granted as sparingly as possible, otherwise it becomes increasingly difficult to retain a clear overview of the actual

access rights, so that security pitfalls are created. In particular, the possibility of granting rights to all users (GRANT ... TO PUBLIC) should not be used.

In general, only the owner of a database object is allowed to grant access rights to other users. However, some database systems also allow the owner of a database object to authorise other users to grant access rights. This facility should only be made use of in exceptional cases, as it no longer allows the access control of data and database objects.

- Restrictive access to data via applications

  Applications should support restrictive access to data, i.e. only those functions and data actually required by users for fulfilling their responsibilities should be made available to them (in accordance with the user IDs and the group memberships). One method of implementing this is through the use of *stored procedures*.

  Stored procedures are sequences of SQL statements which have been stored in the database in a pre-optimised manner. To invoke a stored procedure, only its name and, if applicable, certain parameters need to be entered in order to execute the underlying SQL statements. This is advantageous, because not all of the SQL statements need to be transferred to the database server, thus reducing the load on the network when complex operations are involved. Furthermore, the database system is able to store the SQL statements in an optimised manner, so that they can be executed more rapidly. The greatest restriction which can be imposed for the purpose of access control is to allocate access rights for stored procedures instead of tables or views. If access rights are just allocated for stored procedures, then users can only invoke operations which have been enabled by the database administrators.

Examples:

1. In MS Access, different access rights can be granted for the database itself (open/execute, exclusive, administer) as well as for the tables and queries (read data, update data, delete data, add data). These rights can be assigned to various users and user groups. In MS Access, the groups named "administrators" and "users" have been configured by default; the "users" group contains the "read data" and "update data" rights for tables and queries, and the "open/execute" rights for databases. To allow a detailed control of access rights, it is possible to define separate groups which can be assigned different rights. This can be done in the menu titled **Extras** under the items **Access rights** and **User and group accounts**.
2. In an Oracle database, a group named "Department_1" can be created with the following instruction:

   CREATE ROLE Department_1 IDENTIFIED BY <password>;

   In the following example, the group named "Department_1" is granted the right to establish a connection with a database and to create a session:

   GRANT CONNECT, CREATE SESSION TO Department_1;

   In the following example, the same group is granted the right to perform a SELECT on the table named "Test":

GRANT SELECT ON Test TO Department_1;

In the following example, this group is granted the right to make modifications in the column titled "Comments" of the table named "Test":

GRANT UPDATE (Comments) ON Test TO Department_1;

3. An example of a stored procedure under Oracle with PL/SQL statements is provided in the following:

```
PROCEDURE Example (PArticleno IN NUMBER, PPrice OUT NUMBER) IS
BEGIN
        BEGIN <<Block>>
                SELECT price INTO PPrice
                FROM TabB
                WHERE articleno=PArticleno
        END Block;
END;
```

The procedure named "Example" reads the price of an article in accordance with the article number from table TabB. Staff members who are to be allowed access to TabB exclusively by means of this method only are granted the right to use the stored procedure and **no** rights to access the table directly. This also prevents time-consuming search operations, for example.

Additional controls:

- Have database objects been protected against unauthorised access?
- Have views for individual users been defined and documented?
- Have access rights on data been allocated and documented?

S 2.130 Ensuring the integrity of a database

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator; staff responsible for the individual IT applications

The integrity of a database needs to be monitored and secured in order to ensure the correctness of the related data and the consistency of the database state. The following techniques must be employed to avoid the occurrence of incorrect data and inconsistent states in a database:

- Access control

  Access control implies the protection of the database against unauthorised access by assigning corresponding access rights as described in S 2.129 *Controlling access to database information*. This prevents manipulations of the data and database objects (such as tables).

  The database administrator is responsible for implementing access control.

  A detailed description of access control has been omitted here, as it is provided in S 2.129 *Controlling access to database information.*

- Synchronisation control

  Synchronisation control is intended to prevent inconsistencies which could arise through parallel access to the same data. Several techniques are available for this purpose, including the *locking* of database objects and the allocation of *timestamps*.

  The persons in charge of individual IT applications are responsible for implementing synchronisation control, insofar as a mechanism exceeding the scope of the database management system needs to be provided additionally.

  A detailed description has been left out here, as synchronisation control is performed by most database management systems. We strongly advise against the use of a database management system which does not offer this feature.

- Integrity control

  This involves the avoidance of semantic errors and semantically inconsistent database states through the observance and monitoring of database integrity constraints. These can pertain to individual relations or to groups of several mutual relations (referential integrity). Examples here are the specification of a primary key for a relation, definition of value ranges for individual attributes, and formulation of special constraints by means of an *assertion* clause.

  Integrity control can be carried out by the database management system automatically by means of a monitor created using *triggers* or *stored procedures*. In principle, this allows any type of transaction to be performed; however, the database management system rejects those transactions which would impair the consistency of the database.

Responsibility for implementation lies with the persons in charge of individual IT applications and the application-specific administrator, insofar as the integrity constraints need to be realised in the form of relations, primary keys or general database objects.

The following items must be prepared as part of planning an IT application:

- A data model which maps the database objects as well as their mutual relationships
- A technical concept which includes a description of the conditions under which data can be manipulated.

The following points must be observed during the **realisation** of an IT application:

- The actual implementation of the data model specified during the conceptual phase must be described. This includes the definition and creation of tables, indices, value ranges etc.
- *Triggers* and *stored procedures* are defined during the realisation of the technical concept. Triggers and stored procedures can be used within an application (in the programs) and in the database (for tables). Triggers used on the database level act independently of the overlying applications, and must thus be managed centrally.

  Example: *'Update' trigger* for a table:

  Whenever a data record in the table is modified, the statements defined for the trigger need to be executed. One of these statements can comprise the invocation of a *stored procedure*.

Where applications are concerned, integrity can be ensured through the suitable use of commit and rollback for transactions.

Additional controls:

- Are all the integrity control techniques described above implemented?
- Have all the integrity constraints been agreed with the administrators of the individual IT applications?

S 2.131 Separation of administrative tasks for database systems

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

Administrators need to be appointed in order to ensure the proper operation of database systems. In addition to general administrative tasks, these persons are responsible, in particular, for the management of users and related access rights. They are also responsible for fulfilling the security requirements of the database systems in use.

In addition to the safeguards mentioned in S 2.26 *Designation of an administrator and his deputy* and S 3.10 *Selection of a trustworthy administrator and his substitute*, particular attention must be paid to the following items where database systems are concerned.

In principle, a distinction must be made between two types of administrator roles:

- General technical administration of database software
- Administration for individual applications

These two types of administration tasks must be performed by different persons in order to separate application-specific and general administrative activities relating to the database.

Basic operation of the database management system, maintenance of data backups and archiving of data are examples of a general technical database administration.

In contrast, the application-specific administration involves fulfilling the individual requirements which applications generate for the database. This includes, for example, management of the related database objects, providing users with support in the case of problems and queries, and management of database IDs. The latter activity is only possible if the management of the database IDs of each application is supported by the database software using an appropriate authorisation concept, i.e. if it can be separated from the general access control.

The general administrator configures the application-specific administrator accounts together with the related access rights. This includes, in particular, the right to create databases. In contrast, rights for individual users should be granted separately for each application-specific database, by the responsible application-specific administrator in each case.

Additional controls:

- Have the administrative roles been separated?
- Which administrators have been appointed for the general administration of the database software and the administration of individual applications?
- How is the interaction between the administrators coordinated? Have their tasks and responsibilities been specified in writing?

S 2.132 Provisions for configuring database users / user groups

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Users and user groups need to be configured in order to ensure an appropriate allocation of access rights (refer to S 2.129 *Controlling access to database information*) as well as correct and controlled operation. For this purpose, every database user generally receives an internal database ID with which the database identifies the user. This ensures that only authorised persons can access the database.

As described in S 2.30 *Provisions governing the designation of users and user groups*, a form should be prepared for the purpose of gathering details pertaining to each user and user group:

- Surname, first name
- Proposed user ID (if not assigned by conventions)
- Organisational unit
- Reachability (e.g. telephone, room)
- If applicable: project
- If applicable: intended applications which should be used and need to access the database system
- If applicable: details on planned activities in the database system - including their duration - and the rights required for this purpose
- If applicable: restrictions imposed on times, access rights (for certain tables, views etc.) and restricted user environments
- If applicable: Approval by superiors

A limited number of authorisation profiles must be specified. New users are assigned to one or more profiles, thus receiving precisely those rights which are required for performing their individual activities. Database-specific possibilities of configuring users and user groups need to be considered here. It is advisable to specify naming conventions for user IDs and group IDs (e.g. user ID = abbreviation of organisational unit || serial number).

User, role, and group profiles can be used here. If possible, user-specific profiles should not be employed, as a high number of users would require a great deal of administrative effort. A balance needs to be struck between restrictive and liberal authorisation profiles when defining group profiles. If group profiles are made too restrictive, a large number of groups will need to be maintained, thus requiring a lot of administrative effort. If group profiles are made too liberal, redundancies could arise between the different groups, or granted rights could prove unnecessarily extensive, thus holding a potential for impairing the confidentiality of data.

As a rule, every user should be assigned a separate database ID; several users must not be allowed to operate under the same ID.

Normally, there is no association between a database ID and the user ID of the underlying operating system. However, some database software packages offer the possibility of copying the operating-system ID to the database system. This eliminates the need for users to answer the password prompt for database access if they have already logged in with their operating-system ID.

Oracle allows the use of OPS$ IDs, for example. This type of ID is composed of the prefix "OPS$" and the operating-system ID of the user. If a user logs into the database system with his operating-system ID, the database management system does not request the entry of a password. If a user logs in with a different ID though, a password is required.

However, this possibility poses a hazard that access to the database might no longer be deniable if a security violation occurs on the operating-system level (e.g. if the related password is cracked). Consequently, the security of the database relies heavily on the security of the underlying operating system. This does not generally imply the operating system of the database server - which is usually reliable - but that of the client, which is protected to a much lesser degree in some cases. Consequently, it is not advisable to make use of this possibility; instead, the use of an add-on product for central user management throughout the IT operation (e.g. *ISM Access Master* by Bull) should be considered in order to facilitate handling for users (keyword: *Single-Sign-On*). Here too though, harmonisation is required between the selected add-on product and the applicable security requirements.

Additional controls:

- Which organisational rules exist for the configuration of database users and user groups?
- Have naming conventions been specified for user IDs and group IDs?
- Have authorisation profiles been created?

S 2.133 Checking the log files of a database system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, auditor

The logging and auditing functions available in a database system must be utilised to an appropriate extent. Logging too many events will impair the performance of a database and cause log files to accumulate rapidly. A balance always needs to be struck between the requirement to collect as much information as possible in order to ensure database security, and the capability to store and analyse this information.

In this context, the following occurrences are of particular interest:

- Times and duration of user logins
- Number of database connections
- Failed or rejected attempts to establish connections
- Occurrence of deadlocks within the database system
- I/O statistics for every user
- Access to system tables (refer to S 4.69 *Regular checks of database security*)
- Generation of new database objects
- Data modifications (if required, together with the date, time and user)

However, the logging of security-related events only proves useful if the recorded data can also be analysed. For this reason, the log files should be checked by an auditor at regular intervals. If, for organisational or technical reasons, it is not possible to engage an independent auditor for the purpose of analysing the log files, it will be very difficult to control the activities of the database administrator.

The logged data must be deleted at regular intervals in order to prevent the log files from growing excessively. However, the log files must only be deleted after they have been viewed and analysed. This can be done manually or automatically, if appropriate tools are available.

Furthermore, access to the log files must be carefully restricted. On one hand, intruders must be prevented from concealing their activities through a later manipulation of log files; on the other hand, a selective analysis of the log files allows profiles of users to be generated. Consequently, no modifications should be permitted and read-access should only be granted to the auditors, for example.

To facilitate analysis of the log files, the database administrator can make use of additional tools which automatically perform monitoring. Such products can, for example, analyse the log files of a database system in accordance with specified patterns and output an alarm under certain conditions.

Additional measures which need to be observed in this context are stated in S 2.64 *Checking the log files*.

Additional controls:

- Who analyses the log files? Is the two-person control rule employed?
- Can the activities of the administrator be monitored to a sufficient extent?
- Is the IT security management notified of irregularities?

S 2.134 Guidelines for database queries

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Application developer

The relational database language SQL (Standard Query Language) is a standardised international language for relational database systems; it has found widespread use and is implemented in most database management systems. SQL can be used to modify data (UPDATE, INSERT, DELETE), manipulate database objects (CREATE, ALTER, DROP) and request information (SELECT). To ensure secure operation of a database, the following basic guidelines should be observed when making database queries:

- SQL queries should be formulated as precisely as possible. This applies particularly to SQL queries generated from applications. For example, the SQL statement

  SELECT * FROM <Table> WHERE <Condition>
  inevitably leads to errors or even causes the related application to crash if the table scheme has been modified (addition or deletion of fields, or changes in the field sequence).

- Fields should always be specified explicitly. This ensures that the data is made available in the awaited sequence, and that only the information which is actually required is selected, for instance.

  Example:

  A table consists of the following fields (with the related data types):

  Article number NUMBER(10)

  Net price NUMBER(10,2)

  Article designation VARCHAR(30)

  Intended use VARCHAR(200)

  A new field titled "Order number" and having type NUMBER(8) is added. To optimise memory utilisation, the field is located at the second position of the table, not at the end. The new table then appears as follows:

  Article number NUMBER(10)

  Order number NUMBER(8)

  Net price NUMBER(10,2)

  Article designation VARCHAR(30)

  Intended use VARCHAR(200)

  In the worst case, a SELECT-* statement issued from an application would now lead to a crash, as the data is selected automatically in the specified field sequence. The example shown above not only poses the problem of the table having been extended by one field (whose data are selected additionally), but also of the field sequence having been modified, so that the data is no longer selected in the original order. This leads inevitably to type conflicts and, possibly, to program failure.

- The sequence of the specified selection conditions is of great importance for restrictive database queries (WHERE clause). The WHERE clause should be formulated so that the first condition selects the smallest possible result set, whilst the last condition selects the largest result set. This optimises the performance of the database system through an efficient arrangement of the selection conditions, which notably accelerates search operations. The same applies to database queries formulated for several tables (so-called joins).

  It must be noted here that database management systems often optimise database queries automatically. In fact, many database management systems offer several optimisation strategies which can be selected via various parameters. If a database management system does make use of such *Optimisers* however, it might be possible that carefully formulated database queries are internally not processed as expected.

  In this respect, some database management systems allow the processing of database queries to be monitored (e.g. with EXPLAIN in Oracle or SETOEP in Ingres). It is also possible to use HINTS to explicitly define the processing of database queries, thus eliminating the need for optimisers. However, this option should only be used when absolutely necessary.

  The optimisers supported by a database management system as well as their advantages and disadvantages are usually documented in the manuals accompanying the system. If several optimisers are available, the administrator should be requested to specify a suitable one for use.

- In the case of Joins, it must also be noted that fields are allocated uniquely to tables.

  Example:

TabA:	ID	NUMBER(4)
	Manufacturer#	NUMBER(6)
TabB:	ID	NUMBER(4)
	Article#	NUMBER(10)
	Price	NUMBER(10,2)
	Designation	VARCHAR(30)

```
SELECT TabA.ID, TabB.Designation, TabB.Price
FROM   TabA, TabB
WHERE TabA.ID=TabB.ID
```

  The "ID" field is present in both tables and **must** therefore be specified explicitly together with the corresponding table name in the database query. Otherwise the uniqueness of the selection is no longer ensured, and the database query is aborted with the issue of a corresponding error message.

  All other fields can be allocated uniquely in this case. SQL does not require an explicit specification of the related table name for each field.

Nevertheless, the individual fields should be allocated to the tables, as shown above in the "Price" and "Designation" fields of table TabB. Only in this manner can unforeseeable problems be avoided.

In the above example, the addition of a "Designation" field in TabA would not cause any problems. However, it would if the SQL statement did not contain an explicit allocation of the fields to the tables. In this case, it would no longer be possible to clearly determine whether the "Designation" field should be selected from TabA or TabB, as both tables would contain a field of this name following the modification to TabA. The SQL statement would then be aborted with the issue of a corresponding error message.

- If views exist, they must be used for the formulation of database queries.
- All database transactions must be confirmed explicitly with a COMMIT. If the database management system in use supports an automatic COMMIT, this feature should not be activated, as it might inadvertently lead to inconsistencies in the database.

  Example: Several individual modifications are grouped together logically, and confirmed automatically by a COMMIT. If the transaction is now interrupted in an uncontrolled manner, thus leading to a rollback, the operations already completed are confirmed and remain in the database, while the remainder remains unexecuted.
- To avoid locking conflicts or even deadlocks, a locking strategy should be specified for every application-specific database (e.g. hierarchical locking or explicit locking of all tables at the beginning of a transaction).
- Application developers should check the error status after every SQL statement, to allow the application to respond as quickly as possible to the occurrence of errors.
- If the database management system supports certain system-specific commands which permit the logging function to be deactivated or the locking procedure to be modified, for example, users should be denied the right to use such commands. Precise clarification is required in advance as to the system-specific settings / commands which may be changed / invoked by users and application developers.
- During development of the applications, all database access operations should be grouped in one module or a particular section of the program code, otherwise the entire program code of the application system would need to be scrutinised in order to test the above-mentioned principles. Grouping the operations together facilitates the maintenance and updating of the application system, e.g. in the event of alterations to the data model.

Additional controls:

- Have guidelines for database queries been prepared?
- Are the guidelines for database queries known to the application developers?
- How is adherence to these guidelines checked?

S 2.135 Save transfer of data to a database

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

In many database systems, it is necessary for applications to take over data from other systems. A basic distinction can be made between the following categories here:

- Transfer of initial or old data

  This involves the transfer of data from old systems, required when a new database system is procured in order to increase productivity, for example. In this case, the following measures must be specially observed:

  - The data must be available in a format which is accepted by the destination database
  - The data must be complete, i.e. data must be available for all the fields of the destination database which need to be filled
  - The consistency and integrity of the database must be guaranteed

  Before data is actually transferred, it is necessary to form a concept describing how the data is to be prepared for the process of transfer, and how this process is to take place. In addition, a full backup of the old data is absolutely necessary. If the data is to be transferred in several steps, an independent data backup should be performed before each step.

- Regular transfer of data

  If the destination database already contains data which must remain unaltered during the subsequent transmission of additional data, or if new data is transferred to the database at regular intervals, the following measures must be observed:

  - A full backup of the database must be created before the transfer of new data
  - If possible, data transfer should take place outside regular operating hours
  - Users whose activities will be influenced by the impending transfer of data must be informed duly, particularly if availability and response times are likely to be affected
  - Prior to the initial transfer of new data, it is necessary to form a concept describing how the data is to be prepared for the process of transfer, and how this process is to take place. In particular, this concept must include a description of how to avoid conflicts between the data already existing in the destination database and the data to be transferred, i.e. the extent to which the integrity and consistency of the destination database remain protected. In addition, measures must be taken to prevent multiple transfer of the same data.

Before data is transferred, it is necessary to specify responses to any errors which might occur. For example, this includes ascertaining whether, on the occurrence of a faulty data record, transfer should be continued with the next block or whether the entire process of transfer should be aborted. Furthermore, it is necessary to determine the manner in which data transfer is to be resumed after an interruption.

Additional controls:

- Has a concept of data transfer been prepared?
- Are full backups of the database created before data transfer?
- Are users informed promptly and adequately about impending data transfer?

S 2.136 Observance of rules concerning workstations and working environments

Initiation responsibility: Head of Site/Bldg Technical Service; personnel committee/works council

Implementation responsibility: Superiors; personnel committee/works council; staff members

The regulations and guidelines concerning the configuration of workstations (e.g. screen workstations) and the working environment should apply identically to homes and the institution. In agreement with the telecommuters, the observance of these regulations and guidelines should be assessed by the institution's officers responsible for work, safety and health, the IT security officer, data privacy officer, works council, personnel committee and the immediate superiors of the telecommuters.

S 2.137 Procurement of a suitable data backup system

Initiation responsibility: Head of IT section

Implementation responsibility: Administrators

Many of the errors occurring during the creation or restoration of a data backups are attributable to incorrect handling. For this reason, a data backup system should be selected not only on the basis of the performance it offers, but also for its handling properties and, in particular, its tolerance to user errors.

The selected backup software must fulfil the following requirements:

- The data backup software should be able to identify an incorrect medium and a damaged medium in the backup drive.
- The backup software should be fully compatible with the existing hardware.
- It should be possible to allow backup to be executed automatically at pre-determined times, i.e. at pre-set intervals, without the necessity of manual intervention (except possibly for the provision of backup data media).
- It should be possible to inform one or several selected users, via E-Mail or a similar mechanism, of the result of the backup and of any faults. Data backup procedures, including the backup results and any error messages, must be recorded in a log file.
- The backup software should support securing of the backup medium via a password or, better still, via encryption. Furthermore, it should be able to save the backed up data in compressed form.
- By entering appropriate Include and Exclude lists when selecting files and directories, it should be possible to specify exactly which data ought (and ought not) to be backed up. It should be possible to create backup profiles where the lists can be summarised, saved and re-used for later backups.
- It should be possible to select data to be backed up independent of the date it was created and the last modification.
- The backup software should support the creation of logical and physical full copies as well as incremental copies (backup of changes).
- It should also be possible to store data backups on hard disks and network drives.
- The backup software should be able to carry out an automatic comparison after backup between the backed up data and the original. After restoring data, it should be able to carry out a respective comparison between the restored data and the content of the backup data medium.
- When restoring files it should be possible to select whether the files are to be restored into their original location or onto another disk or directory. In the same way it should be possible to control how the software reacts if a file with the same name already exists at the target location. It should be possible to select whether the existing file is to be always, never or only

overwritten if it is older than the restored file, or that in this situation an explicit request appears.

If, with the used program, the data backup can be protected by a password, use should be made of this option. In this case, the password will have to be deposited safely (cf. S 2.22 *Depositing of passwords*).

Most operating systems are delivered together with data backup programs. However, not all of them meet the demands placed on professional, easy-to-execute data backup products. If no such products are available though, then the system programs should be used.

S 2.138 Structured data storage

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

Poorly structured data storage can lead to a wide variety of problems. For this reason, all IT users should be instructed on how to store data in clear, well-structured manner. Appropriate structures should be specified by the Administrators on all servers. This is also a prerequisite for achieving a differentiated allocation of access rights.

Keep programs and application files separate

Program and work files should always be stored in separate sectors. This makes it easier to obtain an overview, simplifies data backups and ensures correct access protection. In the case of most application programs, very few or no configuration files are modified following installation. If possible, all files which are modified regularly should be stored in separate directories, so that only those directories need to be included in the regular data backups.

Where programs and data are kept properly separated, it is sufficient to only include the data in the regular data backups. It is important to have working files carefully backed up so that, if necessary, the backups can also be worked on on other systems.

In the case of networked systems, it is also necessary to determine which programs and files should be stored on local hard disks or on a network server. Both options have advantages as well as disadvantages, and must be evaluated in accordance with the existing organisational structure as well as the hardware and software in use. For example, files with high availability requirements and the related application programs should be stored on workstation computers rather than on the network server. In this case, appropriate contingency measures also need to be implemented for these workstation computers.

Task-or project-specific directories

Task-specific or project-specific directories should be created in order to facilitate the allocation of files. As few files as possible should be stored in personal directories.

To prevent the existence of different versions of basic files required for ongoing activities, such as letter templates, forms, project plans etc., such files should be managed centrally. For example, these files should be stored on a server so that all users have read access to them, but only one person is authorised to modify each individual file.

The following example shows how data can be structured on a server by specifying directory paths:

```
\
\bin
        \bin\program1
        \bin\program2
        \bin\program3
\user
        \user\user1
        \user\user2
\projects
        \projects\p1
                \projects\p1\texte
                \projects\p1\bilder
        \projects\p2
                \projects\p2\projectplan
                \projects\p2\sub-project1
                \projects\p2\sub-project2
                \projects\p2\sub-project3
                \projects\p2\result
        \standardforms
```

Tidy up directories regularly

A regular check is required as to whether

- data can be removed from the production system through archiving or deletion,
- access rights can be withdrawn after staff members have left the project team,
- the latest versions of forms, templates etc. are stored on all IT systems.

These checks should be performed regularly by users on their IT systems and the directories managed by them, and by the Server Administrators. They should be performed at least once every three months, before staff members forget the contents and origin of the files.

Additional controls:

- Are the directories used for holding data exclusively task-related or project-related?
- When was a check last made as to whether old files can be archived or deleted?

S 2.139 Survey of the existing network environment

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

A survey of the existing network environment is required for a systematic security analysis of the network. Such a survey is also needed if an existing network needs to be extended. The items described below must be taken into consideration during the planning of a network.

A survey of the existing environment must be accompanied by a detailed documentation of the following aspects, which partly depend on each other:

- Network topography
- Network topology
- Network protocols in use
- LAN / WAN connections
- Network performance and traffic flow

The essential details to be recorded during each individual step are specified in the following:

Survey of the existing network topography

A survey of the existing network topography involves a recording of the network's physical structure. Here, it is advisable to use the spatial structure of the network as orientation. A plan containing the following features should be prepared and maintained:

- Current cable routing
- Locations of all network subscribers, in particular, the active network components in use
- Cable types in use
- Specified requirements concerning the protection of cables (S 1.22 *Physical protection of lines and distributors*)

. To support the maintenance of this plan, it is advisable to use an appropriate tool (e.g. CAD programs, special tools for network plans, cable management tools in conjunction with system management tools, etc.). Regular updating of these plans following rebuilding or extension must be ensured, in addition to clear and precise documentation (also refer to S 1.11 *Plans detailing the location of supply lines* and S 5.4 *Documentation on and marking of cables*).

Survey of the existing network topology

A survey of the existing network topology involves a consideration of the logical structure of the network. For this purpose, it is necessary to make a record of the segmentation of the individual OSI layers and, if applicable, the VLAN structure.

The representation of the network topology should make it possible to determine the active network components via which a link can be established

between any two terminal devices. Furthermore, it is necessary to document the configurations of the active network components used for forming the segments. This can involve the configuration files in the case of logical segmentation, and the actual configuration of the network components in the case of physical segmentation.

Survey of the network protocols in use

The network protocols used in the individual segments of a network as well as the configurations required for this purpose (e.g. the MAC addresses, IP addresses and subnet masks for the IP protocol) need to be determined and documented. The documentation should provide details on which services are authorised (e.g. HTTP, SMTP, Telnet), and which services are filtered in accordance with which criteria.

Survey of the LAN /WAN connections

The LAN / WAN connections are to be described, if they have not already been documented. For every LAN / WAN connections between two networks, details must be provided on:

- Which transmission routes are used for this purpose (e.g. wireless communications route for a LAN/LAN link)
- Which communication partners and services are permitted in which directions on such routes
- Who is responsible for their technical implementation.

This should also include a documentation of the WAN protocols in use (e.g. ISDN, X.25). If firewalls are employed (refer to Chapter 7.3 *Firewalls*), their configuration must also be documented (e.g. filter rules).

Survey of the actual network performance and traffic flow

The network performance must be measured and the traffic flow between the segments or subnetworks must be analysed. Corresponding measurements need to be performed for each network protocol in use.

Any time the network environment is modified, the above mentioned surveys are to be repeated. The documentation prepared as part of these surveys must be stored so that it is protected against access by unauthorised parties, but readily available for the security management and administrators.

Additional controls:

- Are performance measurements and traffic-flow analyses conducted regularly?
- Is the documentation updated on a regular basis?
- Is the documentation also clear and understandable for third parties?

S 2.140 Analysis of the existing network environment

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

This analysis is based on the results of the examinations performed in accordance with S 2.139 *Survey of the existing network environment* and requires a specialised knowledge of network topology, network topography and network-specific vulnerabilities. A further prerequisite here is experience in the evaluation of the confidentiality, integrity and availability of the individual IT applications employed. As this extremely complex subject not only requires an in-depth knowledge of all the aspects mentioned, but is also very time-consuming, it might be advisable to hire external consultants for an analysis of the existing network situation. Within the scope of the federal German administration, the BSI can provide assistance here.

An analysis of the existing network situation essentially involves a structural analysis, a determination of protection requirements, and an examination of vulnerabilities.

A **structural analysis** involves an evaluation of the documentation prepared as part of S 2.139 *Survey of the existing network environment.* A structural analysis must be performed by an analysis team capable of interpreting and deducing all possible communications relations. As an outcome, the analysis team must possess a full understanding of the operation of the network and be informed about the principal possibilities of communication. The construction vulnerabilities in a network can often be identified already during structural analysis.

A successful structural analysis is a prerequisite for a subsequent, detailed determination of the protection requirements and an analysis of vulnerabilities.

Detailed determination of the protection requirements

A structural analysis is followed by a determination of the protection requirements exceeding the scope of the measures stipulated in Chapter 2. Requirements concerning the confidentiality, availability and integrity of individual subnetworks and network segments are also considered here. In this context, it is necessary to determine the requirements generated by the various IT procedures in use, and how they influence the existing segmentation of the network. As an outcome, it must be possible to identify the network segments in which special protection requirements need to be fulfilled.

Analysis of vulnerabilities in the network

An analysis of the vulnerabilities in the network is performed on the basis of the results obtained so far. Given corresponding requirements of availability, this includes, in particular, an identification of non-redundant network components (single-points-of-failure). Furthermore, it is necessary to specify the areas in which requirements concerning availability, confidentiality and integrity cannot be fulfilled or require special attention. It is also necessary to determine whether the selected segmentation is suitable in terms of bandwidth and performance (based on the results of traffic flow analysis described in S 2.139 *Survey of the existing network situation*).

Example of a vulnerability: An analysis of performance and traffic flow reveals an overloaded active network component. During a determination of the protection requirements by the affected communications route, high requirements concerning availability and performance were established. This vulnerability requires an adaptation of the network segmentation or a replacement of the network components with a more efficient model (refer to S 5.61 *Suitable physical segmentation*, S 5.62 *Suitable logical segmentation*, S 5.1 Removal, or short-circuiting ond gournding, of unneeded lines and S 5.13 *Appropriate use of equipment for network coupling*).

Additional controls:

- Has the existing network environment been documented in sufficient detail?
- Is sufficient know-how available for a security analysis of the network environment?
- Have requirements concerning the confidentiality, availability and integrity of the network been defined and documented?

S 2.141 Development of a network concept

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

To fulfil requirements concerning availability (also in terms of bandwidth and performance), confidentiality and integrity, the configuration, modification or extension of a network needs to be planned carefully. A network concept needs to be prepared for this purpose.

The development of a network concept can be classified into an analytical component and a conceptual component:

Analysis

First of all, it is necessary to determine whether an existing network needs to be extended or modified, or whether a completely new network needs to be established.

In the former case, the safeguards titled S 2.139 *Survey of the existing network environment* and S 2.140 *Analysis of the existing network environment* need to be realised. These safeguards are not required in the latter case; instead, requirements concerning network communications and the protection requirements of the future network need to be determined.

In order to determine requirements for communications, it is necessary to ascertain the flow of data and traffic anticipated between logical and organisational units, as the expected loads will influence the segmentation of the planned network. The necessary logical and physical communications relationships (with respect to services, users and groups), as well as the LAN / WAN connections must also be ascertained.

The protection requirement of the network is derived from that required by planned and existing IT processes. The result is used as a basis for forming appropriate physical and logical subnetworks (e.g. as regards the confidentiality of data). For example, the security requirements of an IT application influence the segmentation of the planned network.

Subsequently, an attempt must be made to harmonise the derived communications relationships with the protection requirements. In certain cases, it might be necessary to restrict communications relationships in order to fulfil the specified protection requirements.

The available resources need to be ascertained after that. These include personnel resources required to prepare and implement a concept and operate the network, as well as financial resources needed for this purpose.

The results are to be documented appropriately.

Conception

From the points of view mentioned above, the network structure and applicable constraints should be conceived and developed in the stages mentioned in the following, on the basis of a plan which also takes into account future requirements (e.g. concerning bandwidth) and in accordance with local conditions.

The network concept is prepared in a manner similar to that described in S 2.139 *Survey of the existing network environment* and thus essentially involves the following steps; however, these steps need not be executed strictly in the order given below. In some case, the results of executing the individual steps influence one another mutually, so that these results need to be checked and consolidated on a regular basis.

1. Conception of network topography and topology as well as physical and logical segmentation
2. Conception of the network protocols to be used
3. Conception of LAN / WAN connections

The individual steps essentially involve the following activities:

Step 1 - Conception of network topography and topology

Based on the analysis profile (see above) and actual structural conditions, a suitable network topography and topology need to be selected (also refer to S 5.60 *Selection of a suitable backbone technology*, S 5.2 *Selection of an appropriate network topography* and S 5.3 *Selection of cable types suited in terms of communications technology*). However, future requirements such as scalability also need to be considered here. The prepared concept must be documented (cabling plans, etc.)

Based on the ascertained requirements and the anticipated / calculated data flow, an appropriate physical and logical segmentation must be performed during conception of the network topography and topology (refer to S 5.61 *Suitable physical segmentation*, S 5.62 *Suitable logical segmentation* and S 5.13 *Appropriate use of equipment for network coupling*).

Step 2 - Conception of the network protocols

This step involves the selection and appropriate conception of the required network protocols. This includes, for example, the preparation of an addressing scheme for the IP protocol and the formation of subnetworks. During the selection of the network protocols, it must be observed that these protocols are supported by the network topology as well as planned and existing active network components.

Step 3 - Conception of LAN / WAN connections

Based on the anticipated flow of data across the planned LAN / WAN connections as well as requirements concerning security and availability, the LAN / WAN connections can be conceived in this step. This includes the selection of suitable coupling elements (refer to S 5.13 *Appropriate use of elements for network coupling*) as well as their secure configuration (refer to Chapter 7.3 *Firewalls* and S 4.82 *Secure configuration of active network components*).

Additional steps

Based on the developed network concept, measures for preparing a network management concept can now be implemented (refer to S 2.143 *Development of a network management concept*, S 2.144 *Selection of a suitable network management protocol* and S 2.145 *Requirements for a network management tool*) and a realisation plan can be outlined in accordance with S 2.142 *Development of a network realisation plan*.

S 2.142 Development of a network realisation plan

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

When developing a network realisation plan, it is necessary to determine whether a completely new network configuration, or a modification / extension to an existing configuration is required.

During the configuration of a completely new network, the required steps must be inferred from the network concept which has already been prepared (refer to S 2.141 *Development of a network concept*). Once planning has been completed, the network is set up by laying the required communications cables, configuring rooms for the technical infrastructure, installing the technical infrastructure itself, integrating the necessary coupling elements (bridges, switches, routers etc.), configuring the network management stations, fitting the terminal devices with corresponding network adapters and configuring these terminal devices.

If an existing network is to be modified or extended, the network concept prepared in accordance with S 2.141 *Development of a network concept* should be compared with the actual situation as described in S 2.139 *Survey of the existing network environment*. Based on any resulting differences, a realisation plan for network migration can be outlined, taking into account the above-mentioned measures. Here, it must be noted that the greater the deviation between the network concept and the actual situation, the greater the realisation effort.

Example of migrating from a shared Ethernet to a switched Fast Ethernet

Migration from one network topology to another normally takes place in stages. A migration from a shared Ethernet to a Fast Ethernet with switching technology is outlined as an example in the following. Under real conditions however, the constraints need to be checked thoroughly and a special migration concept needs to be prepared for each individual case.

- Migration step 1

  In the first migration step, the existing backbone can be replaced by a Fast Ethernet backbone, or a new one can be installed if necessary. The remaining shared Ethernet segments are connected via the backbone's network components which must accordingly also support Standard Ethernet.

- Migration step 2

  Establishment of structured cabling, i.e. a conversion is performed from a Standard Ethernet with breakout cabling to a cabling concept in which every workstation is connected in star configuration to a distributor room without abandoning the topological bus structure.

- Migration step 3

  The servers are connected centrally to a switch with Fast Ethernet adapters (installation of a so-called server farm).

- Migration step 4

  Migration of the remaining Ethernet segments to a fully switched system. For this purpose, for example, Ethernet switches can be linked to the Fast Ethernet switches of the backbone.

- Migration step 5

  Migration of the remaining Ethernet segments to a fully switched system. For this purpose, for example, Ethernet switches can be linked to the fast-Ethernet switches of the backbone.

S 2.143 Development of a network management concept

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The diversity of IT systems grouped in a local network, such as server systems, terminal devices, printers, active network components etc. should be capable of being managed and monitored centrally from a suitable point. Preference should be given to central instead of decentral management of network components, as the former approach requires a lower administrative effort and allows central definition and control of security requirements. Central network management is primarily used to ensure the availability and integrity of the network, as well as the integrity and confidentiality of the transmitted data. This is a very complex task which needs to be supported through the use of a network management tool.

Before such a network management system is procured and put into operation, it is first necessary to prepare a concept which formulates all security requirements for the network management system and proposes appropriate measures to be implemented on the occurrence of an error or alarm. During the preparation of this concept, the following aspects of network management should be considered in particular and represented in a global context.

- Performance measurements for network analysis (refer to S 2.140 *Analysis of the existing network environment*)
- Responses to error messages from the monitored network components
- Remote maintenance / remote control, particularly of active network components
- Generation of trouble tickets and escalation on the occurrence of network problems (links with the system management and user helpdesk or external message communicators such as pagers and facsimile machines can be established via this feature).
- Logging and auditing (online and/or offline)
- Integration of any existing proprietary systems, or systems with different management protocols (e.g. in the area of telecommunications)
- Configuration management of all IT systems in use (also refer to. S 4.82 *Secure configuration of active network components*)
- Distributed access to network management functions. Remote access to network management functions might be necessary for administration or auditing; a particularly careful definition and allocation of access rights is necessary here.

The specific requirements to be fulfilled by a network management tool are described in S 2.145 *Requirements for a network management tool*. The management tool must allow the implementation of the network management concept.

Additional controls:

- Have all the security requirements for network management been formulated and documented?

S 2.144 Selection of a suitable network management protocol

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The following standard protocols for network management are currently applicable:

- SNMP (Simple Network Management Protocol); SNMP is described in RFC 1157. Request for Comment (RFC) is a standard which has established itself in the Internet.
- CMIP (Common Management Information Protocol); CMIP is described in the ITU-T standard X.711 and in ISO/IEC 9596-1.

The main advantages and disadvantages of these two protocols are described in the following in order to facilitate selection of the suitable network management protocol when the need arises.

SNMP

Two components are defined for SNMP: a manager and an agent. In a local network, one or more managers and one agent per IT system to be monitored and configured via SNMP are installed. The agents gather information about these systems and store this data in a MIB (management information base). They exchange messages with the manager via a connectionless protocol, so that SNMP does not rely on any particular transport protocol. Nowadays, it is usually implemented on UDP/IP. However, other implementations are possible and available (e.g. via OSI, AppleTalk, SPX/IPX). SNMP is available in different versions. In addition to the original version SNMPv1, different variants of version 2 (SNMPv2) are also in use to a limited extent (RFC 1901-1908).

SNMP is an extremely simple protocol which recognises three types of messages. Managers and agents use it to exchange what is known as management information, which basically consists of the values of status variables which are stored in management agents and describe the condition of the related managed object. The management database (MIB) describes which status variables (name and type) exist in each agent. The information is organised hierarchically and each value is assigned a unique identification number which defines a unique sequence of the variables. In detail, the types of messages are:

1. GetRequest: sent from the manager to agents to query the values of one or more status variables from them.
2. GetNextRequest: sent from the manager to agents to query the value or the next values in accordance with the order of the variables in the MIB.
3. SetRequest: sent from the manager to agents in order to set the value of a variable.
4. GetResponse: sent from agents to the manager in order to send the queried values or confirm that the value of a variable has been set.

5. Trap: used by agents in order to inform the manager of exceptional events. Unlike a GetResponse message, a Trap message is not preceded by a query from the manager.

The essential advantages and disadvantages are:

+ SNMP has a simple design and is thus easy to implement. This reduces its susceptibility to faults and improves the stability of the protocol.
+ SNMP is used on a widespread basis and is regarded as a de-facto standard. As a result, it is supported by nearly all products in network and system technology.
+ The protocol can be adapted very easily to future requirements. For this reason as well as the above-mentioned widespread use of SNMP, this protocol can be considered extremely future-oriented, thus providing a high degree of investment protection.
+ SNMP is a simple, connectionless protocol on the transport level. Consequently, the transmission of SNMP packets in a network is more efficient compared with the connection-oriented CMIP.
- The use of SNMP harbours security risks which could allow intruders to obtain detailed information on the system and network environment. Except for the community names (which, in the case of SNMP, allow the formation of groups and provide basic password protection), no real password protection is available for access to network components.
- Due to its simple nature and the features it possesses, the SNMP protocol exhibits shortcomings when operated in very large or rapidly expanding networks.
- The performance of version 1 proves inadequate in the case of complex MIB queries, as the complete MIB tree always needs to be specified.

One of the main disadvantages of version 1 of the SNMP is that it does not support authentication for access to monitored components. Version 2 of the SNMP compensates for some of these disadvantages and provides better performance in the handling of MIB queries.

However, different variants of SNMPv2 exist in terms of the security features supported. Only the variants SNMPv2* and SNMPv2u offer the possibility of symmetric, user-based authentication, while SNMPv2c continues to rely on communities. In SNMP, communities are firstly used to classify individual network components into groups, and secondly used as substitute passwords during access to these groups. SNMPv2* also offers the possibility of data encryption in accordance with the Data Encryption Standard in the Cipher Block Chaining Mode (DES-CBC). Due to the different variants of SNMPv2 presently in use, manufacturers of network components and network management systems are quite uncertain about their installation strategies, as a result of which implementations based on SNMPv2 are not yet encountered on a widespread scale, and are only inter-operable to a restricted extent.

The different variants of SNMPv2 are to be consolidated in the next SNMP version (SNMPv3). The release of SNMPv3 is currently being prepared but has not yet been completed.

For the above-mentioned reasons, only the use of SNMPv1 is recommended from the perspective of IT baseline protection. If the network management protocol or the network security features need to fulfil additional security requirements, use should be made of SNMPv2u or SNMPv2* with user-based authentication, or of CMIP. In principle, aspects related to confidentiality and authenticity are evidently supported to a greater extent by more recent versions of SNMP, although this advantage is accompanied by losses in bandwidth.

CMIP

In contrast to SNMP, CMIP is based on an implemented OSI protocol stack (OSI layers 1 to 3 are implemented as a protocol stack) and is thus also connection-oriented. This restricts the use of CMIP to components which fulfil hardware-related and software-related requirements for the implementation of a complete OSI stack. Due to the high demands placed by this implementation, a "CMIP Over TCP/IP" (CMOT) was also defined (RFC 1189). This allows CMIP to be operated in pure TCP/IP networks too.

One of the objectives of the CMIP concept was to develop an object-oriented management system. Accordingly, CMIP has a consistently object-oriented design. A CMIP machine (CMIPM) performs the tasks which are assigned to the manager under SNMP. This CMIPM, which consists of a software program like the SNMP manager, receives service requests from the agents of the objects to be managed to perform various operations; in response, the CMIPM sends CMIP messages to these agents. In accordance with object-oriented principles, the objects are managed via several trees which exhibit different mutual relations and are characterised by different types of access.

Due to its object-oriented design, CMIP is a very powerful and complex protocol. However, this protocol contains relatively few operations which allow full management on the basis of the above-mentioned object-oriented structure.

The essential advantages and disadvantages are:

+ Due to its object-oriented design, CMIP offers many more possibilities than SNMP, including the execution of actions and the management of instances of management objects.
+ CMIP offers more security than SNMP, particularly through the availability of mechanisms for access control, user authentication and auditing.
+ The CMIP protocol is defined by OSI, thus constituting an official, international standard, whereas SNMP is only regarded as a de-facto standard based on a RFC.
+ CMIP does not have the afore-mentioned shortcomings of SNMP.
- CMIP is a very complex protocol, whose diverse features are rarely required or capable of being used in its entirety. Due to the large number of possible settings, an elaborate configuration of this protocol is very difficult, and requires a great deal of know-how on the part of the administrator.

- CMIP requires roughly ten times as much system resources as SNMP. For this reason, it needs to be operated on powerful hardware which is only offered by a small number of active network components. The OSI protocol stack, which consumes additional resources, also needs to be implemented in general. CMOT constitutes an exception here.
- Due to the complexity of this protocol and the corresponding implementations, CMIP is potentially more susceptible to errors than SNMP implementations.
- Very few implementations of CMIP are presently available; except for in the area of telecommunications, this protocol is encountered very infrequently in practice.

In each individual case, a detailed examination is required as to which network management protocol is suitable for the applications involved. In this context, the security requirements for the network management system need to be formulated and co-ordinated. If the TCP/IP protocol stack is already being used in the local network and the security requirements are low, it is advisable to employ SNMPv1. However, high security requirements could also call for the use of SNMPv2 or CMIP here. If the CMIP protocol is used, a consideration is required as to which protocol stack it should be used on, i.e. either the OSI stack (CMIP) or the TCP/IP stack (CMOT).

Furthermore, it must be noted that CMIP and CMOT are presently not supported by all active network components and network management systems. Before a CMIP protocol is employed, a detailed check is therefore required as to whether the components and clients in use are CMIP-compatible.

Additional controls:

- Have the security requirements for the network management system been formulated and documented?
- Have the active network components and clients been checked for compatibility with the selected SNMP version or CMIP?

S 2.145 Requirements for a network management tool

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The use of a network management tool helps achieve effective network management. A large number of network management products are commercially available at present; all these products need to be checked for compatibility with individual requirements before a decision can be made to procure a particular tool. Here, it is particularly important to fulfil the security requirements stipulated in S 2.143 *Development of a network management concept* and observe the following items:

- The tool must support the selected network management protocol (refer to S 2.144 *Selection of a suitable network management protocol*)
- The product must be scaleable, i.e. it should be capable of adaptation to future requirements.
- It must support all the network components present in the local network.
- It must support all the network protocols used in the network.
- It should have a modular design, in order to easily allow a later integration of additional functions into the existing network management system.
- It should have a graphical user interface, to provide a clear and comprehensible display of relevant information.
- If system management products are also used, it should be possible to combine them with the network management tool under the same user interface, to achieve a "single point of administration".

In addition to these requirements which need to be examined in general, the functional requirements for a network management system must also be defined. The following criteria provide an overview of the possibilities offered by presently available products; however, not all functions are incorporated into all products. Before a product is selected, it is therefore necessary to determine the functions which will be required:

- Topological representation of the network (e.g. including the possibility of integrating background diagrams such as construction plans etc.)
- A choice of topological representations
- Topographic representation of the network (e.g. including the possibility of integrating background diagrams such as construction plans etc.)
- Automatic recognition and representation of network topology and segmentation (auto discovery)
- Indication of the configuration of the active network components on the port level
- Indication of performance on the port level
- Graphic visualisation of the active network components
- Interactive tool for the management protocol (e.g. MIB browser)

- Easy navigation in the network management tool, by means of zoom functions or enlargement of individual sections
- If applicable, integration of a VLAN manager, and graphic display of the VLANs
- Intuitive operation of the tool interface, particularly the section in which the topological and topographical maps are edited (for example, by means of Drag & Drop)
- Display of error and alarm messages by means of freely selectable colours and user-defined criteria
- Possibility of distributed management (client / server and manager-of-manager)
- Possibility of integrating and defining additional MIBs (private MIBs).

Additional controls:

- Have all the requirements for a network management tool been formulated and documented?
- Can the network management concept be realised with the selected network management tool?

S 2.146 Secure operation of a network management system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

For the secure and reliable operation of a network management tool or a complex network management system composed, for example, of several different network management tools, a secure configuration of all the components involved should be ensured. These components include the operating systems on which the network management system is executed, the external databases usually required for the network management system, the protocol in use (refer to S 2.144 *Selection of a suitable network management protocol*) and the active network components themselves. Before a network management system is put into operation, the requirements for preparing and implementing a network management concept should be determined (refer to S 2.143 *Development of a network management concept*).

The following items must be observed in particular:

- To prevent network management information from being intercepted or modified, the computer on which the network management console is operated must be protected appropriately. Measures here include, for example, installation in a specially protected room, the use of screen locks, password protection for the network management console, and further security mechanisms offered by the underlying operating system.
- Safeguard S 2.144 *Selection of a suitable network management protocol* should be taken into account in order to ensure secure operation. In particular, the reading of MIBs and other information by unauthorised persons should be prevented by appropriately configuring the active network components on the basis of the protocol in use (refer to S 4.80 *Reliable access mechanisms for remote administration* and S 4.82 *Secure configuration of active network components*).
- If network management functions are performed decentrally in accordance with the client / server model or through the use of X-Windows technology, their secure operation must also be ensured.
- The integrity of the software in use must be tested at regular intervals in order to allow a timely detection of any unauthorised modifications.
- The response of the network management system in the event of a system crash must be tested. In particular, it should be possible to perform an automatic restart in order to minimise the time interval over which the local network is not monitored. The network management database must not be damaged by a system crash, and must be available again following a restart, as the configuration data it contains are essential for the operation of the network management system. For this reason, these data require special protection, firstly in order to ensure their availability, and secondly in order to prevent the utilisation of old or faulty configuration data following a restart which may have been perpetrated by an intruder

specially for this purpose. If necessary, module 9.2 *Databases* should be noted for the protection of the database in use.

- When restoring data backups, it must be ensured that files relevant to the reliable operation of the network management system, such as configuration-data files, password files as well as meta-configuration files for the network components themselves are fully up-to-date.

  The following data are of relevance to the secure operation of a network management system:

  - Configuration data of the network management system; these data must be stored in appropriately protected directories.
  - Configuration data of the network components (meta-configuration files), which must also be stored in appropriately protected directories.
  - Password files for the network management system. Note must be made here, for example, of password quality factors and the possibility of storing passwords in encrypted form. (refer to S 2.11 *Provisions governing the use of passwords*).

- An administration of active network components via the network should be restricted and replaced accordingly by administration via local interfaces if requirements concerning the confidentiality and integrity of the network management information cannot be fulfilled. Central network management should be relinquished in this case.

Additional controls:

- Have provisions governing the use of passwords for the network management system and network management tool been stipulated?
- Does the network management system support the required security measures?

S 2.147 Secure migration of Novell Netware 3.x servers to Novell Netware 4.x networks

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Under Novell Netware 3.x, every server manages information on its users in a "bindery". One disadvantage of this approach is that in a network consisting of several Netware 3.x servers, an account for a user must be created on each of the servers separately. For administrators, this creation of multiple accounts entails a tremendous effort which can basically not be avoided. In addition, users need to log into each server separately.

In a network consisting of several Novell Netware 4.x servers integrated in a NDS tree however, users only log into the network once, after which they can immediately make use of all the resources which have been released for them (refer to S 2.151 *Design of a NDS concept*).

A complete integration of Netware 3.x servers in a Netware 4.x network is not possible, as these servers continue to operate as independent systems. Users who need to access Netware 4.x as well as Netware 3.x still require multiple accounts in this environment.

A feasible alternative to this is the migration of a Netware 3.x server to a NDS tree. The *NETSYNC.NLM* product accompanying the Novell Netware 4.x packages can be used for this purpose. Operation of a Netware 3.x server in a Netware 4.x network is advantageous in that the user accounts can be managed centrally on a Netware 4.x server, and no longer need to be maintained individually on each Netware 3.x server.

This requires the availability of a Netware 4.x server which can manage up to 12 Netware 3.x servers. This server is designated as the host and is needed for further management of the user accounts, as it transfers NDS modifications to the bindery of the Netware 3.x server. During migration, a large proportion of the NLMs of the Netware 3.x servers is replaced, and the servers are then linked with a host. A restoration of an independent Netware 3.x server would thus entail a great effort.

The following points must be observed to ensure secure migration:

- The bindery context needs to be set for the container in which the Netware 3.x server is to be created.
- The bindery emulation needs to be specified and activated with the instruction *SET BINDERY CONTEXT = ...* in the *AUTOEXEC.NCF* file on the Netware 4.x host.
- After migration, changes must no longer be performed with the utility *SYS:PUBLIC\SYSCON.EXE*. Other utilities such as *SYS:PUBLIC\FILER.EXE* and *SYS:PUBLIC\PCONSOLE.EXE* are replaced by *NETSYNC.NLM* during migration. However, it is advisable to make exclusive use of the *SYS:PUBLIC\NWADMIN.EXE* program for administrative tasks. The *SYS:PUBLIC\SYSCON.EXE* utility should thus be removed.

- If several Netware 3.x servers are to be migrated to the same container or if several bindery emulations have been activated, the related objects must be checked beforehand for name conflicts, as multiple instances of them under the same name are not permissible.

S 2.148 Secure configuration of Novell Netware 4.x networks

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

A secure configuration of a Novell Netware 4.x network involves the following two steps:

- Installation of the related software
- Configuration of the network environment

Installation of the related software

To ensure secure installation of the Novell Netware 4.x software, the *Installation* manual for Novell Netware 4.x needs to be referred to beforehand. The following points must be observed on all accounts:

- Hardware requirements: Before installation, a check is needed as to whether the selected hardware fulfils all applicable requirements (e.g. mass storage and main memory requirements)
- The functionality of all hardware components must be tested under MS-DOS before employment in a more complex environment including, for example, a multi-protocol router
- Documentation of the hardware configuration (refer to S 2.153 *Documentation of Novell Netware 4.x networks*)
- Planning of the NDS (refer to S 2.151 *Design of a NDS concept*)

All other essential steps for installing Novell Netware 4.x software are described in the handbooks entitled *Installation* and *Manual on Netware 4 Networks*.

Availability requirements

To increase the availability of Novell servers and the stored data, the operating system offers a hierarchical set of fault tolerance levels which are described below. Each level contains the functionalities of the previous levels.

- **Hot Fix I and Hot Fix II**

  Novell Netware 4.x supports so-called Hot Fixes as a standard. With this mechanism data losses due to physical hard disk errors are prevented. A distinction is made between Hot Fix I and Hot Fix II. In the case of Hot Fix I, after a write access to a file, the changed data on the hard disk is compared to the original data, which is still available in the main memory of the Netware server. If the two sets of data do not agree, the sector of the hard disk will be marked as faulty and will be locked for future access.

  The data from the memory is then stored in what is known as the "Hot Fix Area" of the hard disk.

  However, in Netware 4.11 or higher, this functionality is deactivated by default. The Netware server's SET parameter accountable for this is called

Enable Disk Read After Write Verify and is set to *OFF* in Netware 4.11. In order to activate the function Hot Fix I, this parameter must be set to *ON*.

Hot Fix II, however, also functions in the default setting of Netware 4.11. Hot Fix II has a similar fault tolerance to Hot Fix I, but only for mirrored or duplexed disks. Unlike Hot Fix I, errors may even be corrected when the data is read, as the information is redundant. If problems are detected when the data is read, the sector of the disk is marked as faulty and a sector from the Hot Fix area is used as a replacement. In this case, the intact information from the mirrored or duplexed disk is read and the information from the replacement disk for this area is automatically added to the faulty sector.

As disks themselves are now highly intelligent and similar mechanisms are available internally, Hot Fix I and II are of little importance today. If sectors in the Hot Fix area are occupied despite modern disks, it is necessary to change the disk immediately.

The Hot Fix area can be configured when a Netware partition is created. Novell Netware suggests a size for the Hot Fix area which is adequate for the size of the Netware partition. The relative size decreases as the size of the partitions increase.

- **Disk Mirroring (System Fault Tolerance II)**

  For disk mirroring two identical hard disks should be connected to the same controller of a server. Nevertheless, it is also possible to mirror hard disks which are not identical. The only requirement is that the data areas of the two Netware partitions of the disks to be mirrored are the same size. The data is stored simultaneously on both hard disks. If one disk fails, the second disk will be used without a loss in availability.

- **Disk Duplexing (System Fault Tolerance II)**

  Disk Duplexing means the installation of two hard disks and their controllers. With this mechanism not only a hard disk failure can be remedied, but also the failure of a hard disk controller can be recovered. In disk duplexing, the power supply of the hard disks should also be redundant, which is usually only possible with external disk systems.

- **Server Mirroring (System Fault Tolerance III)**

  Server mirroring is the highest level of fault tolerance against hardware failures. Two identical Novell Netware 4.x servers are employed simultaneously and "in parallel" in the network. However, it must be kept in mind that the secondary server is only available on standby and does not take over the work in the network unless the primary server fails.

  The servers are connected via their own high speed network. If one servers fails, its tasks are carried out by the secondary server.

  The decision whether measures other than Hot Fixes have to be employed depends on the required availability of the network.

- **Uninterruptible Power Supply (USP)**

  By using an uninterruptible power supply (UPS), the consequences of a power failure can be prevented. Netware supports the utilisation of devices supporting UPS-Monitoring. In case of a sudden power failure the server will be shut down normally at the end of the by-pass time of the UPS. All data residing in caches are written to hard disks. Connections to servers are terminated, as are server processes.

Configuration of the network environment

Novell Netware 4.x offers its own security system for the protection of the network and its resources. However, the corresponding functions must be activated manually by the administrator during configuration of a Netware 4.x network, so the administrator is responsible to a considerable extent for the security of the network.

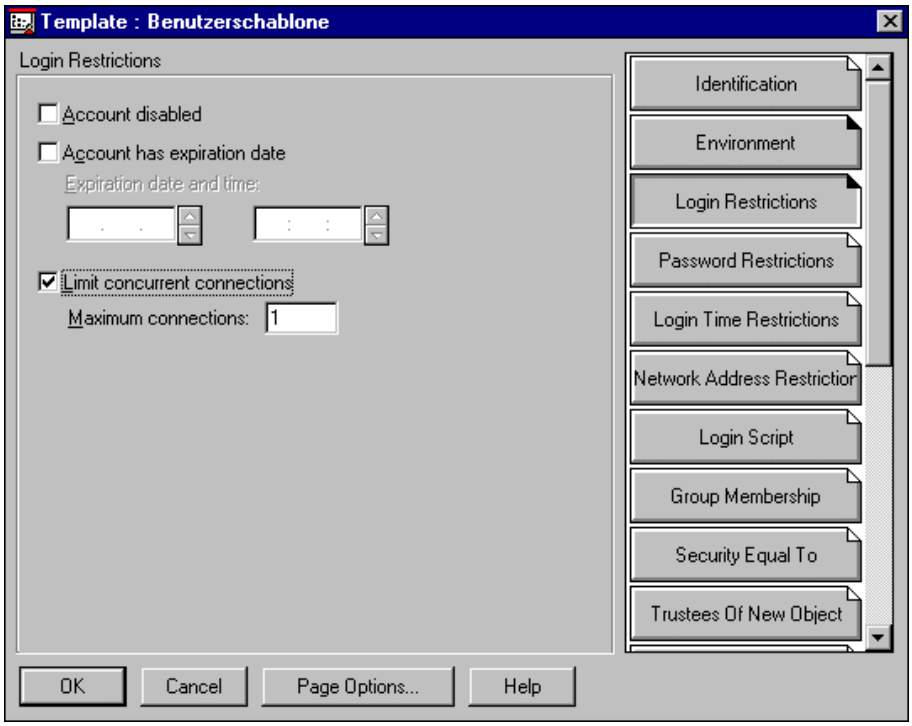
The Novell Netware Administrator is an essential aid in administrating and securing a Netware 4.x network This program comes in the following versions:

- *SYS:PUBLIC\NWADMIN.EXE* for Windows 3.11,
- *SYS:PUBLIC\WIN95\ NWADMN95.EXE* for Windows 95,
- *SYS:PUBLIC\WINNT\NWADMNNT.EXE* for Windows NT and the more recent version,
- *SYS:PUBLIC\WIN32\NWADMN32.EXE* for Windows NT and Windows 95.

The program Netware Administrator allows a wide range of settings, such as setting a minimum password length or the maximum number of simultaneous connections for a user. In the following section, the security-relevant functions of the Netware administrator are listed and explained. The descriptions include specifications of the related parameter settings required for the secure operation of a Netware 4.x network.

One essential step involved in the configuration of a secure Netware 4.x network is the creation of user accounts. Templates for the standard users of each context should be created for this purpose. During the establishment of individual user accounts, the values set in the templates are transferred, which greatly reduces the time and effort involved. The option named **USE TEMPLATE** has been provided for this purpose. The following functions should be set in a template:

Login restrictions

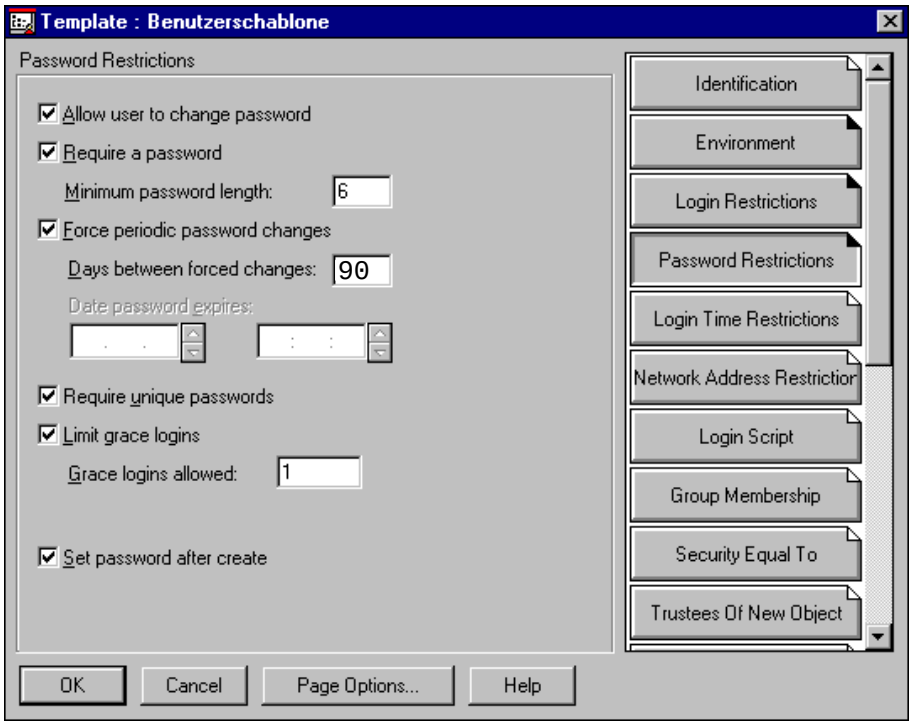


Menu diagram: Netware Administrator Menu “Template: User template / Login time restrictions”

- **Limit concurrent connections**

  This function is used to limit the number of concurrent connections of a user account and the corresponding Netware servers. A value of “1” should generally be selected here, in order to prevent unnecessary usage of connection licences.

Password restrictions



Menu diagram: Netware Administrator Menu “Template: User template / Password restrictions”

- **Allow user to change password**

  This option must be activated to allow users to change their password. If this option is not selected, no further possibilities can be accessed.

- **Require password**

  This option activates the password prompt for every user and offers a possibility of defining the following password rules. "Require password" should always be activated.

- **Minimum password length**

  This specifies the minimum password length. The minimum password length should be no less than six characters (refer to S 2.11 *Provisions governing the use of passwords*).

- **Force periodic password changes**

  When this option is active, users are prompted to change their password on a regular basis. As a rule, this option should be left active.

- **Days between password changes**

  This menu item specifies the general duration of the validity of passwords. This duration needs to be specified individually for each system (refer to S 2.11 *Provisions governing the use of passwords*).

- **Require unique passwords**

  When the password history is active (require unique passwords), the last nine passwords of a user account are compared with the newly entered password, and if a match is found, the new password is rejected by the Netware server. This enforces the use new passwords when a password expired. This option should always remain active.

- **Limit grace logins**

  Grace logins are those which may be performed following the expiry of a password. The number of grace logins should always be limited through the use of this option.

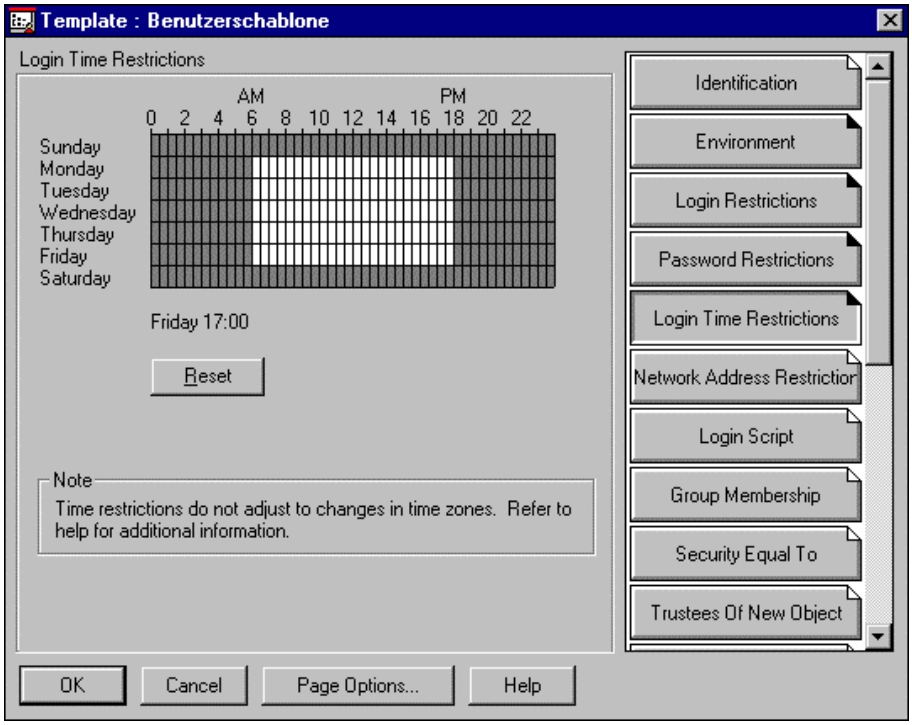
- **Grace logins allowed**

  The number of permissible grace logins should be set to a value of 1, so that when a password expires, it needs to be changed immediately by the user.

- **Set password after create**

  This option should always remain active. It automatically prompts the administrator to enter a password during the creation of a new user account. This prevents the creation of user accounts which are freely accessible on a temporary basis.

Login time restrictions



Menu diagram: Netware Administrator Menu “Template: User template / Login time restrictions”

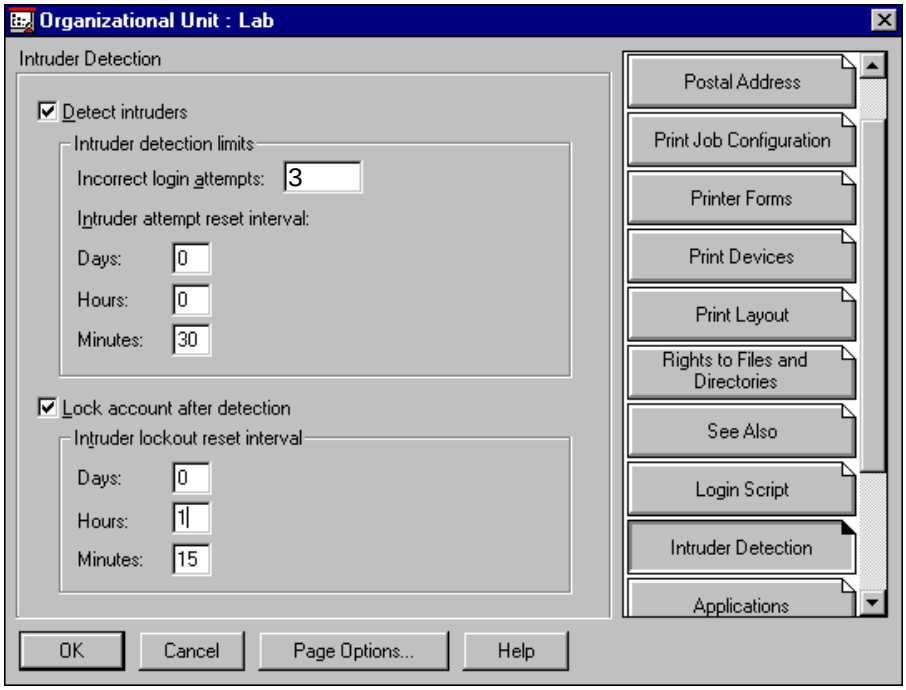
- **Default time restrictions**

  The template designated "Login time restrictions" defines the permissible utilisation periods for user accounts in a Netware 4.x network. Outside the periods specified here, no user is able to log into the Netware 4.x network.

  Subsequent changes to the default time restrictions during the configuration of new user accounts or the maintenance of existing ones, have no effect on the permissible access periods for those users which have already been configured. Different access periods for individual users can be specified with the help of *SYS:\PUBLIC\NWADMIN.EXE* (Objects / Details on multiple users).

The following security mechanisms can additionally be set for individual container objects of the NDS:

Intruder detection



Menu diagram: Netware Administrator Menü "Organizational Unit :Lab/Intruder Detection"

- **Detect Intruders**

  When this option is active, unauthorised login attempts are recognised, and the related user accounts are disabled, if required. This prevents "brute force attacks" under Novell Netware 4.x. This option must be activated with the programme Netware Administrator for every container.

- **Incorrect login attempts**

  This option specifies the maximum permissible number of incorrect login attempts; a value of 3 should generally be set here.

- **Intruder attempt reset interval**

  When this option is active, incorrect attempts at logging into a user account can be traced back through a specified time period. If the number of incorrect attempts at logging into a user account within the defined period exceeds the value set under "Incorrect login attempts", the user account is disabled (provided that the option titled "Lock account after detection" is active).

- **Lock account after detection**

  This menu item should always remain active, in order to disable user accounts for which the maximum permissible number of incorrect login attempts has been exceeded.

- **Intruder lockout reset interval**

  The time interval specified here should always be sufficiently long (> 1 hour), in order to ensure that the reasons for any intruder lockout (i.e. disabling of a user account) can be ascertained by the system administrator and the affected user.

Additional controls:

- Have users been informed on how to handle passwords correctly?
- Is the password quality controlled?
- Are password changes mandatory?
- Has every user been provided with a password?
- Has a user template been generated? Have security aspects been taken into account here?

S 2.149 Secure operation of Novell Netware 4.x networks

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The items described in the following must be observed to allow secure operation of a Novell Netware 4.x network.

Allocation of access rights to directories, files, NDS objects and NDS object properties

The security of a Novell Netware 4.x network and its data can be guaranteed by allocating access rights (trustee assignments) to NDS objects, NDS object properties, directories and files in the network. NDS objects such as users or groups which have been assigned rights to access various NDS objects, NDS object properties, files or directories are termed trustees.

In Netware 4.11, three types of access rights exist. The first two are based on the NDS object rights and the NDS object property rights. The third is based on files or directories.

- **Object rights**

Menu diagram: Netware Administrator Container *zenk_gmbh* "Trustee of this Object..."

Object rights control access by trustees to objects, i.e. users, groups, printers and Netware servers. As can be seen in the above figure, the following object rights are available:

- Supervisor
- Browse

- Create (only for containers)
- Delete
- Rename

A user with these rights over another NDS object, for example another user, is able to sequentially browse, create, delete or rename user accounts. The *Supervisor* right includes all of the other four rights. The *Browse*, *Create*, *Delete* and *Rename* rights do not include any object property rights or file rights. One exception to this in this special case is the Supervisor right to an object. This right also incorporates Supervisor rights to the object properties.

- **Object property rights**

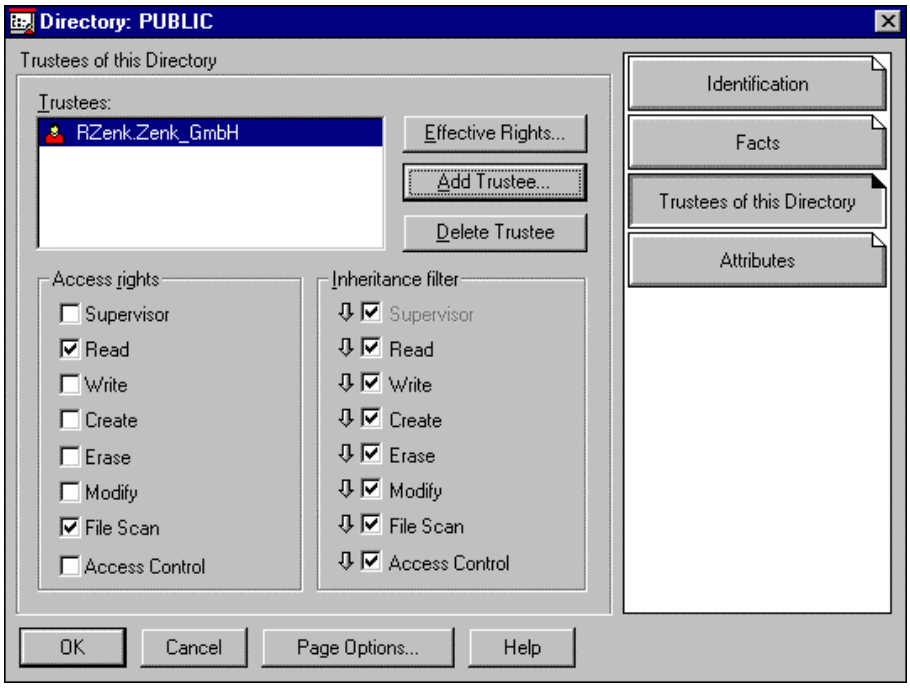
Object property rights control access by trustees to stored details concerning an object, i.e. the object properties. No object rights are required for this. With the exception of the object right *Supervisor*, rights to object properties cannot be obtained with object rights. As can be seen in the above figure, the object property rights are as follows:

- Supervisor
- Compare
- Read
- Write
- Add Self

The object property rights consist of the main rights *Write* and *Read.* The right *Read* contains the right *Compare* and the right *Write* contains the right *Add Self*. The supervisor right is the combination of these four rights and does not have any other effects. With the right *Read*, object properties such as the user's properties *surname* or even the *log-in script* can be read. In order to make changes, the right *Write* is *required*. The right *Compare* allows queries to be made to the NDS, such as if the surname of user XY is *Mustermann*. The answer is then either "true" or "false". The right *Add Self* is only useful for objects with which users are able to enter themselves in a list, as is the case for a group. As an object often has numerous properties, there are two ways of allocating object properties. In principle, it is possible to allocate the same right for all properties. To do this, the option *All Properties* must be selected in the area *Property Rights.* On the other hand, it is also possible to allocate specific rights for particular object properties. This is done using the option *Selected Properties*. It must be noted that when the function *Selected Properties* is used, the rights that were allocated with the option *All Properties* are overwritten.

Rights in the NDS must be allocated even more carefully than rights in the file system. In the file system, an NDS object receives rights to a file or a directory. In the NDS, however, an NDS object receives rights to another NDS object. In the process, it must be carefully checked who is actually to receive the right to who. For example, it may well happen that a user object is supposed to receive rights to a container object, but the container object is given rights to a user object.

- **File and directory rights**



Menu diagram: Netware administrator directory *PUBLIC* "Details: Trustee of this Directory"

File and directory rights control the operations which a trustee, in this case the user *RZenk*, can perform in a file or directory. Just as object rights are independent from object property rights, file and directory rights are completely independent from the two NDS rights. The following file and directory rights exist:

- Supervisor
- Read
- Write
- Create
- Erase
- Modify
- File Scan
- Access Control

With the rights *Read*, *Write*, *Create* and *Erase*, a trustee can read, change, create and delete files or directories. *Modify* is not intended for changing files, but for renaming files and directories. In addition, the right Modify can be used to change the attributes of files or directories. The right *File Scan* allows users to view files or directories, for example with the command NDIR or even DIR. With the right *Access Control*, other NDS objects can be granted file and directory rights, with the exception of the supervisor right.

Unlike the object rights, where the right *Create* is only available at container level, the *Create* right in the file system can also be allocated for files, not just for directories. In the case of files, this right allows a deleted file to be restored through the *Salvage* mechanism. In the NDS, objects cannot be restored once

they have been deleted. This means that the right *Create* is only useful at container level.

For a clearer overview, easier administration and improved auditing capability, access rights should be assigned primarily to user groups (file and directory rights) and to container objects. A container represents all objects, particularly user objects, which are located below the container object in the NDS. These rights really are assigned to all users, not only those who are located directly in the container.

For NDS rights to objects and object properties, there is the object organisational role (OR). The OR can be compared to a group. Groups pass on any file or directory rights they receive to all their users who are entered as members. In the case of an organisational role, the rights are passed on to members of the organisational role. Here, though, the members are referred to as occupants. This is the term used by Novell. Both for groups and for organisational roles, the rights are transferred to the members or occupants with the help of *Security Equal To* mechanisms. As in practice far fewer NDS rights are allocated than file rights, the OR is used much less frequently than for groups.

Rights can also be allocated directly to users and by using *Security Equal To*. However, the clear overview can very easily be lost and these mechanisms should, therefore, seldom be used. To sum it up, the ways in which rights can be allocated are:

- Groups (File and directory rights)
- Organisational role (NDS object and NDS object property rights)
- Containers
- Users
- Security Equal To

To prevent an inadvertent release of directories by users, the system administration should not grant "Supervisor" (S) or "Access Control" (A) rights in the directories and files assigned to the user groups and users.

If certain directories or files are assigned certain attributes - e.g. write-protection (Ro) - with the help of Netware attributes, it must be noted that users who have been granted the "Modify" (M) access right for these directories or files are able to change their attributes. For this reason, the number of users in possession of this access right should be restricted to a minimum.

Inheritance of access rights in the NDS and in the file system

All of the rights dealt with so far are subject to similar mechanisms. This involves important terms such as *inheritance of rights*, *inheritance filters (IRF)*, *effective rights (ER)* and *access control list (ACL)*, which are explained in the following.

Inheritance of rights

Rights are usually inherited both in the NDS and in the file system. This means, for example, that a right which is allocated in the root, either in the NDS tree or in the file system, is inherited by all objects, directories and files, which are located below the root. If a right is allocated further down in the tree

structure, the rights are inherited from this position in the tree. There is an exception to this: rights which are allocated selectively to object properties (*Selected Properties*) are not inherited.

Example 1:

SYS: RZenk [Read; File Scan]
PUBLIC
NWADMIN.EXE
NDIR.EXE

If the user *RZenk* is granted *[Read; File Scan]* rights to the SYS: volume, these rights are in this case also inherited to the *PUBLIC* directory and the *NWADMIN.EXE* and *NDIR.EXE* files contained in *PUBLIC*. It is also possible to restrict the inheritance of certain rights. This is done using the *Inherited Rights Filters (IRF)*, which are discussed below. In the basic state, no rights are filtered. There is another mechanism which prevents inheritance. If the same NDS object is assigned the same right again further down in the tree, the original rights that the object received further up in the tree are no longer inherited from this point.

Example 2:

SYS: RZenk [Read; File Scan]
PUBLIC
NWADMIN.EXE RZenk [Write]
NDIR.EXE

In example 2, the user *RZenk* only has the right *[Write]* for the file *NWADMIN.EXE* as the rights *[Read; File Scan]* of the user *RZenk* are not inherited to the file *NWADMIN.EXE*. All other NDS objects which may have received rights to the file *NWADMIN.EXE* are not affected by this. Even the rights which the user *RZenk* receives for the file *NWADMIN.EXE* via other mechanisms, such as groups, containers, etc., are not restricted by this. These rights are, therefore, additive.

Inherited Rights Filters (IRF)

While trustee assignments grant access to an object, an object property, a file or a directory, an IRF prevents rights being inherited from an object, an object property, a file or a directory to other NDS objects, files or directories in the tree. Each object, object property, file and directory in an NDS directory or file system can have a different IRF.

The only difference between the NDS and the file system concerns the right Supervisor. This right can only be filtered in the NDS. In the file system, on the other hand, this right can no longer be filtered once it has been assigned.

Effective rights

The combination of an Inherited Rights Filter, Trustee Assignment and Security Equivalences is called effective rights (ER). The effective rights which an NDS object has to another NDS object or its property, as well as the effective rights which an NDS object has to the file system, can be specified with the program Netware Administrator (see also previous diagrams).

Access Control List (ACL)

The information regarding which users can access an object and its properties and what rights they have is stored in the object itself. For this purpose, every object has a special property: Access Control List (ACL).

The ACL property contains the Trustee Assignments and the Inherited Rights Filter. Every object entered in the ACL can have other Trustee Assignments. In the file system, the ACL and the IRF are stored in the Directory Entry Table (DET).

Allocation of access rights to directories and files

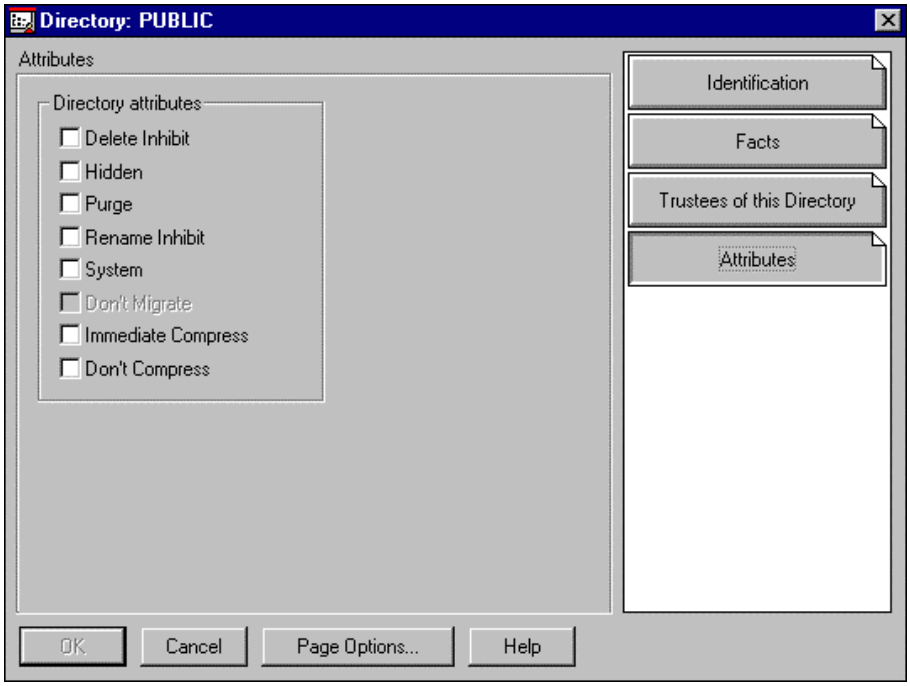
Besides granting access rights to users and groups for files and directories, the allocation of Netware-Attributes to files and directories can increase data security. Attributes are always bound to a file or directory and never to NDS-Objects. These objects are independent of the assigned access rights and are valid for all users including administrators.

Users, who have been granted the "Modify" (M) privilege for the files and directories concerned, can change the Netware-Attributes and thereby carry out every action permitted by their effective privileges.

By installing Netware-Attributes, security takes the form of a subsystem in file and directory security. This means that, although users have the ER to delete a file, they may not be able to do this because the attribute "Delete inhibit" (Di) has been set.

When allocating Netware-Attributes to files and directories, the following properties of Netware-Attributes should be taken into account.

- **Directory Attributes:**



Delete Inhibit (Di): The directory cannot be deleted.

Hidden (H): The directory will be labelled as hidden; it will not show up in a contents list under DOS, neither can it be copied or deleted.

Purge (P): When deleting, the directory and the files contained therein will immediately be physically deleted. It will not be possible to recover the directory.

Rename Inhibit (Ri): The directory cannot be renamed.

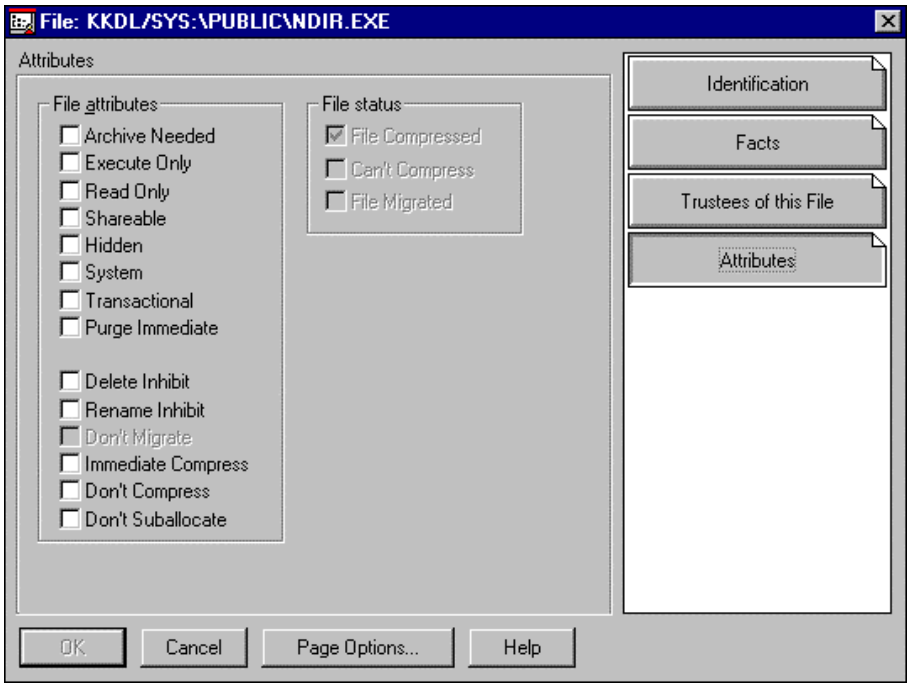
System (Sy): The directory is used by the system; it will not show up in a contents list under DOS, neither can it be copied or deleted.

Don't Migrate (Dm): The directory and the included files are not to be transferred to a secondary data medium (such as a tape drive).

Immediate Compress (Ic): The directory and all files copied into it will be compressed instantly. Files which are already contained in the directory are not affected by this attribute.

Don't Compress (Dc): The directory and all contained files are not to be compressed.

- **File Attributes:**



Archive needed (A): The contents of files labelled thus by Novell Netware have been changed or reinstalled since the last backup. With a sequential backup, data backup software can recognise that the file must be backed up again.

Execute Only (X): Executable program files (**.exe, *.com*) which have been allocated with this attribute may only be executed or deleted. Copying of the file is not possible. It must also be observed that files with this attribute are not saved (e.g. with a full backup)

Read write (Rw): Read and write access to the file is possible.

Read only (Ro): The file may only be read. Write access is not possible. To avoid data loss during simultaneous use, these files should also possess the "Shareable" (S) Attribute.

Executable program files (*.exe, *.com) should be given the "Read only" Attribute to prevent a possible computer-virus attack.

Shareable (Sh): These files can simultaneously be used by many users. Files that have been given the "Shareable" Attribute should also possess the "Read Only" Attribute. The "Shareable" Attribute is only relevant for programs that open files in a non-networkable mode.

Hidden (H): The file will be labelled as hidden; it will not show up in a contents list under DOS, neither can it be copied or deleted. I

System (Sy): This file is used by the network operating system; it will not show up in a contents list under DOS, neither can it be copied or deleted.

Transactional (T): Files with this attribute are subject to transaction control from Novell Netware. Transaction, in this context, means a series of changes in one or more files. Installing this attribute causes only completely executed transactions to be taken over by the data contained in the file. Transactions that have been interrupted before they were completed will be undone by Novell Netware.

Purge (P): Files with the "Purge" Attribute will, when deleted, not only be immediately logically deleted, but also physically. The consequence being that the file cannot be restored. In this context it must be mentioned that a physical deletion of files can not only be achieved by the use of the attribute purge but also with the command *"PURGE filename"*.

Copy Inhibit (Ci): Files of this type cannot be copied. However, this Netware Attribute is only designed for APPLE Macintosh workstations.

Delete Inhibit (Di): The file cannot be deleted.

Rename Inhibit (Ri): The file cannot be renamed.

Don't Migrate (Dm): The file is not to be transferred to a secondary data medium (e.g. tape drive).

Immediate Compress (Ic): The file will immediately be compressed by the operating system and then stored on the volume.

Don't Compress (Dc): The file is not compressed by the operating system, even if compression is enabled for the volume.

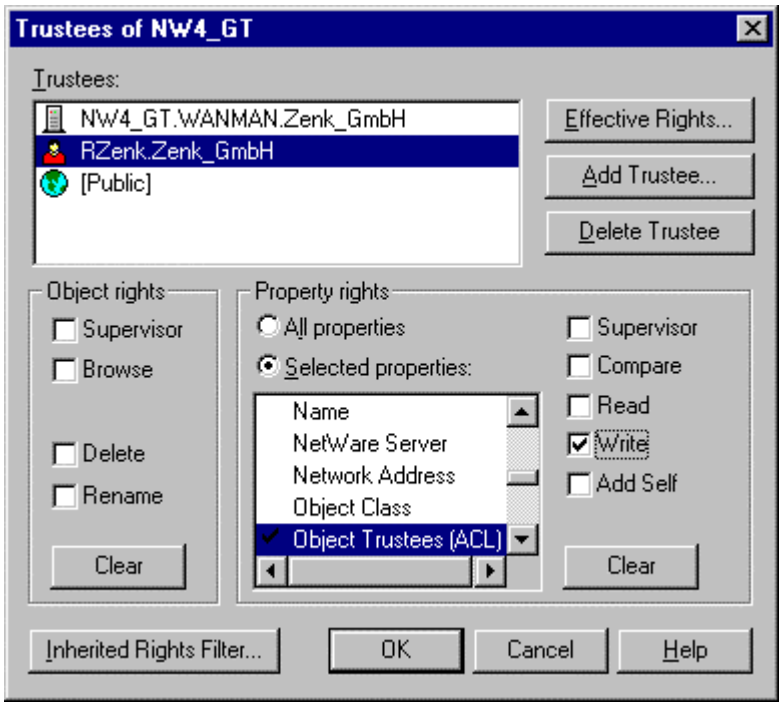
Don't Suballocate (Ds): When storing this file no suballocation will be carried out. Even if this feature is enabled on the system.

File Compressed (Co), Can’t Compress (Cc), File Migrated (M): With these attribute, corresponding information about a file is stored by the operating system. These attributes can only be changed by the operating system.

Careful allocation of rights

File rights, NDS object rights and NDS object property rights are completely independent. There are two exceptions to this: If users receive supervisor

rights to an NDS object, they automatically have supervisor rights to the NDS object properties as well. This phenomenon does not occur the other way round. Supervisor rights for NDS object properties are not equivalent to Supervisor rights for the NDS object itself. In must be borne in mind in this context, however, that the object property *Object Trustees (ACL)* is a property of each and every NDS object. If users receive supervisor rights for the properties of an NDS object or simply the right *WRITE* for the property Object Trustees (ACL), they are able to grant themselves or other NDS objects any rights they choose. An important exception is the NDS object *Server*. If, as in the above example, the user Rzenk receives the right *WRITE* for the object property *Object Trustees (ACL)* of the server, this is the same as receiving supervisor rights for the entire file system that is assigned to this server. The property *Object Trustees (ACL)* of the server is therefore the interface between the NDS and the file system.



Menu diagram: Netware Administrator Server *NW4_GT* "Trustee of this Object..."

In order to prevent supervisor rights in the file system being obtained through improper allocation of NDS rights, Inherited Rights Filters (IRF) can be activated for every server. This allows the object rights to be separated from the directory rights. The supervisor right must be filtered for NDS objects and NDS object properties and the right *WRITE* for the property *Object Trustees (ACL)* must also be filtered. It is of course preferable to be aware of the details of how particular rights take effect.

Restricted usage of accounts with supervisor rights on the file level

The account "Admin" should only be used in an emergency, and not as part of regular administrative activities. Nevertheless, to ensure proper system administration, every user on the Netware security level "Supervisor" should

be assigned an account with the same rights as the supervisor object (explicit trustee assignment, see also *Protection against a loss of administrative capability*) which should usually be used to perform system administration. If administrative tasks are not performed on a full-time basis, additional accounts need to be created specifically for each non-administrative activity.

The account of the administrator or that of the administrator's representative should continue to be used only in workstations defined for this purpose, as the integrity of other workstations could be manipulated.

The account "Admin", which has the sole administrative rights by default, should have its rights removed because it is a target for attack. The necessary supervisor rights should be transferred to another, less conspicuous user account. However, it is possible to simply rename the Admin account, choosing a name that complies with the general regulations for assigning names within the NDS, as laid down in the planning of the NDS for the company.

Protection against a loss of administrative capability

A new function as of Netware Version 4.x allows a decentral administration of Novell Netware networks. This can be achieved by means of certain administrative facilities such as the definition of a separate administrator for each container object. If only one user account has been configured for this purpose and this account is deleted inadvertently, the related container can no longer be managed (refer to T 3.25 *Negligent deletion of objects*).

To achieve the desired effect, an **additional measure is thus required in the form of an explicit trustee assignment** for at least one of the user objects of the user administrator. Therefore, the administrator right should not result from the mechanism *Security Equal To*. This prevents a loss of administrative capability for the container in case the organisational function object is deleted. This applies in particular to the allocation of rights to the central administrators of a Netware 4.x network.

Information on Novell Netware patches

During the development of the Novell Netware network operating system, weak points and shortcomings were discovered, most of which the manufacturer subsequently remedied with the help of patches or service packs for versions 3.x and 4.x. These patches can also be obtained from the manufacturer via the Internet (http://support.novell.com and http://support.novell.de). Shortcomings identified during operation of the network can thus be fixed by obtaining information on the network's functionality and, if necessary, loading the patches which have been made available. In particular, additionally installed software products, e.g. for the purpose of performing data backups, often require a certain patch level of the network operating system. Here though, it must be noted that the offered patches should by no means be loaded "blindly", but only after a thorough research if a concrete requirement for them has arisen ("never change a running system"). As not all patches are error-free, they should first be checked in a test configuration.

Apart from the international discussion forums in the Internet (Usenet) regarding Novell Netware (at present, comp.os.netware.announce,

comp.os.netware.misc, comp.os.netware.security, comp.os.netware.connectivity), there exists a german-speaking Novell forum for german users (at present, de.comp.sys.novell). A number of experienced Novell administrators are present, who can help solve even the most complicated problems. In addition, files are available over the Internet to answer the most frequently asked questions (FAQs). The most frequent problems are dealt with and solutions are offered.

Furthermore, patches and information regarding Novell Netware are made available by other service providers such as Compuserve, Fidonet and Mailboxes.

However, no guarantee can be given as to the correctness and comprehensiveness of the respective information in the usenet discussion forums or in the FAQs (Frequently Asked Questions). It should be noted that a complete description of the problems arising, as well as a description of the respective network configuration (Client, Server), is highly advantageous when searching in the Internet (Usenet).

Furthermore, difficulties in network operation can often be remedied by making enquiries with the network operating system salesperson or by exchanging information with colleagues. As before, solving problems will be made considerably easier with a complete description of the configuration.

Testing for Computer-Viruses

Computer viruses harboured by programs and files stored on a Novell Netware server can cause considerable damage in the network.

For this reason, the programs and files on a Novell Netware server should regularly be checked for the presence of computer viruses using a recent virus scanning program.

For this purpose, it is advisable to create a special user account in the Novell Netware 4.x network, which has "Read" (R) and "File Scan" (F) access to all files. A scan for computer viruses should not be performed with supervisor rights or equivalent rights, as a virus scanning program which is itself infected with a virus will transfer it to all programs and files.

Users and user groups, too, should only be granted the "Read" (R) and "File Scan" (F) rights to access directories and files containing executable program code, to prevent them from being infected by viruses which might appear on local computers. In addition, executable programs should be assigned the Netware attribute "Read only" (Ro).

When compression is enabled, all compressed data must be decompressed during a search of the Netware volumes. This is very time-consuming and considerably increases the server's response times.

Regular checks of time synchronisation and NDS replication

To monitor time synchronisation and the comparison of several NDS replications on different Netware 4.x servers, a separate Netware screen can be activated on the console. This is done by entering the following two commands:

- SET TIMESYNC DEBUG = 7 and

- SET NDS TRACE TO SCREEN = ON.

The console then indicates the packets which are transferred between the servers. The comparison of the individual replications of each server can be monitored on this NDS trace screen. Successful comparison is indicated in green lettering, error messages are displayed in red. As this screen is updated regularly, some information might be overlooked. Therefore, it is absolutely necessary to check the console messages on a regular basis. For this purpose, it is advisable to use a network management tool, which allows the status of the network to be ascertained and monitored much more reliably:

In the case of an error, the utility NDS manager (*SYS:\PUBLIC\WIN95\ NDSMGR32.EXE - for Windows 95 or Windows NT*) is extremely useful. This tool can also be used to monitor the replication.

Regular checks of the utilisation of the system hard disk

To allow trouble-free operation, it must be ensured that the system volume on each Netware server has sufficient free disk space. This is particularly important when compression is enabled. For example, if the generation of temporary files is left uncontrolled and these files are not deleted from time to time, they will eventually fill the system volume. Furthermore, large printer queues could lead to an overflow of the system volume if a large number of users need to print large documents at the same time.

For this reason, a separate volume should be configured for printer queues and other directories in which temporary files are stored. If this is not possible, at least restrictions should be imposed on the size of such directories, so that they do not grow unchecked. This prevents the system volume from being fully occupied, and ensures that enough space is always available for system-specific operations by the Netware server.

Additional controls:

- Have all measures to ensure reliable operation of a Netware 4.x server been implemented?
- Have substitute user accounts been created for protection against a loss of administrative capability, and have these accounts been assigned explicit trustees for accessing the related NDS objects?
- Are the hard-disk utilisation levels and console messages checked regularly?
- Are supervisors' rights to access objects checked regularly?

S 2.150 Auditing of Novell Netware 4.x networks

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Auditors

One important technique of ensuring the security of a network is to allow independent auditors to check the events taking place in a network. For this purpose, Netware 4.x allows a large number of events to be tracked in the NDS and the file system through activation of an auditing function with the utility program named *SYS:PUBLIC\AUDITCON.EXE*. Netware 4.x permits any required number of users to be assigned the role of an auditor. This program offers the following functions, among others:

- Auditors can monitor all NDS file events on the Netware server, in the containers, or on a particular volume.
- Auditing of the file system can be activated on the volume and container levels.
- Auditors can trace network events and activities, but except for the auditing data and auditing log files, they can only open or edit files for which they have been granted access rights by the administrator.

Note: If the logging function is activated, the log file can become very large. For this reason, a limit should be imposed on the maximum size of the file in order to prevent a shortage of memory. As the maximum size depends on the number of users and the activities they perform however, no fixed values can be specified here.

The data accumulated in this process is usually related to persons, and thus subject to the Federal Data Privacy Act. These data must only be used so as to ensure data privacy, maintain data backups and guarantee correct operation (also refer to S 2.110 *Data privacy guidelines for logging procedures*).

To configure an independent auditor who can check the activities of an administrator, but possesses no other administrative rights in the network, the following steps must be taken:

- In the case of Netware 4.10, the auditing for the file system and for the NDS must be activated and a password must be assigned. Anyone who knows this password is able to evaluate the audited data. Under Netware 4.10, therefore, great care must be taken to ensure that no unauthorised persons obtain this password. No further allocation of rights is required under Netware 4.10.

  In Netware version 4.11 and higher, the information is stored in the NDS audit file objects. This considerably improves the security. In addition, there is much more scope for monitoring under Netware 4.11, as the number of auditing mechanisms and functions has been substantially increased.

- Create a user object for the auditor. The authorisation should not be granted for a conventional user account, as this could destroy the security.

- In Netware version 4.11 and higher, the auditor must receive the necessary right to the corresponding NDS audit file objects.
- Activate the network auditing function. The person who creates the NDS audit file object receives the supervisor right for the NDS audit file object and the right Write for the access control list property. This user also receives the rights Read and Write for the audit policy property and the right Read for the audit contents property. The creator of this NDS audit file object is therefore able to administrate and evaluate the auditing.
- The allocation of a auditor password in the utility *SYS:PUBLIC\AUDITCON.EXE* in order to become independent from the administrator (Netware 4.10 and for reasons of compatibility also in Netware 4.11).

  In Netware version 4.11 and higher, the auditor should be made independent from the administrator through the allocation of NDS rights. It can also be determined whether a particular auditor is allowed to view audit files and/or manage the auditing.

If, for carefully considered reasons, it is not desirable or possible to configure the role of an independent auditor, the log files can also be evaluated by the administrator. Should this be the case, it should be pointed out that the Administrator's activities are difficult to monitor. Consequently, the results of evaluation should be presented at least to the IT security officer, IT in-charge, or another specially appointed staff member.

Additional controls:

- Who evaluates the auditing files?
- Can the activities of the administrator be monitored to a sufficient extent?
- Is the IT security management notified of irregularities?
- Has a limit been imposed on the maximum size of the log files in order to prevent memory shortages?

S 2.151 Design of an NDS concept

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

One of the most important new features in Novell Netware 4.x are the *Novell Directory Services* (NDS). NDS are used to manage the logical structure of a network and all the resources contained therein, such as users, groups, printers and Netware servers.

NDS technology replaces the bindery which was used in Netware 2.x and Netware 3.x. The bindery contains a one-dimensional list of all users, groups etc. However, if several Netware 3.x servers are in use, the administrator faces the "problem" of having to manually perform every modification (for example, the addition of a user) on every Netware 3.x server, that is to say on all servers for which a user is to be granted access rights.

In contrast, the Novell directory services are independent of any particular server and based exclusively on the underlying network. This means that administrative activities, such as configuration of a user account, are performed by the Novell directory services on all affected servers, without the need for manual intervention by the administrator.

The resources are managed in a database using a tree structure; this structure is thus also termed NDS tree. In this tree, all users, groups, printers, Netware servers etc. are managed as objects of an NDS directory database. A distinction is made between two types of objects here: *container objects* and *leaf objects*. Whereas a leaf object is located at the end of a branch and does not contain any further objects, a container object can contain additional containers or leaf objects.

The following container objects exist, among others:

- **Root**

  This is the root of the NDS directory tree. Every NDS directory tree has exactly one such object which is created during installation, after which it can neither be renamed nor deleted. Each NDS directory tree can only contain one such object.

- **Country**

  The country object allows a geographical partitioning of the entire structure of the NDS directory tree, i.e. a division of the network by country. However, this object is optional and therefore not specified as default during the installation of the NDS.

- **Organisation**

  The organisation object is intended for a hierarchical arrangement of other objects in the NDS directory tree. No fixed rules apply here, as a result of which, for example, an enterprise can designate the organisation with its own name or those of its various offices. Every NDS directory tree must contain at least one organisation.

- **Organisational unit**

  An organisational unit can only be created within an organisation and is intended for further partitioning of the NDS. For example, offices, departments and project groups can be divided into organisational units. The organisational unit is an optional item used to improve structuring in accordance with the number of leaf objects involved.

Leaf objects include, for example, users, groups, printers, servers and data volumes. It is not possible to create additional objects under leaf objects. The following leaf objects are used most frequently:

- **Netware server**

  This object represents a Netware server in a network, which must contain at least one such server. The object is referred to by many other objects which use the services provided by the server, and is created by the installation program.

- **printer**

  This object represents a printer present in the network, and is always accompanied by the printer queue and print server objects.

- **Users**

  This object is intended to manage and store information on network users, particularly their rights to access network resources.

- **Groups**

  Although several users can be assigned to a group, it represents a leaf object, not a container object. It is intended to simplify administration, as the rights of a group can be transferred to its members.

- **Volume**

  This object represents a physical volume for storing data. As a rule, volume objects are created by the installation program.

A detailed description of the remaining leaf objects is provided in Netware manuals. There are no restrictions on the number of objects, as objects can be added or deleted by applications.

As already mentioned, the directory objects and their attributes are managed in a database which constitutes an essential element of the NDS. In networks possessing WAN links, it is advisable to partition this database into logical segments which are then copied to various Netware servers. When planning the replications, it is important to take slow WAN links into account.

This logical segmentation is termed *partitioning*. The process of copying logical segments to Netware servers is termed *replication*.

Every partition consists of at least one container object and any additional objects contained therein. Additionally, several read or read/write copies of a partition, but only one master partition, can exist.

The physical partitioning of the NDS is transparent for users, i.e. internal Netware mechanisms ensure that this partitioning is not noticed by the users.

In principle, the design of a NDS directory tree is not subject to any restrictions, so that any type of form and degree of complexity is possible. However, careful and thorough planning is required here in compliance with the following basic guidelines:

- A clearly configured NDS should have a maximum depth of between 4 and 8 levels.
- An organisation or organisational unit should contain no more than 1500 objects.
- Several small departments should be grouped into one organisational unit, in order to reduce numbers and improve clarity.
- Descriptive yet reasonably short names should be used (e.g. "R&D" instead of "Research and Development"), as the total path length in an NDS tree must not exceed 255 characters. This restriction is only implemented indirectly, as DOS line commands do not allow longer commands to be entered. This path is termed *Context*.
- In addition to the main partition, each partition should have two read/write partitions. This results in redundancy, which means that a loss of NDS information is highly unlikely. However, backup of the NDS is still obligatory.
- The same version of the *Directory Service* (*DS.NLM*) Netware Loadable Module (NLM) should be used on all servers within an NDS tree, in which the same Netware versions are installed. Otherwise, synchronisation problems may arise. In NDS trees in which, for example, servers with Netware versions 4.10, 4.11 and 5.0 are installed, the versions of the *DS.NLM* must be different for the individual Netware servers. Only the *DS.NLM* for all Netware servers in versions 4.10, 4.11 and 5.0 must be installed in the same version to avoid unnecessary problems. Although it is possible to use a combination of versions, experience shows that the most stable and easily-manageable servers are those which only use Netware versions 4.10, 4.11 or 5.0.

Planning of the NDS is decisively influenced not by the size of the network, but by the characteristics of the environment, such as the hardware, communications links, LAN/WAN topology and organisational structure. For example, a greater amount of planning is required for a small network with several WAN links than for a large network without any WAN links, as unique physical attributes are related to the different types of WAN architecture. At least the following items should be covered during planning:

- Specification of a standard for naming objects (in particular, naming conventions for user IDs and printer IDs)
- Structuring of the NDS tree
- Determination of the location of network resources (e.g. printers and servers) within the directory tree or container, in order to provide users and administrators with a clear overview of the network
- The NDS tree should reflect the organisational structure of the company

- Standard and co-ordinated positioning of network resources at various locations in order to minimise the training period for users who frequently change locations
- Determination of the partition and replication strategy which, amongst other things, are highly dependant on WAN links.

For more information on NDS planning, refer to Novell's *Manual on Netware 4 networks*, which provides a detailed description of the implementation of a Netware 4.x network.

Additional controls:

- Is regular co-ordination performed between the administrators of the individual locations?
- Have all planning guidelines been observed?
- Are the NDS planning guidelines and the decisions of the administrators documented?

S 2.152 Design of a time synchronisation concept

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The stability of a Netware 4.x network depends to great extent on the time synchronisation and is closely related to the Novell Directory Services (NDS).

In this case, time synchronisation means that, in a network incorporating NDS and containing several Netware servers, the clocks on these servers must display the same time. The standard tolerance is two seconds. In other words, the time deviation must not exceed two seconds between any of the clocks on the Netware servers of the NDS. If this is ensured, the clock time in the network is said to be *synchronised*.

In a multi-server network, several replications and/or partitions of the NDS are generally distributed among the Netware servers. If one of the NDS partitions is modified, it is supplied with a time stamp. During the next NDS comparison, this modification is forwarded to the partitions and replications on the other Netware servers in the network. If the clock on one of the Netware servers which receives this modification is an hour behind and is thereby not *in sync*, the changes for this NDS replication or partition can only be synchronised when the affected server is *in sync* again.

In principle, a distinction can be made between the following two scenarios:

- **Single reference model**

  This time model is recommended by Novell for networks with up to 30 Netware servers. It is very easy to configure, and does not require detailed planning of the time synchronisation.

  In this model, one single Netware server acts as the source of the clock signal (single reference), while the remaining Netware servers only act as signal recipients. The single-reference server indicates the time for the entire network, and thus needs to be linked with an external time source (e.g. a radio clock).

  A major disadvantage of this time model is that a failure of the single-reference server would lead to a lack of time synchronisation, as well as all the resulting consequences.

- **Time provider groups**

  In large networks, it is advisable to use time provider groups. These groups are easy to configure but require appropriate planning. Several Netware servers share the time server role. One of them is the reference server, which should be connected to an external time source.

  Primary time servers are located one level below the reference server; at least two primary servers must exist in a network. There is hardly any difference between this type of time server and a reference server. Together, all reference and primary servers determine the valid network time and pass on this time to the secondary servers. The reference server is the stable factor in the network. As the reference server does not adjust its

clock to agree with the network time, the network time must be adjusted to agree with the reference server. It is therefore the reference server that must be used when the network time is to be corrected. Primary servers, on the other hand, adjust their clocks to agree with the network time.

A decisive advantage of this model is that the primary servers serve as substitute sources of the clock signal, thus allowing time synchronisation to be continued even if the reference server fails. In spite of Novell's recommendation to use this model in networks consisting of 30 or more Netware servers, its use is also possible with a notably lower number of Netware servers.

In the standard configuration, time servers, single-reference servers, reference servers and primary servers are published dynamically in the network with SAP/RIP mechanisms. This has the disadvantage, that it is not possible to influence which time servers communicate with each other. This may be particularly undesirable in the case of WAN links. For this reason, it is possible to work with configurable lists and disable the SAP/RIP mechanisms.

The following items need to be observed during the design of a time synchronisation concept:

- An external time source (e.g. radio clock) should be installed in all networks containing more than one Netware server.
- For WAN links within a network, in which the NDS is implemented, at least one timer should be present at a location with several Netware 4.x servers, so that the local secondary servers can fall back on a local time server.
- If, due to a faulty configuration, the clock time set on a Netware server lies far in the future (say, one year), the server would issue after the conversion to the correct time the error message "Synthetic time ..." for all NDS events for a period of one year. This error message could be removed by declaring a new time phase in the *DSREPAIR.NLM* program. This would delete and recreate the entire NDS on the server. To interfere with the NDS in this way is a rather drastic measure and should therefore be well thought out.

Additional controls:

- Has the time synchronisation been planned appropriately?

S 2.153 Documentation of Novell Netware 4.x networks

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

One measure which is important for ensuring reliable operation but often neglected due to a lack of time or personnel, is documentation of the essential information pertaining to a Novell Netware 4.x network. As a change in responsibilities or a shortage of personnel can occur at any time, it is absolutely necessary to record all relevant information concerning every Netware server and supply this information in clearly arranged documents. This facilitates training and orientation if a replacement becomes necessary, and shortens downtimes in case of a failure.

This documentation should provide the following information (together with all the required parameters) in a form which is transparent and can easily be updated:

NDS

Particular attention must be directed to the documentation of the NDS, because instead of being located on a single, central server, it might be distributed among several partitions and stored on different Netware servers - particularly in the case of Netware networks with many WAN links. In individual cases, this can mean, for example, that a server with a read/write replication needs to be converted to a master replication partition, if a hardware failure entails a new installation of the current master partition. However, this problem can be avoided using suitable security mechanisms. This example alone demonstrates the potential complexity of an extensively branched NDS tree, and the accompanying need for appropriate documentation, which should certainly contain the structure of the NDS, as well as information on the allocated NDS and file rights.

Time synchronisation

As NDS and time synchronisation are closely related topics, it is advisable to link them together in the documentation too. This is because all relevant pieces of information exchanged via a Netware 4.x network carry time stamps.

To allow proper time synchronisation in a Novell Netware 4.x network and ensure that the time-related information yields the desired results on every server, a clear specification is required as to which server should act as the clock-signal source and which time model should be used. For this reason, a correct representation of the time synchronisation and the related NDS services is indispensable in order to allow the right steps to be taken in the event of an error.

The table below provides an example of this type of documentation.

SERVER	TIME TYPE	PARTITIONS			
		[Root]	Public	Hamburg	Berlin
Hamburg-S1	Reference	Main partition	Main partition		
Hamburg-S2	Secondary	Read/write replication	Read/write replication		
Hamburg-S3	Secondary			Main partition	Main partition
Berlin-S1	Primary	Read/write replication	Read/write replication		
Berlin-S2	Primary				Read / write replica-tion

Hardware configuration

It should be noticed here that, during a new installation of a Netware server (e.g. following a system crash), all details concerning the hardware settings must be known in order to allow quick and proper re-configuration of the server. If these settings are not known, they need to be scanned using appropriate programs or read off on the device, which proves quite time-consuming. This applies especially to the rectification of time-critical errors.

As concerns each of the hardware components used on the server, such as network adapter cards, graphic cards, communications interfaces (serial, parallel, USB, PS/2) as well as SCSI, IDE and RAID controller, the following information must be recorded, among others:

- Interrupt
- I/O interface
- DMA channel
- SCSI and LUN address
- Memory address
- Node address
- Slot number
- External IPX network number
- Frame type

The documentation of the server hardware must also cover external devices such as

- Printers and

- External sub-systems (hard disk cabinets etc.)

For examples and help, refer to C8 in *Appendix C: Sample templates* of the original documentation of Novell Netware 4.11 (Netware 4 manual).

Software configuration

Software configuration is another important point. The following aspects must be covered here, among others:

- Patch level
- NLMs (Netware Loadable Modules)
- Drivers
- Configuration files (*AUTOEXEC.NCF, STARTUP.NCF*, *DHCPTAB,* etc, see also the description of *CONFIG.NLM* and *Config-Reader*).

As, in some cases, important programs only operate from a certain patch level onwards, the documentation must specify the system updates necessary for execution of these programs (e.g. backup utilities). For this reason, a note must be made of which updates and patches are installed on the Netware server for which purpose.

A tool is available for scanning these configuration details and storing them in an ASCII file. This tool is the program *CONFIG.NLM*, which must be started on the server console and creates a file *CONFIG.TXT*.This configuration file can be analysed with the help of the Windows program *Config-Reader*. Both programs can be found on the Internet under *http://support.novell.com*. Within seconds, the entire configuration of the Netware server is stored in the file *CONFIG.TXT*. This makes it much easier to restart the server after a hardware failure.

Additional controls:

- Has all the relevant information concerning the Netware servers been documented?
- Is the documentation updated regularly?

S 2.154 Creation of a computer virus protection concept

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management

In order to obtain effective protection against computer viruses for an entire organisation, it is essential to select and implement co-ordinated and appropriate protective measures. This calls for a conceptual approach to ensure that suitable measures are applied to all IT systems concerned and that the necessary protection is maintained by a programme of updating.

The table of contents of a computer virus protection concept is shown below.

Table of contents of a computer virus protection concept

Part A: Awareness raising

1 Dependence of the institution on the use of IT
2 Description of the hazard potential
  2.1 Computer viruses
  2.2 Macro viruses
  2.3 Trojan horses
  2.4 Hoaxes
3 Damage scenarios
4 IT systems potentially affected

Part B: Necessary protective measures

5 Computer virus protection strategy
  5.1 Non-networked IT systems
  5.2 Networked terminals
  5.3 Servers
6 Updating computer virus scanning programs
  6.1 Non-networked IT systems
  6.2 Networked terminals
  6.3 Servers

Part C: Regulations

7 Regulations on protection against computer viruses
  7.1 Ban on using non-approved software
  7.2 Training of IT users
  7.3 Rearranging the boot sequence
  7.4 Creating an emergency floppy disk
  7.5 Procedures in the event of computer virus infection
  7.6 Measures for IT systems with non-resident virus-checking
    7.6.1 Periodic running of a computer virus detection program
    7.6.2 Virus checking on exchange of data media and during data transmission
    7.6.3 Checking of incoming files for macro viruses
8 Regulation of responsibilities
  8.1 Who to contact in relation to computer viruses
  8.2 Responsibility of administrators
  8.3 Responsibility of individual IT users
  8.4 Responsibility of IT security management

Part D: Resources

10 Procedures in the event of computer virus infection
11 Reporting channels in the event of computer virus infection
12 User's Guide for the computer virus detection program

The measures described in the following explain how some important parts of this concept can be put into practice.

Additional controls:

- Has the computer virus protection concept been put into effect by management?
- Is the computer virus protection concept known to all those affected by it?

S 2.155 Identification of IT systems potentially threatened by computer viruses

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section

When creating a virus protection concept, the first essential step is to identify the IT systems at the agency or institution which are potentially under threat from computer viruses. From an overview of all IT systems currently in service or whose use is planned, it is possible to pick out all IT systems for which computer viruses represent a threat or via which computer viruses may be distributed. This overview can also be obtained from the results of the determination of protection requirements in accordance with the IT Baseline Protection Manual, Chapter 2.2.

Systems typically affected by computer viruses are all IT systems with PC-based operating systems such as DOS, Windows 3.x, 95/98 or NT, or those running application programs such as Microsoft Word or Excel, which may be infected by macro viruses.

Although servers are not generally threatened directly by computer viruses themselves, they may be a distribution point for infected programs and files.

The possibility of computer viruses also posing a threat where other operating systems or IT application programs are used cannot be ruled out. In a few individual cases this applies to Unix systems and OS/2 systems, for example, but in view of the lack of widespread use these constitute only a low potential threat (see G 5.23).

For each IT system that is identified in this way, the possible infection paths which computer viruses may take can also be determined in a subsequent step. This information can be used for the later selection of which action to take. An infection by computer viruses may take place in the following ways, for example:

- When using floppy disks, CD-ROMs or other exchangeable data media
- When installing new software
- As a result of access to files that are not stored on the local hard disk but on a server in the network or in a shared directory within a peer-to-peer network
- As a result of access to files received from an external source (for example an e-mail attachment or files from the Internet)
- In the course of external maintenance work

It makes sense to draw up a table showing the interfaces via which a computer virus infection may occur for each identified IT system or, by way of example, for each identified IT system type. These interfaces may be as follows:

- Any reading devices for exchangeable data media available locally at the computer (floppy disk drives, CD-ROM drives, streamers, removable hard disks etc.)

- Any portable reading devices for exchangeable data media that can be connected locally to the computers (floppy disk drives, CD-ROM drives, streamers, removable hard disks etc.)
- Links to other IT systems in the local security area (LAN servers, peer-to-peer connections)
- Interfaces via which data can be transferred from external IT systems to the local IT system (modem, Internet connection)

The most important aspect of an overview of this nature is the nomination of people to contact for the respective IT systems, who are responsible for implementing the necessary measures and who are the people who users turn to when needed. As the IT landscape in any organisation is subject to constant change, this information must be updated whenever necessary to reflect changes to existing systems.

Example of a survey:

Existing and planned IT systems / interfaces

Designation and type	Locally net-worked	Local reading devices	External reading devices	Communi-cations cards	Point of contact for virus problems
Server dept. X, Novell 4	x	Floppy disk, CD-ROM drive	Streamer	Modem	Administrator Joe Miller
Clients dept. X Windows 95	x	Floppy disk, CD-ROM drive			PC support engineer Harry Meyer
Laptops, Windows NT		Floppy disk drive			Laptop administration Jim Jones
Server dept. XI, Unix	x	Floppy disk, CD-ROM drive	Streamer		Administrator Tom Smith
Workstations dept. XI Unix	x				-
PCs secretary's office Windows 95	x				Jane Peel
...	...	...	...	...	

Additional control:

- How is it ensured that the necessary measures within the virus protection concept will be taken into account when changes are made to existing IT systems or new IT systems are put into service?

S 2.156 Selection of a suitable computer virus protection strategy

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section

In order to implement computer virus protection it is necessary to deploy human and financial resources, which must be in reasonable proportion to the actual potential threat. Details of the following influencing factors must be collected for all of the identified IT systems potentially threatened by computer viruses:

- How often does a data transfer that could lead to an infection or the dissemination of computer viruses take place via the existing interfaces?
- What consequences can be expected in the event of an actual infection if no protective measures are taken?
- How reliably do the IT users perform IT security measures which need to be initiated periodically?
- How much time can the IT users be expected to spend on computer virus protection measures?

Given knowledge of the frequency of computer virus infections derived from the data collected as described above and from technical publications, and knowledge of the possible consequential damage, a decision has to be taken in conjunction with management as to which financial resources have to be made available for necessary measures and which human resources will be made available.

Once it is known which financial and human resources are available to provide protection against computer viruses and which IT systems have been identified as being potentially threatened, strategies for achieving suitable protection can be chosen.

A number of possible strategies are described in the following.

Computer virus scanning programs on every terminal

The use of an up-to-date resident computer virus scanning program (i.e. a program that runs permanently in the background) in an IT system ensures that an infected program cannot be executed or a file with a macro virus cannot be loaded. Checking of the interfaces on the terminal is taken care of by the resident scanning program. This ensures that no viruses are transferred to the IT system. It is not advisable to rely solely on the exclusive use of non-resident computer virus scanning programs (which are only activated when the program is explicitly started by the user). There is no significant financial advantage to be obtained from this nowadays, but the disadvantages on the part of the IT users are considerably increased because they must be relied upon to activate the program on a regular basis.

If all terminals are equipped with a resident computer virus scanning program, it can be guaranteed that computer viruses will be identified immediately after they appear and that they will not be disseminated from the terminal. In

addition, even where resident virus scanning programs are used it should be possible to activate a program on a case-by-case basis on every client as the need arises, for example to check e-mail attachments selectively before they are opened.

Advantages:

- An appropriate, up-to-date and resident computer virus scanning program ensures maximum protection while at the same time minimising effort and complexity for the IT user.

Disadvantages:

- Procurement costs and administration work are applicable to every terminal.
- Older IT systems may not have sufficient main memory. There may also be complications with regard to interoperation with other programs.

Computer virus scanning programs on all terminals with external interfaces

In networked IT systems a resident computer virus scanning program is only installed on those IT systems which in addition to interfaces to their own internal network also have other external interfaces (floppy disk drive, CD-ROM, modem). Networked IT systems without direct external interfaces are not equipped with computer virus scanning programs.

Advantages:

- Procurement costs and administration work are limited to those IT systems with external interfaces.

Disadvantages:

- Changes to the IT systems which result in the setting up of new external interfaces must be painstakingly followed up because it may become necessary to retrofit IT systems with computer virus scanning programs.
- Encrypted files or programs which contain computer viruses and which are not decrypted until they are on an unprotected terminal will cause infections. This may also be true of compressed files in the same way, if the scanning program is not suitable.

Computer virus scanning programs on all servers

In this case every server in a networked IT system is equipped with a resident computer virus scanning program, but the terminals connected to the server are not. This ensures that it is impossible for computer viruses to be transferred from one terminal to another, and that therefore a possible infection remains locally isolated.

Advantages:

- Procurement costs and administration work are restricted to the servers.
- Protecting the servers prevents re-infections, for example after archived files are retrieved.

Disadvantages:

- For terminals with external interfaces, users have to start the computer virus scanning program located on the server manually in order to check incoming external data media, but also to check data media and files being sent.
- Encrypted files or programs which contain computer viruses and which are not decrypted until they are on an unprotected terminal will cause infections if there is no incoming check. This may also be true of compressed files in the same way, if the scanning program is not suitable.
- It is impossible to rule out the possibility of a terminal with external interfaces becoming infected with a computer virus.
- If use is also made of peer-to-peer functionality, computer viruses can also be transferred between terminals without being checked by the protected servers.
- Detrimental effect on performance, because all communication content has to be checked.

Computer virus scanning programs on all servers and terminals

This combination of the above strategies offers the greatest protection, because computer viruses are immediately detected when they appear and are not distributed further via servers. In addition, computer virus scanning programs from various vebdors can be used, so as in that way to increase the detection rate for computer viruses.

Advantages:

- An appropriate, up-to-date and resident computer virus scanning program ensures maximum protection while at the same time minimising effort and complexity for the IT user.
- Computer viruses are not disseminated further via servers.

Disadvantages:

- Procurement costs and administration work for every server and every terminal.

Computer virus scanning programs on the communication servers

Computer virus protection programs can be installed exclusively or additionally on all communication servers, i.e. the IT systems via which data exchange with external IT systems is carried out, for example firewalls or mail servers. However, the effect of this is that the terminals are only protected against computer viruses if they do not have any other interfaces, such as CD-ROM drives etc.

Advantages:

- All files are checked at the entrance to the LAN, and not only when they are inside.

- Computer viruses are not disseminated further via servers. They can, however, be spread on the terminals if files are exchanged between them directly (for example on floppy disk).

Disadvantages:

- This method is susceptible to error: in some circumstances, e-mail attachments may not all be recognised. Often scanning programs only check for the presence of attachments within the first few lines of an e-mail or in the mail header. It can also happen that the procedure with which the attachment has been processed (e.g. uuencode) is not supported by the virus scanning program. This is possible with MIME, for example: problems may arise if one or more files encoded with uuencode are simply inserted into the body of the e-mail.
- Detrimental effect on performance, because all communication content has to be checked.
- Only a minimal operating system should be installed on all communication servers, in other words only the most essential services (see also S 4.?? *Minimal operating system*).
- In order to avoid denial-of-service attacks, a computer virus scanning program should never be installed on a firewall – at most on a proxy, if at all.

Data hygiene and central checking of files

All incoming and outgoing files and data media are checked at a central point by a computer virus scanning program. In addition, there is a rule that the IT users must not use any files, programs or data media of doubtful origin.

Advantages:

- The number of licences for computer virus scanning programs that need to be purchased is considerably reduced.

Disadvantages:

- If external data media are used frequently, central checking for computer viruses takes up a great deal of time and delays operational procedures. It is impossible to rule out infection by a computer virus entirely, because checking of a data medium may be forgotten by mistake.
- All computers which do not have a computer virus scanning program must be checked for infection by a computer virus at regular intervals.

Regardless of which strategy is chosen for providing protection against computer viruses, there is always a residual risk that computer virus scanning programs will only detect those computer viruses that were known at the time when the program was developed. This means that new viruses may not be detected and could cause damage.

The choice of correct strategy, which must also be appropriate from the cost point of view, is dependent on the particular IT environment in each case. However, in view of the fact that the cost per licence is usually greatly

reduced when purchasing multiple licences of the commonly used, suitable computer virus scanning programs, it is advisable to give consideration to fully equipping all servers and terminals.

Additional controls:

- Have computer viruses occurred in the past? What damage did they cause (financial losses, loss of working time, ...)?
- Is the decision about the commitment of resources for computer virus protection taken by management?
- Is there assurance that consideration will be given to adaptation of the computer virus protection strategy when changes are made to the IT environment?
- Have the disadvantages associated with the chosen strategy been made plain to IT security management?
- Will the resultant residual risks be covered?

S 2.157 Selection of a suitable computer virus scanning program

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section

German federal authorities obtain current virus protection programs from the BSI. Users in other areas must select computer virus protection programs suitable for their purposes from among the large number of programs available on the market.

A functionality class for anti-virus products (F-AVIR) has been developed for ITSEC, the Criteria for the Evaluation of the Security of IT Systems. This can be used as an aid when selecting a suitable virus scanning program.

The F-AVIR functionality class describes security functions and requirements for a secure working environment for anti-virus products which should be used as criteria for the selection of a suitable computer virus scanning program.

Volume 2 of the BSI series of publications on IT security, "Informationen zu Computer-Viren", includes the text of this functionality class. To help, the corresponding extract from the CD-ROM has been enclosed with the IT Baseline Protection Manual.

Essentially, the computer virus scanning program to be selected should satisfy the following conditions:

- The range of computer viruses detected should be as large as possible and correspond to the currently known inventory; in particular, all highly widespread computer viruses must be detected.
- Constant updating with reference to new computer viruses must be ensured by the vendor.
- The program should also find computer viruses even when they are in compressed form; commonly used compression functions such as PKZIP should be supported.
- When computer viruses are found, the full path must be displayed.
- The program must first establish that it is itself free of viruses before the scanning function is executed.
- If possible, the product must allow constant computer virus checking by running as a resident program.
- It makes sense to use a functionality which enables detected computer viruses to be removed without causing further damage to programs or data.
- The program should have a logging function which records the following data:
  - Program version number
  - Date and time of the scan
  - Specification of all parameters used

  - Scan result with indication of the scope of the scan
  - Number and identification of files and objects which could not be checked
- The program should issue a warning when it establishes that it has obviously not been updated (if the gap between the last updating of the program and the system date is greater than 6 months).
- The program should contain a list of detectable computer viruses and their descriptions. In addition, descriptions must be provided of immediate measures to be taken and measures to remove the computer virus.

S 2.158 Reporting computer virus infections

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section

When a computer virus infects a system, the priority is to prevent other IT systems from becoming infected. To this end, a contact person should be appointed at the institution, to whom a computer virus infection must be reported without delay. On the basis of the documents produced in accordance with S 2.155 *Identification of IT systems potentially threatened by computer viruses*, this person can immediately decide which users need to be informed about the occurrence of a computer virus as appropriate. These alerting routes must also be established within the framework of the reporting system.

In addition to the institution's own staff, all externals who may be affected by the virus infection must also be informed. These include in particular those people who it is presumed have forwarded or received the virus.

To obtain an overview of the current threat posed by computer viruses, the BSI maintains a set of statistics about all virus infections that have occurred. For this purpose, a virus reporting sheet was issued on which a virus incident should be recorded. The virus report is used by the BSI for statistical purposes only; it can also be submitted anonymously (a preprinted form is provided in the appendix).

The appointed contacts are then finally also the people via whom the measures leading to elimination of the detected computer virus infection are to be initiated. These should document all infections with computer viruses, their effects and their elimination. This information forms a basis for updating the virus protection concept, and provides a record of incidences of damage that have occurred and of the effort and expense of correction.

In order to set up the reporting system, it is necessary for the contact person to be made known to all staff in an appropriate form. This may take the form of a leaflet, for example (cf. S 6.23 *Procedures in the event of computer virus infection*). Especially when there is a hoax (see T 5.80 *Hoaxes*) it is important that users forward these supposed security instructions only to the contact person appointed to deal with virus problems, and do not spread them further.

In the same way, the contacts must regularly keep themselves informed of any new computer viruses that appear so that they can arrange for the computer virus scanning programs to be updated or those users affected to be alerted, as the need arises.

Additional controls:

- Has it been ensured that the contact person for computer virus infections is known to all IT users?
- Has it been ensured that the contact person can alert all those potentially affected by an acute computer virus infection as quickly as possible?

S 2.159 Updating the computer virus scanning programs used

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section

Where IT systems are equipped with computer virus scanning programs, these programs must be updated regularly so as to ensure reliable detection of new computer viruses. To do this, a procedure must be laid down to specify responsibility for and procurement and distribution of the updates.

At the time of procurement of a suitable computer virus scanning program (see S 2.157), attention should be paid to the need to update it at short intervals (no greater than 6 months). As virus scanning programs are also updated for specific reasons, for example because of the appearance of new viruses, the person responsible for the problem of viruses should check with the software producer for information on updates on a regular basis (at least once a week).

The BSI has set up a mailing list for fighting computer viruses for Federal authorities. Up-to-date information about virus problems is distributed to members of the mailing list. In cases of an extremely serious virus danger, in future a virus warning will be issued. Special drivers to deal with new viruses not yet detected will also be distributed over this channel. Staff working for Federal agencies can join this mailing list over the IVBB Intranet under *http://www.bsi.ivbb.bund.de/antivir/mailing.htm* or else by sending an unstructured e-mail to *antivir@bsi.de*.

When updates to the computer virus scanning program are distributed, steps must be taken to ensure that the updates are indeed loaded promptly onto the IT systems. If this cannot be performed automatically (in the case of networked IT systems), the update should be made available to the relevant IT users quickly.

Because virus scanning programs are updated so frequently and tested within very tight timescales, they are susceptible to error and must be tested in actual operation before release or installation (see also S 2.83 *Testing Standard Software*). When updates are installed, particular care must be taken that the existing configuration of the computer virus scanning program is not changed by preassigned parameters. For example, an update could cause a previously resident computer virus scanning program to be switched to an offline mode.

In addition, steps must be taken to ensure that computers which are not allocated to any individual person and are not networked, for example laptops, are also supplied with updates.

Additional controls:

- Were the copies created for distribution of the updates made on an IT system which was demonstrably virus-free?
- How long does it take to disseminate an update throughout the entire institution?
- Are occasional checks made as to whether updates have been implemented?

S 2.160 Regulations on computer virus protection

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section

In order to obtain effective protection against computer viruses, certain additional measures must be put in place over and above the use of virus scanning programs. With this in mind, it is necessary to address the following points, among others:

Use of computer virus scanning programs

The use of these programs is to be specified and documented in accordance with the chosen strategy and the chosen product (cf. S 2.156 *Selection of a suitable computer virus protection strategy*, S 2.157 *Selection of a suitable computer virus scanning program*). In addition it is necessary to determine how, at what intervals and by whom the computer virus scanning programs will be updated (cf. S 2.159 *Updating the computer virus scanning programs used*).

Training of IT users

The IT users affected must be informed of or given training in (cf. S 3.5 *Education on IT security measures*, S 3.4 *Training before actual use of a program*, S 6.23 *Procedures in the event of computer virus infection*) matters relating to the dangers posed by computer viruses, macro viruses, Trojan horses and hoaxes (cf. T 5.23 *Computer viruses*, T 5.43 *Macro viruses*, T 5.21 *Trojan horses*, T 5.80 *Hoaxes*), necessary IT security measures, behaviour in the event of computer virus infection and handling of the computer virus scanning program.

Ban on the use of non-approved software

The installation and use of non-approved software, in particular software that has not been virus-checked, must be forbidden (cf. S 2.9 *Ban on using non-approved software*). Over and above that it may be necessary to stipulate that checks on observance of the ban are performed regularly (cf. S 2.10 *Survey of the software held*).

Protective measures on the IT system

The boot sequence during operating system startup must be rearranged such that as a rule the system is started first from the hard disk (or from the network) and only then from an external medium (floppy disk, CD-ROM; cf. S 4.84 *Use of BIOS security mechanisms*). In addition, an emergency floppy disk must be created for every available computer type, in order to allow a successful cleanup in the event of a computer virus infection (cf. S 6.24 *Creating a PC emergency floppy disk*). If a new computer virus does cause damage despite the precautions, a backup must be used. Data backups must therefore be created on a regular basis (cf. S 6.32 *Regular data backups*). When data backups are reloaded, care must be taken that no files infected by the computer virus are restored to the system as a result.

Measures for IT systems with non-resident virus checking

In IT systems on which no resident computer virus scanning program is installed, as an alternative it is necessary to stipulate the regular use of a computer virus scanning program (cf. S 4.3 *Periodic runs of a virus-detection program*), checking for viruses when data media are exchanged and data is transferred (cf. S 4.33 *Use of a virus scanning program on exchange of data media and during data transfer*) and checking for macro viruses when incoming files are received (cf. S 4.44 *Checking incoming files for macro viruses*) in order to ensure the rapid detection of computer viruses and to prevent their being spread further.

Reporting of computer viruses

It must be stipulated to whom the discovery of a computer virus must be reported without delay. The form of the report (form sheet) and the means of communication (by telephone, in person, in writing, by e-mail) must also be regulated (see S 2.158 *Reporting computer virus infections*).

Regulation of responsibilities

The tasks, authorities and responsibilities for protection against computer viruses must be laid down for the following:

- The contact person for computer viruses
- The administrator of network servers
- IT users of terminals
- IT security management

Updating the computer virus protection concept

When changes are made to IT systems, when new IT systems are installed and when networking changes are made, the computer virus protection concept must be updated and adapted (cf. S 2.34 *Documentation of changes made to an existing IT system*).

These arrangements must be made known to those people affected. The observance of these arrangement should be checked from time to time in order to ensure that the computer virus protection concept is consistently implemented.

Additional controls:

- When was the last check made? Have the results been documented?
- How are the people concerned informed of the relevant arrangements?

S 2.161 Development of a cryptographic concept

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

Nowadays companies and agencies are increasingly dependent on their information technology infrastructure. This is why it is necessary to have security services which go beyond mere encryption, and why they have to be integrated into the system as a whole.

Given the diversity of cryptographic problem situations and variety of influencing factors, there are also many different approaches to solutions and possible means of implementation. It cannot be assumed that there is one solution which is capable of dealing with all security problems in computer networks and/or communication systems. On the contrary, what is important is harmonised interaction between appropriately selected components in order to achieve the necessary degree of security. It is therefore necessary to develop a cryptographic concept that is integrated into the agency's or company's IT security concept.

The choice of suitable cryptographic components must be based on this concept. A critical element in the whole crypto concept is key management. Concepts and approaches to solutions can only be successfully devised and put into practice precisely where they are needed when it is clear which specific security functionalities and security services are required. Beyond this there are also a number of system-related questions and aspects which do not specifically belong in the field of security technology. This includes performance requirements, for example, or requirements relating to system links, interoperability and conformity with standards.

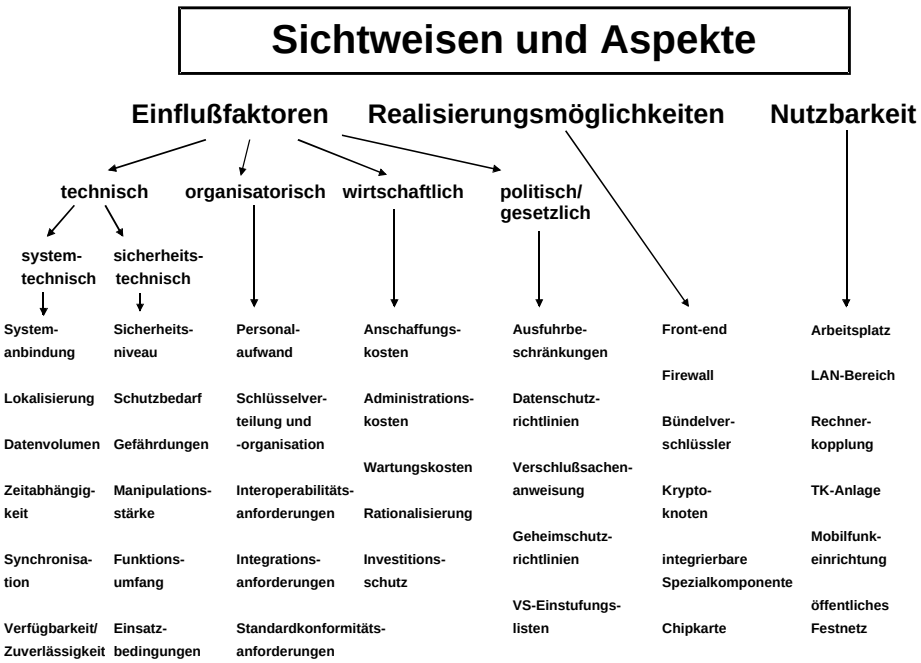


Figure: Perspectives and aspects in the selection of cryptographic procedures and components

In networked IT infrastructures it is no longer sufficient to guarantee the security of an individual domain. Instead, the security of all terminal equipment and transmission systems forming part of the network must be dovetailed to act in concert. Such harmonisation proves to be especially difficult particularly in those cases where the equipment is not networked within one organisational unit (such as a LAN environment) but rather where there is a combination of IT installations with different areas of responsibility and fields of application.

The use - but also the functionality and technological design - of an IT security system is determined by numerous influencing factors, such as localisation, the level of security, and the frequency and scope of application, which represent important terms of reference and decision-making conditions for IT security management. Furthermore the technical means of implementing and designing an IT security system are also widely varied: for example integrated in an application on a workstation, in a firewall or as a special component for network components such as switches or routers. It is only possible to achieve an affordable price level for a crypto product if it can be used for a broad cross section of purposes. A standardised system link and uniform operating conditions play an important role in this, for example. One last point relates to the interaction of the security services on various protocol layers. The security services on the higher protocol layers (according to the OSI reference model) generally only provide sufficient protection if the lower layers also provide protection (see S 4.90).

It is also important to define a cryptography policy specific to the organisation. The following points must be clarified from the standpoint of the management:

- What are the protection requirements or what security level is it considered necessary to achieve?
- What budget and how many staff are available in order to set up the planned security mechanisms and - very important - also to guarantee operation?
- What system link is aimed for and what are the prevailing operating conditions for security components?
- What scope of functions and performance is aimed for?
- Who takes responsibility in the final analysis?

The crypto concept must also include a description of the technical and organisational use of the cryptographic products, i.e. the following points, for example:

- Who is given which access rights?
- What services are offered remotely?
- How is the management of passwords and keys to be handled, with regard to their period of validity, use of characters, length and allocation?
- Does the data have to be encrypted or signed, and if so, when and how?

- Who can communicate with whom with or without cryptographic protection?
- Who is allowed to assign certain rights, etc.?

On this basis and in accordance with the basic systems engineering conditions regarding

- the data volume under consideration and time dependence
- availability requirements and the risk situation
- the type and frequency of applications to be protected etc.

suitable implementation options can be analysed and a conception drawn up and technical design finalised for specific fields of use, such as a PC workstation, within a LAN or in connection with a PBX system. A holistic approach of this nature is essential in order to assemble the fundamental data and conditions needed to take decisions about cryptographic products if their application and use is both appropriate from a security point of view and is economically justifiable. It should be pointed out, however, that the subdivision described above is by no means obligatory or of fundamental significance, but is at best helpful. The only key factor is that the scope of the questions must consistently reflect the starting scenario after the situation has been clarified as comprehensively as possible. In practice, of course, there are reciprocal effects and dependencies between certain questions and answers, but in general these contribute to completing the overall picture.

The various influencing variables affecting the use of cryptographic procedures must be established and must be documented in a comprehensible form (see S 2.163 *Determining the factors influencing cryptographic procedures and products*). Subsequently, a suitable course of action must be developed and documented for their use. Finally, implementation must be arranged by the agency or company management.

The results should be recorded within the crypto concept in a form which can be updated and expanded as required. An example of a crypto concept is shown in the following table of contents:

Crypto concept: Table of contents

1. Definitions
- Cryptographic procedures
- ...

2. Threat scenario as motivational background
- Dependence of the institution on the data stock
- Typical threats such as ...
- Causes of damage specific to individual institutions
- In-house cases of damage

3. Specifying the organisation's internal security policy
- Specification of responsibilities
- Objective, security level

4. Influencing factors
- Identification of the data to be protected

- Confidentiality requirements
- Integrity requirements
- Data availability requirements
- Performance requirements
- Distribution of keys
- Data volumes
- Type of data (local / distributed (LAN/WAN))
- Type of applications for which cryptographic procedures are to be used
- Frequency of use of the cryptographic procedure
- Requirements concerning the resistance of the algorithms and procedures (manipulation resistance)
- Restorability of backed up data
- Personnel costs
- Required functionality
- Costs including follow-up costs (maintenance, administration, updates, ...)
- Knowledge and data-processing skills of IT users

5. Determining the use of the concept

- Type of cryptographic procedures
- Conditions of use for the cryptographic products
- Frequency and time of use
- Nomination of staff responsible
- Stipulation of organisational rules and regulations
- Implementation of staff-related measures (training, deputisation arrangements, obligations, apportioning of functions)
- Documentation of conditions of use / configuration
- Interoperability, conformity with standards, protection of investment

6. Key management

Individual aspects of this concept are described in more detail in safeguards S 2.162 *Determining the need to use cryptographic procedures and products*, S 2.163 *Determining the factors influencing cryptographic procedures and products*, S 2.166 *Provisions governing the use of crypto modules* etc.

Drawing up a crypto concept is not simply a once-only task, it is a dynamic process. Regular adaptation of the crypto concept to current circumstances is therefore essential.

Additional controls:

- Is the present concept up to date?
- Are all relevant IT systems included in this policy?
- How are staff members informed about the sections of the concept which are applicable to them?
- Is adherence to the concept monitored?
- How are changes in the influencing factors taken into account?

S 2.162 Determining the need to use cryptographic procedures and products

Initiation responsibility: IT Security Management

Implementation responsibility: Administrators; staff responsible for the individual IT applications

In order to arrive at realistic, reliable and appropriate indications of requirements and basic conditions for the use of cryptographic procedures and products in relation to the processing and transmission of sensitive information, it is first necessary to identify and assess the data that is worth protecting.

Identification of the data to be protected

First it is necessary to identify the tasks for which cryptographic procedures are to be used and the data which these procedures are intended to protect. The use of cryptographic procedures may be necessary for a variety of reasons (see also S 3.23):

- To protect the confidentiality and/or integrity of data
- For the purpose of authentication
- To provide proof of sending or receipt (non-repudiation)

It may make sense to use various different cryptographic methods, such as encryption or hash functions, depending on the intended purpose. The typical fields of use for cryptographic procedures are:

1. Local encryption
2. Communication security, at the application level and/or at the transmission level
3. Authentication
4. Non-repudiation
5. Integrity

A number of examples from the various typical fields of use for cryptographic procedures are described below:

- A PC hard disk contains data which is to be protected by encryption to prevent unauthorised access.
- Information is to be forwarded via telephone, fax or data networks, for example it is to be sent by e-mail or transferred by the exchange of data media.
- The information that needs to be protected is not under the sole control of the responsible organisational unit (the LAN runs through parts of the building that are used by other companies; a server storing personnel data is managed by staff who do not belong to the personnel department).
- Remote access is to be secured by strong authentication.
- In the case of e-mails, it must be possible to determine without doubt who the sender was and whether the content has been delivered unchanged.

In order to establish which cryptographic procedures and products are required and which data needs to be protected by these means, the first step should be to determine the current IT structure (see also Chapter 2 on recording the details of IT systems and applications). The following facts should be established:

- What IT systems are there which are used for processing or storing data (PCs, laptops, servers, ...) or for transmitting data (bridges, routers, gateways, firewalls, ...)
- What transmission routes are used. The logical and physical networking structure should also be recorded in this connection (see also S 2.139 *Survey of the existing network environment*).

Degree of protection required for the data (confidentiality, integrity, authenticity, non-repudiation)

All applications and data for which there are particular requirements in terms of confidentiality, integrity, authenticity or non-repudiation should be identified (see Chapter 2). However, cryptographic products are not required solely for IT systems, applications or information with high-level protection requirements, they are also needed for those with medium-level protection requirements.

Examples of data with particular requirements regarding confidentiality include:

- Person related data
- Passwords and cryptographic keys
- Confidential information, the publication of which could result in recourse claims
- Data from which a competing company could derive financial gain
- Data which would jeopardise the fulfilment of a task if it did not remain confidential (e.g. results of an inquiry, register of sites or endangered plants)
- Data which could result in an injurious falsehood if published

Note: The accumulation of data increases the protection requirements of a data collection, such that encryption may become necessary even if the individual records in the collection are not particularly sensitive.

Examples of data with particular requirements regarding integrity include:

- Financial data, the manipulation of which could cause financial loss
- Information which, if published in a corrupted form, could result in recourse claims
- Data which, if corrupted, may lead to incorrect business decisions being taken
- Data which, if corrupted, may result in a deterioration of product quality

An example of applications with particular authenticity requirements is remote access. An example of data with particular requirements regarding non-

repudiation would be orders or bookings where the person ordering or booking should be identifiable.

Once the protection requirements have been determined, the next step should be to establish which applications or data are to be protected by cryptographic means. This stipulation can be further refined later, and should be revised regularly.

The result obtained in this way is an overview of all storage locations and transmission links which have to be secured by cryptographic means. The outcome is therefore effectively an IT map with crypto areas marked on it.

Survey of needs and requirements

As an aid to investigating what is required, it makes sense to use a set of questions covering the subject areas in the breakdown shown in the table below. The technical, organisational and economic aspects can each be divided into 4 further subcategories.

Survey of needs and requirements		
Technical aspects	**Organisational aspects**	**Economic aspects**
User services and applications	Field of use	Rationalisation aspects / cost savings
Utilisation profile	Migration concept	Quantities
Network infrastructure	Envisaged timescale	Procurement costs
IT terminal	Operational circumstances	Administration and maintenance expenditure

Figure: Classification criteria for creating a questionnaire

Among the technical aspects it is important to find out under „User services and applications“ for example whether the data concerned is mainly real-time or not. In the utilisation profile category it is necessary to identify the applications and data for which cryptographic procedures are to be used, for example for external communications or for the short-term or longer-term processing of confidential data. Furthermore, information about the network infrastructure and the terminal needs to be established, for example the connection configuration.

The organisational aspects to be considered are the field of use, i.e. user domain or network domain, the question of whether there is an existing migration concept, the envisaged timescale and the operational circumstances for the end user.

The key aspects from the economic standpoint are:

- Rationalisation aspects, for example using a product with transparent encryption instead of manual activation
- Estimates as to quantities required and procurement costs
- Anticipated administration and maintenance costs

Using this survey as a basis, an operations and requirements concept as close to practical reality as possible can be drawn up; this is then used as the starting point for actual implementation decisions and the selection of suitable crypto components and products (see S 2.165 *Selection of a suitable cryptographic product*).

The approach described above is intended to help staff responsible for security to determine, assess and coordinate the use of security technology in various system localities, network gateways and terminal equipment, as well as the extent to which the technology is to be used. In addition, the question of the appropriateness of IT security is to be answered in the course of the planning phase by determining the necessary degree of protection (protection requirements). The course of action outlined here is a pragmatic approach and takes account of security aspects in open, distributed IT infrastructures, as found in many instances.

The investment in security viewed in this way must be economically justifiable for the respective field of use. The mode of operation of security strategies that are put into practice must take account of the expectations of the end users with regard to flexibility, transparency and performance. The security services, whether planned or integrated, must not impose any restrictions on the end users over and above that which is necessary.

S 2.163 Determining the factors influencing cryptographic procedures and products

Initiation responsibility: IT Security Management

Implementation responsibility: Administrators; staff responsible for the individual IT applications

Before a decision can be taken as to which cryptographic procedures and products are to be used, details of a number of influencing factors need to be ascertained. The system administrators and staff responsible for the various IT systems and IT applications can be interviewed for this purpose. The results are to be comprehensibly documented.

The following influencing factors must be determined for all storage locations and transmission links specified in S 2.162 *Determining the need to use cryptographic procedures and products*:

Security aspects

- What are the protection requirements or what security level is it considered necessary to achieve?
- Which cryptographic functions are necessary for this (encryption, protection of integrity, authenticity and/or non-repudiation)?
- Potential of intruders: what type of intruders are to be expected (time available, financial resources, technical skills)?

The answers to these questions are derived from S 2.162 *Determining the need to use cryptographic procedures and products*.

Technical aspects

Operating heavily branched IT infrastructures with their large numbers of individual components and special equipment (network nodes, servers, databases, etc.) means that security systems must also be heavily branched, with several functional units (security management, security servers, security application components, etc.). Generally speaking the systems have to be examined with a view to not only the functionalities per se but also structural and organisational aspects. It is also necessary to differentiate in respect of the specific technical placement of security components and their integration into non-security components, because this has a direct influence on the implementation of the security functions, on the support required from the operating systems, on expenditure and the cost factor, and not least on the attainable level of security. The geographical localities and the levels of the protocol stack at which the respective security services are implemented and the way in which they are incorporated in the processes of the IT system being protected are quite crucial for the security evaluation. The following questions thus arise:

- Protection offered by the environment: what protection does the environment offer (in terms of infrastructure (access), organisation, staff, technical facilities (protection by operating system, ...))?
- IT system environment: what technology is used, which operating systems, etc.?

- Data volume: what volume of data needs to be protected?
- Frequency: how often is there a requirement for cryptographic services?
- Performance: how fast do cryptographic functions have to operate (off-line, on-line rate)?

Personnel and organisational aspects

- User-friendliness: do users require basic knowledge of cryptography? Does the use of a crypto product hamper them in their work?
- Reasonableness: what burden of extra work can users reasonably be expected to take on (working time, waiting time)?
- Reliability: how reliably will users handle the crypto technology?
- Training requirements: to what extent do users need training?
- Personnel requirements: are additional staff required, for example for installation, operation or key management?
- Availability: is it possible that availability will be reduced by the use of a crypto product?

Economic aspects

- Financial constraints: how much is cryptographic protection allowed to cost? How high are the
  - non-recurring investment costs
  - running costs, including personnel costs
  - licence fees?
- Investment protection: do the planned cryptographic procedures and products conform to existing standards? Are they interoperable with other products?

Key recovery

If the keys used for encryption are lost, this generally also means that the data protected by the keys is also lost. Many crypto products therefore include functions for data recovery in such instances. Before these functions are used, it is important to be clear about the risks involved: if it is possible to restore confidential keys by these means, it must be ensured that this can only be done by those with the appropriate authorisation. If it is possible to access the original key user's data without his or her knowledge, the user has no possibility of proving that malicious manipulation has taken place. On account of the mistrust with which it is viewed, the use of key recovery mechanisms also often results in reservations being expressed within the company or organisation where they are used, but also among communication partners. Generally, therefore, key recovery should not be used in relation to data transmission. There is no need for this, either, because if a key or data is lost, it can simply be sent again. Careful thought should be given to the use of key recovery when data is stored locally (see also S 6.56 *Data backup when using cryptographic procedures*). The CD-ROM accompanying the IT Baseline Protection Manual contains an article on the possibilities and risks of key recovery in the Auxiliary Materials directory.

Life span of cryptographic procedures

Cryptographic procedures and products must be checked regularly to establish whether they still represent the state of the art. The algorithms that are used may become too weak as a result of technical developments, such as faster or cheaper IT systems, or because of new mathematical knowledge. The cryptographic products in use may exhibit implementation errors. A time limit for the use of cryptographic procedures should therefore be stipulated at the time of their selection. When the time limit is reached, a thorough review should take place again as to whether the crypto modules in use still offer the expected level of protection.

Legal framework

Various general legal conditions must be observed in relation to the use of cryptographic products. In some countries, for example, cryptographic procedures are not allowed to be used without approval. It is therefore necessary to examine the following points (see S 2.165 *Selection of a suitable cryptographic product*):

- Whether restrictions on the use of cryptographic products have to be observed in the countries belonging to the area of use (there are no restrictions of any kind within Germany)
- Whether any export restrictions applying to products under consideration have to be observed

However, there are not only maximum requirements applying to the cryptographic algorithms or procedures used, there are also minimum requirements. For example, encryption procedures with a sufficient key length must be used for the transmission of person-related data.

Examples of technical solutions:

In the following there are a number of examples of application relating to the various fields of use for cryptographic procedures. It can be seen that most products cover several fields of use at the same time.

Example 1: Hard disk encryption

The sensitive data stored on the hard disk of a standalone PC needs to be protected in such a way that the following conditions apply:

- The PC can only be booted by authorised users
- Only authorised users are given access to the stored data
- The stored data must be adequately protected against perusal by unauthorised users when the PC is switched off - also in the event of it being stolen.

The foremost priority in this case is the safeguarding of confidentiality. With this in mind, the PC is to be protected against the following threats:

- Unauthorised disclosure of the data stored on the hard disk
- Manipulation of the data stored on the hard disk
- Manipulation of the crypto system

In the event of the PC or hard disk being stolen or lost, the offender has a great deal of time available to gain unauthorised knowledge of the data. A protective measure must guarantee the confidentiality of the stored data even when subject to such extended-length attacks.

The protective measure used should therefore be a product with boot protection and hard disk encryption. Various solutions are available on the market. The choice lies between encryption software (solution A), a hardware encryption component (solution B) or a combination of a hardware component and a software component (solution C). Solution C will typically consist of encryption software in combination with a chip-card reader to provide access control. Which solution is chosen is dependent on various decision criteria:

- Security (crypto algorithm and key length, encryption operating mode, access protection, key generation / distribution/ storage / entry, integration in the operating system, etc.)

  Depending on the operating system platform on which encryption is performed, certain limits are inevitably reached with software solutions (solutions A and C). If there cannot be assumed to be a secure operating system with a strict separation of tasks and memory areas (to date, that has not been reliably proved of any operating system), the key used during encryption and decryption must be held unprotected in the memory of the PC for at least a short time. The confidentiality of the key is therefore no longer guaranteed. Hardware encryption components (solution B) may offer more (but not necessarily). The key can be loaded into the hardware component and stored there in a form that secures it against being read out. The key will never leave the hardware component again, and is protected against attempts to search it out. It can only be activated by authorised users with the appropriate ownership and knowledge (e.g. chip card and password). Other aspects are also important, such as the algorithms used for encryption (usually a block encipherment algorithm), their modes of operation (e.g. CBC) and the way in which they are integrated into the PC system. Ideally, the encryption hardware should be integrated in such a way that it compulsorily encrypts the entire hard disk and cannot be deactivated or bypassed by attacks without this being noticed. If contrary to this only individual files are encrypted, there is a risk that the contents of these files may additionally be written to the hard disk in plain text in an uncontrollable manner at least in part (for example to the swap files of various operating systems or to backup files).

- Performance (speed of executable programs)

  Software encryption utilises the system resources of the PC; it is therefore a burden on the CPU and uses main memory. At the latest when the entire hard disk is encrypted, the performance of the PC will fall. Hardware components with their own processor may perform encryption without burdening the PC's CPU and consequently without any notable loss of performance. In this respect the throughput rate of the encryption hardware used is one of the crucial factors, depending on the design.

- Organisational/personnel costs (administration, key management, training, etc.)

  Expenditure on organisational matters and personnel is dependent on the way the security policy is implemented and on the level of „convenience“ of the encryption components. General decision criteria for or against one of the three solutions cannot be formulated with universal validity.

- Economic efficiency (procurement, training/administration costs, ...)

  It is difficult to make any general statement about economic efficiency. If only the procurement costs are taken into consideration, software solutions will often be better value than hardware solutions. However, if the losses that can arise as a result of inadequate protection in the longer term are taken into account, investment in more secure and perhaps more expensive solutions may be worthwhile in comparison. Economic disadvantages may accrue in certain circumstances because of performance losses in the PC system.

- Residual risks (operating system, compromising of the hard disk key, etc.)

  Consideration of residual risk plays a significant part in the selection of a suitable encryption component. The questions that arise include:

  - What residual risks can be considered acceptable?
  - What residual risks are or can be minimised by other measures (such as physical or organisational measures)?

  It is perfectly possible to obtain several different acceptable solution options by combining various measures.

Example 2: E-mail encryption

The exchange of electronic mail (e-mail) via or within computer networks is becoming ever more important. If this involves exchanging sensitive information (for example company secrets) over unprotected networks, mechanisms to safeguard the confidentiality and/or guarantee the authenticity of messages are required. This is the purpose of e-mail encryption programs. The most widespread of these are two program packages or standards of American origin:

- PGP (Pretty Good Privacy) and
- S/MIME (Secure Multipurpose Internet Mail Extensions)

PGP is a software package that was originally available over the Internet as freeware and has therefore entered widespread use. The S/MIME standard is used in (among others) the secure e-mail applications from Microsoft, Netscape and RSA Data Security Inc.

What does an e-mail encryption program of this type have to do?

The answer is of course dependent to a certain extent on the security measures surrounding it. The requirements are no doubt at their highest when the messages are to be sent via a large, open, insecure network such as the Internet. In this case it may even be that people not known to each other personally want to communicate with each other confidentially and with authentication. What cryptographic services are required in order to be able to do this?

Confidentiality

As the messages are to be encrypted, one or more encryption algorithms must be implemented. On account of the higher performance that they offer, symmetrical procedures tend to suggest themselves.

Key management

- Creation: the keys for the symmetrical procedure must be generated by a suitable (random) process in such a way that guessing or predicting further keys is practically impossible, even if some of the preceding keys are known.
- Key agreement/exchange: as the central provision of keys by means of symmetrical procedures is out of the question in the Internet simply because of the sheer mass of potential communications partners, the use of asymmetrical procedures for key agreement and key exchange is imperative.

Authenticity

As an asymmetrical procedure is implemented anyway because of the requirements relating to key management (and non-repudiation may be required), a digital signature is used for this purpose. Signature keys should be used solely for the purpose of attaching signatures. In this connection, as is always the case when using public key techniques, the problem of the authenticity of public keys has to be solved.

Non-repudiation

Non-repudiation requires a public key infrastructure (PKI: registration of users and certification of public keys by a trustworthy third party, including rules of use). At present, however, there is no such thing as a global PKI, and it is therefore difficult to obtain a non-repudiated proof of origin for e-mails from previously unknown users. In a local network a suitable PKI would have to be created for this purpose.

Conformity with standards

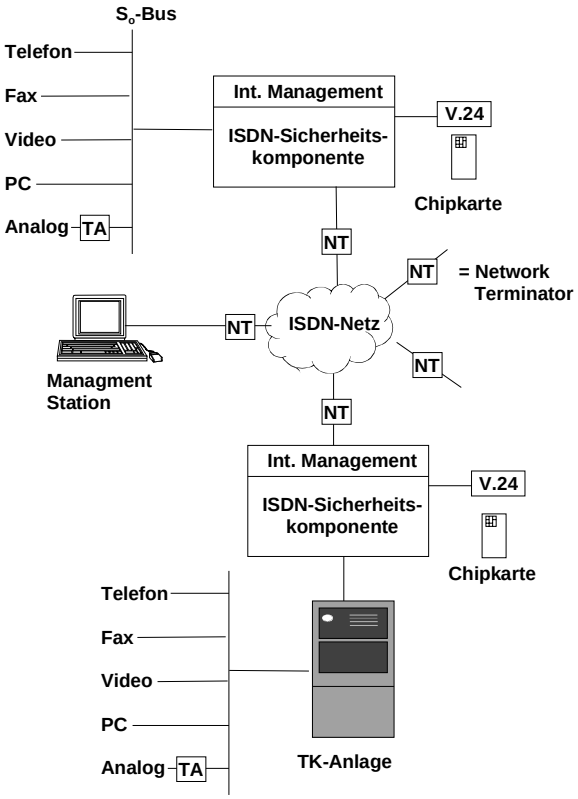
For reasons of interoperability and to protect investment, it makes sense to use Internet standards which are as widespread and broadly accepted as possible. Both S/MIME and PGP are still at the standardisation stage.

Example 3: Secure voice and data communications over ISDN network connections

The following example of application looks at communication via ISDN. The applications to be protected are speech traffic and video conferences, together with data traffic between computer networks. The aim is to ensure the effective protection of confidential information and non-repudiated personal data transferred via the connections. It is assumed that all information that is to be transmitted is available in digital form (PCM code) and that the voice compression commonly used in corporate networks and PBXs can be deactivated for encrypted applications so that the user information channels (B channels) can be encrypted.

To achieve this, an ISDN security component is to be used to protect an S0 connection with two 64 kbit/s channels. It is of no consequence whether individual ISDN terminal devices (telephone, fax, PC with plug-in ISDN card

etc.) are connected to the S0 bus or a small PBX is connected on the outgoing side. It should be possible to set up and operate all connections either with encryption or without, as required. The system configuration is shown in the illustration below.



The chosen component is an ISDN crypto device that can be protected against unauthorised use with a chip card. Alternatively there is also a serial V.24 interface available which allows the security component to be configured with the aid of a PC. The user or the end application can control encryption directly with the chip card or by preselection of a special code number. It is also possible to configure the ISDN security component in such a way that certain connections (numbers) are preset as being encrypted or unencrypted. A management station is connected at a central point of the ISDN network for the purpose of key management, i.e. the generation and distribution of key certificates. This ensures that the individual ISDN security components are registered throughout the network and can be supplied with up-to-date key material.

The possibilities available for the secure transfer of information and data worth protecting in an ISDN network are varied and complex. Every relevant basic threat must be met by a specific security measure. In order to guarantee confidentiality, online encryption of the data stream being transferred is most effectively performed on the data link layer. To achieve this, the data is automatically encrypted by crypto hardware before it is transferred, and is decrypted again at the receiving end. Encryption is entirely transparent for the end user and for application programs. The crypto module that is used not only allows real-time processing, it also provides a higher level of protection against attempted attacks in comparison with file encryption (software

solution). In order to secure the transmission of data that is binding or subject to proof, it can additionally be assigned a digital signature from the originator. In this way the source and authenticity of the message can be verified by the recipient, and any manipulation that has been carried out in the public network can be reliably detected. To ensure the secure generation and storage of the signature key, use is made once again of the chip card, which is an essential component of the security concept. One extremely important point concerning the connection of computers is the need for appropriate measures to prevent the possibility of inadvertent incorrect switching, which is not usually detected before or during the transmission – in contrast with telephone calls. This can be achieved with built-in firewall functionality in the ISDN security component. With monitoring of the signalling channel (D channel), the security component can be set up in such a way that only explicitly preconfigured crypto connections will be established. In connection with PBXs, there is also provision that certain call numbers and functions can be disabled in the exchanges. This helps to limit the extent to which the vulnerable "remote maintenance" and "call deflection" functions can be exploited.

In order to obtain both secure key management and fast real-time encryption of the user data, hybrid techniques should be used. The method of symmetrical information encryption is retained, while a key known as the session key is exchanged with the aid of an asymmetrical procedure. In practical operation, this proceeds entirely automatically. In this way it is possible to agree new session keys for every new ISDN connection without any significant detriment to operating convenience.

From the security standpoint, the end user should apply the following usage criteria and conditions when selecting and using an ISDN security component:

(Rating: + = important to +++ = very important):

- The individual user keys and authentication information must be stored on a secure medium (e.g. a chip card) and safeguarded with the aid of a trustworthy signature (+++).
- For the purpose of encrypting a communication relationship (voice, data, video, etc.), a new secret key, known as the session key, is to be agreed for each transmission (++).
- The security services are performed automatically and are fully transparent to the end system or end user (+).
- The security component is always set up in crypto mode for selected connections (+++).
- The existing infrastructure should be retained in its entirety when the security components are used (+).
- It should be possible to perform security administration for the security components on a network-wide basis and, if possible, from a central point (+).
- Online operational monitoring and registration of all security components in dialogue with the management station is desirable (+).

The ISDN security components that are selected should have standardised interfaces, should not require any changes in the terminal equipment being protected, and should be easy to integrate into an existing communications environment.

S 2.164 Selection of a suitable cryptographic procedure

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

The selection of a cryptographic procedure is divided into two subsidiary tasks:

- Selection of the cryptographic algorithm
- Selection of a means of technical implementation

Before users commit themselves to a particular procedure, they should have a precise conception of their requirements in terms of the confidentiality and authenticity of the processed data at every point of the information-processing system.

Selection of cryptographic algorithms

When selecting cryptographic algorithms it is first necessary to clarify which type of cryptographic procedures are required, in other words symmetrical, asymmetrical or hybrid procedures, and then to select suitable algorithms, i.e. those with the requisite mechanism strength.

Encryption techniques

- Symmetrical encryption: The advantages and disadvantages of symmetrical techniques are described in S 3.23. Suitable algorithms include triple DES, IDEA and RC 5 for example; in the case of RC 5 the key length should be at least 80 bits.
- Asymmetrical encryption: The advantages and disadvantages of asymmetrical techniques are described in S 3.23. Suitable algorithms include RSA, for example, or encryption techniques based on elliptical curves (see below for key length).

Authentication techniques

- Authentication of messages

  Various techniques can be used for the authentication of messages, such as a message authentication code (MAC) or a digital signature procedure. It is advantageous to use a MAC if extremely high throughput rates are required (or if only low computing capacity is available) and the risk of key disclosure is very low at both ends. It is advantageous to use a digital signature procedure if the risk of (signature) key disclosure is considerably higher at one end than it is at the other; generally it is imperative if non-repudiation services are required. It should be noted once again that an infrastructure of trusted third parties must be in place for a non-repudiation service.

  The best known MAC algorithm is the encryption of a message with DES or another block encryption technique in CBC or CFB mode. This involves appending the last encrypted block to the message as the MAC. Variants

such as these are specified in the ANSI X9.9, ANSI X9.19, ISO 8731-1 or ISO 9797 standards, for example.

Suitable algorithms for digital signatures include RSA, DSA (digital signature algorithm) or DSA variants based on elliptical curves, for example ISO/IEC 15946-2, IEEE standard P1363, Section 5.3.3 (Nyberg-Rueppel version) or IEEE standard P1363, Section 5.3.4 (DSA version).

- Authentication of users or components

  One simple method of authentication is the use of a password prompt. However, if the passwords are sent across a network without being encrypted, it is relatively easy to read them. Better techniques should therefore be used in this case. Examples of suitable techniques include:

  - One-time passwords (see also S 5.34 *Use of one-time passwords*), which can be generated with software or hardware support. Preference should be given to hardware-based authentication methods in this case, because they require less organisational work and offer greater security.
  - Authentication by means of PAP, or preferably CHAP, which are used in conjunction with the point-to-point protocol (see S 5.50).
  - Authentication by means of CLIP/COLP, which is used for communication via ISDN (see S 5.48).
  - One other familiar procedure is the authentication protocol Kerberos, which was developed at MIT (Massachusetts Institute of Technology). It is used in networks for the mutual authentication of users/clients and servers. The central authority in Kerberos is the ticket-granting server, which issues tickets by means of which clients and servers can authenticate themselves to each other. Once authentication has been completed, users can request session keys for a wide variety of services with the aid of these tickets.

Hash techniques

Suitable algorithms include MD5, SHA-1 and RIPEMD-160, for example.

Selection criteria

- Mechanism strength / key length

  One major criterion for the selection of cryptographic procedures is their mechanism strength. With symmetrical procedures a particular requirement is that the key length should be sufficiently large. The larger the key length used with a cryptographic procedure, the longer it takes to calculate it by a brute force attack, for example. On the other hand, the procedures become slower when longer keys are used, so it is always necessary to consider which key length is appropriate with regard to benefit/performance factors. As a rule of thumb for good procedures (triple DES, IDEA, RC5,...) and average protection requirements, it is currently thought that the keys used should be at least 80 bits long. When block ciphers are used, relatively large, structured quantities of data should not be encrypted in ECB mode. CBC mode or CFB mode should be used for this instead. At least one of these operating modes should therefore be implemented.

In the case of asymmetrical procedures, the chosen mechanism strength should be such that solving the underlying mathematical problems requires an unjustifiably high or practically impossible amount of computation (the mechanism strength that should be chosen is therefore dependent on the present state of algorithm development and of computing technology). Currently it can be assumed that you will be "on the safe side" with:

- module lengths of 768 bits with RSA or
- subgroup orders of the order of magnitude of 160 bits in the case of ElGamal procedures on a suitable elliptical curve

.

No "unknown" algorithms should be used, i.e. the algorithms that are used should be ones which have been published, have been intensively investigated by a broad spectrum of experts and which are not known to have any security weaknesses. Vendors frequently offer security products with new algorithms which are supposedly "even more secure and even faster" than other algorithms. However, great caution must be exercised when using unknown algorithms from sources whose cryptographic competence is not sufficiently proven.

- Symmetrical or hybrid procedures?

  For performance reasons, no implementations based solely on public key techniques are used for encryption purposes. All common implementations of public key cryptography use hybrid procedures (see S 3.23).

  In applications with large or open user groups it is usually advisable to use a hybrid procedure (because of the advantages for key management). Where user groups are small and closed (and in particular of course in the case of a single user), it is possible to keep to symmetrical procedures. If hybrid procedures are used, it makes sense to tailor the symmetrical and asymmetrical parts to work together. With the asymmetrical procedure it is generally the case that before a key change many keys for the symmetrical procedure are encrypted, so therefore the asymmetrical algorithm should normally be somewhat stronger.

- Feasibility of technical requirements

  The enciphering algorithms must be designed such that the technical requirements, in particular the required performance, can be fulfilled if a suitable implementation is put in place. These include requirements relating to error propagation (for example if data is sent via very noisy channels), but also requirements as to synchronisation overhead and time delay (for example if "real-time" encryption of large quantities of data is required).

  Example: Voice encryption with ISDN

  When a communication network is being planned, a range of parameters have to be taken into account which have an influence on the expected speech quality and which become noticeable in the form of noise, clicking, crosstalk or singing. Such influencing factors include the encryption procedures, for example. In order to be able to achieve satisfactory speech

quality, all of the equipment along a transmission path has to be examined and assessed. Although looking at a single component in isolation should not be considered justified on account of the coupling of all relevant individual effects, it is nevertheless important to be aware of the influencing factors applying to each component (such as the crypto component). The basic conditions for both implementation and selection can be derived from this knowledge. The behaviour of an encryption component is mainly characterised by the following factors:

- The period of time elapsing during encryption of a data block (generally results in delays)
- The control information inserted additionally into the data stream for synchronisation purposes (may result in fluctuations)
- The maximum data throughput to be achieved by the crypto component (also results in fluctuations if buffer storage is necessary)
- The error propagation resulting from encryption (generally results in an increase in the error rate)

In the case of voice encryption (real-time service), in particular, the above influencing factors have a negative effect in the form of an increase in end-to-end propagation time, fluctuations in propagation time and a higher error rate, i.e. in a reduction in quality which can be measured and can be attributed to the crypto component.

- Other influencing factors

Some cryptographic algorithms (such as IDEA) are patented; licence fees may have to be paid to enable them to be used in commercial applications (to which the field of government agencies etc. also belongs). This must be noted in particular when using methods such as PGP, of which there are also implementations which can otherwise be used as public domain software.

S 2.165 Selection of a suitable cryptographic product

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

The spectrum of cryptographic applications is very wide, ranging from simple programs for file encryption on a single-user PC through firewall computers with crypto functions for protecting a local network to the real-time hardware encryption of video conferences. Given this range, it is plain that recommendations on the selection of cryptographic products have been kept to generalities.

Before a selection is made, the user should determine **all** requirements that the product is expected to meet. The selected product should cover the user's requirements to as great an extent as possible.

Functionality

The selected product must exhibit the functionality specified by the user; in particular, it must:

- perform the required basic cryptographic services
- satisfy any special requirements imposed by the application environment (e.g. single-user/multi-user PC, LAN environment, WAN link)
- exhibit the required technical performance characteristics (e.g. throughput rates)
- offer the required security functionalities; in particular the cryptographic mechanisms used must be of the required strength

Interoperability

The selected product is generally incorporated into an existing IT environment. It must be as interoperable as possible within that environment. It is essential to observe internal standards in order to ensure interoperability with the IT system and system components already in place. The use of international standards for cryptographic techniques should be a matter of course; among other things it makes it easier to evaluate the security of the cryptographic component.

Cost-effectiveness

The selected product should be as cost-effective as possible. Procurement costs, the quantities required and the costs of maintenance and product updating must be taken into account, but also the savings made through any rationalisation effects.

Certified products

Over the past decades, an internationally recognised methodology for evaluating IT security products has become established: the European ITSEC (Information Technology Security Evaluation Criteria) and the subsequent development, CC (The Common Criteria for Information Technology Security Evaluation). The ITSEC and CC provide a framework within which the security functionalities of an IT product can be fitted into a precisely specified

hierarchy by the application of established criteria. The information security authorities of several countries have each set up a national certification scheme according to these criteria.

The use of a certified product provides a guarantee that the security functionality of the product has been independently tested and does not fall below the standard specified in the evaluation level (see also S 2.66 *Consideration of the contribution of certification to procurement*).

Imported products

In several countries, especially in the USA, the export of strong cryptography is at present (still) subject to severe restrictions. In particular, the strength of essentially strong encryption products is artificially diminished (by reducing the number of possible keys). These artificially weakened procedures do not generally reach the mechanism strength necessary for medium-level protection requirements.

In Germany and most other countries, cryptographic products are not subject to any restrictions when used within the national boundaries. When imported products are used, attention should always be paid to whether they provide the full range and scope of capabilities.

Transnational use

Many companies and agencies are increasingly faced with the problem that they also want to secure their international communications, for example with overseas subsidiaries, by cryptographic means. First it is necessary to examine the following points:

- Whether restrictions on the use of cryptographic products have to be observed in the countries concerned
- Whether any export or import restrictions applying to products under consideration have to be observed

Security against improper use and malfunctions

The dangerous aspect of cryptographic products is that they lull users into a (sometimes false) sense of security: no problem: it’s all encrypted"! This is why measures against being compromised as a result of operating errors or technical failure are particularly important, because their consequences cannot be limited to a simple defect but may immediately lead to a security breach. However, there is a large range in terms of redundant system design and additional monitoring functions - and hence equipment costs - so that in this regard the measures have to be determined in each individual case, in accordance with requirements.

Implementation in software, firmware or hardware

Cryptographic algorithms can be implemented in software, firmware or hardware. Software implementations are usually controlled by the operating system of the respective IT system. The term firmware covers programs and data which are permanently stored in hardware in such a way that the stored contents cannot be dynamically altered, nor can they be modified during execution. Hardware solutions entail the implementation of cryptographic

procedures directly in hardware, for example as a separate security module or as a plug-in card.

It is not possible to offer any general recommendation on which type of implementation should be chosen, because various factors have to be weighed up before the decision is made:

- The protection requirements applying to the data to be protected by the cryptographic procedure, or the security level aimed for
- The intended data throughput
- Economic considerations and constraints
- The operating environment and surrounding safeguards
- National classification of the data being processed, if applicable

Software solutions offer the advantage of being easily adaptable and low-cost. Hardware implementations generally offer both greater resistance to manipulation (and therefore greater security) and a higher throughput rate than software implementations, but they are usually also more expensive.

Firmware solutions can be seen as a compromise between the two other options. However, the advantages and disadvantages of each implementation always relate only to local aspects (including key management, above all). Once the data has been encrypted and is on the communication path, the way in which the encryption came about is essentially no longer relevant.

One example of (relatively) inexpensive, transportable and user-friendly crypto modules is chip cards, which can be used in the field of local encryption as a secure storage medium for cryptographic keys or in the field of authentication for password generation and encryption.

When all of the requirements to be met by the cryptographic product have been defined, you have at your disposal a portfolio of requirements which can then also be used directly in an invitation to tender, should one be necessary.

S 2.166 Provisions governing the use of crypto modules

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

A range of security requirements on the use of crypto modules also has to be imposed in the course of ongoing operation. These must be appropriately integrated into the technical and organisational environment in which they are used.

To achieve this, certain organisational regulations have to be put in place:

- Certain members of staff must be nominated as having responsibility for drawing up the cryptographic concept, for selecting the cryptographic products and for ensuring their reliable operation.
- Suitable personnel measures must be specified and implemented (training, user support, deputisation arrangements, obligations, apportioning of functions).
- Users should not only be trained in how to handle the crypto modules that they are to operate, they should also be made aware of the benefit and the necessity of the cryptographic procedures and be given an overview of basic cryptographic terms (see also S 3.23).
- There must be a clear definition of what needs to be done if problems occur in the use of crypto modules, or if there is even a suspicion of a security incident. All users must be informed of the relevant procedures and reporting channels.
- Within the framework of the cryptographic concept it must be established who is obliged or allowed to use which crypto products when, and what marginal conditions need to be observed (e.g. key escrow).
- There should be regular checks that the crypto modules are being used correctly. It should also be regularly examined whether the cryptographic procedures in use still represent the state of the art (for further details see also S 2.35 *Obtaining information on security weaknesses of the system*).
- Replacement crypto modules should be held in reserve in accordance with the defined availability requirements, in order to guarantee smooth operation. This is important in particular where access to encrypted data is dependent on the functional capability of an individual crypto module, for example in the case of data archiving or ISDN encryption.

Reliable, secure operation of the crypto modules must be ensured; this includes:

- Before they are put into operation, the optimum configuration of the crypto modules must be determined, for example regarding key lengths, operating modes or crypto algorithms.
- Once defined, the configuration must be documented so that it can be set up again quickly after a system failure of if reinstallation becomes necessary.

- The crypto products must be pre-configured by the administrator for the users so as to automatically achieve the maximum possible degree of security.
- If the crypto products are relatively complex, suitable manuals must be available.
- The crypto modules must be securely installed and subsequently tested (for example whether they encrypt correctly and whether they can be operated by the users).
- The demands on the usage environment must be determined; if necessary, supplementary measures may have to be taken in the IT environment. The security-related requirements applicable to the IT systems on which the cryptographic procedures are used are shown in the respective system-specific modules, for example Chapter 5 for clients (including laptops) and Chapter 6 for servers.
- It must be determined who has to maintain the crypto modules, and how often.

Various specifications also have to be laid down in relation to key management (see S 2.46 *Appropriate key management*):

- Specifications on the generation and selection of keys
- Specifications on the secure storage of cryptographic keys
- Stipulation of the key change strategy and intervals

Additional controls:

- Have regulations been defined for the use of cryptographic procedures?
- Is the crypto concept up to date?
- Who is responsible for answering users' queries concerning the use of crypto modules?

S 2.167 Secure deletion of data media

Initiation responsibility: Head of IT Section

Implementation responsibility: IT Procedures Officer

A regulated procedure for the **deletion** or **destruction** of data media will prevent misuse of stored data. Before data media can be reused, the stored data must be fully deleted, for example by being completely overwritten or by formatting the media. This is especially important when data media are to be passed on to third parties. After receiving the data medium, the recipient must also check whether the protection requirements of the data require the data medium to be erased immediately after the data has been transferred to another IT system.

There are various different methods of deleting information from data media, for example with deletion commands, by formatting, by overwriting or by destroying the data medium. The method that should be chosen is dependent in this case, too, on the protection requirements of the data to be deleted; protection against the restoration of residual data increases in the order shown below.

Deletion commands

When deletion commands are used, especially in DOS-based operating systems it should be noted that the file information is not in fact deleted at the same time, only the reference to that information in the table of contents on the data medium. The file remains available. There are a large number of programs which can be used to restore the information that is believed to have been deleted (such as UNDELETE in DOS).

To delete files irrevocably, all entries on the data medium must be overwritten. Programs such as PC Tools ("Overwrite" option to overwrite data media or WIPE program to overwrite individual files) or Norton Utilities (WIPEINFO program) can be used for this purpose.

Formatting

To return data media to their original state and therefore also to erase any information that they may contain, they can be formatted. How reliably the old data is deleted by this, however, is heavily dependent on the underlying operating system. Whatever the case, overwriting the old data is more reliable.

When DOS data media are being formatted, care should be taken for example that the parameter */U* (e.g. as in DOS 6.2 *format a: /U*) is used so that the formatting process cannot be reversed by the *unformat* command. For the same reason, formatting under Windows 95 and Windows NT must be executed with the parameter *complete*, and not *quick-format*.

Overwriting

Physical erasure sufficient for medium-level protection can be achieved by overwriting the entire data medium or at least the used sectors with a certain pattern. Certain commercially available products even allow the physical erasure of individual files.

Uniform patterns such as "0000" should not be used for overwriting, but rather patterns such as "C1" (hexadecimal, corresponds to the bit sequence 11000001). Following on from that, in a second pass a complementary pattern (for example 3E, corresponding to the bit sequence 00111110) should be used so that if at all possible each bit has been changed once.

The overwrite procedure should therefore be repeated at least twice, or preferably three times, as this provides a better protective effect.

Of course, write-protected media or media that cannot be written to more than once, such as CD-ROMs or CD-Rs, cannot be deleted and should be destroyed.

Erasing devices

Flexible magnetic data media (floppy disks or tapes) can be erased with an erasing device. These devices expose the data media to an external constant or alternating magnetic field (erasure by magnetomotive force). Suitable erasing devices which conform to DIN 33858 are listed in BSI publication 7500.

Basically the data media are reusable after they have been erased. It should be noted, however, that data media with a magnetically recorded servotrack (e.g. IBM 3590, Travan 4 and MLR tape cartridges and ZIP disks) are unusable after erasure.

Erasing hard disks

If hard disks containing sensitive data are to be passed on to third parties they should also be erased, especially if they are removed from service or sent for repair. It should also be borne in mind that passing on "cleaned-up" hard disks which contain only the operating system and standard software is liable to give rise to licensing problems.

Hard disks that are to be erased should therefore undergo low-level formatting at least. To do this, first all existing partitions should be deleted (under DOS with the *fdisk* command) and one large partition should be created. Then the entire hard disk should be formatted (under DOS with the *format /U* command).

As an additional security measure, new data can then also be loaded onto the hard disk, for example pattern sequences with the WIPE program.

If a relatively large number of hard disks (of identical type) need to be erased, as an alternative first one hard disk can be overwritten with a pattern and this can then be copied to all other hard disks with an image copying program.

If the hard disk is faulty, erasure by overwriting is no longer possible. The only option is therefore erasure with an erasing device, even though these devices are not intended for erasing hard disks. Due to the differences in the design of hard disk drives, in particular the number of disks, no general comments can be made on what erasure effect can be achieved. Using an erasing device on a hard disk usually makes the disk unusable.

Destroying the data media

A simple method of destroying data media is the cutting up of diskettes/magnetic tapes and the mechanical destruction of hard disks.

However, if there are rather large quantities of data media to be destroyed this is too cumbersome, nor is it adequate if protection requirements are high.

Suitable devices for destroying magnetic tapes, floppy disks and CD-ROMs in conformance with DIN 32757 are listed in BSI publication 7500. These destruction devices either shred or melt down the data media. There are no known destruction devices for hard disks.

Additional controls:

- Is there are a standard procedure for erasing data media?

S 2.168 IT system analysis before the introduction of a system management system

Initiation responsibility: Head of IT Section

Implementation responsibility: Administrators

Before a system management system is introduced, the IT systems that are to be administered in future must be examined and analysed. The resulting system documentation can then be used as a basis for planning and decision-making for the system management strategy being defined (see S 2.169) . It is important that if possible all relevant information about the administered systems should be available at the planning stage so as to rule out the possibility of wrong decisions being taken because of a lack of information. Specific requirements that have to be met by the management system being purchased can also be formulated on the basis of the local circumstances (K.O. criteria).

The following measures (and subsidiary measures described with them) have to be taken, ideally during planning and during ongoing operation of the system in accordance with the Baseline Protection Manual:

- Survey of the existing network environment (see S 2.139)
- Documentation of the system configuration (see S 2.25): All IT systems should be recorded and documented. Especially in heterogeneous systems, for example, details of all operating systems in use must be noted so as to be able to formulate the requirements that the management system has to satisfy.
- Determining and reviewing the software inventory (see S 2.10): If the system management tasks are also to include the administration of software (application management), an inventory should be taken at this stage. Alternatively, automatic establishment of the software inventory ("autodiscovery", "software discovery") can be formulated as a requirement for the management system . Which of the two variants is required in each individual case is dependent on the duties to be performed in software management. For example, if the management system is acquired for the purpose of automatic management of an existing software inventory whose composition is not entirely known (because of software updates or new software being loaded), the management system must be capable of detecting the software inventory automatically after it is installed. If individual software packages are also to be administered at the application level within the framework of application management, it is necessary to examine whether the software actively supports this (for example with a suitable protocol), which means that a prior inventory of the existing software is required. Requirements then arise as to the functional scope of the management system being acquired (such as support for the application administration protocol). If a Web server is to be administered via an HTTP-based management interface, for example, the management system must have HTTP-based management functions itself or provide an expansion interface which allows the integration of your own developments.

In addition to documentation of the current situation, future planning for the IT system must also be taken into account because a management system should also be designed to allow for changes to the IT system in the future (e.g. scalability).

S 2.169 Developing a system management strategy

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section, Administrator

Administrators have to carry out regular administration work on the components in a network. The duties to be performed range from setting up new users to installing new software; the distributed nature of the software requires the installation of part software on each individual computer (workflow system, document management system, etc.). In large organisations merely setting up a new user who is supposed to be able to log on at all computers to which he or she has access means a great deal of administrative work, because if the computers are run in stand-alone operation each one has to be configured accordingly. Today's network-capable operating systems (such as Unix, Windows NT or Novell) therefore include mechanisms that are intended to reduce the amount of administrative work (for example central user administration). However, if the administration of all hardware and software components in a local network is to be performed in a uniform manner at all levels (in both technical and organisational terms), technical aids in the form of management systems must be employed, but whether or not they are used successfully is also dependent on the management strategy that is to be drawn up. The specifications and rules imposed by the management strategy are then put into practice by system administration with the aid of the management software. Each management strategy must be adapted to the needs of the respective company or agency on a case-by-case basis. This entails working through the following steps.

Determining the objects to be administered by the management system

After the inventory has been taken (see S 2.168 *IT system analysis before the introduction of a system management system*) it must be established which areas of the IT system are to be administered by the management system that is to be procured:

- Which computers and other hardware are to be incorporated in the management system?
- Which software is to be included?
- Which users and/or user groups are to be included?

Determining the security guidelines to be applied in the management system

In addition to these decisions, existing regulations and methods also have to be incorporated into the system. For example, the established security policy at the agency or company, the privacy protection guidelines and the guidelines on the introduction of new software have to be brought into the management concept because the regulations currently in force also have to be observed and implemented when a management system is put in place. Rules also have to be adopted on the use of the management system itself, or the validity of existing rules has to be examined, and where necessary they must be adapted before being applied. This applies in the following fields, in particular:

- Access rights to management information
- Documentation of the management system
- Drafting or adjustment of emergency plans to deal with the failure of the management system or individual components

The response to violations of security policies in the field of system management should also be determined in advance. In much the same way as in other fields of IT, a security policy must be defined for the field of system management or the company's or agency's existing security policy must be applied to the field of system management. As a management system interacts with important network and system components and administers and monitors their operation, violations of the security policies in this sphere are to be viewed particularly seriously. In particular, provisions and procedures must be defined which will be deployed in the event of any such security violation. These are on the one hand technical (for example assigning new passwords for all users after compromising of the management console), but also of an organisational nature.

Auditing, data privacy officers and IT security management should become involved during the planning phase. After the management system is introduced, the duties incumbent upon them in relation to the management system must be clear. Example: the data privacy officer can pay attention to the observance of the privacy protection guidelines during the planning phase, for example monitoring which user information is intended to be or allowed to be recorded as part of the system management process. After the system is introduced, the privacy officer must also be in a position to check the observance of the guidelines. Much the same applies to the areas of responsibility of the auditor and the IT security officer.

Determining the boundary conditions for selecting the management system product

The introduction of a system management system calls for extensive and careful planning. Parts of the system management strategy are also dependent on whether or not they can be implemented with a specific product. Consequently the drafting of the management strategy and the selection (or preselection) of a product must be reexamined.

The following points should be taken into consideration when drawing up the system management strategy:

- Is more than one management domain needed? If so: how are they to be formed? Management domains allow the components of the administered system to be divided into groups. The individual groups can be administered separately from each other. Breaking a system down into various management domains is not obligatory for small or medium-sized systems, but it does encourage structured system management. For large systems, dividing the system into various management domains is generally a necessity. The planning of the management regions is dependent on a number of factors:
  - Network topology

For medium-sized systems, in particular, it makes sense to divide the system into management domains in accordance with the actual network topology (especially if there are no differences in areas of responsibility, for example).

- Organisational responsibilities within the company or agency

  The organisational structure can be emulated by the management system, giving rise to domains such as "Accounting", "Programming", "Production Division" or "Software Development Division", for example.

  Security-related factors which have an effect on management policy can also result in the creation of multiple management regions. This is the case in particular when management tasks for certain organisational units need to be delegated, without the local administrator being given access rights to the management functions for the components outside his or her sphere of responsibility.

- Existing infrastructure

  Examples of factors to be examined include the geographical distribution of branches or the spatial distribution of work teams across the storeys of a building.

- Safety considerations

  - Multiple management regions may be necessary if the management product supports different encryption mechanisms for each region but normally only one mechanism can actually be used per region. If different mechanisms are indeed used between individual management components, multiple management regions are necessary. Example: The system being administered comprises several database servers with sensitive data and the associated clients, which do not store data themselves. The management console should always communicate with the servers using strong encryption, because the databases are also administered via the management system. Communication with the clients, on the other hand, should be only weakly encrypted, for performance reasons. In this case it is normally necessary to create two management regions: one region containing the servers and a second region containing the clients.

  - Multiple management regions increase reliability, because for example in the event of the failure of one management region the other regions can continue to be administered independently of the failed region.

  - The number of computers to be administered per management region also has an influence. Most products give recommendations as to the number of computers that can be administered by the management server of one region. A figure of 200 computers per server is not unusual, however.

- What types of computer should be used as management servers? There can generally be expected to be performance losses as the number of clients connected to one management server increases. This must be taken into consideration when planning.
- What physical arrangement must the management servers have, and where will they be installed? The location of a server has an influence on, for example, how computers that are to be administered by the server are connected to it via the network. On some platforms, for example, there are minimum requirements for the communications bandwidth between the server and clients (e.g. TME 10 does not support the linking of clients via lines rated lower than 14.4 kbps). This has direct consequences on the possible management system configuration, and may make it necessary to purchase new computers or expand network connections.
- Are gateways or proxies necessary, which allow hierarchically structured management and/or connection to products from third parties?
- Some systems distinguish between what they refer to as managed nodes and endpoints. Both of these are workstations, but they differ in terms of the way they are integrated into the management system: endpoints, for example, in contrast with managed nodes, do not maintain a local database of their own with management information, nor can they be used for forwarding management information to other computers. It has to be decided which machines are to be incorporated into the management system as managed nodes and which are to be administered merely as endpoints. Generally speaking, most workstations should be included as endpoints.

The management strategy drawn up in this way necessarily brings with it a series of demands on the management product that is to be purchased. Specific product selection can be made by weighting the requirements. The management strategy must then be examined to determine whether it can be implemented in full with the available range of functions. It may be necessary to reformulate the strategy in certain areas as a result. Example: product selection reveals that the system that supports strong encryption unfortunately does not allow the delegation of administration tasks to subadministrators. The management strategy has to be adapted as a result (assuming the weighting of the requirements is correct).

S 2.170 Requirements to be met by a system management system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The purpose of a system management system is to provide support to an administrator of a local network (or virtual local network). A system management system therefore has to satisfy certain prerequisites in order to be able to give the administrator appropriate support. The requirements that any such system has to meet, however, are substantially dependent on the planned use (see S 2.169 *Developing a system management strategy*) and on the chosen architecture of the system management system (see S 2.171 *Selection of a suitable system management product*).

A system management system should provide the following functions:

- User management

  This includes adding, changing and deleting user accounts and group accounts.

- Policy management

  It should be possible to manage access rights both for access to and from the local network and for access to and from the Internet.

- Software management

  The system management system should allow the addition, deletion and updating of software components.

  As well as this, the automatic detection of installed software may be important, especially during the introductory phase. Although the administration of software licenses would be desirable, this is rarely supported by today's systems (see also application management below. Exception: licenses may be available in the form of files, so it may be possible to manage the license files within the framework of the file distribution mechanisms of a management system).

- Determination, modification and administration of system configuration data

- Administration of application data

  It must be possible to manage files in a database system or configuration files belonging to an application so as to allow the distribution of a new version of a database, for example, or the distribution of new configuration files.

- Monitoring of system components

  This may also make sense for external components which are not subject to an administration system of their own, for example for the router of an Internet service provider (ISP) via which an Internet connection is implemented.

- Application management

  It should be possible to manage software at the application level, for example to manage HTTP access rights to the data on a WWW server (the realm). This form of management is generally hardly supported at all, because the co-operation of the application itself is required for this.

Ideally, a system of this type would allow the delegation of administrative tasks, such that for example a system administrator could grant a workgroup system administrator the right to install software on the workgroup's computers. This mechanism is necessary in medium- to large-sized networks, in particular.

Network and system administration is normally performed by the same administrative units within a company or agency. As the division of duties between network administration and system administration is not clear in some areas, it is advisable to have regard for the extent to which an existing network management system can be integrated into the system management system that is being procured.

In addition to these mainly functional requirements, there are also technical requirements among the criteria that are relevant to the selection of system management software (see S 2.171). Of these, the following are particularly worth pointing out here:

- The management system must be capable of supporting the operating systems of all of the computers used for management and all of the computers being managed (operating-system-specific components of the management system, graphical user interface).
- If a local database system is already in place, the management system should have the possibility of storing its management information in the existing database system.
- The management system should be expandable. This relates on the one hand to the components of the management system (e.g. a modular concept with the possibility of purchasing and integrating additional modules at any time), but also to the function of the management system (e.g. programming API, to be able to connect in-house components).

Generally speaking the criteria for the categorisation of requirements described in S 2.171 can be used within the framework of this safeguard. For selected categories the requirements are obtained by specifying a stipulation within the scope of the particular "range of values".

S 2.171 Selection of a suitable system management product

Initiation responsibility: Head of IT Section

Implementation responsibility: Administrators

After the current system situation has been surveyed (see S 2.168) and the management strategy determined (see S 2.169), a suitable system management system must be selected. Depending on the size of the system to be managed, different implementations may be appropriate here:

- For small systems, system management can be handled „manually“ by the system administration team.
- For small and medium-sized systems, system management can also be performed by a collection of individual tools.
- A system management system should be used for large systems.

Today’s network-capable operating systems normally already incorporate functions which allow the central administration of users and user groups, for example. In the Unix world, NIS or NIS+ could be named in this connection, for example, while in the Windows world the Windows NT domain concept allows central user administration via the domain controller. Novell also offers similar opportunities with Intranetware. Generally there are also possibilities of running a network-wide policy management system.

In relatively small or medium-sized networks, on the other hand, software management, management of computer configurations and the monitoring of system components are the most pressing problem areas. In this case additional software tools can then be used which can take over the individual tasks. Consideration can be given to using a network management tool, especially in areas that are also covered by the disciplines of network management (configuration management, monitoring).

Various tools could be mentioned for the Windows environment, such as the Novell Zero Administration Kit, which supports administrators in the installation of new computers, the Microsoft Management Console, which provides a uniform centralised view of all administration tools, and the Microsoft Systems Management Server (SMS). The SMS product, for example, offers administrators the following possibilities:

- Drawing up inventories of hardware and software components
- Installation and distribution of data and applications on network computers
- Checking the execution of network applications
- Support for the administration of computers via the network
- Monitoring of network traffic

SMS is not designed for a heterogeneous environment, however. Moreover, remote maintenance is only semi-automatic and requires an administrator to be available on site, which means that its use is only appropriate for relatively small and geographically compact networks.

In the Unix world, "rdist" is a program that can be used for the administration and distribution of software, for example, enabling software to be installed or updated on remote computers. One feature is that it is possible to pick out from a central software pool precisely those products which staff require to perform their particular tasks and install them on the relevant computers. Other add-on programs, some of them available free of charge (usually from the university world), allow monitoring of the network via SNMP, for example.

Solutions assembled in this way provide a cost-effective alternative for relatively small and medium-sized networks. Generally, though, they are dependent upon a skilled administrator, someone who in some cases may make adaptations to local circumstances with extra programming, or who is able to integrate additional functionality.

Such solutions are unsuitable for larger and very large networks, however, because the functionalities are incorporated in various non-integrated tools. The only practicable solutions for large corporate or agency networks are system management systems. Before any such system is introduced, it should be noted that this generally constitutes a considerable intrusion into the running system and must be well planned. It is not rare for the introduction to take more than 12 months, with investment of at least a six-figure sum for relatively large networks. It is therefore important to choose well suited management system. The following criteria should be taken into account when choosing the system to be procured:

- What range of functions does the product offer?
- Costs
  - Purchasing the software
  - Purchasing additional hardware (in some systems one or more central management servers will have to be purchased)
  - Installation and operating expenses (in some cases it may even be necessary to employ external staff)
  - Training of staff
  - Miscellaneous (e.g. migration costs on an existing platform, adaptation/new development of local software, building work – for example a secure server room)
- Safeguarding of investment
  - To what extent is the system management product scalable (e.g. number of computers expandable)?
  - Can the platform grow with the company (e.g. number of possible management domains, delegation of tasks)?
  - What are the migration paths to the platform?
  - What are the migration paths from this platform to another platform?
- Possibility of integration with other products
  - Which server and client system platforms are supported?

  - Can an existing network management system be integrated into the system?
  - Can an existing data backup system be integrated into the system?
  - What applications from third parties are available for this product?
- Reliability and security against failure
  - Are there any statements or even guarantees as to maximum downtimes?
  - Is it possible to hot-swap central components?
  - Does the system have its own backup and recovery mechanism? In the event of failure of the management system, there must be mechanisms for regulated restarting within the management system. These may include the loading of data from a backup and automatic checking of consistency – ideally with the resolution of conflicts if inconsistencies are detected.
  - Are updates regularly made available? Are they easy to install?
- Security: restrictions for accessing management functions
  - Can access be restricted at the user ID level (which user is allowed to do what)?
  - Can access be restricted at the component level (which computer is allowed to do what)?
  - Can access to executable commands be restricted on a user-dependent or system-dependent basis?
  - Can administration tasks be divided up? For example, can the administration of components be restricted to certain areas (e.g. only the department computers)?
- Security: administration of computers via the network
  - How is remote access secured?
  - Can remote access be performed using encryption?
  - Is it ensured that (strong) authentication is required before remote administration is carried out?
  - Is it possible to restrict the authorisation for remote administration to certain individuals or roles?
  - Is the user automatically informed of remote accesses?
- Security: data integrity, privacy protection
  - Is the data that is gathered securely stored (access restrictions, encryption)?
  - Does data transfer between the management components take place on a secure basis (authentication, encryption, protection of integrity)?

  - Can the type of information that is gathered be regulated (anonymisation, tracking, provability)?
  - Is it possible to integrate virus scanning programs?
  - What possibilities are provided for logging?
  - Can local software loading be monitored or prevented?
- User-friendliness
  - Does it have a graphical user interface (e.g. X-Windows, Motif, Windows interface, Web browser)?
  - How easy is navigation?
  - Is the local language supported, or (if the system is used globally) multiple languages?
  - Are programs easy to execute (also on remote computers)?
  - How easy is it for the user to adapt the interface?
  - Is there appropriate indication of exceptions and alarms?
  - Is monitoring adjustable, including the level of detail?
  - Is the complexity of network components suitably "hidden" (such that the user does not have to be an expert on the component currently being managed)?
  - Can all functions be accessed via the same user interface?
  - Are user guides and online help available?
- Ergonomics in the management of complex systems
  - Are different network protocols, network components and operating systems supported?
  - How does the platform deal with geographically distributed systems and how are they represented?
  - How easy is it to integrate new components or to remove components from the system (by autodiscovery or manually)?
- Conformity with standards (depending on the environment, conformity with at least one standard may be necessary)
  - Platforms
    - Distributed Management Environment (DME) from the Open Software Foundation (OSF)
    - Specification of the Desktop Management Task Force (DMTF)
    - OMNIpoint specification by the Network Management Forum (NMF)
  - Database
    - Which DBMSs (database management systems) are supported?

  - Is SQL supported as a query language, assuming that the management software includes its own database?
- CORBA (Common Object Request Broker Architecture) from the Object Management Group (OMG)
- Application Programming Interface (API), in case the company or agency needs to add its own extensions to the management system (e.g. APIs for SNMP, XMP, DMI)

The considerations listed above are meant to be used as pointers in the assessment of management systems. The requirements to be met by the management system should be formulated in accordance with the local conditions and on the basis of the current system situation (see S 2.168) and the specified management strategy (see S 2.169); these can then be used as K.O. criteria when taking the decision. The above criteria should always be assigned a weighting to reflect local preferences.

It is not usually possible to fully reconcile the requirements that the management system is expected to meet and the services provided by the chosen management system. This means that after a specific product has been selected it is necessary to adapt the existing management strategy to the functional scope of the product.

S 2.172 Developing a concept for using the WWW

Initiation responsibility: Agency/company management; IT Security Management

Implementation responsibility: Head of IT Section, Administrator

Before use is made of WWW services, a concept must first be drawn up describing which services are to be used and which are to be offered. This must include consideration of how the WWW server will be secured, as well as the WWW clients and the communication links between them.

WWW servers can be used solely as an internal information database, as the central point of an intranet, or as an external WWW server that offers a variety of services. The security demands made of the WWW server also vary according to the form that the planned implementation is to take.

In a small organisation in which a WWW server is operated as an intranet server with no critical applications, the requirements are quite different from those imposed on a WWW server that is to be connected to the Internet and perhaps even contains data that should not be retrievable by just anyone.

If it is intended to offer WWW services both in the intranet and on the Internet, it is advisable to use two separate systems: one intranet WWW server and one Internet WWW server. If it is intended to connect the Internet WWW server to the internal network, the connection to the internal network must be protected by a firewall. Factors which have to be taken into account regarding the configuration of information servers are also described in S 2.77 *Secure configuration of other components*.

The connection to the Internet can only be implemented when it has been checked that all risks can be handled by the chosen WWW concept and the personnel and organisational conditions.

A WWW server used for an organisation’s Internet presence does not have to be operated by the organisation itself. If the running costs or administration costs are too high, or if the residual risks appear too incalculable, it is also possible to make use of the services of Internet service providers or other service companies and have them operate a WWW server.

S 2.173 Determining a WWW security strategy

Initiation responsibility: Agency/company management; IT Security Management

Implementation responsibility: Head of IT Section, Administrator

WWW servers are highly attractive targets for hackers, because a successful attack often attracts a great deal of publicity. The provision of security for a WWW server must therefore be given a high priority. Before a WWW server is set up, a WWW security strategy must be defined describing which security measures need to be implemented, and to what extent. The requirements specified in the WWW security strategy can then be used as a basis for regular checking of whether the measures taken are in fact adequate.

The WWW security strategy must include a security strategy for the use of the WWW as well as a security strategy for the operation of a WWW server.

WWW security strategy for the operation of a WWW server

The security strategy for the operation of a WWW server should provide answers to the following questions:

- Who is allowed to load which information onto the server?
- What boundary conditions need to be observed when operating a WWW server?
- How are the staff responsible for the server trained, in particular with regard to potential hazards and the security measures that have to be observed?
- Which files are not allowed to be placed on the WWW server because of their content (for example because the content is confidential, not suitable for publication or is not in line with the company's or agency's policies)?
- What restrictions on accessing the WWW server need to be implemented (see also S 2.175 *Setting up a WWW server*)?

One part of a security strategy also has to be the regular gathering of information about potential security weaknesses so as to be able to take precautionary action in good time. In addition to the information sources mentioned in S 2.35 *Obtaining information on security weaknesses of the system*, the "World Wide Web Security FAQ" in particular is a valuable source of security tips on using the WWW. The master copy of this document is to be found at *http://www.w3.org/Security/Faq/*.

WWW security strategy for using the WWW

The security strategy for using the WWW should provide answers to the following questions:

- Who is given access to the WWW?
- What boundary conditions need to be observed when using the WWW?
- How will users be trained?
- How is the availability of technical assistance for users ensured?

Organisational rules or technical measures are required in order to meet the following conditions, in particular:

- The browsers intended for users should be pre-configured by the administrator so as to automatically achieve the highest possible level of security without further intervention by the users (see also S 5.45 *Security of WWW browsers*).
- Files whose content is liable to cause offence must be neither placed on nor retrieved from WWW servers. It must be established what type of content is considered offensive.
- After files have been downloaded, they must be explicitly checked for computer viruses.

All rules and instructions concerning the use of the WWW must be specified in writing and should remain available to employees at all times. A sample of such rules is given on the CD-ROM accompanying the IT Baseline Protection Manual, in the Auxiliary Materials directory.

In order to prevent operating errors and to ensure observance of the organisation's internal guidelines, users must be given training before they use the WWW, both in operation of their WWW browser and in the use of the Internet. In particular, they must be made aware of potential hazards and of the security measures that have to be observed.

Supplementary checks:

- Is there a security strategy for the operation of a WWW server?
- Is there a security strategy for the use of WWW services?
- Are the arrangements that have been made adequate?

S 2.174 Secure operation of a WWW server

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

WWW servers are attractive targets for attackers and therefore have to be very carefully configured so that they can be operated securely. The operating system and the software must be configured in such a way that the computer is given optimum protection against attacks. The computer must not be connected to the network until such time as it is appropriately configured.

A WWW server that offers information on the Internet should be installed in accordance with the following stipulations:

- Only a minimum of programs should be installed on a WWW server, i.e. the operating system should be reduced to those functionalities that are absolutely essential and otherwise, too, only programs that are really necessary should be installed on the WWW server (see S 4.95 *Minimal operating system*).
- In particular, a WWW server should not include any unnecessary network services; different services should be installed on different computers (see S 4.97 *One service per server*).
- Access to files or directories must be protected (see S 4.94 *Protection of WWW files*).
- Communication with the WWW server should be restricted to a minimum through the use of a packet filter (see S 4.98).
- Administration of the WWW server should always be performed via a secure connection; this means that administration should be performed directly on the console, with strong authentication (if access is from the LAN) or via an encrypted connection (if access is from the Internet).
- Furthermore, the WWW server should be secured from the Internet by a firewall proxy or at least by a packet filter (see S 4.98). This must not be located between the firewall and the internal network, because an error on the WWW server could otherwise allow access to internal data.

There are various possible methods of providing protection, depending on the type of WWW server. A common feature of all of these methods, however, is that only a restricted set of rights should be assigned to the WWW server's actual server process, namely the http daemon. Usually it must be started with root privileges, but after being started it should continue operating as quickly as possible with the rights of a less privileged new user. A separate user account, such as *wwwserver*, should be created for this purpose. It is important that this user should not have any rights to write to the log files. Otherwise an intruder could manipulate these files using the rights of the HTTP server by exploiting an error.

If an intruder does exploit a weak point in the http daemon, therefore, he will not have access to the operating system as such. If possible, the http daemon should be restricted to part of the file tree. Under Unix, this can be done with the *chroot* program, for example. Besides this, the cgi programs supplied with

the system by the manufacturer should be entirely removed, because errors have repeatedly appeared in these programs in the past.

The directory in which the retrievable files are stored should be located on a separate partition of a hard disk so as to make it easier to restore it after a hard disk defect. Moreover, the subdirectories and files should belong to a specific user (for example *wwwadmin*) and be protected against unauthorised access by being given minimum access rights.

During configuration of an HTTP server, a number of options should be taken into account which are relevant to security. These include, for example:

- Listing directory contents

  This option should be deactivated. If the complete contents of a directory are disclosed to the outside, it is often the case that too much information is divulged. This is dangerous in particular if the directory contains files whose existence is not supposed to be made known externally, i.e. password files, for example, or files that are not generally accessible. It is better to use index files in order to make the contents of directories known externally.

- Use of symbolic links

  This option should be deactivated, because symbolic links can be used to gain access to files outside the approved Web directory. During the configuration of the server, the area which the server is allowed to access in order to disseminate files via HTTP is specified as the DocumentRoot. Files outside the DocumentRoot and the cgi-bin directory are not disseminated, even if the HTTP daemon possesses read rights.

  If it is necessary to make the same document accessible via various URLs, it is more advisable to use the route via a Redirect in the *.htaccess* file.

- Anonymous use of the server

  Even if user-defined access protection is set up on a WWW server, it is often also desirable to grant access to new, as yet unknown users, i.e. to new customers, for example. Provision can be made for anonymous access for this purpose. To gain access, a user can either not log in at all or log in with his or her e-mail address as the password. If this is wrongly configured, however, the entire contents of the server may be freely available as a result. This option should therefore be used with particular caution.

The following checklist is recommended:

1. Are only necessary components installed? It is advisable to compile the http daemon yourself; in that way, unnecessary functions will not be compiled in the first place.
2. Is the http daemon configured to be as restrictive as possible? Either cgi programs should be entirely disabled, therefore, or the cgi programs should be restricted to their own directory. File access by the http daemon should be limited to part of the directory tree. Separate, unprivileged user rights should be used for administration and operation of the server.

3. Have all superfluous cgi programs and WWW pages been deleted?
4. Is the HTTP port (usually port 80) the only accessible port on the computer (see S 4.97 *One service per server*)?
5. Is appropriate regular backing up of the stored data ensured (see Chapter 3.4 Data backup policy)?
6. If cgi programs are used, are these programmed sufficiently securely? It is not permitted to accept any input values unchecked. It must be ensured that buffer overflows and race conditions are ruled out. The taint check should be activated in all Perl scripts.
7. Is there a functioning routine for a regular integrity check (e.g. Tripwire; see S 4.93 *Regular integrity checking*)?

Example: Setting up a simple WWW server

On a WWW server of this type the contents of individual pages change only rarely; no cgi programs are used and there is no particular access protection. The individual WWW documents are loaded onto the WWW server via a data medium. On a server like this, all system files and also all HTML pages can be given write protection. Although an attacker is able to modify temporary files and log entries in a setup of this kind, he cannot make any changes to the system itself. Access protection in this form should be implemented by a physically write-protected medium, for example one or more CD-ROMs or a write-protected removable hard disk. At the very least, however, regular integrity checks should be performed (see S 4.93).

Functionalities in the http daemon that are not required should be deactivated, i.e. those such as the possibility of executing cgi scripts. Whatever the case, cgi programs supplied with the system should be removed.

In one frequently encountered variant of a simple Web server, the documents can be modified interactively on the WWW server with corresponding authorisations. In this case, protection against unauthorised changes and a regular integrity check at short intervals are especially important.

S 2.175 Setting up a WWW server

Initiation responsibility: Agency/company management

Implementation responsibility: Head of IT Section, Administrator

Commissioning a WWW server

In order to set up a WWW server, in addition to appropriate hardware it is also necessary to procure corresponding software. A large number of products are available for this purpose. When the products are selected, apart from stability particular importance must be attached to the security mechanisms (for notes on procurement and installation see also Chapter 9.1 Standard software).

Adapting the organisational structure

Consideration must be given to what information is to be made available on the Internet or in an intranet. It is also necessary to clarify how and where documents are compiled, who produces which documents, which documents are used where, and who requires these documents. Guidelines on presenting a uniform identity for documents, file names and directory names should then be drawn up on the basis of these findings, and if possible standardised development tools should be specified.

Nominating responsible personnel

During operation of a WWW server, whether internally or externally, it should not be possible for every user to load files at will. One responsible member of staff should therefore be nominated for loading information, and this person should also check new files to ensure that they conform to the guidelines. Depending on the size of the organisation, other staff members can also be given subsidiary responsibility for individual organisational units or specific areas of the WWW server. The assignment of rights and the directory structure on the WWW server must also be specified in accordance with the chosen organisational structure. In particular, every person responsible for a subsection should have access only to those subdirectories which they are managing.

In order to ensure that the files and directories that are created always meet the respective guidelines, observance of the guidelines should be checked automatically, for example using appropriate scripts or macros. A prepared program should be made available to everyone, and should be invoked every time a change is made. Particular attention should be paid to checking the following points:

- Whether the access rights have been correctly set for all directories
- Whether the access rights have been correctly set for all files
- Whether the access rights have been correctly set for all CGI scripts (if set up)

A file detailing the changes that have been made should also be generated directly.

Restrictions on accessing the WWW server

Before a WWW server is commissioned and every time before it is updated, it must be established who is permitted to retrieve information from the WWW server. It must be clarified whether only staff within the company's or agency's own organisation, plus teleworkers, are allowed to access the provided information, or also any external user or only a restricted circle of users. These restrictions may also vary according to the type of information on offer in each case.

If access to the WWW server is to be made possible for a limited group of people only, measures to ensure this must be implemented, as described in S 4.94 *Protection of WWW files*, for example.

It is also necessary to clarify whether it is fundamentally possible only to retrieve information or whether users should also be able to load new information themselves. In this case, too, it must be established which group of people has which rights.

Clear structuring

As HTML files do not have to be arranged hierarchically, the directory structure with a WWW server is of no relevance to its mode of operation. To facilitate maintenance, however, care should be taken to ensure that the structure is clear.

It may be the case that links to your documents will be created on other WWW servers; changes to document names or directory names should therefore be avoided. Consequently the directory structure must be planned with expansion in mind.

Making documents available

Once the organisational hurdles have been overcome, work can begin on making information available on the network. An Internet WWW server is a form of presenting the organisation to the outside world, so the Internet presence should be prepared with commensurate care.

It is advisable to gain experience with an intranet WWW server first, before connecting a WWW server to the Internet. It is best to start with a small number of simple applications.

Information can be made available in the form of HTML files or can be integrated into HTML files, such that the information can be read directly when accessed with a browser. Alternatively it can also be made available as files ready for downloading, in any other required format. In this case the files first have to be stored on the user's IT system before they can be viewed or used for any purpose.

All HTML documents and WWW files intended for publication on the Internet should be subjected to quality control and have their content approved before publication in exactly the same way as any other published document.

HTML documents can be produced with special-purpose HTML editors, or documents produced in other formats can be converted to HTML with HTML converters.

If it is intended to make a large number of documents available which often change, it is advisable to link the WWW server to a document database. This approach gives users the means to search for and view documents quickly, and to perform document administration. It can also be useful if a database link allows users access to previously available corporate data.

Before new files are loaded onto a WWW server, they must be checked to determine whether they still contain any residual information (see S 4.64 *Verification of data before transmission / elimination of residual information*).

Configuration management

Experience shows that the contents of WWW pages frequently change, so it is important to have set up a properly functioning configuration management procedure. Links and references must be checked to ensure that they are up to date, and a virus check must be performed with an up-to-date computer virus scanning program before the pages are published.

It is equally important that all publications should pass through a specified and retraceable checking procedure. This should include quality control of the contents but also formal approval of the document. It is also necessary to examine whether the information is suitable for publication at all, or whether it is confidential, for example, or is subject to data privacy protection rules or is copyright-protected or restricted in some similar way.

Information that has been released for publication via electronic media should be digitally signed in order to give all readers the possibility of checking the authenticity of the information.

Publications which do not reflect the opinions of the organisation must be identified as such.

S 2.176 Selection of a suitable Internet service provider

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section

A provider via which users are connected to the Internet accumulates information not only about incoming and outgoing e-mail but also about all of the WWW pages which the users call up. In addition, all data that is exchanged between the user's computer and a server in the Internet passes through the provider's IT systems.

When selecting an Internet service provider, the following questions should be asked:

- Whether staff are available around the clock to deal with technical problems, and how competent they are.
- How well the provider is prepared for the failure of one or more of his IT systems (contingency planning, data backup concept).
- What level of availability the provider can guarantee (maximum downtime).
- Whether the provider regularly checks whether the connections to customers are still stable, and if not, whether he takes appropriate steps.
- What the provider does to ensure the security of his IT systems and that of his customers.

Confirmation of secure operation of the provider's IT systems should be obtained, i.e. for example proof that the conditions specified in S 2.174 *Secure operation of a WWW server* have been fulfilled. All relevant measures specified in Chapter 6 on networked systems and in Chapter 7 on data communication equipment should be put into practice. An IT security concept and security guidelines should be a matter of course with every provider. It should be possible for external users to inspect the security guidelines. The staff of the provider should be made aware of IT security aspects and be under obligation to observe the security guidelines; they should also be given regular training (not only in security matters).

The provider stores user data for invoicing purposes (name, address, user ID, bank account) as well as connection data and transmitted contents (over a period of time which varies from one provider to another).

Users should ask their provider for how long which items of data concerning them remain stored. When selecting a provider, it should be taken into account that German providers must comply with data privacy regulations applying to the processing of this information.

Supplementary checks:

- According to which criteria has the provider been selected?
- Which security measures does the provider implement?

S 2.177 Security during relocation

Initiation responsibility: Head of IT Section

Implementation responsibility: Head of Organisation, Head of Site Technical Service; Head of IT Section; IT Security Management

Relocation of an office entails not only transporting furniture between sites but also moving quite different data media (e.g. hard copies, diskettes, magnetic tapes) and IT systems. While the move is going on, information, IT systems and other material is taken out of the secure office environment and transported by personnel who normally are not authorised to access it. Especially where a large part of the organisation is affected by the move, the risk of a certain amount of chaos can never be excluded and it is simply not possible to have every removal crate watched at all times Nevertheless, care must be taken that sensitive data does not get lost, damaged or fall into the hands of unauthorised persons during the move.

When planning the move, IT Security Management and the Data Privacy Officer should be involved as early as possible so that they can specify the IT security requirements.

- When planning a move, details must be drawn up in advance of who will be moving with what cargo to which location and at what time. This is of course essential in order that work can be resumed as smoothly as possible after the office move has been completed.
- The requirements which must be adhered to during transportation must be determined in accordance with the level of protection the data requires. For example, lockable transport containers should be used for more sensitive data (see S 2.44 *Secure packaging of data media*) or alternatively the data media should be encrypted prior to transportation.
- Data backups should be made before any IT systems are moved. In addition to the parameters specified in S 6.35 *Stipulating data backup procedures*, care should be taken here to ensure that under no circumstances are the backups transported together with the IT systems backed up. This will ensure that it is not possible for all storage media to be damaged or go missing at the same time.
- An instruction sheet which provides details of all the IT security measures to be taken should be prepared for all the employees concerned.

During a relocation, the actual removal is not the only critical phase: the periods immediately before and after the move are equally critical. Experience suggests that many items go missing in the phase immediately following the move before standard security procedures such as access control can be put in place. Certain organisational minimum requirements must therefore be satisfied during the removal as well:

- Transport documents should be completed for all materials to be transported. These should make clear

  - whether the items require a particular form of transport (e.g. fragile objects, special transport for computers etc.),
  - where they are to be taken to,
  - the names of the authorised recipients,
  - the names of the persons who collected and delivered the items (together with the date and time).
- The shipment itself must be marked in such a way that it can be uniquely identified and the transport route is also clear. However, labelling should not include any information regarding the sensitivity of the content. The labelling scheme should be designed so that it is not easy to copy. To achieve this, those planning the removal could provide special labels.
- Again, comings and goings during a move should be subject to controls. The authorised removal companies should provide advance information regarding the identity of the staff they plan to use. Where staff are changed suddenly due to holidays, sickness etc., the names of stand-in staff should be notified promptly. Depending on the particular location and circumstances, the doormen or other company employees can then check the names of those seeking access against a list of names of those involved in the removal either sporadically or continuously. Any external contractors involved in the removal should be provided with identity passes which show clearly who has rights of access.
- Shipments, especially data media, must be held securely both before and after the move. Any rooms in which removal activities are not taking place but which are not supervised by staff, for example, rooms which have not yet been cleared or have already been cleared, should be locked.

Once the move has taken place, controlled operations should be resumed as quickly as possible. Priority should be given to the infrastructural and organisational security of the new offices, for example,

- full access control measures should be resumed;
- fire loads should be removed from corridors, i.e. removal crates should be taken to the new working areas;
- shipments should be checked on delivery to ensure that they are complete, in working order and have not been manipulated.

Particular care should be taken when planning the relocation of any servers and network switching elements, as failure of one component alone could be sufficient to put the entire network out of action.

Prior to a move, the central IT administration should therefore take a number of precautions to ensure that everything goes smoothly:

- Before the relocation phase gets under way, a plan covering any necessary changes in user connections should be prepared in good time. In particular, an analysis should be performed as to whether any new equipment is necessary to ensure the smooth changeover of the computer connections of staff. For security reasons it is also important to know what changes will occur in the communication behaviour of the IT systems as a result of the

move. Depending on the level of protection required for the work of different members of staff, it can be necessary, for example, to encrypt a network connection or to prohibit access to certain data stocks.

- Before an employee relocates, care should be taken to ensure that he can be reached over the local network in his new office and that his applications and services are working. This may require changes not only to the terminal device (routing, software configuration etc.), but also early changes on the server side in the LAN or even to routers in the WAN. It may be necessary here to set up new addresses or routes and/or to delete old ones. It may be necessary to procure and install new network components in advance.
- During a relocation it is often also necessary to set up user accounts on a new server for the staff who are moving offices. Steps must be taken to ensure that the required access rights and access to applications and protocols have been configured. The security settings of the user environment must be retained in accordance with the relevant security profile. Old user entries and terminal device access entries must be modified on the old system or deleted. Nevertheless, users should continue to have access to user-specific data areas for a transition period, albeit with the proviso that the appropriate delete operation must be performed after a defined period. Once this period has expired, deletion must be effected by the administrator.

Special precautions must be taken where components of the computer centre, such as data or communications servers, are being moved. The measures described below are aimed at minimising component downtime:

- If possible, a new server should be installed in advance and tested in the new premises. If this is not possible, then the old server should be preconfigured as far as possible and only be adjusted at a time when access demands may be expected to be low and after issuing sufficient prior notice. The old configuration should always be backed up prior to commencing such work.
- The server should be backed up completely before the move. A bootable backup medium should be created if this is not already available. Sensitive parts of the server such as hard disks should always be duplicated (image backup) in case the original fails, and should be transported separately from the server. Care should be taken to ensure that the data backup, the image copy and the server are all secure during transportation (e.g. using encryption, locked box, security guard).
- Prior to the move, steps should be taken to ensure that the infrastructure needed for error-free server operation is available in the new premises and has been tested. It is not just a question of availability of the network (power supply, LAN, WAN) but it is important also that the components are moved in the correct sequence. For example, there is little point in having the Internet Web server moved first when the firewall with its communications router will not be set up until considerably later.
- Prior to the move, a check should be made to see whether the IT components to be transported include any which require special

environmental conditions during the move. For example, some large and expensive IT systems have controllers which not only have to be operated in air-conditioned premises but need to be air-conditioned during transportation as well.

Steps must also be taken to ensure that the new telephone numbers are already working by the time staff have moved into their new offices. Where the move is within a single city, if possible the old telephone numbers should be retained for at least a transition period. During the move telephone access must be possible both in the old premises and in the new location so that in the event of any problems staff are contactable at all times.

Additional controls:

- Have security guidelines been prepared in good time before a planned move?
- Have all staff been informed of the IT security measures which are to be taken prior to, during and after the move?

S 2.178 Stipulating a set of security guidelines for the use of faxes

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

Before any fax servers are installed, configured and cleared for use, a set of security guidelines should be specified for use of faxes. The points outlined below normally fall within the scope of such guidelines.

1. Concept of use

Before a fax server is cleared for use, the manner in which the system will be operated must be specified. For example, it might be desirable to have one fax server used solely to receive faxes over the LAN and then to send them outside. But a fax server can also receive incoming fax transmissions from outside. In this case how the incoming fax transmissions are forwarded to recipients must be specified. Under the first option, these transmissions are routed by the fax server itself, possibly using a connection to an existing E mail or workflow system. Another option is manual forwarding of incoming fax transmissions via the fax mail centre. Once again forwarding could be performed using E mail. However, another possibility is that the fax mail centre prints out incoming faxes and sends these printouts on to recipients (see S 2.181 *Selection of a suitable fax server*).

2. Integration with business operations

The mode of operation of the fax server also determines how faxes which have been sent or received are integrated within business operations. A procedure whereby the fax mail centre prints out all incoming faxes and sends the printouts to the relevant recipients corresponds to the way in which fax machines are customarily used. However, procedures whereby faxes are sent directly from an application on the user's workstation or incoming faxes are sent directly to the recipient from the fax server are significantly different from those which apply to the use of conventional fax machines. Hence in this case the guidelines for the use of faxes need to specify which incoming and outgoing faxes have to be printed out for the files.

3. Procedures controlling the use of fax servers

To ensure that a fax server is operated and used securely, a number of rules must be drawn up (see S 2.179 *Procedures controlling the use of fax servers*).

4. Restrictions as to material which may be faxed

The fax security guidelines must specify what information is allowed to be transmitted by fax. The fax security guidelines can also specify which communication partners may receive what information. This ensures that recipients are actually authorised to handle the information. For example, the guidelines could specify that price lists may only be sent to buyers or that project documents can only be sent to project team members by fax.

5. Contingency planning and operational reliability

The fax security guidelines should also cover contingency planning and fail-safe fax operation. If availability is an important factor, it may be appropriate to have redundant fax servers. In this connection consideration should also be given to the question of whether conventional fax machines should be kept available for use in emergencies (see also S 6.69 *Contingency planning and operational reliability of fax servers*).

6. Data backup

The fax server should be included in the data backup policy of the organisation (see Section 3.4). In particular, the data backup policy must specify who is responsible for taking the backups and what should be backed up. The items subject to backup can include software, configuration data, saved or archived fax data and even log files. The intervals at which backups are taken and the number of generations which must be kept should also be specified, as must the person responsible for checking any log files generated during data backup. Finally, the fact that a backup has been performed or that the log files have been evaluated should be documented.

7. Training

In addition, the fax security guidelines should be supplemented by an organisation-wide training concept. As a first step, the staff responsible for administering the IT system and the fax server application must be given appropriate training. The users must then be made aware of the dangers which apply where a fax server is used in comparison with a conventional fax system.

Additional controls:

- Are there any security guidelines for the use of faxes?
- Are the security guidelines for the use of faxes regularly updated in line with changes to the environment in which they are used?

S 2.179 Procedures controlling the use of fax servers

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator of the fax server, fax mail centre

To ensure the smooth operation of the fax server(s), procedures must be put in place covering the points set out below.

1. Specification of responsibilities

A fax server consists of an IT system, the operating system installed on it and the fax server application. Then there are the fax clients of the users. Accordingly the maintenance for the fax server must be organised. Depending on the existing organisational structure, persons who will have responsibility for these areas must be appointed. In some cases this can mean that each of these areas is supported by different administrators. For example, the operating system could be administered by the organisational unit which is also responsible for administration of the other IT systems. On the other hand, the fax application should be administered in the fax mail centre. Depending on the type of use, the mail centre is also responsible for ensuring that incoming fax transmissions are forwarded to the responsible person. Responsibility for issuing access authorisations for the fax server should lie in the mail centre as well. Other tasks include resetting passwords and configuration of new users. Thus it is especially important to define the tasks and responsibilities of the fax mail centre (see S 2.180 *Setting up a fax mail centre*).

2. Definition of the user community

The group of persons who are authorised to use the fax server must also be specified. Authorisations for incoming fax transmissions could include the following:

- Read rights,
- Forwarding rights
- Delete rights.

Authorisations for outgoing fax transmissions could include the following:

- Send rights,
- Suspend rights,
- Delete rights,
- right to alter transmission options.

These classes of authorisation should if possible be granted only to user groups and only in exceptional cases to individual users, as is customary in administration generally (see also S 2.30 *Provisions governing the configuration of users and user groups*).

3. Specification of utilisation profiles

The question of how much use authorised users may make of the fax server should also be covered in the procedures. This is especially important to avoid overloading of the server with serial faxes.

4. Times of use

Consideration should be given as to whether use of fax servers should be permitted only at certain times. Thus it would be possible to prohibit the sending of faxes outside working hours.

5. Configuring groups

Where incoming faxes are to be automatically routed to recipients through the fax server, separate fax numbers should be configured for certain functions and tasks. All members of a group can then be granted access to the incoming fax transmissions associated with a given call number. This also simplifies procedures for covering absences.

For example, supposing a fax server is operated in a company so that it automatically forwards incoming fax transmissions to their recipients. A fax call number is assigned for the Order Entry department. The fax server forwards all fax transmissions with orders which are transmitted to the company using this call number, not to one individual person but to all members of the Order Entry department. This requires that the company specifies the sequence in which employees process incoming fax transmissions in order to avoid executing orders twice.

6. Arrangements for covering staff absences

Where fax servers which deliver incoming faxes to individual users are used, it is essential that arrangements are in place to deal with absences, and provisions dealing with this point must be included in the security policy. Otherwise there is no way of ensuring that important incoming faxes cannot remain unread for prolonged periods. In this respect, the procedure for use of fax servers is significantly different from that which applies to the use of conventional fax machines. In the latter case incoming faxes are noticed by staff standing in, as the faxes are available as hard copy.

7. Logging

Procedures should be defined for dealing with any log data generated. These should specify who is tasked with analysing what logged data and at what intervals (see S 2.64 *Checking the log files*).

8. Address books

Which address books are used and who is responsible for maintaining them. Many fax server applications provide facilities for creating address books both for individual users and also for use throughout the organisation. Moreover, it is often also possible to synchronise fax server address books with distribution lists and address books already available in e-mail systems. Whereas address books which are to be used throughout the organisation should be maintained centrally through the fax mail centre, users must perform the task of maintaining their own address books themselves. Users should also be

required to check recipients' call numbers in the case of important fax transmissions (e.g. individual quotations).

9. Use of the fax server

Procedures covering use of the fax server by staff must also be drawn up (see S 3.15 *Information on the use of faxes for all employees*). Finally, which rights employees may exercise on the fax server must also be specified.

10. Protection of the fax client

Appropriate organisational and technical measures must be taken to ensure that no faxes can be read without authorisation or can be sent either without authorisation or unintentionally. Users must therefore be trained in use of the fax programs and made aware of the potential risks.

Authentication of employees on the fax server is especially important. This can be effected explicitly via a fax client or else by logging on to a directory service, a domain controller (in a Microsoft Windows NT environment) or an e-mail system. Where employees are authenticated to the fax server over a client, if possible the logon password should not be stored on the hard disk as that would invalidate its value as a security mechanism. Anyone who has access to the appropriate fax client can send faxes under another name and read incoming fax transmissions without authorisation. Moreover, employees should be encouraged to log off from the fax server after collecting incoming fax transmissions and sending outgoing faxes. Steps should be taken to ensure that the computer is protected when staff leave their desks, e.g. through the use of password-protected screen savers or some mechanism of the operating system used (see S 4.1 *Password protection for IT systems* and S 4.2 *Screen lock*).

11. Repairs and maintenance

There should also be procedures covering repairs and maintenance work performed on the fax server. System administrators must know whom to contact when maintenance work or a repair is necessary. Procedures for handling faulty data media and especially faulty hard disks must also be defined.

Additional controls:

- Are the procedures for use of the fax server regularly updated in line with changes to the environment in which they are used?
- Are procedures covering the forwarding of incoming fax transmissions when recipients are absent from the office absent in force?
- Are there any procedures relating to training of staff in the use of fax programs?

S 2.180 Setting up a fax mail centre

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

To ensure smooth operation of the fax server(s), a fax mail centre must be set up and a person responsible for faxes must be appointed. The fax mail centre is responsible for a number of organisational and technical tasks which depend on how the fax server is used.

Careful selection of employees

As the staff in the fax mail centre generally have access to all incoming and outgoing fax transmissions, the staff chosen to man it must be subject to the same rigorous selection procedure as is necessary for administrators.

The fax mail centre also needs to work closely with those responsible for the other communications services (especially E mail and private branch exchange).

Continuous access

The fax mail centre should be accessible to all users at all times. The procedures covering staff absences must ensure that the fax mail centre is always manned.

Typical tasks of a fax server mail centre are as follows:

- Administration of the fax server application. This includes:
  - configuration of new users,
  - assignment of access authorisations to users and user groups,
  - resetting of passwords,
  - checking of communications links
  - analysis of any log data generated,
  - point of contact for users in case of problems,
  - maintenance of central address books and distribution lists,
  - carrying out of data backups where these are not the responsibility of the operating system administrator(s),
- Delivery and archiving of faxes,
- Correction of errors in fax delivery,
- Co-ordination between those responsible for private branch exchanges and E mail systems.

Support for the fax client

Finally, the fax client software on the workstations needs to be supported. This task can be performed either through the fax mail centre or else through the organisational unit which provides support to the workstations.

The tasks should be considered in the context of incoming faxes as these depend on the mode of operation of the fax server.

Manual forwarding of incoming fax transmissions

Where incoming fax transmissions are not automatically delivered to recipients, they must be manually forwarded by the fax mail centre. For example, this could take the form that the fax mail centre prints out copies of incoming faxes, which are then forwarded to recipients in the normal manner. This procedure is not significantly different from that which applies to the use

of a conventional fax machine. However, it is possible that incoming fax transmissions are digitally archived on external data media.

Automatic forwarding of incoming fax transmissions

Where incoming fax transmissions are automatically forwarded to recipients (automatic fax routing) it is possible once again for the fax mail centre to print them out for archiving purposes. Here again it is possible for incoming fax transmissions to be digitally archived on external data media.

Handling of incoming faxes which cannot be delivered

Where it is not possible to deliver a fax transmission, the fax mail centre must be informed and must rectify the source of the error. If attempts to deliver the fax completely fail, the originator must be informed appropriately. Possible reasons why it is not possible to deliver incoming faxes could include:

- the originator has used the wrong direct dial number;
- the recipient has left the organisation;
- automatic forwarding of incoming fax transmissions is performed on the basis of the originator identifier (CSID) and the originator is not known in the organisation or else there is no corresponding assignment rule.

In all these cases, incoming faxes must be manually forwarded by the fax mail centre. Where all attempts to deliver an incoming fax fail, the originator must be notified.

Additional controls:

- Who is the person responsible for faxes?
- What happens to fax transmissions which cannot be delivered?

S 2.181 Selection of a suitable fax server

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section

A fax server generally consists of the following components: the IT system itself, the operating system, the communications component (e.g. fax modem, active or passive ISDN card or dedicated fax card) and the actual fax server application. In addition the workstations may require a corresponding fax client.

Before a fax server is procured, the essential factors which will affect its usage must be ascertained. These are:

- the volume of faxes expected to require processing,
- the number of staff who are to use the fax server,
- fax server availability requirements,
- requirements for incorporation into existing E mail and workflow systems,
- requirements for logging on the fax server,
- requirements as to the manner in which incoming fax transmissions are forwarded to recipients.

IT-System

The choice of IT system is generally determined by the performance characteristics required by the software and the operating system. In addition, the IT system must be compatible with the operating system selected. Depending on the requirements for fax server availability, the use of additional protection mechanisms can be considered. Options for ensuring and/or increasing availability include:

- RAID
- replication
- load distribution

Operating system

Fax server applications are available for all common network operating systems such as Unix, Microsoft Windows NT and Novell Netware. When choosing the operating system, the extent to which integration into the existing network is possible and the requirements of the fax server application should be the decisive factors. Where only one network operating system has previously been in use in an organisation, e.g. only servers which run under Unix are used, then if possible that network operating system should be selected and an appropriate fax server application should be purchased. Nevertheless, if a particular software application is the only one to offer a user facility which is urgently required but which will only run on a different operating system platform from that used up to now, then that operating system should be chosen. A change of network operating system brings with it a significant increase in administrative effort. If different network operating systems are already in use on the network, then the one which offers the easiest path to integration should be chosen, provided that the desired fax server application supports it.

Communications component

The communications components establish the connection between the server and the public switched telephone network. Communications are processed using the T.30 protocol. This protocol determines amongst other things the connection setup, the exchange of originator fax numbers and transmission and acknowledgement of the document. Transmissions using the Group 3 standard are generally effected at 9,600 bps and 14,400 bps. In addition, the Modified Huffmann, Modified Read and Modified Modified compression techniques are also in use. The Group 3 standard is the most widely used. There is also a Group 4 standard; however, this requires ISDN. Transmission speeds of 64 KB per second are possible with this standard. The Group 4 standard has not succeeded in becoming as well established in the last few years, as appropriate stand-alone devices are relatively expensive. Moreover, the Group 3 and Group 4 standards are mutually incompatible.

At the start of communication, both the transmission speed and the compression method are negotiated between the devices. The highest speed and the best possible compression procedure which are supported by both devices are selected.

The following communications components can be considered when using a fax server:

a) Fax modem

Fax modems are available very cheaply. However, they are not always sufficiently tamper-resistant and moreover are not supported by all fax server applications when operated continuously. Therefore they should be confined to private usage and to individual workstations.

b) Passive ISDN cards

Passive ISDN cards are simple to build and hence inexpensive. The main communication load is borne by the computer. This can be a problem where heavy use is made of the fax server (e.g. when it is used for serial fax transmissions). With passive ISDN cards, assuming that the recipient has an appropriate device, transmission using the Group 4 standard is generally also possible. If fax data has to be transmitted using the Group 3 standard, then the data has to be converted accordingly. As in the case of fax modems, passive ISDN cards should be used only on a single workstation or in the private domain.

c) Active ISDN cards

Active ISDN cards, also known as ISDN controllers, have a processor of their own. This means they can handle the ISDN protocol largely independently. According to the specification of the Common ISDN API (CAPI), the fax data must be transmitted to the ISDN card in Structured Fax File (SFF) format. Conversion must take place on the fax server. Like modems, active ISDN cards in the Group 3 standard only support transmission rates of 9,600 and 14,400 bps, using the Modified Huffmann compression code. A major disadvantage both of fax modems and also of active and passive ISDN cards is the fact that these can also be used for other purposes than fax transmission, e.g. in modem operation or as a remote access component. However, for

reasons of network security this is precisely what one does not want with a fax server. Active ISDN cards can make up to 30 ISDN channels available. When active ISDN cards are used, the ISDN signalling possibilities are also available for automatic fax routing. Despite the fact that they can be used for non-fax operations, active ISDN cards are still positively recommended for use in fax service.

d) Fax cards (if necessary, with ISDN interface)

Special fax cards are optimised for handling the T.30 protocol. They assume the tasks of connection setup and "negotiation" of communications parameters. Data conversion and compression can be performed on the card, thus considerably reducing the load on the fax server. Fax cards which offer fax data transmission rates of at 9,600 and 14,400 bps and use of all three compression techniques are available. These cards also have the advantage that they generally can only handle the T.30 protocol and therefore cannot be used either for modem operation or as a remote access component. Some fax cards are enhanced to include an ISDN interface. The advantage of this is that ISDN signalling can be used for fax routing.

Use active ISDN cards or fax cards

To conclude, therefore, as a rule only active ISDN cards or fax cards should be used on fax servers. The card must be compatible with the application software as not every card is supported by all fax server applications. The number of cards that are necessary depends on utilisation of the fax server. Each channel can transmit approx. 40-50 pages of fax data per hour and per line.

Fax server application

When selecting the applications software, both the volume of faxes which will have to be processed over the fax server and the number of users need to be considered.

Integration into an E mail or workflow system

If an E mail or workflow system already exists in the organisation, then it should be possible to integrate the application software with these systems. It may then be desirable for incoming and outgoing faxes to be exchanged between the user's personal computer and the fax server using the existing workflow or E mail system. In this connection it is also of interest whether and how any existing address books and distribution lists can be synchronised with the fax server's address books. Moreover, archiving of incoming and outgoing fax transmissions should be possible in existing workflow systems.

Transmission from workstation to fax server

Another factor to be considered is how fax transmissions should pass from the user's workstation to the fax server and at what point the data should be converted into a data format which the fax server can accept. Conversion of the outgoing fax data at the workstation is normally effected using a printer driver or a special fax client application. The converted data can then be passed to the fax server either via E mail or else using the fax client application. One option is that the user copies the converted data to a special directory on the fax server. Finally there are fax servers for which a print queue is configured on the network. Fax data is written to this queue by the application software, e.g. a word processing program. It is also possible for full data conversion to be performed on the fax server. In this case, the user creates the file which is to be sent as a fax using appropriate application

software, e.g. a word processing program, and this file then has to be sent to the fax server. This can be done using E mail, an appropriate fax client application or by copying to a shared directory on the fax server. It should be borne in mind that conversion of the fax data at the workstation uses up resources there. This is not generally a problem if only a few faxes are sent per day. However, where serial faxes need to be sent, this can mean that the workstation is tied up for a considerable time. On the other hand, if demand is great at the fax server, conversion there will require appropriately high-performance hardware and software.

Logging at the fax server

A final consideration when selecting suitable application software is the logging facilities which are available on the fax server. As well as error reports, transmission reports are also of interest. As a first step the transmission protocols for the relevant fax transmissions should be made available to the users through the fax server. This is the only way to ensure that users respond promptly, e.g. to connection errors. Furthermore it should be possible to calculate the charges incurred from the transmission reports and to distribute these to the relevant cost centres.

Transmission from fax server to workstation

Another factor to be considered when selecting the application software is the question of how incoming faxes reach recipients. Digital forwarding of incoming faxes over the network is also referred to as fax routing.

Printout on paper

The option that is simplest to implement from the technical point of view is of course to print out incoming faxes at a central location (fax mail centre) and to forward the printout to the recipient. The advantage of this solution is that the incoming faxes are printed out centrally for the files. Moreover, the incoming fax transmissions can be archived both digitally and manually. Furthermore, existing procedures for dealing with staff absences can be accommodated without problem. One disadvantage, however, is the workload at the fax mail centre which it can induce. Again, this approach means that the faxed data is not then available in electronic form at workstations.

Manual forwarding by E mail

Another option is for the fax mail centre to send the incoming faxes to recipients by E mail. Once again, this solution has the disadvantage of creating extra work for the fax mail centre. Nor is every incoming fax automatically printed out. If such a printout is desired for organisational or other reasons, appropriate procedures must be adopted.

Automatic routing

The following options are available for the automatic routing of incoming fax transmissions to recipients over the network:

a) Line routing

Under this method, a fixed recipient is assigned to each line. The number of recipients who are directly accessible is limited to the number of lines which are available.

b) Processing and interpretation of originator identifier

A second approach involves assigning faxes on the basis of the transmitted originator identifier (CSID - Call Subscriber ID) of an incoming fax. The fax server is instructed that incoming faxes from certain originators should be routed to a particular recipient. The disadvantage of this approach is that only incoming faxes from originators already known to the system can be

automatically routed. All other incoming faxes have to be manually redirected to the recipients. Another problem is that there are no constraints on the choice of originator identification by senders of faxes, so that sometimes these are not a reliable form of identification.

c) Signalling using ISDN

Where ISDN is used, additional possibilities for automatic fax routing are available. A distinction must be made here between "point-to-multipoint connections" and the system connection.

With a point-to-multipoint connection, 2 lines and up to 10 call numbers are available per connection. The call numbers are issued by the relevant telephone company. As long as the fax server is equipped with an ISDN card or a fax card with ISDN interface, the recipient can be determined on the basis of the call number used by the sender. Due to the upper limit of 10 call numbers, it is only possible to distribute incoming faxes to a maximum of 10 recipients.

With an ISDN system connection, a private branch exchange is switched between the public telephone network and the organisation's internal telephone network. With this type of connection the fax server can detect the call number used by the sender and route an incoming fax automatically to the appropriate recipient on the basis of this number. The maximum possible number of recipients is considerably higher with this solution. It is implemented by giving every person expected to receive incoming faxes from the fax server a second direct dial number. The PBX forwards incoming faxes which arrive on this second number directly to the fax server. The only disadvantage of this approach is that the organisation requires a larger pool of call numbers, so that the private branch exchange needs to have a high capacity.

d) Processing and interpretation of the recipient using optical character recognition

Another, but little used method of automatically routing incoming faxes is to use optical character recognition (OCR). An attempt is made here to recognise names or numbers contained in the incoming fax, e.g. in the address field. This solution requires powerful OCR software and appropriate computing power as well as relying on maximum use of standard address fields in the incoming faxes.

e) Other procedures

There are two other procedures for automatic routing of incoming faxes, the Dual Tone Multi-Frequency procedure and the Direct Inward Dialling procedure However, as neither method is usable in Germany, they are simply mentioned here for the sake of completeness.

Automatic routing with high fax volume

Automatic routing of incoming fax transmissions has the advantage of reducing the workload of staff in the fax mail centre. It also means that incoming fax transmissions reach the intended recipient more quickly. The main disadvantage when ISDN signalling is used is that heavy demands are placed on the pool of call numbers. On the other hand this is the most effective way of implementing automatic routing of incoming fax transmissions. When

the volume of incoming faxes is high, preference should be given to this solution. Where incoming fax transmissions are only sent to a few workstations or groups and generally they are received from the same originators, processing and interpretation of the originator identification is also a practicable solution. If the volume of incoming fax transmissions is only low, then manual distribution may be a viable alternative.

Additional controls:

- Are compatibility issues considered during selection of the fax server?
- Can the expected volume of faxes definitely be handled by the selected communications cards?
- Does the selected fax server application support all the user facilities which are required?

S 2.182 Regular revision of IT security measures

Initiation responsibility: IT Security Management

Implementation responsibility: Head of IT Section, IT Security Management

Unannounced revisions

In the IT Baseline Protection Manual a number of procedures are presented which are necessary if the desired level of IT security is to be achieved. However, it is not sufficient simply to make these procedures known, but it is also necessary to monitor adherence to them on a regular basis. However, in this context "regular" does not mean that revisions takes place at times which are predictable, as pre-announced checks generally produce a distorted picture of the object under investigation.

Revisions should be geared towards remedying defects. If revisions are to be accepted, it is important that this is recognised by all those involved as the objective of the revision and that staff do not feel they are being treated like schoolchildren. It is therefore a good idea to discuss possible solutions to problems with participants during a check and to pre-prepare appropriate remedies.

Tailor procedures to work routines

When employees ignore or circumvent a procedure, this is generally a sign that the procedure cannot be reconciled with work routines or that it is not possible for staff to implement it. For example, an instruction not to leave confidential material unattended on the printer is inappropriate if the only resource available for printing is a network printer some distance away.

Remove causes of security shortcomings

If shortcomings are identified during security revisions, the aim should be not simply to remove the symptoms. It is far more important to determine the causes of these problems and to identify solutions. These could, for example, involve changes to existing procedures or taking additional technical measures.

Avoid assigning blame

Revisions should help to remove the sources of errors. It is extremely important if revisions are to be accepted by staff that it does not result in any individuals being exposed or identified as "guilty". When employees live in fear of being exposed in this way, there is a danger that they will not be frank in reporting weaknesses and security shortcomings they are aware of but that they will instead attempt to hush up existing problems.

Additional controls:

- Are all procedures and IT security measures reviewed to ensure that they are implementable?
- How often are checks carried out to ensure that existing procedures and IT security measures are adhered to?

S 2.183 Performing a RAS requirements analysis

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Before a system is used for remote access, a requirements analysis should be performed. The aim of the requirements analysis is, firstly, to determine all the operational scenarios likely to occur in the specific case and, secondly, to derive from these the requirements for the hardware and software components that will be needed. If practical scenarios are drawn up and "acted out", any special requirements can be identified, so that any corresponding requirements (critical criteria) as regards the RAS system architecture or the RAS software can be formulated.

The issues to be clarified in the course of the requirements analysis include the following:

- Which users will have RAS access (teleworkers, employees working out in the field, employees on business trips)?
- Are any mobile users to have RAS access?
- For what purpose will RAS access be used in each case (to retrieve information, upload information, use programs)?
- Will the remote users need to access the entire LAN, i.e. all the data and services available there?
- Will special software products need to be accessed remotely?
- Will special protocols need to be used during RAS access?
- From which (remote) locations will remote access be required (national, international)?
- Which telecommunications access technologies may be used (fixed network, mobile phone, Internet)?

The requirements for the planned scenarios should be documented and agreed with network administrators and technical staff. These requirements will then determine how one proceeds from here (architecture, procurement, use).

Additional controls:

- Has a RAS requirements analysis been performed?
- Have all the special requirements which are specific to the local circumstances been captured?
- Has the list of requirements been agreed with the network administrators and technical staff?

S 2.184 Development of a RAS concept

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section, Administrator

Establishment of a RAS system requires that a RAS concept is developed after the requirements analysis has been performed (see safeguard S 2.183 *Performing a RAS requirements analysis*) and prior to technical implementation of the system. Essentially the concept specifies what RAS system architecture should be chosen and what rules should apply to use of the RAS system for all those concerned. The concept can be roughly broken down into three sub-areas.

1. *The organisational concept.* This covers all matters which are of interest to the organisation in relation to the RAS system. Care should be taken to ensure that the RAS system is integrated into existing organisational processes so that their homogeneity and consistency are preserved.

Organisation

2. *The technical concept*. This specifies the technical implementation of the RAS system. The technical concept should cover the requirements which have been identified during the requirements analysis and, as far as is implementable, it should accommodate all the access scenarios that will be necessary. With regard to technical planning, the existing technical situation must be considered in order to avoid any technical incompatibilities.

Technology

3. *The security concept*. This covers the security-relevant aspects of the RAS system. As security can generally only be assured through a combination of organisational and technical safeguards, the security concept should be specified separately and not just constitute a subsection within the organisational and technical concepts.

IT Security

The essential questions which need to be answered in connection with each of the sub-areas are listed below. Depending on the particular situation, there may be a special, additional need for co-ordination that is tailored to the particular organisational and technical circumstances.

The **organisational concept** should address the following points:

- The various responsibilities for the RAS system should be specified (installation, administration, review, monitoring). Depending on the organisational structure, this will either require the responsibilities associated with existing roles to be extended or new roles to be created (see also safeguard S 2.1 *Specification of responsibilities and of requirements documents for IT uses*).

Definition of responsibilities

- Binding rules as to which users should be allowed remote access over the RAS system should be specified. It is recommended that different groups with different access authorisations should be defined for RAS access as well. The groups to which individual users may belong should be controlled through an appropriate requirements profile which determines what conditions must be satisfied in order to acquire membership of a group. These conditions might include necessity (teleworkers, staff working out in the field), length of service and approval from the line

Authorisation concept

manager. Whether and how permissions for remote access should be restricted must in each case be decided within the organisation. Often equivalent rules will already exist, e.g. regarding permission for Internet access, which can then be adapted.

The access authorisations granted must be recorded as part of the RAS system documentation and must be updated in the event of changes.

- For fixed remote locations (e.g. telecommuting workstations) requirements which specify what conditions (e.g. in relation to security and technical equipment) the remote working place must satisfy in order to be allowed RAS connections from there to the local network. The concept can also provide for an initial review of the premises and subsequently for repeat reviews at periodic intervals, and specify how and by whom these reviews should be performed.

Requirements relating to business locations

- Normally the locations of RAS clients are not under the control of the LAN operator and therefore also possess a particular threat potential. It is possible to limit the potential exposure to threats of stationary clients (for example as used in teleworking) through appropriate provisions, but it must be assumed that the degree of risk to which RAS clients are exposed is very high. Not every location which satisfies the technical preconditions for remote access connection is also suitable for this. Therefore rules must be drawn up which specify from which remote locations RAS connections may be established to the destination LAN. Depending on the planned operational scenario, however, it may be easier to draw up a negative list of locations which are particularly unsuitable. This could include, for example, hotel foyers, hotel business centres or train carriages.

- Procedures for RAS administration should be specified which determine how changes to the RAS configuration must be implemented. Since breaches of security relating to RAS access could potentially result in the entire LAN being compromised, changes to the RAS configuration must always follow a predefined procedure (for example: request, review of the planned configuration, implementation, review of the change implemented).

Change management

The **technical concept** should address the following points:

- The technical concept should specify the hardware and software components with which the RAS system is to be technically implemented. The components are only defined in terms of their functionality. Through a subsequent analysis of existing system components and of the new components available on the market, the elements in the concept can then be assigned to actual equipment and software components (see S 2.186 *Selection of a suitable RAS product*).

Technical equipment

- All the possible points of access and the access protocols to be used over them must be specified.

- All the services and protocols which are permitted over the RAS link must be listed together with the resources which can be accessed over them.

- A decision must be made as to which subnets should or must be accessible over the RAS link (see also RAS security concept).

The **RAS security concept** should address the following points:

- A set of security guidelines covering RAS usage should be drawn up. These RAS security guidelines must be oriented to the existing organisation-wide security guidelines. As a general rule, permissions granted for access over the RAS system should be less far-reaching and checks should be tougher than with local access.

RAS security guidelines

- The type and manner of user authentication and the mechanisms to be used for this purpose should be specified.

Authentication

- All components involved in authentication should be recorded and their functions and interactions should be described.
- All components involved in access control should be recorded and their functions and interactions should be described. In this way it is possible to determine whether, for example, existing access control mechanisms can be configured in such a way that more restrictive settings automatically apply during remote access.

Access control

- As part of the security design, all points of RAS access to the local network must be recorded and the manner in which these access points are connected to the LAN must be specified (see also module 7.3 *Firewalls*).

Recording of all RAS access points

- Proceeding on the basis of the current network structure, the security concept must analyse which subnets can be remotely accessed. For bus-based networks (e.g. ethernet) typically all the computers in the subnet in which the RAS access resides can be accessed. In this connection consideration should be given to the possibility of creating dedicated access networks from which only controlled access to the operational network is possible (e.g. with the aid of routers, packet filters or an internal firewall). The creation of access networks requires the purchase and maintenance of additional hardware and software (see also S 5.77 *Creation of subnets*).

Restrictions on external access

- Organisational reporting channels must be planned so that in the event of a security incident a targeted and rapid response is possible. The technical concept should lay down appropriate mechanisms which enable the detection of security incidents and calling in of the responsible administrator who constitutes the initial point in the organisational reporting channel.

Reporting system for security problems

- Since remote access to a LAN poses special security risks because of the generally insecure environment in which RAS clients are used, every user who is to be allowed RAS access must be given special training. This training should ensure that users are made aware of the dangers and also instruct them in how to handle the technical devices and software.

Training and security awareness

- If any authentication tokens are to be used, users must be informed of the proper manner in which they should be handled.
- Again, the administrators must be given thorough training on the products used and they must also be made aware of all the potential security risks.

- The administrators must have sufficient time not only to operate the RAS systems but also to seek information on current security weaknesses and to learn how to use any new components.
- Existing rules regarding the separation of roles (e.g. administrator and internal auditor) should be transferred to the administration of the RAS system.
- Finally the requirements regarding the availability of RAS systems must be specified. Moreover, if necessary contingency solutions which can be used as an alternative in the event of failure of a RAS system should be provided.

Availability requirements

The RAS requirements analysis and design will by its nature throw up specific requirements for the hardware and software components which should be used. These should be refined and made specific for procurement purposes, as described in safeguard S 2.186 *Selection of a suitable RAS product*.

Additional controls:

- Does a security concept governing the use of RAS exist?
- Are there any security guidelines covering RAS usage to which the users can orient themselves?
- Is there an authorisation concept for remote access?
- Are the safeguards contained in the RAS security concept regularly checked to ensure that they have been correctly implemented?

S 2.185 Selection of a suitable RAS system architecture

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

Depending on the planned operational scenarios, different RAS system architectures can be used to implement remote access to a LAN. The various system architectures inevitably have different characteristics and therefore differ as to which particular operational purposes they are suitable for. Theoretically every combination is possible, but the wrong choice could entail additional expense (e.g. the need to purchase additional hardware or more time spent on administrative tasks).

The RAS scenarios described below and to which in each case one typical system architecture can be assigned are commonly encountered in practice.

1. **Connection of individual computers to a LAN**

   In this case an architecture known as "direct dial-in" is necessary. The RAS software is installed on the remote user's computer. The computer has a connection to a telecommunications network. For example, the connection can be over an analogue modem, an ISDN card or even over a mobile phone. To establish a connection, the RAS client software dials the telephone number through which the RAS server software can be accessed. The RAS server is also connected with the telecommunications network via a modem or an ISDN card. Depending on the RAS server product (also known as the access server), one server can establish several communications links (e.g. via "modem pools") so that several RAS clients can dial in simultaneously.

   The advantage here is that through this method a given computer can be connected to the LAN from any location. This is especially useful for users who do not work from a fixed location. Although direct dial-in to the RAS server of the destination LAN only switches the connection over the telecommunications network of the telecommunications providers used, nevertheless, it is recommended that mechanisms are used to protect communications here as well, e.g. encryption, digital signatures, authentication.

   One drawback with this approach is that the telephone charges incurred, which generally have to be paid by the remote user (unless special provisions are taken), will vary according to the distance to the destination LAN. This variant is not suitable where several users who are all located in the same remote location need to access the LAN, as a dedicated connection between client and server needs to be established in every case. Every client must therefore be equipped with its own modem and it is not possible for several client computers to share a common connection simultaneously.

2. **Connection of several computers to one LAN**

   In this case an architecture known as "direct LAN-to-LAN dial-in" is often used. Here, the computers of the remote users constitute a separate LAN.

The RAS client software is generally not installed on one of the user's computers, but instead the RAS functionality is made available through dedicated hardware in the form of a router. When data packets need to be transmitted from one LAN to the other, the RAS client contained in the router automatically establishes a connection with the destination LAN when it dials in to the RAS server on that LAN. In this configuration generally a symmetric architecture is chosen for both LANs, so that the RAS server into which the RAS client dials is also contained in a router and a point-to-point connection is established. Alternatively, several remote LANs can be connected over one access server (a RAS server which permits several simultaneous connections).

The advantage of this is that thanks to the functional separation of RAS client and the remote user's computer it is possible for *several* remote IT systems to be connected to the destination LAN over *a single* connection. The router which contains the RAS client makes the established connection available to all the computers connected to the remote LAN simultaneously. But the downside is that the connection capacity is divided among the remote IT systems accessing the destination LAN and cannot be used exclusively.

Another obvious disadvantage is that the clients are no longer mobile.

3. Connection of a computer or a LAN through a service provider

A more elaborate version of the two above scenarios is for a computer or LAN to also be connected through a special access phone number of a service provider. In this case the RAS client contacts a special telephone number which is frequently a local phone number or a number that is toll-free. Calls to these special numbers are forwarded by the service provider to the RAS server of the destination LAN within the communications network. This variant is a useful way of allowing staff on business trips to establish a connection without incurring high telephone charges.

4. Connection of a computer or a LAN over the Internet

This case differs from the scenarios described above in that initially the client connects to an Internet Service Provider (ISP). Only then is the client connected to the destination LAN, over the existing Internet connection. This approach requires that the remote user's access rights permit him to access the ISP concerned and that the destination LAN has an Internet connection. In this case, communication with the destination LAN is effected using Internet protocols. It is not necessary for the destination LAN to have its own RAS server (for direct connections over a telecommunications network).

This variant is generally used in order to keep down the telephone charges incurred by the remote user (e.g. so that local call charges apply) but it can prove quite complicated to configure. As the Internet access of a LAN is generally protected via a firewall, the possibility of Internet-based access by remote users must be considered when the firewall architecture is being planned (see also module 7.3 *Firewalls*).

5. Setting up a Virtual Private Network (VPN)

In addition to the possibility of accessing data on the internal network with the aid of Internet-based protocols and programs (e.g. telnet, ftp, POP3), *tunnel protocols* can also be used. These allow a direct connection between the RAS client and the RAS server of the destination LAN to be *simulated*, using the Internet as transport medium. The actual RAS communication occurs over this apparently direct connection (see also S 5.76 *Use of suitable tunnel protocols for RAS communication*). This procedure requires that the RAS server of the destination LAN can be accessed over the Internet. Often firewall products offer RAS support so that RAS access can be configured with the aid of the firewall administration tools provided by the products.

The advantage of such a solution is that Internet access is very widespread nowadays so that it is a relatively simple matter to build on an existing connection network. However the disadvantage is that, due to its open structure, the Internet was not designed as a secure network. For this reason it is particularly important to protect communications. With tunnelling, this is achieved through the use of cryptographic procedures, resulting in the creation of a Virtual Private Network (VPN).

Once a connection has been successfully established, a connection exists over the Internet between the remote computer and LAN, normally bypassing the firewall. However, from the point of view of IT security this is problematic as an aggressor could under certain circumstances have extensive opportunity to access the destination LAN if he succeeds in penetrating a client computer. It is therefore imperative for the security of the entire system that all clients are adequately protected. In addition, due to the impossibility of guaranteeing a particular throughput for communication over the Internet, it must be assumed that the quality of service will generally be lower than with direct and dedicated connections to the LAN over the telephone network. With this architecture, the effects on IT security and performance should therefore be carefully looked into.

The scenarios and system architectures presented above are variants that are commonly employed for the implementation of RAS access; however, they should be viewed only as examples. The actual choice of system architecture depends very much on the operational scenarios that are planned. Often there is also a requirement to accommodate several scenarios at the same time (e.g. telecommuters and mobile users). In particular, mobile users should be offered as much freedom as possible in the choice of access technology so as to ensure that they can access the local network from as many locations and work environments as possible.

However, from the point of view of IT security it should be borne in mind that the use of different access technologies generally also requires different access points in the destination LAN. Generally a LAN which has several external access points is exposed to a greater number of threats than a LAN which can only be accessed over a single external access. On the other hand, the fact that there are different access points enhances the availability of the RAS system.

S 2.186 Selection of a suitable RAS product

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section, Administrator

RAS products differ as to the range of functions provided, the security mechanisms offered, ease of operation and cost-effectiveness. Moreover there are differences in the hardware and software components in the operational environment which they require for smooth operation.

Before a RAS product is purchased, a list of requirements against which the products available on the market can be evaluated should therefore be drawn up. An informed purchase decision which will ensure that the product purchased satisfies the requirements when put into operation can then be made on the basis of the evaluation.

A RAS system generally consists of several hardware and software components so that, strictly speaking, one should not really talk about a RAS product as if it were a single entity. Initially a rough distinction can be made between LAN-side and client-side components. The specific components which have to be purchased depend on the chosen RAS system architecture. Thus, in the simplest case, for example, a Windows-based PC and a laptop, each of which is fitted with an ISDN card (see also S 2.106 *Purchase of suitable ISDN cards*), can function as RAS server and client and use the Windows NT Remote Access Service. On the other hand, large organisations often operate many RAS connections concurrently for different operational purposes. Solutions here generally require special IT systems (hardware and software) which are specifically designed for use as RAS servers.

The list below provides a rough summary of the possible general evaluation criteria, but does not claim to be exhaustive and can be extended to include other general requirements. In addition to the criteria listed here, further specific requirements which result from the planned actual operational scenarios must be identified as part of the RAS requirements analysis (see safeguard S 2.183 *Performing a RAS requirements analysis*).

1 General criteria

1.1 Performance and scalability

- Can the system satisfy the performance requirements?
- Can transparent load balancing or data compression be configured for the system?
- Can the system be designed in such a way that it can cope with future growth requirements (e.g. through modular system structure, simple integration of new RAS servers, no separate user administration for new RAS connections)?

1.2 Maintainability

- Is the product simple to maintain?
- Does the vendor offer regular software updates?
- It is possible to conclude maintenance contracts for the product?

- Can maximum response times for problem resolution be defined in the maintenance contract?
- Does the vendor offer a competent technical customer service (call centre, hotline etc.) which can provide immediate assistance in the event of problems?

1.3 Reliability / operational reliability

- How reliable and fail-safe is the product?
- Does the vendor offer high availability solutions?
- Is it possible to use the product in continuous operations?

1.4 User-friendliness

- Is the product simple to install, configure and use? Does the product meet the relevant ergonomic regulations?
- Is the user interface, especially that of the RAS client, designed so that even inexperienced users can work with it without having to accept reduced security (e.g. through the provision of context-sensitive help, on-line documentation, step-by-step guidance with comprehensible explanations, "wizards", detailed error messages)?
- Is it possible to configure use of the RAS client in such a way that as far as possible users do not have to bother with technical details? Is security still guaranteed if this is the case?

1.5 Costs

- How much do the hardware and software cost to purchase?
- What are the expected ongoing costs of the hardware and software (maintenance, operation, support)?
- What are the expected ongoing staff costs (RAS administrator / internal auditor)?
- Do additional software or hardware components need to be purchased (e.g. dial-in server, server for additional authentication services)?
- How much will it cost to train the staff and administrators who will be using the RAS product?

2. Operation

2.1 Installation and initial operation

- Do the RAS system’s default settings ensure that the RAS will be securely configured after installation?
- Can installation of the RAS client software be automated with predefined configuration parameters?
- Is it feasible for less technically-minded staff to install the RAS client software?
- Can important configuration parameters be protected against modification by users?
- Does the product work with commonly available hardware and software (operating systems, plug-in cards, drivers)?
- Is the RAS system compatible with commonly used system management systems?

2.2 Error handling

- Is the security of RAS connections also assured after a critical failure or error (e.g. by preventing any further connections after abnormal termination)?
- Can the system behaviour be reconfigured after a critical failure or error? For example, is it possible to configure the system so that after a critical error it is automatically rebooted or the Administrator is informed?

2.3 Administration

- Does the documentation delivered with the product contain a full description of all the technical and administrative details?
- Can the administrative functions be accessed via a graphical user interface which is intuitive to use? Are the administrative functions designed so that attention is drawn to any incorrect, insecure or inconsistent configurations settings or these are prevented?
- Do the administrative functions permit both command line data input and entry via a graphical user interface?
- Is access to the administrative functions protected through adequate access control, e.g. using password entry, implementation of a role concept (Administrator, Internal Auditor), two-person rule?

2.4 Logging

- Does the product offer logging facilities?
- Is it possible to configure the amount of detail logged? Is all the relevant data captured by the logging?
- Do the logging facilities allow data to be captured in different categories (e.g. by connection, user, protocol, service)?
- Are there constraints on who may access the logged data?
- Does the product allow the logged data to be stored not only locally but also on remote computers (central logging)? Are different data transmission methods offered for remote storage, so that external logging systems can also be used (e.g. syslog)? Can the logged data be transmitted securely?
- Does the product offer a component enabling analysis of the logged data?
- Is the logging mechanism compatible with the system management system used (transmission format, transmission protocol)?
- Does the product offer facilities enabling the administrator to be informed or suitable protective measures (rejecting the RAS client, blocking of user accounts) to be automatically implemented in the event of certain predefined events occurring (e.g. denial of access, several successive unsuccessful attempts at authentication)?
- Can logging be performed in such a way that the data privacy protection regulations can be satisfied?

2.5 Communication and data transmission

- On the LAN side, does the server software support all the network technologies that are used locally (e.g. ethernet, Token Ring, ATM)?
- On the WAN side, do the client and server software support all the access technologies which will be used (e.g. ISDN, mobile phone, analogue telephone line, X.25)?
- Does the RAS server allow several RAS clients to dial in at the same time?
- Does the RAS product support different protocols for remote access over telecommunications networks (e.g. PPP, SLIP)?
- Does the RAS product support different service protocols for remote access (e.g. TCP/IP, NetBEUI, XPC, DECnet)?
- Are tunnel protocols (e.g. PPTP, L2F, IPSec) supported for Internet-based access?
- Depending on the access technology used, does the RAS product allow the use of additional, technology-dependent mechanisms (e.g. channel bundling for ISDN, callback of the RAS client by the RAS server)?

2.6 Security: communication, authentication and access

- Does the product allow secure data transmission?
- Does the product allow the use of alternative security mechanisms (IPv4 mechanisms, IPSec)?
- Is communication protected using standard mechanisms? In particular, all the cryptographic algorithms used should be established and state-of-the-art. The product should comply with current standards.
- Does the product architecture allow subsequent installation of new security mechanisms?
- Are remote users granted access to the local network only after successful authentication?
- Does the system allow remote users to be authenticated using several authentication mechanisms (e.g. user name and password, Challenge-Response, Calling Line Identification - CLI)?
- Is the system architecture designed in such a way that new authentication mechanisms can be subsequently integrated?
- Does the RAS system allow the use of one or more commonly used external authentication services (e.g. SecureID, RADIUS, TACACS+)?
- Is it possible to integrate additional external authentication services?
- Does the RAS system transmit the information necessary for access control of access to data in the local network (user ID, security ID) to the local access control mechanisms?

Once all the requirements for the product to be purchased have been documented, the products available on the market must be thoroughly researched to establish to what extent they satisfy these requirements. It is likely that not every product will satisfy all the requirements at the same time or equally well. Therefore each requirement should be weighted in a manner

which reflects the importance of satisfying it. Similarly, the extent to which a given requirement is satisfied by a single product can be broken down into several stages. On the basis of the product evaluation performed (against the catalogue of requirements which has been drawn up) an informed purchasing decision can then be made.

S 2.187 Definition of a set of RAS security guidelines

Initiation responsibility: IT Security Management Team

Implementation responsibility: IT Security Management Team, Administrator

Document and update rules

As part of the process of planning RAS access to a LAN, it is also necessary to define a set of security guidelines for remote access. The organisation-wide IT security guidelines must be modified and expanded accordingly. The RAS-specific rules must be documented and updated in the event of any changes.

Inform all users

The security rules governing remote access to the local network must be distributed to all users who will be allowed remote access (see also S 2.184 *Development of a RAS concept*). The rules contained in the security guidelines should cover the following subject matter:

- Which users may access what data?
- Which users may use which applications?
- Which users may access which services and computers?
- Which users may establish a connection, at what times and with which RAS connection?
- Which administrators have which tasks?
- Which authentication mechanisms must be used for access?
- Which access rights are granted to each RAS user?
- Is Write access to data permitted?
- Is only a special data area to be used for Write access (e.g. incoming directory)?
- How are multiple authentication errors handled (e.g. by lengthening time-out, blocking users or blocking RAS access)?
- Under what circumstances can a blocked RAS connection be activated again? What is the organisational sequence of events that this entails?
- Under what circumstances can a RAS connection also be released remotely? What is the organisational sequence of events that this entails?
- What data is logged?

Take into account existing guidelines

This list of questions must be expanded, modified and made specific so as to take local circumstances into account. This process should entail consideration of the existing security guidelines. The general security requirements must not be undermined by the RAS security guidelines.

Within the framework of the IT security concept, the rules provided in the RAS security guidelines should also specify possible responses to breaches of the rules. Every RAS user must be aware of these.

Additional controls:

- Are all relevant RAS components (client, server, network switching elements) covered in the RAS security guidelines?
- How is compliance with the RAS security guidelines checked?
- Are the RAS security guidelines updated to accommodate changes in the underlying environment?

S 2.188 Security guidelines and rules for the use of mobile phones

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section, IT Security Management

A number of different ways of protecting mobile phones against misuse are available. In order that the methods are also used, a set of security guidelines specifying all the security mechanisms to be implemented should be drawn up. In addition, a short and clear instruction sheet covering the secure use of mobile phones should be prepared for the users.

Data classes found

As soon as a mobile phone is switched on, it registers itself with the network provider through the nearest base station. At the network provider, data on the identity of the user, the serial number of the mobile phone and the identity of the base station over which registration has occurred is logged and stored. This is done even if no conversation takes place. Moreover, every time a number is dialled this event is stored, irrespective of whether a connection is established or not.

The classes of data generated during use of mobile phones fall into three rough categories:

- *Inventory data* (or master data) is data which is permanently held in a service or network and is kept available. This includes the call number and, if necessary, the name and address of the subscriber, information about the type of terminal device, if appropriate any features and authorisations relevant to the connection as well as data about the assignment of subscriber groups.
- *Content data* is the real "useful data", i.e. the information and messages transmitted.
- *Call data* provides information about the detailed instances of communication. This includes data on communication partners (e.g. call numbers of the calling and called connection), time and duration of the connection, system services used, connections used, lines and other technical facilities, services and, in the case of mobile services, the location IDs of the mobile terminals.

Recommendations are provided below as to how this data can be protected against misuse.

Protection against card misuse

The mobile phone and SIM card must always be kept safe. They should never be left unattended during business trips. In particular they should not be left in parked vehicles.

Mobile phones and related services offered can be protected at various points by means of PINs and passwords. These include:

- access to the SIM card,

- access to the actual terminal device, i.e. the mobile phone,
- access to certain functions of the mobile phone, e.g. the telephone directory,
- access to the mailbox, i.e. to the answer phone function, or to other services of the network provider,
- access to data held by the network provider (e.g. when a caller queries the hotline about billing, sometimes a password has to be given).

All these security mechanisms should be used (see also S 4.114 *Use of the security mechanisms provided on mobile phones*). Under no circumstances should the personal identification number (PIN) be kept in the same place as the SIM card for the mobile phone.

If the SIM card is lost, arrangements should be taken immediately for the network provider to block the card so as to prevent possible misuse and any resulting financial loss (see S 2.189 *Blocking of the mobile phone in the event of its loss*).

To ensure that misuse of the SIM card is noticed promptly, the itemised call breakdown should always be checked for inexplicable charges and destination numbers.

Itemised call breakdowns

The network provider stores the call data for billing purposes. In Germany, under the directive concerning data protection for companies which provide telecommunications services (TDSV) the network provider is only allowed to retain this data up to the date on which an invoice is prepared, but no longer than 80 days. However, it can be appropriate for the customer to allow the network provider to store the call data for longer in case any problems should subsequently occur in connection with invoicing.

Every customer should demand itemised call breakdowns in order to be able to review mobile phone usage. In Germany customers are entitled to receive itemised call breakdowns free of charge. The following data can be obtained from this source:

- invoice date,
- numbers called (full number or else the last numbers may be unavailable)
- beginning, end and duration of the call,
- cost of the call.

All users who share the telephone must be informed of the fact that an itemised call breakdown has been requested and what data will be collected by this means.

If an organisation maintains and analyses itemised call breakdowns for cost control reasons, the procedure must be agreed with the works council or staff council, and the Data Privacy Officer and users must be advised.

The itemised call breakdowns should always be checked following receipt to ensure that they are correct. This will provide insight into possible ways of reducing costs.

Disclosure of call numbers

It is possible to choose whether and what data on mobile phone connections should be entered in public phone directories and/or be available to users of directory enquiry services. If a call number is entered it is easier for other people to call one. However, this is not appropriate for all applications, e.g. where a mobile phone pool is used or if it is desirable to keep the number of incoming calls low.

If the calling number display function is enabled, persons called can see the number from which they are being called (assuming their equipment has the appropriate configuration). This service can generally be enabled or disabled by the network provider for a given mobile phone.

Call number suppression

In the GSM network, the number from which a call is being made can be indicated to the recipient of a call. If this is not desirable, then the precautions suggested in S 5.79 *Protection against call number identification during use of mobile phones* should be heeded.

Protection against interception of phone calls

The only effective protection against interception of the contents of phone calls is to employ interoperable, network-wide end-to-end encryption. As this encryption is not implemented, every connection over either the landline network or the mobile communication network can potentially be intercepted. However, in Germany and most other countries communications between mobile phone and base station are automatically encrypted.

The following measures are recommended as a means of reducing the threat:

- Phone calls should not be made at any time and in any place. To make a phone call, a quiet area should be sought (this will also mean less disturbance to other people).
- As a matter of principle, confidential information should not be communicated on the telephone.
- Some mobile phones indicate on the display when the transmission between mobile phone and base station is not encrypted. If such a display is provided, users should be told about it. From time to time users should glance at the display to satisfy themselves that calls are actually being encrypted. Thus, for example, there are some countries in which communications between mobile phone and base station are not encrypted.
- There are also a few, relatively expensive mobile phones which allow end-to end encryption of communications. However, to avail oneself of this facility, both the caller and the person receiving the call must use compatible equipment. If there is a need to frequently communicate highly sensitive information over mobile phone, it may be appropriate to invest in such equipment.
- Where data is to be transmitted e.g. from a laptop over GSM, it should be encrypted on the terminal device prior to transmission. A number of programs are available for achieving this relatively simply.

- When mobile phones or SIM cards are passed around a circle of users, it requires a lot of effort to intercept telephone calls in a targeted manner. It may therefore be appropriate to employ such means when highly sensitive information or data is to be transmitted.

Itemised call breakdowns should be examined for unknown call numbers.

- A check should be made as to whether all call charges are billed to the subscriber. If certain connections do not incur any charges, this could be a sign that interception is taking place.

Raising the awareness of users

Because people are often careless about the danger of communications being intercepted, organisations should check that existing measures aimed at creating staff awareness of the relevant dangers are sufficient. If necessary it may be appropriate to inform staff at regular intervals about the dangers of having their calls intercepted and of making them fully aware.

Circumspection in the disclosure of information

Employees should also be briefed on the requirement not to disclose confidential information on the telephone without taking additional precautions. In particular, checks should be made as to the identity of callers before giving out any detailed information (see also T 3.45 *Inadequate checking of the identity of communication partners*). Where mobile phones are used, care should also be taken to ensure that confidential information is not discussed in public.

Spectacular but false warning messages are always in circulation (see also T 5.80 *Hoaxes*). To avoid wasting valuable working time checking whether such messages are true or not, all staff should be informed as soon as possible following the occurrence of a new hoax. There are various information services which send out appropriate warnings.

Rules on the use of mobile phones

Where mobile phones are used in an organisation, a number of aspects needs to be subject to control. These concern the use of both private and also work mobile phones.

Use of private mobile phones

If there are not enough mobile phones to go round within the organisation, it is possible that private mobile phones could be used for business purposes. However, the following aspects must be settled in advance:

- Who pays for business calls and how will they be settled?
- Modern mobile phones contain diaries, address books, e-mail support and other functions. To make the most of these functions it is usually necessary to synchronise the phone with a PC. Therefore the issue of whether installation of the hardware and software necessary for this is permitted must be resolved.

Use of business mobile phones

Similarly, a number of items need to be regulated with regard to the use of mobile phones belonging to the company/organisation:

- A policy must be established as to whether private calls may be made with work mobile phones and, if so, to what extent.
- Consideration should be given to whether only calls to certain communication partners should be allowed, e.g. to avoid unnecessary expense and/or restrict the disclosure of information (see also S 2.42 *Determination of potential communications partners*). This can be achieved through either an organisational procedure or technical means, as described below under the keywords "Call restrictions" and "Closed User Group".
- Even where work mobile phones are used, users should be informed of the related costs in order that these can be kept as low as possible. Thus, users should be informed of the tariff structure and roaming agreements in order that, for example, they can select the most favourable network provider when making calls abroad.
- Users should be informed as to the care they should take with their mobile phones to avoid loss or theft and to ensure that the equipment has a long useful life (e.g. looking after batteries, care of phones outside office or living rooms, sensitivity of equipment to excessively high or low temperatures).
- The administration, maintenance and issue of mobile phones should be controlled. For this purpose it is recommended that a mobile phone pool is set up (see S 2.190).
- Every time a change of user occurs, all the necessary PINs must be passed on securely (see S 2.22 *Escrow of passwords*).

General rules

Irrespective of whether the mobile phones used have been purchased privately or by the business, the employer should issue the following rules in writing:

- Anyone driving a vehicle on business must not make any calls during the journey, as otherwise in the event of an accident the organisation could be held jointly liable.
- Business secrets must not be disclosed over the mobile phone. The threat here is not so much that the communication will be intercepted on the communications link (over the network) as that it will be overheard by persons in the immediate environment.
- Users should satisfy themselves as regards the identity of the person they are talking to and should not jump to hasty conclusions before passing on information that is internal to the organisation.

As far as possible, a mobile phone should never be left unattended. If a mobile phone has to be left behind in a motor vehicle, then the device must not be visible from outside. Alternatives are to cover the device or to lock it up in the boot. Mobile phones have a certain value which could attract potential thieves.

If the mobile phone is used on-site in offices which do not belong to the organisation, then the security rules in force in the organisation being visited must be observed.

Mobile phones should not be left around unprotected on third-party premises such as hotel rooms. All password protection mechanisms should be enabled now if this has not already been done. Locking the phone up in a cabinet will discourage casual thieves.

Cost information

Every year GSM phone calls become cheaper, but there are certain options which in the long run can incur high charges. As charging structures are changed frequently, users should be informed at regular intervals as to how much the various types of connection cost and how these are affected by the time of the call, as well as the cost of other options.

When mobile phones are used, receiving a call itself can cost money if the person being called is abroad, for example, or has activated call forwarding to the landline network. As the caller has no means of knowing where the person he is calling is, the forwarding costs are not charged to him.

Rules regarding contactability

Even when people have a mobile phone there are times when they either cannot or would not wish to be called. Thus it can create a bad impression if mobile phones are used at every opportunity. If possible, mobile phones should be switched off during meetings or presentations. As a minimum, the ringing tone should be disabled or be set so that it is barely noticeable. Whenever it will not be possible to talk freely (e.g. during meetings, in restaurants etc) use of the mobile phone should be avoided from the outset.

On the other hand, steps should be taken to ensure that the user can be contacted. Various options are available for ensuring this. For example,

- times when users are to be contactable can be specified;
- the answerphone function can be used;
- or the phone can be configured so that calls are diverted to a secretary.

Banning the use of mobile phones

Consideration should be given as to whether the use or even the carrying of mobile phones should be restricted in all or certain areas of the company/agency. For example, this could be a good idea for meeting rooms (see also S 5.80 *Protection against bugging of indoor conversations using mobile phones*). If the IT security policy of the institution does not allow mobile phones to be brought into the building, clear notices to this effect must be placed on all the entrances. Checks should then be made at regular intervals to ensure that the policy is being adhered to.

Do not place mobile phone on servers!

The use of mobile phones can sometimes have an adverse effect on the proper functioning of other technical devices. This is why mobile phones have to be switched off, for example, in aircraft or intensive care wards. Mobile phones can also exercise interference on other, sensitive IT systems. For example, such interference has been observed in server rooms and computer centres. The lower the transmitting power of the mobile phone or the further away that the mobile phone is from any sensitive equipment, the less likely it is to cause interference.

Protection against transfer of data over mobile phones

Where IT systems are used to process sensitive data or are connected to a computer network, no mobile phone cards should be permitted (see also S 5.81 *Secure transmission of data over mobile phones*).

There is no foolproof way of protecting against the unauthorised transmission of data over mobile phones, especially by insiders. However, taking mobile phones into sensitive areas should be forbidden and checks should be made at regular intervals to ensure that this ban is being adhered to.

Telephone directories

Call numbers and the associated names and/or additional details can be stored in the telephone directory of a mobile phone. Telephone directories can be stored on the terminal device, i.e. on the mobile phone or SIM card. They do not have to have the same content. PINs can be used to restrict access to a given telephone directory in the memory of the terminal device and/or of the SIM card.

Whether it is best to hold telephone numbers in the mobile terminal or on the SIM card will depend on various factors, for example how easy it is to back up the data to other media (see S 6.72 *Precautions relating to mobile phone failures*). Generally it is recommended that the data is stored on the SIM card, since

- if the SIM card is replaced, the data can be made available on other devices and
- any sensitive data can be easily cleared from the device (this is important, for example, where repair work is necessary or a change of user occurs).

If possible, only one type of storage should be chosen. All important call numbers should be stored in this telephone directory to ensure that they are available at all times. The stored call numbers should be checked from time to time to ensure that they are still correct and are necessary. All call numbers should be stored in such a way that they can be called from anywhere in the world, i.e. including the country and area codes. Since only the country code is internationally agreed, and not the zero, every call number should be entered with a "+" at the beginning, followed by the country code (e.g. +49 for Germany), area code without leading zero and then the actual phone number. For example, a possible entry might be *+492289582369 GS hotline*.

If the mobile phone is used by several users, only phone numbers which are shared should be stored here. In addition, any facilities allowing the prevention of changes to the telephone directory via the existing blocking mechanisms should be used.

Use of answerphone functionality

Most network providers offer a service allowing an answerphone function on a mobile phone. Under such arrangements, incoming calls are stored at the network provider's in a mailbox or mobile box which can be retrieved by the user at any time. This can be very useful, but generally use of the service incurs additional costs.

Access to the mailbox should be protected by a PIN. Even when the mailboxes not used, the preconfigured PIN should be changed early on to prevent use by third parties.

Messages recorded should be listened to at regular intervals. All the users must be informed as to how the answerphone function works.

Call diversion

The call diversion function enables incoming calls to be diverted to the mailbox or to a different call number. There are several variants of this:

- All incoming calls are diverted.
- Calls are only diverted when the line is busy.
- Calls are only diverted if a connection cannot be established to the phone, e.g. due to a gap in coverage or because the mobile phone has been switched off.
- Certain types of call can be diverted, e.g. voice, data or fax calls.

However, it should be noted here that call diversions to landline network connections can incur high charges as the person who is being called has to pay the diversion costs himself.

Call restrictions

Call restrictions can be used to block calls to or from a call number. These functions are provided via the network provider and can be modified on the mobile phone. Normally it is necessary to enter a password.

Call restrictions can be a good idea if the mobile phone is to be passed on to third parties. There are various types of call restrictions:

- Barring of all outgoing calls

  This means that only incoming calls can be handled, and apart from emergency numbers it is not possible to initiate any outgoing calls.

- Barring of all outgoing international calls

  This restriction means that only numbers in the country in which the user is currently located may be dialled. Calls from abroad can continue to be received.

- Barring of all outgoing international calls except for calls to the user's home country.

  This allows calls to be made back to the home country (i.e. the country of the network provider). Calls to other countries are barred.

- Barring of all incoming calls

  It is only possible to make outgoing calls. This ensures that there are no interruptions from incoming calls.

- Barring of all incoming calls when the user is abroad

  Within the home country calls can continue to be made as normal. However, when the user is abroad, no telephone calls can be received any

more. This option can be useful as the reception of calls sometimes attracts high charges in foreign countries.

Whether any call restrictions should be chosen and, if so, which ones, will depend on the way in which the mobile phone concerned is used.

Closed User Group

The "Closed User Group" service allows communications to be restricted to the members of that group (see also S 5.47 *Configuration of a Closed User Group*).

The group members must be registered with the network provider. The "Closed User Group" option can be activated on the mobile phone. It can be appropriate to set up closed user groups, for example, to restrict the transmission of data by mobile phone.

Additional controls:

- Is there an up-to-date set of security guidelines for the use of mobile phones?
- How is adherence to the security guidelines on the use of mobile phones checked?
- Does every mobile phone user have a copy of these mobile phone guidelines or an instruction sheet which contains a summary of the most important security mechanisms?
- Are the security guidelines for the use of mobile phones included in the training given on IT security measures?
- Are mobile phone users informed of the rules which they are expected to observe?
- Are mobile phone users informed of the importance of taking proper care of the equipment?

S 2.189 Blocking of the mobile phone in the event of its loss

Initiation responsibility: Head of IT Section, IT Security Management, users

Implementation responsibility: Users

In the event that either the SIM card or the mobile phone are lost, any costs incurred as a result of misuse of the mobile phone connection will be borne by the SIM card holder. Therefore arrangements should be made immediately for the network provider to block the SIM card in order to exclude the possibility of the card being misused and the associated financial loss.

In addition, the requirement to enter the SIM card's PIN should always be enabled (see S 4.114 *Use of the security mechanisms provided on mobile phones*). If the card should be stolen or lost, this prevents the SIM card being used or evaluated by an unauthorised person. However, the user will only be required to enter the PIN if the mobile phone is switched on. If the mobile phone is stolen when it is already switched on, a third party could use it to make calls until the battery is exhausted!

If the mobile phone is lost or stolen, it is also possible for the network provider to prohibit further use of the mobile phone by placing it on a "blacklist". To do this, the network provider needs the identifying number of the phone, the International Mobile Equipment Identifier (IMEI). This is often found on the back of the phone and should therefore be written down and kept apart from the device.

Care should be taken to ensure that the IMEI which goes with the mobile phone is notified in writing at the time of purchase. This number can also be read from the mobile phone itself, however the procedure involved is not standard for all mobile phones. The identifying number is often to be found on the identification plate underneath the battery or it can be displayed by entering "*#06#".

To ensure that misuse of the SIM card is noticed promptly, the itemised call breakdown should always be checked for inexplicable charges and destination numbers.

Get SIM card blocked as soon as it is lost!

All the data which is required to block the SIM card or mobile phone should be at hand but kept separately from the mobile terminal itself. This data is as follows:

- the call number of the mobile phone connection and the associated SIM card number,
- the serial number of the mobile phone,
- the service number of the network provider which has to be called in order to have the phone blocked and
- the service number password and customer number, i.e. the data which is needed in order to authenticate oneself to the network provider.

S 2.190 Setting up a mobile phone pool

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

Setting up a mobile phone pool

If a large number of mobile phones are in use within the organisation and their users change frequently, it may be advisable to keep those mobile phones which are temporarily not in use in a pool.

Steps must be taken to ensure that all mobile phones are kept charged so that they can be used immediately. It should be noted here that a battery discharges over time even if it is not being used. If the mobile phones are frequently used for long periods then a stock of extra spare batteries should be held.

Note: the battery chargers should be assigned uniquely to the mobile phones in a manner which makes them easy to identify. Most battery chargers look very similar but unfortunately they are generally not interchangeable.

In addition, returns and issues of mobile phones must be documented so that it is clear at any time which device is being used by whom. Every user should be entered in the issue journal by name, organisational unit, date and time.

The following points must be borne in mind in connection with the issue and return of mobile phones:

Issue:

- The new user should be given all the necessary PINs and passwords required to use the mobile phone. If any of these are changed by the user himself, the new values must be documented when the equipment is returned.
- In addition, the user must be given the call number of the mobile phone.
- The new user should be provided with an instruction sheet on the secure handling of the mobile phone. He should also be given the operating instructions for the mobile phone. As well as being able to use the phone in the normal manner, it is important that the user should also be able to interpret any warning displays (such as icons shown on the display).
- The mobile phone should be handed over charged and together with the appropriate battery charger. If the mobile phone is to be used for long periods at a time, an additional replacement battery should also be supplied, likewise charged.

Return or transfer:

- The user should provide the most recently used PINs and passwords. These must be checked to make sure they are correct. They must be written down (and kept in a safe place).
- The equipment, accessories and documentation must be checked for completeness. The device should be checked for any faults.
- The user must ensure that all data still required is transferred to data media which he can access (e.g. his PC) prior to returning the equipment. In

addition, the user himself must take steps to ensure that all data generated by him (e.g. phone numbers) has been deleted.

- The number memory of the mobile phone will contain details of the phone numbers called most recently. The numbers of the people who called most recently will also be held if a caller identification function is available and has been enabled. These numbers should be cleared prior to a change of user. It is also possible for call numbers to be stored in telephone directories both on the mobile phone itself and also on the SIM card. Personal call numbers should similarly be deleted prior to transferring possession of the phone. The call numbers which are important for business communications purposes should be permanently available to all users.
- Again, short messages, faxes or e-mails may be held on the mobile phone or the SIM card. These too should be deleted before passing on the equipment.

Additional controls:

- Are users informed of the rules and security precautions which they are expected to observe when they are issued with a mobile phone?
- Are users informed of the importance of taking proper care of the mobile phone when they are issued with it?
- Are issues and returns of mobile phones documented?

S 2.191 Establishment of the IT security process

Initiation responsibility: Agency/company management

Implementation responsibility: Agency/company management

The enforcement and maintenance of a reasonable and adequate level of IT security for a complex set of IT assets requires planned and organised action on the part of all those involved. Strategic key statements must be prepared, design requirements worked out and the organisational framework established to enable the company or agency to function with proper and secure IT support. A controlled IT security process which will lay the groundwork for the thoughtful design and efficient implementation and success monitoring of IT security measures is initiated by Management.

Optimal framework

As the highest echelons of Management are not only responsible generally for the systematic and proper functioning of an organisation but also for guaranteeing IT security, the IT security process must be initiated, directed and monitored from that level. Ideally, the following specific conditions should be satisfied:

- The initiative for IT security should originate from Management.
- Responsibility for IT security should reside there.
- The "IT security" function should be actively supported by Management.

Alternatives

If this framework does not exist in a given situation, as a first step an attempt should be made to implement the missing IT security measures at "shopfloor" level. In all cases, however, every attempt should be made to make Management aware of the importance of IT security to ensure that it takes its responsibility in this area seriously. Although many aspects of the IT security process can be initiated on the shopfloor and will result in an improvement in the security situation; there is no guarantee that such actions will lead to a permanent raising of the IT security level.

The establishment of a functional IT security process can be achieved through the following steps:

Step 1: Drawing up of an Information Security Policy

A set of IT security objectives that are derived from the overriding business objectives, marketing strategy and the general security objectives of the company or agency should be defined. The greater the dependence of the organisation on the use of IT and the operational capability provided through IT, the more important it is to consider the IT security objectives at all levels of the organisation.

The Information Security Policy should be based on the IT security objectives agreed at Management level. It should define the internal organisational structures, guidelines, rules and procedures which are necessary to achieve the IT security goals. Depending on the size of the organisation, it may be appropriate in addition to the enterprise-wide Information Security Policy to prepare one (or more) sets of departmental or site-specific information security policy documents derived therefrom.

The Information Security Policy must be made available to all the staff affected by it in a suitable form. By this means, Management can ensure that there is full visibility of the importance of IT security to the organisation.

Full details of this task are provided in S 2.192 *Drawing up an Information Security Policy*.

Step 2: Selection and establishment of an appropriate organisational structure for IT security

If a functioning IT security process is to be established, it is essential that an appropriate organisational framework is created and that the relevant responsibilities are delegated. The choice of such an organisational structure must reflect the size of the agency or company. This should entail establishment in a suitable manner of an IT Security Management Team and/or appointment of an IT Security Officer. In addition, responsibilities, tasks and authorities must be assigned in a systematic manner and notified.

This subject is described in more detail in S 2.193 *Establishment of a suitable organisational structure for IT security*.

Step 3: Preparing a schedule of existing IT systems

It is absolutely critical for the IT security concept, which is created in Step 4, that there is a complete schedule of the IT systems employed in the company or agency, the IT applications run on them and the data handled thereby. If such a schedule does not already exist, then it must be drawn up at this stage.

A list of the information that is absolutely essential to the creation of the IT security concept will be found in S 2.194 *Drawing up a schedule of existing IT systems.*

Step 4: Definition of the procedure for drawing up the IT security concept

To raise IT security to an appropriate level, it is necessary to identify existing vulnerabilities and to select and implement appropriate IT security measures. A number of possible procedures for ascertaining vulnerabilities and selecting appropriate measures are available. These include:

- baseline protection analysis following the recommendations contained in this manual,
- performing a risk analysis based on the IT Security Manual,
- performing vulnerability analysis in selected areas (e.g. networking) and
- penetration testing.

As well as deciding on the methodical approach, a decision must be made as to the sequence in which existing IT provision will be examined and to what extent.

In general it should be noted that standard security measures consistent with IT baseline protection are also essential to IT systems with a high protection requirement. A further consideration is that where high security systems are in use, any standard security measures employed are likely to need to be supplemented by more stringent measures. When selecting the approach, it

should be noted that little prior knowledge is needed to implement the methodology used to establish baseline IT protection. On the other hand, a high level of specialist knowledge is needed for detailed risk analyses, and especially to identify vulnerabilities and safeguards that will protect against them.

The BSI therefore recommends that any baseline IT protection safeguards which are not already in place should be implemented for all IT systems and that, in parallel, a detailed security analysis should be performed for those elements which require a high level of protection. In this way, a comprehensive level of IT security can be achieved in a relatively short time, so that even during the transition period up to the point where the detailed security analyses have been completed any IT systems which have a high protection requirement will have a certain degree of protection.

The procedure to be followed in drawing up a security concept is described in detail in S 2.195 *Drawing up an IT security concept*.

Step 5: Implementation of IT security measures

The implementation of the IT security measures identified during the process of drawing up the IT security concept must be organised and specified in an implementation plan. This will serve as a planning tool when it comes to co-ordinating implementation of the measures and as a control instrument to be used during actual implementation. All the actions and responsibilities necessary to update or implement security measures should be specified in writing in this plan.

Once implementation is complete, it is necessary to establish in every case whether all the measures have been implemented in accordance with plan and "work" as intended. During testing of the effectiveness of these measures, it may be sufficient to perform spot checks in previously determined areas.

The procedure to be followed in preparing an implementation plan for IT security measures and their implementation is described in S 2.196 *Implementation of the IT security concept in accordance with an implementation plan*.

Step 6: IT security in ongoing operations

In order that an IT security concept can be effective in everyday operations, it is necessary that all employees of a company or agency correctly implement the measures which affect them, identify any remaining vulnerabilities and play an active role in eliminating these. This requires that all staff receive adequate training on IT security issues and that steps are taken to ensure that their awareness of the risks and of the possibilities for improvement during ongoing operations is built up and continually enhanced. These points are also essential to staff acceptance of the IT security measures.

Safeguards S 2.197 *Drawing up a training concept for IT security* and M 2.198 *Making staff aware of IT security issues* present principles and possible approaches for achieving this objective.

Step 7: Maintaining secure operations

In order that attainment of the aspired-to security level is not a one-off occurrence but is maintained in the long-term, the IT security measures implemented must also remain operable in ongoing operations. In perhaps no other area does a security level once established become so rapidly outdated as in the dynamic IT environment. In particular, lessons learned from security-relevant incidents, changes in the technical and/or organisational environment, changes in security requirements and the advent of new threats require that existing IT security measures are modified.

Safeguard S 2.199 *Maintenance of IT security* contains detailed recommendations on how to ensure that these are properly updated.

Often modifications of the IT security process require a decision from the uppermost echelons of management. To this end, Management must be informed as to the level of IT security achieved and of any existing problems and vulnerabilities. For this purpose an "IT Security" management report should be prepared at regular intervals.

Safeguard S 2.200 *Preparation of management reports on IT security* contains advice on how to prepare and present such reports.

To ensure the continuity and consistency of the entire IT security process, it is essential that the IT security process is documented. Only in this way can basic weaknesses in the process be reliably detected and any departures from course be nipped in the bud.

Recommendations as to the content and scope of this documentation will be found in safeguard S 2.201 *Documentation of the IT security process*.

Additional tools and aids regarding the IT security process are presented in safeguards S 2.202 *Preparation of an IT Security Organisational Manual* and M 2.203 *Establishment of a pool of information on IT security*.

Further literature

Readers who wish to gain a deeper understanding of the "IT security process" subject-matter are recommended to read Part 3 of ISO/IEC Standard 13335 "Guidelines on the Management of IT Security".

Additional controls:

- Has an adequate IT security process being established?
- Is Management sufficiently supportive of the IT security process?

S 2.192 Drawing up an Information Security Policy

Initiation responsibility: Agency/company management

Implementation responsibility: Agency/company management; IT Security Management Team

Purpose

The Information Security Policy defines the level of IT security to which the organisation aspires. The Information Security Policy contains the IT security objectives which the organisation has set itself and the IT security strategy it pursues. In this way it constitutes both an aspiration and a statement that the IT security level specified is to be achieved at all levels of the organisation. Preparation of the Information Security Policy should be considered under the following headings:

1. Responsibility of Management for the Information Security Policy
2. Convening of a team responsible for development of the Information Security Policy
3. Determination of the IT security objectives
4. Content of the Information Security Policy
5. Distribution of the Information Security Policy
6. Drawing up of additional IT system security policy documents

An example of an Information Security Policy is enclosed as an aid on the CD-ROM at word20\hilfsmi\13policy.docVerweis.

Procedure

The preparation of the Information Security Policy requires the following stages:

1. Responsibility of Management for the Information Security Policy

The Information Security Policy documents the strategic position of Management with regard to the creation and implementation of the security concept, achievement of the IT security objectives at all levels of the organisation and the priorities which apply to the various types of measure.

Management has overall responsibility

It is important that Management is 100% behind the Information Security Policy and the objectives stated therein. Even if individual tasks relating to the IT security process are delegated to persons or organisational units which are then responsible for their implementation, overall responsibility remains with Management.

2. Convening of a team responsible for development of the Information Security Policy

If an IT Security Management Team already exists within the organisation, then this should be responsible for developing and/or reviewing and re-working the Information Security Policy. The draft document is then submitted to Management for approval.

Composition of development team

If IT security management is only being established for the first time, then a development team should be established to draw up the Information Security Policy. This team can assume the function of IT Security Management Team during the IT security process. It is a good idea that this

development team should include representatives of the IT users and the IT operational team plus one or more additional employees who already possess sufficient knowledge and experience in matters of IT security. Ideally, a member of Management who is able to assess the importance of IT to the agency/company should be called in from time to time.

Further information on this subject is provided in S 2.193 *Establishment of a suitable organisational structure for IT security*.

3. Determination of the IT security objectives

Classification of IT applications

An assessment should be made at the outset as to what information and information processing systems contribute towards the accomplishment of tasks and what value should be attributed to them. To do this, it is important to classify the information, the technical infrastructure and the IT applications of the agency/company. In the context of IT security what is of primary relevance here is the significance of IT for the organisation and its work. The strategic and operative importance of IT is particularly critical here. It is therefore important to consider more than just the material value of the IT itself and understand the extent to which the accomplishment of work within the organisation depends on the use of IT and its smooth functioning. To assist in assessing the extent of such dependence, the following are some of the questions which need to be considered:

- What critical tasks within the agency/company cannot be performed at all without IT support or can only be partially performed or with considerable additional effort?
- What essential decisions made within the agency/organisation rely on the confidentiality, integrity and availability of information and information processing systems?
- What are the consequences of deliberate or unintentional IT security incidents?
- Are the IT assets used to process information which requires particular protection due to its confidential nature?
- Do major decisions depend on information that is processed using IT being correct and up-to-date?

The outcome of these deliberations can now be used to specify what degree of IT security is sufficient and reasonable for this particular organisation.

Some example criteria for an assessment of this kind are listed below. The importance of IT, the specific threat situation and the relevant statutory requirements play a critical role here. The IT security level (low, moderate, high or maximum) which applies will be the one whose defining statements are the most relevant to the organisation.

Maximum:

- The protection of confidential information must be guaranteed and comply with strict secrecy requirements in critical areas.
- It is critically important that the information is correct.

- The central tasks of the institution cannot be carried out without IT. Swift reaction times for critical decisions require constant presence of up-to-date information. Downtime is unacceptable.

Summary: failure of IT may be expected to result in the total collapse of the agency/company or have serious consequences for large parts of society or industry.

High:

- The protection of confidential information must comply with stringent legal requirements and be increased in critical areas.
- The information processed must be correct; any errors must be detectable and avoidable.
- Time-critical processes run in central areas of the institution or large-scale tasks which are only possible using IT are carried out. Only short periods of downtime can be tolerated.

Summary: in the event of damage, central areas of the agency or company can no longer function. The result of damage is considerable disruption to the agency/company itself or to third parties.

Moderate:

- The protection of information only intended for internal use must be guaranteed.
- Minor errors can be tolerated. Errors which considerably disrupt the fulfilment of the tasks must, however, be detectable and avoidable.
- Extended periods of downtime which lead to deadlines being missed cannot be tolerated.

Summary: damage causes disruption within the agency/company.

Basic:

- Confidentiality of information is not required.
- Errors can be tolerated, provided they do not render the fulfilment of tasks impossible.
- Long-term failure should be avoided, moderate periods of downtime are, however, acceptable.

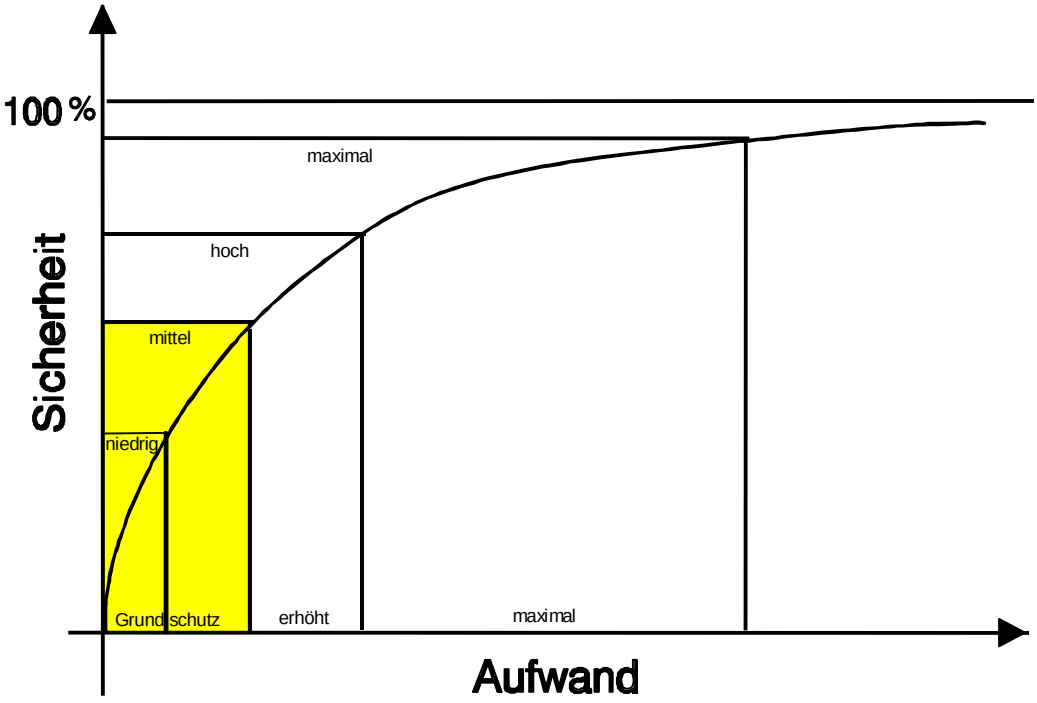
Summary: damage causes only minor disruption within the agency/company.

Cost-effectiveness

Achievement and maintenance of a given degree of IT security requires a corresponding effort. Therefore when specifying the IT security level for a given organisation, care should be taken to ensure that the costs associated with attaining this level are appropriate to the circumstances and are also affordable.

Cost-benefit trade-off

The diagram below is intended to illustrate the relationship between financial outlay and the aspired-to level of IT security. The diagram conveys an idea of the personnel, time and monetary resources required to achieve the IT security level. As a point of orientation, the financial outlay in private industry for IT security per year is an average of 5% of the total IT investment.



Text zum Bild:
Security
Basic - Moderate - High - Maximum
Baseline protection [Grundschutz]
Enhanced [erhöht]

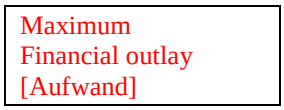


Figure: Cost-benefit trade-off for IT security

IT security objectives

After the overall security level for the agency/company has been specified using the approach described above, the IT security objectives which go with that security level must be defined.

Examples of possible IT security objectives are listed below:

- ensuring the high reliability of actions, particularly with regard to deadlines (IT availability is required here), correctness (the integrity of the IT) and confidentiality;
- ensuring the good reputation of the institution in the eyes of the public;
- preserving the value of the investment in technology, information, work processes and knowledge;
- protecting the high and possibly irretrievable value of information processed;
- protecting the quality of information, e.g. where it serves as the basis for major decisions;
- satisfying the requirements resulting from statutory provisions;
- reducing the costs arising in the event of damage (through both avoidance and prevention of damage), and
- ensuring the continuity of the work processes within the organisation.

IT security strategies

The individual IT security objectives can be implemented in different ways. In this connection general IT security strategies should be developed. Some examples of possible IT security strategies are:

- rigorous data backups in all IT areas,
- strict encryption of all information leaving the organisation,
- use of strong authentication procedures for all accesses to IT systems,
- isolation of particularly sensitive IT applications on stand-alone IT systems.

Specific requirements

These general IT security objectives and strategies apply to most organisations working with IT support. In order to determine the specific IT security objectives and IT security strategies of an organisation, it is essential to express these objectives in relation to the work and projects carried out in the organisation.

Example: Where person related data which falls within the ambit of the Data Privacy Act is handled (e.g. in Human Resources), the requirements regarding confidentiality and integrity specified in that Act must be

satisfied through adherence to the technical organisational framework conditions.

The results of such considerations should be specified in the Information Security Policy.

4. Content of the Information Security Policy

The Information Security Policy should contain the following information as a minimum:

- importance of IT security and IT to the accomplishment of work,
- security objectives and the security strategy for the IT used.
- assurance that the impetus for implementation of the Information Security Policy comes from Management,
- description of the organisational structure established for implementation of the IT security process (see S 2.193 *Establishment of a suitable organisational structure for IT security*).

It may also include statements on the following:

- classification of information, access control, control of access to information and security of information processing systems;
- assignment of responsibilities in the IT security process, notably to the IT Security Management Team, the IT Security Officer, the IT users and IT administrators;
- account of how the Information Security Policy is enforced, including procedures for dealing with security breaches and the disciplinary consequences of such breaches;
- overview of documentation of the IT security process;
- statements regarding periodic reviews of the IT security measures;
- statements regarding programmes to promote IT security through training courses and measures intended to raise awareness of security issues.

Updating

The Information Security Policy should be written in a concise style. It should be examined at regular intervals to ensure that it is still up-to-date, and be amended as necessary. It may be appropriate to document these cycles in the policy document.

5. Distribution of the Information Security Policy

It is important that Management presses home its objectives and expectations by having the Information Security Policy distributed, and that it stresses the value and importance of IT security in the organisation as a whole.

As Management has ultimate responsibility for the Information Security Policy, the policy should be set down in writing. The document must have been formally approved by Management.

Finally, all members of staff should be made aware of the fact that commitment, co-operation and responsible behaviour are expected of them not only with regard to the fulfilment of tasks in general, but also with regard to the fulfilment of the "IT security" task.

6. Drawing up additional IT system security policy documents

Separate IT system security policy documents should be prepared for IT systems or IT services which are located in a security-critical area, whose configuration is complex or which are relatively complex to use. Examples here include system security policy documents for firewalls, anti-virus protection measures, the use of e-mail or the use of Internet (see appendix on Additional Aids (in German)). The IT system security guidelines should contain:

- a description of the functionality of the system, the external interfaces and the requirements relating to the operational environment;
- a description of the threats against which the system is to be protected;
- a description of the actions which persons or technical processes may perform on data or programmes;
- a description of the protection requirements for the system objects;
- a description of the residual risks which the operator of the system can accept;
- all the safeguards which are to be implemented in the system to counter the threats;
- all the known vulnerabilities of the system.

Additional controls:

- Has the Information Security Policy been distributed to all staff affected?
- Are new members of staff referred to the Information Security Policy?
- Is the Information Security Policy updated at regular intervals?
- For which IT systems are there separate IT system security policy documents?

S 2.193 Establishment of a suitable organisational structure for IT security

Initiation responsibility: Agency/company management

Implementation responsibility: Agency/company management; IT Security Management Team

Roles and tasks

IT security is of particular importance to all IT projects, all IT systems and all IT users in an organisation. The aspired-to level of IT security can only be achieved if the IT security policy is implemented throughout the agency/company. This organisation-wide character of the IT security process makes it necessary to specify particular roles within the agency/company. Appropriate tasks must be assigned to each role, and these roles must be served by staff with the appropriate skills. This is the only way to ensure that all important aspects are taken into consideration and that all tasks are carried out efficiently and effectively.

Central roles

IT security management depends on the size, nature and structure of the organisation concerned. The following central roles should be defined in every case:

- the **IT Security Officer**, who builds up his own specialist expertise in IT security and is responsible for all IT security issues in the organisation; and
- the **IT Security Management Team**, which in larger organisations regulates all organisation-wide matters of IT security and develops plans, procedures and guidelines.

To guarantee direct access to Management, these should both be organised as special staff functions.

Basic rule:

The most important considerations in the definition of roles in IT security management are:

- *overall responsibility for the proper and reliable fulfilment of tasks (and thus IT security) rests with Management*
- *responsibility for IT security at the various workstations should be delegated in precisely the same manner as responsibility for the original task.*

Organisational structure of IT security management

Tailored to the size of the organisation

Depending on the size of the organisation, there are three possible ways of structuring IT security management. These are illustrated in the diagrams below. The first diagram shows the organisational structure for IT security management in a large organisation. The second diagram shows the organisational structure in a medium-sized organisation in which the roles of the IT Security Management Team and IT Security Officer are merged. The third diagram presents an organisational structure for IT security management in a small organisation, where all the tasks are performed by the IT Security Officer.

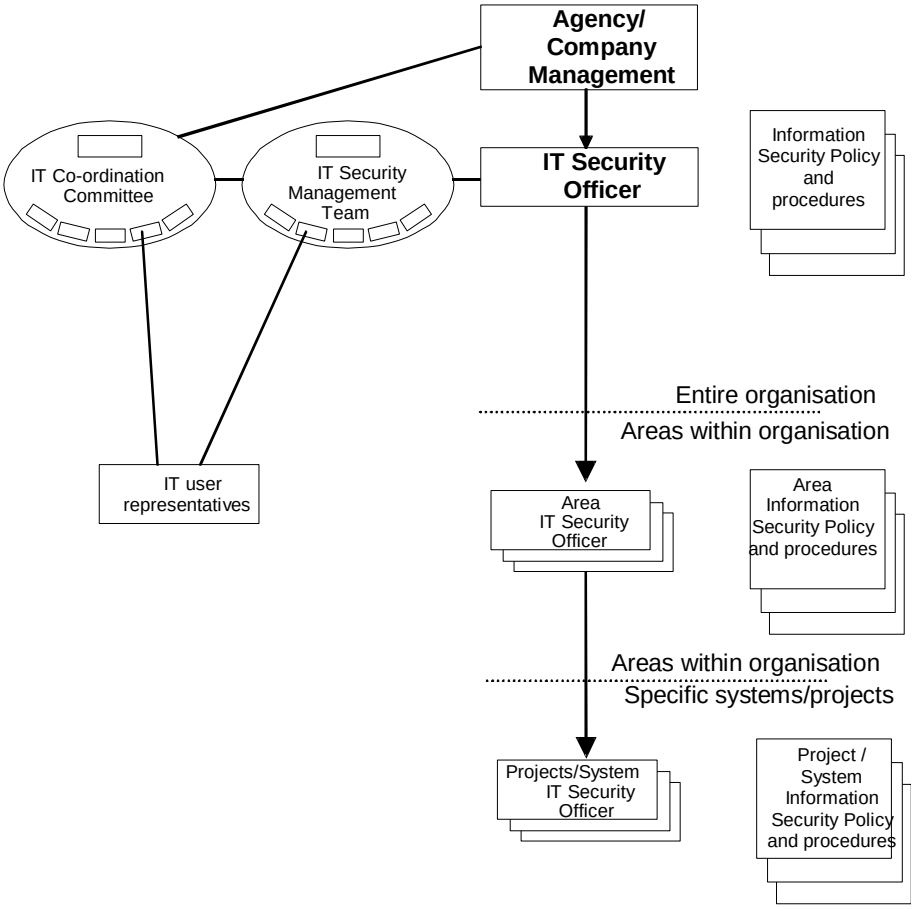


Figure 1: Organisational structure of IT security management in a large organisation

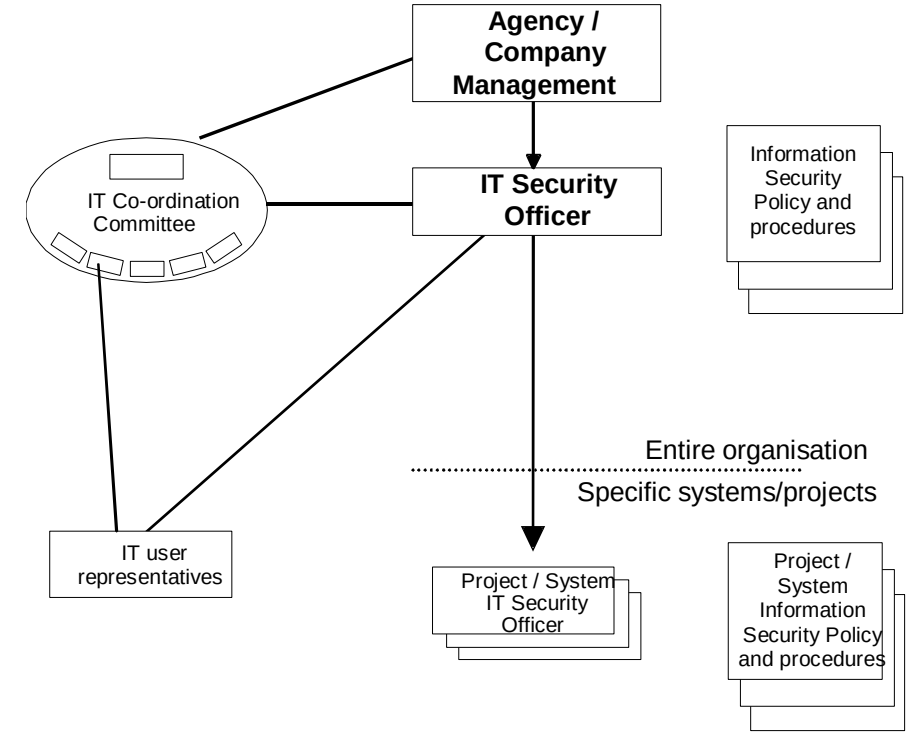


Figure 2: Organisational structure of IT security management in a medium-sized organisation

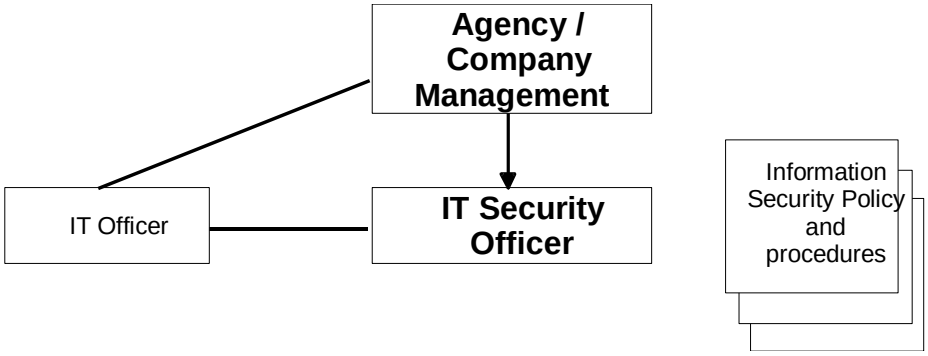


Figure 3: Organisational structure of IT security management in a small organisation

Necessary resources

At this point it should be made clear that these central roles do not necessarily have to be performed by more than one person. Staffing arrangements should reflect the size of the organisation concerned, the existing resources and the aspired-to level of IT security. On the other hand, it should be emphasised that IT security comes at a price. Those in positions of responsibility must have sufficient resources at their disposal so that they can devote sufficient effort to the "IT security" task. This will have more than paid for itself if there are fewer damaging incidents due to lack of security provision.

IT security management tasks, responsibility and authority

Integration into the organisational structure

The IT Security Officer and the IT Security Management Team must have clearly defined tasks, responsibilities and authorities, which must be laid down by Management. In order to be able to perform their tasks, they should both be

involved in all relevant procedures and decisions. The roles should be integrated into the organisational structure in such a way that all those involved can communicate with each other. The roles of IT Security Officer and of being a member of the IT Security Management Team should be entrusted to staff who possess the relevant specialist skills. If necessary, to support these roles tasks can be delegated to the specific IT Security Officers appointed for a given division or department, IT project or IT system.

The IT Security Officer

As the responsibility for IT security is delegated in the same way as the responsibility for task accomplishment, the danger presented by unclear delegation is that IT security is transformed into "someone else's problem". The result is that the responsibility for IT security is shifted around until no one takes responsibility for it any longer. To avoid this happening, responsibility for IT security should be given directly to a specific role, that of the IT Security Officer. This person is responsible for looking after all matters of IT security within the organisation. The tasks of the IT Security Officer are:

- to be involved in the entire IT security process,
- to draw up IT system security policy documents,
- to co-ordinate drawing up of the Information Security Policy,
- to co-ordinate drawing up of the contingency planning concept and other policy documents,
- to prepare the plan for implementation of IT security measures and initiate and review the implementation,
- to report to the IT Security Management Team and Management,
- to ensure a smooth flow of information between the divisional/departmental, project and system IT Security Officers,
- and to identify and examine any security-relevant incidents which occur.

Requirements profile

In order to carry out these tasks, it is desirable that the IT Security Officer has knowledge and experience in the areas of IT security and IT. As this task requires a variety of skills, the person appointed to this position should possess the following qualifications and attributes:

- He should identify with the objectives of IT security and appreciate the necessity of IT security.
- He should be able to liaise and work as a member of a team. (Few other projects require such a high degree of skill in working with other people: Management must always be involved in central issues of the IT security process, decisions must be sought and the IT users must be involved in the IT security process, possibly with the help of the divisional/departmental IT Security Officer).
- He must possess experience in project management, ideally in the area of systems analysis (these are the main aspects which are also important in the "IT Security" project and particularly in risk analysis).

Working together with IT users requires a high degree of skill as these users must first be convinced of the necessity of IT security, which some of them may perceive as a burden. Equally difficult is questioning IT users about sensitive incidents and weak spots. In order to guarantee success here, the IT users must be convinced that honest answers will not cause them problems.

Co-operation

The IT Security Management Team

The IT Security Management Team supports the IT Security Officer with the performance of his tasks by co-ordinating measures which impact the entire organisation, compiling information and performing supervisory tasks. The precise shape of the team will depend on the size of the organisation concerned, the aspired-to level of IT security and the available resources. In extreme cases the IT Security Management Team may consist of only one person, the IT Security Officer, who in this case is responsible for all the tasks in the IT security process.

Tasks of the IT Security Management Team include:

- specifying IT security objectives and strategies and developing the Information Security Policy,
- reviewing implementation of the Information Security Policy,
- initiating, directing and monitoring the IT security process,
- helping to draw up the IT security concept,
- examining whether the IT security measures planned in the Information Security Policy function as intended and are appropriate and effective,
- approving the IT security measure implementation plan and making available the necessary resources,
- preparing the programme of IT security and IT security awareness promotion training courses, and
- advising the IT Co-ordination Committee and Management on IT security issues.

Composition of the team

In order to be able to carry out its tasks effectively, the IT Security Management Team members should have knowledge of IT security, technical knowledge of IT systems and experience in organisation and administration. In addition, the IT Security Management Team should reflect the different operational areas within the organisation. As a minimum, the IT Security Management Team should include an IT Officer, the IT Security Officer and an IT user representative. If a similar body already exists in the organisation, its tasks could be extended accordingly. However, to underline the importance of IT security it is advisable to set up an IT Security Management Team and to place at its disposal the resources it needs.

Team members to have sufficient time available

Only a few organisations, either very large ones or ones with high IT security requirements, will be able to make full-time staff available to the IT Security Management Team. Normally these tasks will have to be performed in addition to the employees' primary duties. An exception to this, however, might be the first occasion that the IT security process is set up. If possible, the members of the IT Security Management Team should be released from

most of their other duties during this phase. The decision as to whether staff should be released and to what extent this is appropriate will depend on the distribution of tasks between the IT Security Management Team and the IT Security Officer. The final decision here lies with Management. Whatever arrangements are adopted, the IT Security Management Team should meet *regularly* to ensure continuous oversight of the IT security process.

Area IT security officer, IT project and IT system security officers

In large organisations it can be necessary to employ separate IT Security Officers in each of the various business units (referred to below as the "Area IT Security Officer"). The Area IT Security Officer is responsible for all security aspects of the IT systems and applications in his area (e.g. department, branch etc.). Depending on the size of the business unit, the task of Area IT Security Officer can be assumed by somebody who is already entrusted with similar tasks, e.g. the person might already perform the role of Divisional IT Officer (if such a position exists). Care should be taken during selection of the Area IT Security Officer to ensure that he is familiar with the tasks, conditions and work processes in the relevant business unit.

The various IT systems and applications within an organisation often have different IT security requirements, which may be compiled in a separate IT system security policy document and require different IT security measures. The analogous situation applies to the IT project Security Officer, with the distinction that his role is IT project-specific instead of IT system-specific.

The *tasks* of the IT Project, IT System and Area Security Officers include:

- implementing the procedures defined by the IT Security Officer,
- implementing the IT security measures in accordance with the IT system security policy,
- collecting IT system-specific information and forwarding it to the IT Security Officer,
- acting as contact person for the local IT users,
- being involved in the selection of IT security measures used to implement the IT system security policy,
- passing information about IT users' training or IT security awareness promotion requirements to the IT Security Officer,
- monitoring and evaluating log files at regular intervals, and
- reporting any security-relevant incidents to the IT Security Officer.

Persons in these roles should possess the following *qualifications*:

- in-depth IT knowledge, as this makes it easier to talk to IT users on-site and facilitates the search for IT security safeguards for the special IT systems;
- knowledge of project management - this is helpful when it comes to interviewing IT users and drawing up plans for the implementation and monitoring of IT security measures.

Additional controls:

- Has an IT Security Officer been appointed?
- Is there a need to support the IT Security Officer through an IT Security Management Team?
- Are all the tasks and powers within the IT security process clearly defined?

S 2.194 Drawing up a schedule of existing IT systems

Initiation responsibility: IT Security Management Team

Implementation responsibility: Head of IT Section, IT Security Management Team

Creation of an IT security policy and also the review, maintenance, troubleshooting and repair of IT systems require a complete and correct record to have been made of existing and planned IT systems. It is particularly important that such a schedule should be complete and up-to-date. In particular, it should also contain a detailed connectivity plan.

IT equipment register & connectivity plan

If a complete IT equipment register and a connectivity plan already exist, then the information required can be taken from these. If such a register does not exist or it does not contain the information, then this will have to be collected now.

As a minimum the schedule must contain the following information for all IT systems:

- serial number assigned,
- name and type of IT system,
- installation location of the IT system,
- networking of IT system,
- type of IT system (stand-alone, client, server etc.),
- status of the IT system (operational, in test stage, in planning stage)
- users of the IT-system,
- applications on IT systems,
- other components of the system (e.g. printer, disk drive, monitor etc.).

In addition, a connectivity plan which shows clearly the networking structures including connections to the outside world should be available.

Grouping of items

If there are such a large number of IT systems that a complete listing would not appear appropriate, similar IT systems can be grouped together if, from the point of view of application structure and sequence, comparable IT applications run on these systems. This applies particularly to PCs, large numbers of which often have a similar configuration.

Updating

It is important to check such a schedule at regular intervals to ensure that it is up-to-date and complete. This requires that steps are taken to ensure that the IT Security Management Team is informed of every change in the IT assets used.

Additional controls:

- Is there a list of existing and planned IT systems? Does it contain all the information that is necessary?
- Is there an *up-to-date* networking plan?
- Are the inventory schedule and networking plan reviewed at regular intervals to ensure that they are complete and up-to-date?

S 2.195 Drawing up an IT security concept

Initiation responsibility: Agency/company management; IT Security Management Team

Implementation responsibility: IT Security Management Team

The IT security concept is the "central" document in the IT security process of a company/agency. Every security measure implemented must in the final analysis be derived from this.

Status description

First of all an IT security concept contains a description of the current status of the IT assets and the information to be handled on them. "IT assets" refers here to all of the technical components which are used in connection with the performance of tasks. This includes the IT systems and the IT applications. The current status of the IT assets covers not only a description of the technical components, the IT applications operated and the information to be handled using these applications but also a list of any existing vulnerabilities, possible threats and measures already implemented.

Protection requirement

Depending on the protection requirements of the existing IT assets (which must be determined in advance, with rationale) and the information to be handled, the amount of effort involved in proceeding will be different. The BSI's recommendation here is to implement the safeguards contained in this manual on every IT system and in parallel to perform a supplementary IT security analysis for any components which have a high or very high protection requirement.

Co-operation

All staff who come into contact with the IT assets to be examined and the information handled on them should be involved in the preparation of an IT security concept in a manner which reflects their usage of the assets. Similarly, creation of an organisation-wide IT security concept presupposes that there are records of all the existing IT systems (see S 2.194 *Drawing up a schedule of existing IT systems*).

When drawing up an IT security concept, the approach described below is recommended. (A detailed description of the recommended procedure for drawing up an IT security concept which provides IT baseline protection is provided in Chapter 2 of this manual.)

1. **Determination of protection requirements**

   When determining the protection requirements, the question of how great the maximum damage would be if the availability, integrity and confidentiality of the IT systems to be examined and the information handled on them were to be impaired must be answered. To answer this question, the following steps must be carried out:

1.1 **Definition and recording of all components of the area under examination**

   This step requires by its nature that all the IT systems to be examined and information handled on them are recorded and described with reference to the technical task involved. This description should be supplemented to include a statement as to

whether these IT systems and this information are very important, important or less important to task performance.

1.2 **Assessment of the captured IT systems and the information to be handled**

This stage involves determining the maximum damage which could be sustained in the event of loss of the three basic parameters of availability, integrity and confidentiality by every IT system and by the information handled thereon. The potential damage can be classified into various damage scenarios.

These might include:

- violation of laws, regulations or contracts
- impairment of informational self-determination,
- physical injury,
- impaired performance of duties,
- negative consequences for the image and
- financial consequences

Based on the amount of potential damage and the consequences of this, a distinction is made between two protection requirements categories:

- basic to moderate
- high to very high

2. **Capture of information relating to the current security situation**

To determine the current security situation it is necessary to examine the IT systems in-depth. This should entail collecting information both about existing security measures and also about security shortcomings (comparison between planned and actual situation).

3. **Selection of IT baseline protection safeguards**

For all the IT systems and information under investigation, irrespective of the protection requirements category to which they have been assigned, the recommended safeguards contained in the present manual should now be implemented.

4. **Supplementary security analysis**

There are a number of reasons for carrying out an IT security analysis. For example, this can be appropriate where the protection requirement for an IT system and the information to be handled on it is "high" or "very high", or where the IT systems concerned have not yet been covered in the IT Baseline Protection Manual so that no IT baseline protection safeguards yet exist for them.

In addition to penetration testing and vulnerability analysis for selected areas, risk analysis is another possible procedure for such an IT security

analysis. The BSI IT Security Manual describes how to perform a risk analysis. It can be performed as follows:

4.1 **Analysis of vulnerabilities and threats**

The aim of the analysis of vulnerabilities and threats is to identify as many as possible of the existing vulnerabilities and all "significant" threats.

4.2 **Assessment of the risks identified**

This step entails assessing current risks posed by threats in terms of the damage these could cause and the frequency of such damage.

4.3 **Determination of appropriate security measures**

Additional measures must be selected for any risks identified in the previous analysis as being intolerable, taking into account the current security situation and the vulnerabilities and threats identified.

5. **Consolidation of all measures**

For the IT security measures identified in steps 3 and 4 as being necessary, a check must be made as to whether these are complementary or have negative effects on each other. If appropriate, IT baseline protection safeguards can be replaced by more stringent measures. During the consolidation process, these overlaps are removed.

6. **Consideration of cost-benefit trade-off, overall cost**

The safeguards contained in the IT Baseline Protection Manual are standard security measures. In other words, they constitute a set of requirements to be implemented so as to afford a state of the art protection to the IT systems under consideration. These safeguards may thus be generally considered to be reasonable. Most of them do not require any financial investment. However, some of them, especially safeguards presented as optional, do require financial resources.

It is important to prepare a cost plan. This will give the person responsible a good idea of the costs that will be incurred. Approval should be sought from Management for the necessary labour and financial resources.

7. **Consideration of residual risk**

If the personnel and financial resources provided for IT security are not sufficient to implement all the missing IT security measures, those which have priority should be implemented. However, if some of the safeguards are not implemented, some security loopholes may remain for the time being. The resulting residual risk, defined in terms of the amount of possible damage and an assessment of the quantitative or qualitative likelihood of occurrence, should be presented to Management for approval. If necessary, additional residual risks can be reduced if the budget is increased.

Structure

The security concept is a document which in practice is often used to check out the implementation of specific security measures or to review their currency. It should therefore be structured so that

- specific areas can be found rapidly,
- it can be updated with minimum effort and
- it is adequately documented so that if standby staff ever need to use it they are able to perform security-specific tasks using it.

To this end it is recommended that a security concept is structured by responsibility or by subject-matter. Thus, a security concept based on IT baseline protection should mirror the structure of the organisation or network under examination.

Confidentiality

A security concept can contain information which should not be passed on freely, for example information about vulnerabilities which have not yet been eliminated. This information must be kept confidential. This is achieved by only making it available on a need-to-know basis. This will be facilitated if the security concept is structured accordingly.

Additional controls:

- Does an IT security concept exist?
- When was it last updated?
- Where is the concept kept?
- Who is allowed access to it?
- Are people given access at least to those sections of the security concept which directly concern them?

S 2.196 Implementation of the IT security concept in accordance with an implementation plan

Initiation responsibility: IT Security Management Team

Implementation responsibility: Head of IT Section, IT Security Management Team

Once the IT security concept has been prepared, it must be put into practice. A distinction must be made here between a conceptual design phase and the actual implementation.

Conceptual design phase

During the conceptual design phase the basic suitability of every safeguard recommended for use on existing IT assets must be checked and the recommendations regarding safeguards must be fleshed out so that they can be used to generate organisation-specific rules. The IT security concept must therefore specify not only initiation responsibilities but also responsibilities for the implementation of the safeguards.

Initiation

Initiation responsibility covers performing the groundwork necessary for effective implementation and also specification of objectives. This presupposes that the responsible person has the necessary resources available to him by right.

Initiation generally includes:

- specification of objectives together with a description of the expected planned state or the expected behaviour,
- the allocation of resources (working time, financial resources) and
- a realistic time target.

Implementation

Implementation responsibility may be broken down into the formulation of rules, creation of aids, design of processes and the provision of information to the staff concerned. Strictly speaking, implementation terminates when a safeguard is applied in practice. Responsibility for implementation and application can be divided between several people. Implementation includes:

- the design of technical or organisational sequences of operations at the workplace,
- modification of task descriptions,
- the provision of instructions and information for security awareness promotion measures and training courses, and
- the provision of aids and implementation of the safeguard at the workplace.

Co-operation

Depending on the range and type of safeguard (technical or organisational), it may not always be possible to draw a clear-cut line between initiation and implementation. The implementation of safeguards frequently requires co-operation between several different positions. Thus, for example, persons with system responsibility are needed to procure, install and maintain technical facilities - for example, in the establishment of security interfaces - while on the other hand persons with organisational responsibility are needed to create and document the appropriate rules regarding their use.

Implementation phase

A structured implementation plan is essential if the IT security measures identified are to be properly implemented. The IT Security Management Team is responsible for drawing up the implementation plan. Depending on their type and scope, the individual safeguards are implemented either by the user of the IT system concerned or a responsible IT adviser. Implementation of the safeguards must be supported by the IT Security Management Team. In particular, every employee must know in advance to whom he should turn in the event of any problems occurring.

The following should be documented in an implementation plan:

- name of the person responsible for implementation of a safeguard,
- priority of the safeguard to be implemented,
- statement of the time by which the safeguard must have been implemented,
- person to whom implementation of the safeguard must be reported, once complete,
- provision of resources (manpower, resource requirements, space requirements, costs).

It is a good idea to pave the way for or accompany implementation of the safeguards by providing appropriate training for the IT users and raising their security awareness (see safeguards S 2.197 *Drawing up a training concept for IT security* and M 2.198 *Making staff aware of IT security issues*).

Additional controls:

- Do the recommendations regarding security measures contained in the IT security concept define clearly who is responsible for initiation and implementation?
- Is there an implementation plan?
- Are reviews performed and documented?
- Is Management informed of the results?
- Are the rules for implementation of IT security measures documented?

S 2.197 Drawing up a training concept for IT security

Initiation responsibility: IT Security Management Team

Implementation responsibility: Line managers, IT Security Management Team

Sufficiently knowledgeable

The shared task of "IT security" can only be performed in the proper manner if everyone involved in the IT security process has a reasonable level of knowledge about IT security generally and in particular about the dangers and countermeasures in their own particular work areas. Although ultimately all users should be motivated to keep up-to-date on their own initiative, nevertheless it is up to line managers to help them do this by providing suitable training courses. Given the large range of possible training topics and the importance of IT security, a co-ordinated approach is required in the selection of training content. This must be presented and documented in training concepts.

Specific requirements Target groups

In larger organisations with heterogeneous workstations, a *single* concept will generally not be sufficient. Instead, it will be necessary to tailor training concepts by scope and content to the importance and complexity of IT use in each target group. For example, an IT administrator or software developer obviously needs to know more about IT security than a commercial person or a typist. The first stage in drafting an IT security training concept is therefore to assign the staff of an organisation to *target groups* so that a separate training concept can be prepared for each of them. It is important to ensure here that *every* employee whose field of work involves IT either directly or indirectly is allocated to one of these groups, that implementation of this concept is verifiable and that evidence that training has taken place is retained. This ensures that training is of the appropriate breadth and depth.

Integration with existing training concepts

The IT security training concepts must be prepared in close co-ordination with the other training concepts of a company/agency, especially with training courses for IT users. The extent to which it is possible to integrate training topics on IT security into courses for IT users should be considered here. Including IT security within the syllabus of such courses has the advantage that IT security is perceived directly as another aspect of the use of IT. It is essential here that the lecturers demonstrably have the right skills and expertise. In the design of training courses it is critical that the "IT security" component is given sufficient coverage within the overall plan. A brief talk on the subject on a Friday between 1 p.m. and 2 p.m. is definitely not sufficient.

Minimum content

An IT security training concept should contain as a minimum the following points for all IT users:

- Risks and threats in IT use
- Basic terms and basic parameters of IT security
- The organisation-wide Information Security Policy - what does this mean to my everyday work?
- Responsibilities and reporting channels in our organisation (to include introducing the IT Security Officer)
- How can I contribute to IT security?

- How can I tell if a security-relevant incident has occurred and what should I do?
- How can I educate and inform myself in matters of IT security?

Specific content

Depending on the type and depth of IT use, additional topics should be included for particular target groups, for example:

- secure electronic communication,
- security aspects of particular IT systems and applications,
- secure software development and
- drawing up and audit of IT security concepts.

Selection of suitable lecturers

In each case it is necessary to check which subjects can be handled by in-house staff and which ones would be better dealt with through external courses. External courses are especially necessary for fields of work where IT penetration and complexity are high, and for the training of staff who will be responsible for IT security, whose training is particularly critical.

Updating of knowledge

Due to the speed at which IT changes, knowledge previously acquired rapidly becomes out of date. New IT systems, and also new threats, vulnerabilities and possible defensive measures make it imperative that knowledge of IT security matters is continually refreshed and extended. Training provision on these matters should therefore not be directed solely at new staff but refresher and supplementary courses should be provided at regular intervals for experienced IT users as well. With this in mind, it is important that the training concepts are updated regularly and modified to new circumstances as necessary.

Training and security awareness

To keep training knowledge constantly updated it is important to closely co-ordinate training courses and measures aimed at promoting awareness of IT security issues (see also S 2.198 *Making staff aware of IT security issues*). Thus, for example, training courses should refer to existing information sources and especially to the possibilities available for further private study (self-study courses, books etc). An example of a target group-specific training concept will be found on the CD-ROM (see appendix on Additional Aids, in German only).

Additional controls:

- Are written IT and IT security training concepts available for all IT user groups in the organisation?
- Is the IT Security Management Team involved in the planning and delivery of IT training?
- Do update plans exist for training concepts and are these adhered to?

S 2.198 Making staff aware of IT security issues

Initiation responsibility: IT Security Management Team

Implementation responsibility: IT Security Management Team, IT support

Experience shows over and over again that a large proportion of security incidents relating to the use of IT facilities are caused not by outsiders but are the result of inappropriate conduct by an organisation's own staff. Improvement of employees' knowledge of IT security and giving greater responsibility to each IT user can be a particularly effective and relatively inexpensive way of increasing the level of IT security. Again, if security-relevant incidents are to be detected promptly as such, it is important that knowledge of IT security is good. All staff should have an adequate knowledge and understanding of IT security matters and be aware of the risks which exist in their everyday use of IT. This objective can be achieved through a combination of an IT security training concept (see S 2.197 *Drawing up a training concept for IT security*) and repeated sessions given by those responsible for IT security, line managers and colleagues aimed at raising the awareness of IT security issues of all staff.

Guiding principle of awareness training

IT security awareness training should be geared towards the objectives contained in the Information Security Policy. All members of staff must be made aware that adherence to the security objectives, the conscientious implementation of security measures and maintenance and enhancement of the security level achieved are basic duties they are expected to perform routinely within the company/agency.

Effective ways of making staff aware of IT security issues include:

- staff workshops on the subject "What part does IT security play in our work?
- times at which the IT Security Officer is available for consultation,
- setting up a "security forum" on the Intranet,
- publication of "IT security reports" on the Intranet,
- *visible* promotion of IT security way of thinking by Management;
- placing information (from the press) on IT security incidents and approaches to solutions on noticeboards,
- placing specialist publications on IT security in a prominent place,
- discussions at the workplace and during work breaks on the subject of IT security.

Procedure: co-operative but single-minded

To maximise acceptance of the IT security process of the whole, it can be a good idea to present the IT security awareness sessions as an informative, discussion among colleagues rather than in the form of authoritarian lectures. To this end it is very important that every employee has someone he can turn to close by without having to worry about loss of face. This is particularly important when it comes to reporting any security-relevant incidents that have been detected. It also means that any shortcomings in the security awareness of individual members of staff should not immediately lead to embarrassing

reprimands but should be handled locally and with as little fuss as possible. Only if this approach repeatedly fails should further measures (including measures affecting staff) then be rigorously adopted.

The good example

It is critical to the *acceptance* and *credibility* of IT security awareness promotion measures that all those responsible for IT security and also Management act as role models as regards their own awareness and, especially, their own rigorous implementation of the security measures.

Additional controls:

- Are specialist publications on IT security available to those responsible for IT security and, if appropriate, to all staff?
- Are staff informed in a suitable form of IT security incidents which have occurred either within the organisation or which have become public knowledge, and are they told how to avoid them?
- Do generally accepted and used forums for in-house communication on IT security issues exist?
- Are those responsible for security sufficiently versed in the psychology of how to give motivating talks?

S 2.199 Maintenance of IT security

Initiation responsibility: IT Security Management Team

Implementation responsibility: IT Security Officer

In the IT security process what is important is not simply to achieve the aspired-to level of IT security, but to ensure that it is maintained *in the long term*. To maintain and continuously improve the existing level of IT security, all IT security measures should be regularly reviewed.

Regular and event-triggered checks

These reviews should be performed at predetermined times (at least every two years) and, if warranted by particular events, they can also be held in the interim. In particular, information gained from security-relevant incidents, changes in the technical or organisational environment, changes in security requirements or threats require that existing IT security measures are adapted. The outcomes of individual reviews should be documented and the question of how to proceed with the results of the review must be determined. It should be stressed here that reviews can only maintain IT security effectively if the results of these reviews are also translated into the necessary corrective actions.

Co-ordinated approach

It should be determined in advance in the agency/company how the activities relating to these reviews are to be co-ordinated. Which IT security measures are to be reviewed, when and by whom must be determined. This will avoid duplication of effort and also ensure that all parts of the organisation are covered.

Audit and update

A review can establish firstly whether the IT security measures are working properly at all levels on a day-to-day basis. At the same time, the extent to which the IT security measures are suited to the security requirements and are effective at protecting the organisation from threats can also be established from a review. Two types of review should be distinguished here, the *IT security audit* and the *update check.*

The purpose of an **IT security audit** is to establish

- whether the IT security measures implemented agree with those documented and
- whether the IT security measures function in the manner intended.

This comparison of the actual versus planned situation might reveal, for example, that some IT security measures have not been implemented or that they are not producing the results intended in practice. In both cases the reasons for the discrepancy should be established. Depending on the cause, possible corrective actions could include:

- adapting organisational measures,
- taking staff-related measures, e.g. further training or measures aimed at promoting IT security awareness, or instituting disciplinary measures,
- infrastructure measures, e.g. initiating structural changes in the building,
- taking technical measures, e.g. changes to the hardware and software or communications links and networks,

- seeking decisions from the responsible line manager (up to Management level).

In every case of a discrepancy between actual practice and what was planned a corrective action should be suggested. The person who will be responsible for implementing the control measure and the date by which it is to be implemented should also be established.

The IT security audit also includes a check as to whether log files and filter settings have been evaluated and monitored where necessary.

The purpose of an **update check** is to establish

- whether the IT security measures are still adequate to achieve the IT security objectives,
- whether the IT security measures are still sufficient to reduce the risk,
- whether the IT security objectives are still relevant.

It could transpire as a result of this update check, for example, that so many changes have taken place that the IT security measures no longer provide protection against current risks, the IT security process does not run in an optimal fashion or mistakes are being made in IT security management. In all three cases the reasons for the security loopholes should be established. Depending on the cause, possible corrective actions could include:

- changes in IT security management,
- adaptation of the IT security process
- identification of new threats,
- use of new technology (IT systems and applications),
- use of new IT security technologies,
- changes in the IT security measures
- action in response to new laws and statutory instruments or amendments to these, and
- action in response to changes in the latest version of the IT Baseline Protection Manual.

A corrective action should be suggested for every instance of a security weakness. Moreover, the person responsible for directing and monitoring the corrective measures should be established or, if appropriate, the additional risk could be considered to be acceptable.

The update check also includes examining whether changes of every kind have - where necessary - met with an adequate response

Procedure

The points listed below regarding performance of the review apply to both types of review, both the IT security audit and the update check.

Planning

The scope and depth of the review should be determined with reference to the purpose of the review. The IT security concept and the existing documentation of the IT security process serve as the basis for the review. The review, which can be performed either in-house or by external consultants, must be planned

carefully. During the review all relevant information captured should be documented and evaluated.

IT security report

The results should be documented in an *IT security report*. This should contain a technical description of the corrective actions proposed. The IT security report, which may contain confidential information and therefore need to be protected, should be presented to the IT Security Officer (assuming that he did not perform the review himself) and be notified to the manager of the division or department reviewed as well as to the IT Security Management Team. Where serious problems exist, Management should be involved so that any far-reaching decisions can be made promptly. For this purpose, a management report on IT security should be prepared, as described in S 2.200 *Preparation of management reports on IT security*.

Corrective actions

On the basis of the results of the review, decisions must be made as to where to proceed from here; in particular all the corrective actions which are necessary must be determined and specified in the form of an implementation plan. Responsibilities for implementation of the corrective actions, which are carried out in a similar fashion to the procedure described in S 2.196 *Implementation of the IT security concept in accordance with an implementation plan*, must be assigned and the persons concerned provided with the necessary resources.

In summary, it may be said that a given level of IT security can only be maintained if

- maintenance of IT security in ongoing operations is facilitated by appropriate organisational rules;
- responsibility for maintenance of IT security has been clearly assigned;
- measures are implemented in their entirety as described;
- measures are checked regularly to see if they are functioning as intended;
- measures are properly applied and adhered to and are accepted;
- measures are adapted if any new vulnerabilities come to light;
- measures are adjusted in line with changes in personnel, organisation, hardware or software.
- changes in tasks or the importance of tasks to the organisation are taken into account;
- changes to buildings, e.g. after moving premises, are taken into account;
- modifications are implemented in response to changes in threats and/or vulnerabilities.

New security risks

All these changes have a significant effect on the security risks. New security risks should be identified at the earliest possible opportunity in order to permit a timely response. Should it transpire that the actual risk differs from the actual risk accepted in the IT security concept, resources should be made available to change this situation.

Additional controls:

- Are IT security audits performed regularly?
- When will the next update check be performed?
- If appropriate, are IT security audits also performed by an audit department (if one exists)?

S 2.200 Preparation of management reports on IT security

Initiation responsibility: IT Security Management Team

Implementation responsibility: IT Security Management Team

The tasks of the IT Security Management Team include supporting Management in the execution of its overall responsibility for IT security. A major tool for use here is a report on the current IT security situation. The aim of such a paper should be to provide Management with the information it needs to make the decisions it has to make.

A basic distinction should be made here between two different forms of management report.

1. Regular management reports

The effect of submitting "IT security" management reports as regularly as possible is to ensure that this subject is kept fresh in the minds of Management. In this way, management reports serve to some extent as a tool for raising the IT security awareness of those in positions of overall responsibility. For this reason, such a report should be prepared at least once a year.

The "IT Security" management report should cover the following areas:

- the extent to which the requirements specified in the organisation's IT security concept have already been addressed;
- areas in which security weaknesses, and hence residual risks, remain;
- the extent to which the IT security level matches the organisation's security requirements and its exposure to threats;
- whether the activities performed in pursuit of IT security have been a success;
- whether the IT security measures have proved a suitable means of achieving the IT security objectives.

The report should also consider any further developments expected in organisation-wide IT security.

2. Event-triggered management reports

As well as regular management reports on IT security, it may also be necessary to prepare event-triggered management reports if IT security problems occur unexpectedly or because of risks associated with new technical developments. These are needed above all when it turns out that these problems cannot be resolved "at shopfloor level" because, for example, extra material resources are needed over and above those approved or extensive staff-related rules need to be modified or drawn up. IT security incidents such as global computer virus attacks (e.g. Melissa or Loveletter e-mails) are constantly hitting the mass media headlines. It has proved appropriate to also prepare management reports in these instances in order to show the extent to which this organisation has been affected by these security incidents.

When writing management reports it should be borne in mind that the people who will be reading them are generally not technical experts. Accordingly, the text should be concise and easy to understand. The author should concentrate on the major points, i.e. in particular on existing vulnerabilities but also on successes achieved, and not attempt to convey a "complete" picture.

Basic principle: keep it brief and easy to understand

Management reports - especially those prepared in response to particular events -should always end with a list of recommended actions, *clearly prioritised*, together with a *realistic assessment of the expected cost of implementation of each of these actions*. This will ensure that the decisions needed can be obtained from Management without undue delay.

White Paper

Wherever possible, the "IT Security" management report should not simply be provided to Management in writing but should also be presented in person by a member of the IT Security Management Team. Personal delivery of the report in this way allows special emphasis to be placed on important points, especially on any existing or anticipated security defects. At the same time, the person responsible for IT security making the presentation is directly available for further questions and also to provide fuller explanations, and experience shows that this in turn speeds up the decision process. At the same time, such personal contact offers the opportunity to establish a "small official channel", whose existence could prove extremely useful in an emergency. Instead of or in addition to personal presentation of the management report, another option which should be considered is to make one senior manager who has the appropriate technical background and interest available as a point of contact. Such a course of action can also prepare the way for Management decisions and eliminate problems in advance.

Suitable presentation

Co-operation with Management

As part of the ongoing IT security process, all the "IT security" management reports, if appropriate annotated with the decisions made, should be archived in a systematic fashion together with the other IT security-relevant documents and be made readily accessible to all those in positions of responsibility for security on demand (see S 2.201 *Documentation of the IT security process*).

Documentation

As the IT security management reports will generally contain sensitive information about existing security loopholes and residual risks, they must be kept confidential. Reliable means must be adopted to ensure that they are not disclosed to unauthorised person.

Confidentiality

Additional controls:

- Are the "IT Security" management reports archived together with other documents relating to the IT security process?
- Are there any "suitable" senior managers in the organisation with whom the management report can be agreed in advance so as to prepare the way for its submission?

S 2.201 Documentation of the IT security process

Initiation responsibility: IT Security Management Team

Implementation responsibility: IT Security Officer

The individual phases of the IT security process and the results of the process should be documented. Such documentation is important to maintaining IT security and hence to ensuring that the process continues to develop in an efficient manner. It facilitates identification of the causes of problems and operations which have gone wrong and their elimination. It is important here that not only should the latest version of the documents concerned be easy to get hold of, but central archiving of superseded versions should also be undertaken. This will ensure continuous traceability of developments in the area of IT security, so that it is clear what decisions have been made.

Documentation of the IT security process should as a minimum extend to the following documents:

- Information Security Policy,
- schedules of IT assets (including connectivity plans etc),
- IT security concept(s),
- plans for implementation of IT security measures.
- procedures for the proper and secure use of IT facilities,
- documentation of reviews (checklists, interview notes etc.),
- minutes of meetings and decisions made by the IT Security Management Team,
- management reports on IT security,
- IT security training plans and
- reports on security-relevant incidents.

Controlled access

It is the task of the IT Security Officer to keep documentation up-to-date at all times. He should also ensure that controlled access to the documentation is possible. Here he must ensure that information can be passed to authorised persons rapidly, while at the same time safeguarding the confidentiality of details internal to the organisation.

Additional controls:

- Do procedures aimed at safeguarding the confidentiality of documentation exist?
- How up-to-date are existing documents?

S 2.202 Preparation of an IT Security Organisational Manual

Initiation responsibility: IT Security Management Team

Implementation responsibility: Head of Organisational Section

During the IT security process not only are the documents mentioned in the present safeguards produced but during the implementation phase additional rules covering either the entire organisation or particular jobs are developed. Procedural rules or instructions on actions to be taken are written, and these must be available to every employee as the basis for his actions or omissions at the workplace. These rules must be compiled and made available in a suitable form to each target group. Whereas documentation of the IT security process is an essential tool for the IT Security Management Team, the IT Security Organisational Manual serves as a set of guidelines for all staff affected by the IT security process. In practice, sections of these recommendations are used under names such as "PC Guidelines" or "IT User Guidelines". Different rules, which are geared towards the same key statements but also contain information on rights and duties which are specific to a given function, are needed by different target groups within the organisation. In this way sets of guidelines which specify tasks and responsibilities for different target groups are prepared. Such guidelines could be structured together with superordinate chapters in an IT Security Organisational Manual as shown below:

IT Security Organisational Manual	
Chapter 1	Information Security Policy of the organisation
Chapter 2	IT security guidelines derived from the ISP 2.1IT systems 2.2IT applications
Chapter 3	IT Security Management 3.1 Organisational structure 3.2 IT security-specific tasks 3.3 Responsibilities for meeting security requirements 3.4 Operational structure for the proper and secure use of IT facilities 3.5 Strategic elements of IT security management

Chapter 4	Guidelines on IT security 4.1Guidelines for IT users 4.2Guidelines for IT administrators 4.3Guidelines for technical managers ... 4.n Rules for other responsibilities

Appendices	
IT workstation	A.1 Service instructions for the secure use of IT
	A.2 Handling of secure facilities
Operators	B.1 Service instructions for system operators and administrators
	B.2 Handling of secure facilities
...	

Additional controls:

- Are the key statements and rules on IT security documented?
- Are these documents available to all the staff affected?

S 2.203 Establishment of a pool of information on IT security

Initiation responsibility: IT Security Management Team

Implementation responsibility: Management, IT Procedures Officer

Now that IT is used widely, traditional work routines are undergoing a transformation which requires not only adaptation of organisational structures but also a change in the skills and competence of staff.

It is therefore not sufficient just to compile the necessary rules together from an objective point of view, but active steps must also be taken using didactic techniques to change the skills and competence of staff. IT security awareness promotion and training programmes can assist with this, but at the same time the opportunities presented by the new technologies should also be used to make the necessary information available at the workplace in a context-specific manner. With this objective in mind, the BSI has created an IT Security information desk ("Info Desk") which makes general information, key security policy statements and specific guidelines available online over a graphical user interface in the Intranet of an organisation.

A demo version of this "Info Desk" will be found on the CD-ROM for the manual (see appendix on Additional Aids, German version only). The application is designed so that it can be adapted to the particular circumstances of different agencies or companies. The BSI offers support with setting this up through a set of correspondence course lessons. Beginning with modification of the user interface to reflect the organisation's corporate identity, over a cycle of 18 months the organisation’s own information security policy and specific IT security concepts are integrated into the Info Desk. The correspondence course lessons are sent out by e-mail, which is also used for experience sharing. Further information may be obtained from schulung@bsi.de.

Additional controls:

- Has a pool of information on IT security been set up on the Intranet?

S 2.204 Prevention of Insecure Network Access

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, Auditor

Every insecure access to a network constitutes an enormous security loophole. Therefore every communication to the internal network must without exception be effected over a secure channel. This could, for example, be a firewall (see Section 7.3).

Procedures must be laid down to ensure that no other external connections can be established by circumventing the firewall. All the users must be informed as to the dangers associated with the creation of unchecked access routes, e.g. using modems which staff have brought into work with them.

All external network access routes should be recorded centrally (see Section 2.1). Furthermore, sampling methods should be used to review whether additional network access routes have been established over modems or by any other means. For example, predefined auto-dial call numbers specified can be tested to see whether any data transmission facilities are activated in response.

Data transmission should be properly controlled in all organisations. All data transmission facilities should be approved and their use should be subject to clear rules and procedures. This concerns not only routers, modems and ISDN cards, but also infrared or radio interfaces.

Data transmission should be properly controlled in all organisations. In particular, the following points should be specified:

- persons responsible for installation, maintenance and support
- the user population and usage entitlements
- predefined requirements and security measures covering usage
- possible communications partners
- times during which facilities may be used
- arrangements for covering staff absences
- record-keeping
- secure configuration of data transmission facilities

Examples of the above will be found in S 2.61 *Procedures Governing Modem Usage* and S 2.179 *Procedures Controlling the Use of Fax Servers*.

Additional controls:

- Are all external network access routes documented?
- Have procedures been defined for the use of data transmission facilities?
- Are the procedures governing the use of data transmission facilities regularly adapted to the operational environment and to technical developments?

S 2.205 Transmission and Retrieval of Person-related Data

Initiation responsibility: IT Security Management, Data Privacy Officer

Implementation responsibility: Head of IT Section, Data Privacy Officer

If any person-related data is transmitted from the employer's or customer's premises to a "remote" workplace (e.g. of a telecommuter), the relevant data privacy protection provisions must be adhered to. Under §9 of the Federal Data Protection Act (BDSG), it is especially important in such cases to prevent unauthorised persons using the data transmission facilities to access IT systems (user supervision). Furthermore, steps must be taken to ensure that it is possible to check and determine in which offices or locations person-related data can be transmitted using data transmission facilities (transmission supervision).

The transport route or transmission method should be selected in such a way as to provide assurance of both the confidentiality and integrity and also the authenticity (proof of origin) of the person-related data.

If the transmission of person-related data occurs in the context of an automated retrieval procedure, the special requirements relating to reliability contained in the relevant legislation must be complied with.

General aspects

- The occasion and purpose as well as the persons or offices involved in the retrieval procedure must be established.
- Retrieval permissions must be defined and monitored.
- The type and scope of the data held must be specified.
- Retention periods and deletion dates must be defined for data.
- The cases in which the person/office holding the information must be informed of the person/office retrieving it must be specified.
- The transport route must be specified, e.g. access over an ISDN dial-up line, callback protection based on CLIP or COLP (see S 5.49).
- Suitable cryptographic procedures (e.g. symmetric and asymmetric encryption or digital signature) must be employed in order to prevent violation of the data privacy protection legislation during transmission of sensitive data. Section 3.7 *Crypto Concept* describes how to select procedures and products that are suitable.
- If person-related data is exchanged regularly or continuously over a transport route, then transmission should be protected using a virtual private network (VPN) (see S 5.76 *Use of Suitable Tunnel Protocols for RAS Communication* and S 5.83 *Secure Connection of an External Network with Linux FreeS/WAN*).

Safeguards against unauthorised retrieval

Retrieval of data by unauthorised persons must be prevented by means of suitable precautions:

- Every user must be uniquely identified and authenticated to the IT systems from which the person-related data is retrieved.
- Authorisation should be blocked after a specified number of unsuccessful attempts.
- Passwords must be changed at regular intervals. As far as possible, this must be enforced by the relevant programs.
- Program-controlled checking procedures should be used to review the log files.
- The type and scope of logging must be specified (see also S 2.110 *Data Privacy Guidelines for Logging Procedures*).
- Random sampling checks should be performed or else continuous logging should be carried out.
- The place at which logging is performed must be specified (the retrieving and/or originating party).
- Logging must be designed in such a way that it is possible to determine after the event which retrieval permissions were used when data was retrieved.
- The reasons for retrieving the data must be logged.
- Where data is retrieved, which connection and which terminal devices were used during transmission must be logged.

Measures for organisational supervision

- All staff, especially those in the office which retrieves the data must be under an obligation to maintain confidentiality of the data. Passing on of data to third parties must be contractually prohibited.

Additional controls:

- Have the technical and organisational measures implemented been documented?
- Is there a concept covering the review and assessment of the reliability of data transmissions involving automated retrieval?

S 3 Safeguard Catalogue - Personnel

S 3.1	Well-regulated familiarisation/training of new staff with their work
S 3.2	Commitment of staff members to compliance with relevant laws, regulations and provisions
S 3.3	Arrangements for substitution
S 3.4	Training before actual use of a program
S 3.5	Education on IT security measures
S 3.6	Regulated procedure as regards termination of employment
S 3.7	Point of contact in case of personal problems
S 3.8	Avoidance of factors impairing the organisation climate
S 3.9	Ergonomic workplace
S 3.10	Selection of a trustworthy administrator and his substitute
S 3.11	Training of maintenance and administration staff
S 3.12	Informing all staff members about possible PBX warning notices, warning symbols and acoustic alarm signals
S 3.13	Increasing staff awareness of potential threats to the PBX
S 3.14	Briefing personnel on correct procedures of exchanging data media
S 3.15	Information on the use of fax machines for all employees
S 3.16	Briefing personnel on the operation of answering machines
S 3.17	Briefing personnel on modem usage
S 3.18	Log-out obligation for PC users
S 3.19	Instructions concerning the correct use of the security functions in Peer-to-Peer networks
S 3.20	Instructions concerning the operation of protective cabinets
S 3.21	Training and further education of telecommuters as regards security-related issues
S 3.22	Regulations concerning substitution of telecommuters
S 3.23	Introduction to basic cryptographic terms

S 3.1 Well-regulated familiarisation/training of new staff with their work

Initiation responsibility: Agency/company management; Head of Personnel Section

Implementation responsibility: Personnel Section; superiors

New staff must be made aware of the in-house IT-related regulations, practices and procedures. Without adequate training to the job, they do not know who to turn to as regards IT security issues; they do not know which IT safeguards have to be implemented and what IT security policy is pursued by the agency/company. This can result in disruption and damage affecting IT operations. Consequently, great importance must be attached to the well-regulated familiarisation of new staff with their work environment.

Familiarisation / training should, as a minimum, include the following:

- planning of the required training activities; training schemes specifically designed for the respective workplaces (cf. also S 3.4 *Training before actual use of a programme* and S 3.5 *Education on IT security measures*);
- introduction of all persons acting as points of contact, particularly for IT security questions;
- explanation of the in-house regulations and rules as regards IT security.

For the purpose of training staff for their jobs, it is useful to have an inter-office slip or a checklist showing the various activities and the familiarisation level attained.

Additional controls:

- What provisions have been made for training new staff to their jobs?
- How much time are new staff members allowed for training to the job?

S 3.2 Commitment of staff members to compliance with relevant laws, regulations and provisions

Initiation responsibility: Head of Personnel Section; departmental data privacy officer; IT Security Management

Implementation responsibility: Personnel Section; superiors

When new staff members are employed, they should be put under obligation to observe the relevant legal provisions (e.g. Section 5 of the *Federal Data Protection Act*: data secrecy), regulations and in-house rules. For this purpose, new staff members must be made familiar with the existing IT security rules and regulations and, at the same, be motivated to comply with them. To achieve this, it is advisable not only to impose such an obligation but also to provide the staff concerned with the required copies of the pertinent rules and regulations and to have them sign a receipt, or to submit these copies to employees in a central position for the purpose of review.

Additional controls:

- In which way is such an obligation imposed?
- Is the compliance commitment laid down in writing?
- Are copies of the pertinent documents supplied to new staff for reference and keeping?
- Are the employees aware of the legal framework which determines their tasks?

S 3.3 Arrangements for substitution

Initiation responsibility: Head of Organisational Section; IT Security Management

Implementation responsibility: Superiors

Substitution arrangements are designed to ensure continuity of operation in case of absence or loss of personnel, both foreseeable (vacation, business/official trip) and unforeseeable (illness, accident, notice of termination of employment). Therefore, before such a situation arises, provisions will have to be laid down on who will substitute for whom in what fields of activity and with which authorities. This is of particular importance as regards information processing which usually requires special knowledge precluding that persons unfamiliar with the subject matter could be given training in good time to act as substitutes.

For substitution, the following general conditions must be met:

- For assumption of tasks by substitutes, sufficient documentation must be provided on the current status of the relevant procedures and on the respective project.
- As a rule, designation of a substitute will not suffice; consideration must be given to the training required by substitutes so that they will be qualified to assume the specific tasks. If it comes to light that there are persons who, on account of their specialist knowledge, cannot be replaced at short notice, their unavailability constitutes a serious threat to normal operations. In such cases, training of a substitute is of crucial importance.
- It must be laid down what range of tasks will have to be assumed by which substitute(s).
- Designated substitutes may be granted the necessary entry and access rights only when they actually have to act as deputies.
- If, in exceptional cases, it is not possible to designate or train a competent substitute, early thought should be given to which external staff might be called in to act as substitutes.

Additional controls:

- What provisions are made by the various organisational units as regards substitution?
- Are substitutes available who are sufficiently competent?
- Has the unforeseen need arisen recently to provide substitutes?
- Within the organisational unit, is there a *single source of knowledge*, i.e. one person who, by himself/herself, has all the expertise required for IT uses?

S 3.4 Training before actual use of a program

Initiation responsibility: Head of Personnel Section; superiors

Implementation responsibility: Superiors; staff responsible for the individual IT applications

Damage caused by improper handling of IT applications can be avoided if the users are given a detailed briefing on the respective IT applications. Therefore, it is a must for users to be sufficiently trained before assuming IT-supported tasks. This refers to both the use of standard programme packages and specifically developed IT applications.

In addition, training will also have to be provided in case of extensive changes to a given IT application.

Where self-explanatory user manuals on IT applications are available, autodidactic training may be requested. in this case, it is essential that the staff members concerned be given sufficient time for such self-education.

Additional controls:

- Have staff members who are to assume an IT function with which they are not yet acquainted been sufficiently trained? Has a training schedule been developed as regards the introduction of a new IT application?
- Which IT applications have been added since the last review? How have the staff been familiarised with such tasks? Which training activities have since then been attended by staff members?

S 3.5 Education on IT security measures

Initiation responsibility: Superiors, IT Security Management

Implementation responsibility: Superiors, IT Security Management

In the majority of cases, damage in the IT field is caused by negligence. In order to prevent this, everybody must be motivated to exercise care in the use of information technology. In addition, procedures must be provided which help the individuals concerned to better understand IT safeguards. In particular, the following subjects should be included in training on IT security safeguards:

- **Building IT security awareness**

  Every staff member must be made aware of the need for IT security. A suitable first step for introducing staff to the subject is to make them aware of the dependence of the agency/company, and hence of their jobs, on the smooth functioning of IT systems. In addition, the value of information should be highlighted, especially with regard to confidentiality, integrity and availability. These awareness-building activities should be repeated periodically, possibly also supplemented by practical information, e.g. through in-house circulars.

- **Staff-related IT safeguards**

  Under this heading, information should be provided on all safeguards which have been developed within the framework of an IT security policy and which are to be implemented by the various staff members. This part of the training effort is very important since many IT safeguards can be applied effectively only after adequate education and motivation.

- **Product-related IT safeguards**

  Under this heading, information is provided on IT safeguards inherent in a particular product and already present when the product is supplied. These can, for example, be registration passwords, screensavers, or encryption features for documents or data fields. Recommendations regarding the structure and organisation of files containing transaction data can facilitate the granting of access rights and considerably reduce the work involved in data protection.

- **Conduct in the event that a computer virus appears on a PC**

  Staff members should be instructed on how to handle computer viruses. Such training might cover the following (cf. S 6.23 *Procedure in case of computer virus infection*):

  - detection of computer infection,
  - action and types of computer viruses,
  - immediate response when virus infection is suspected,
  - measures to eradicate the computer virus,
  - preventive measures.

- **Proper use of passwords**

  In this context, the importance of a password for IT security and the overall prerequisites for ensuring effective use of passwords should be explained (cf. also S 2.11 *Provisions governing the use of passwords*).

- **The importance of data backup and its implementation**

  Regular data backup is one of the most important IT safeguards in any IT system. Trainees must be instructed in the data backup policy (c.f. Chapter 3.4 *Data Backup Policy*) of the agency/company and about the data backup tasks to be carried out by each individual. This is of particular significance for PC uses where data backup is incumbent on each user individually.

- **Handling of person related data**

  Person related data requires particularly careful handling. Staff members who work with person related data (both in IT systems and in written records) must be trained in the statutory safeguards required. Subjects to be covered are: handling of information requests, requests for amendments and corrections from the individuals concerned, legally stipulated deletion deadlines, protection of privacy and communication of data.

- **Briefing on emergency measures**

  All staff members (including persons not directly concerned with IT, e.g. entrance control staff or guards) must be briefed on the established emergency measures. Their briefing should include information on emergency exits/escape routes, procedures in case of fire, handling of fire extinguishers, the emergency reporting system (who must be notified first by what means) and use of the Emergency Procedure Manual.

- **Prevention of social engineering**

  Staff should be informed of the dangers of social engineering. The patterns which attempts to gain confidential information through targeting individuals typically take should be explained, as well as the relevant methods of protection. As social engineering often involves the pretence of a false identity, staff should be regularly instructed to check the identity of communication partners and not to provide confidential information over the telephone, in particular.

When implementing training courses, it should always be remembered that it is not enough to only train a member of staff once during his entire term of employment. With most forms of training, especially front desk training courses, if a lot of new information is presented at once participants can be overwhelmed. Only a small amount of the information reaches long-term memory, and 80% is generally forgotten again at the end of the training course.

For this reason, staff should receive regular training on the subjects of IT security and indoctrination regarding its importance. For example, this could take any of the following forms:

- short events devoted to current IT security topics,
- inclusion at regular events such as departmental meetings, or

- interactive training programs which are available to all staff.

Additional controls:

- Which subjects regarding IT safeguards have already been covered by training activities?
- Are new staff members appropriately briefed on the IT safeguards?
- What training is offered at what intervals?
- Are all the required areas covered in the training courses?

S 3.6 Regulated procedure as regards termination of employment

Initiation responsibility: Head of Personnel Section; superiors; IT Security Management

Implementation responsibility: Personnel Section; superiors

In case of termination of employment, the following should be observed:

- Before termination of employment, the designated successor of the individual concerned must be given a briefing on the tasks.
- All documents, issued keys, borrowed IT equipment (e.g. laptops, data media, documentation) must be recovered. In particular, agency/company passes must be collected in from the staff member terminating his/her employment.
- All entry and access rights held by the departing staff member must be revoked or deleted. This includes external access authorisations over data communications equipment. If, in exceptional cases, several persons shared one access right to an IT system (e.g. by using a common password), the access rights must be altered upon termination of employment by one of those individuals.
- Before the person leaves, it should be explained to him explicitly one more time that all confidentiality agreements remain in force and that no information obtained in the course of his work may be disclosed.
- If the departing staff member was assigned any functions under a contingency plan, the plan must be updated.
- All persons entrusted with security tasks, especially entrance control staff, must be informed of the departure of the person.
- Individuals no longer employed with the agency/company must be denied uncontrolled access to the agency/company premises, especially entry into rooms housing IT systems.
- Optionally, all entry and access rights relating to IT systems may be revoked even for the period from giving notice of termination to actual termination of employment, and in addition, the individual concerned may be prohibited from entering rooms requiring protection.

A useful way of doing this is to use inter-office slips which lay down the various steps to be taken by a staff member before leaving the agency/company.

Additional controls:

- Are regular provisions applied in case of termination of employment?
- Are the relevant bodies informed of the termination of service by a staff member?
- What steps are taken to ensure that all entry and access rights of a staff member terminating his/her employment are revoked and deleted?

S 3.7 Point of contact in case of personal problems

Initiation responsibility: Head of Personnel Section; personnel committee/works council Implementation responsibility: Personnel Section; personnel committee/works council Inadequate performance of duties may often be due to personal problems of an employee. Examples of such problems are, for instance, a high level of indebtedness, addiction-related illness, or difficulties encountered at the place of work (excessive or too little demands made upon an employee; mobbing). In order to help the individual concerned to cope with such problems, it may be helpful in many cases if he/she can turn to a confidant. That person, acting as a point of contact, should both attend to the interests of the individual concerned and offer him/her practical assistance and safeguard the interests of the company/agency and, jointly with the individual concerned, explore possible solutions.

However, it must be possible also for superiors and colleagues to turn to such a confidant (e.g. shop stewards) when peculiarities by third parties have been observed which point to lessened reliability of the individual concerned. The confidant must be able to speak, and offer help, to the individual concerned.

Such a role can be assumed by the personnel committee, works council, company medical officers. All staff members must be informed of the establishment of such a point of contact. External advice is provided, for instance, by the counselling centres of statutory health insurance funds.

Additional controls:

- Who can be contacted by staff members if they have any personal problems?

S 3.8 Point of contact in case of personal problems

Initiation responsibility: Head of Personnel Section; personnel committee / works council

Implementation responsibility: Personnel Section; personnel committee / works council

Appoint a confidant

An employee's inadequate performance of duties may often be due to personal problems. Examples of such problems include a high level of indebtedness, addiction-related illness, or difficulties encountered at the place of work (e.g. excessive or too few demands made on an employee, mobbing). It can often help the individual concerned to cope with such problems if he/she has a confidant to turn to. That person, acting as a point of contact, should attend to the interests of the individual concerned and offer him/her practical assistance, while at the same time safeguarding the interests of the company/agency and, jointly with the individual concerned, explore possible solutions.

However, it must also be possible for line managers and colleagues to turn to this a confidant when strange actions or behaviour have been observed in another individual which suggest he/she has become less reliable. The confidant must be able to speak to and offer help to the individual concerned.

Such a role can be assumed by the staff council, works council or company medical officers. All staff members must be informed of the establishment of such a point of contact. External advice is provided, for instance, by the counselling centres of statutory health insurance funds.

Additional controls:

- Who can be contacted by staff members if they have any personal problems?

S 3.8 Avoidance of factors impairing the organisational climate

Initiation responsibility: Agency/company management; Head of Personnel Section; personnel committee/works council

Implementation responsibility: Superiors; Personnel Section; personnel committee/works council

A positive organisational climate motivates staff to observe IT security safeguards, while at the same time reducing the incidence of negligent or deliberate acts which can cause disruption to the IT operation. Efforts should therefore be made, also from an IT security point of view, to achieve a positive working atmosphere. There are so many ways available for achieving this that only a selection of measures is given here, the appropriateness of which must be determined on a case-by-case basis:

- provision of a social centre,
- avoidance of overtime,
- observance of rest breaks,
- regulated division of responsibilities,
- even distribution of workload,
- performance-related pay.

Resolve any communication problems

Communications problems in an organisation almost inevitably lead to security problems as well. In extreme cases, this can result in deliberate security violations. But even if the users merely find the security measures "annoying" because they have not been informed of the purpose of the measures, this can result in their being circumvented.

Being the one to report bad news must not mean that the messenger has to live in fear of punishment. The organisational climate should be such that every person concerned is able to report security incidents within his/her own organisation and to tackle them openly as well.

Staff motivation

Financial incentives are not the only way to motivate staff, but it is especially important that they should feel their work is valued. Wherever possible, staff should be included in decisions. At the very least, they should be informed of the reasons for the decisions which have been made so that they become actively involved in implementing them.

For example, often protests against the choice of certain hardware or software are couched in arguments on the part of the users that the hardware or software they have been allocated is not a secure as the one they preferred.

Additional controls:

- How is the organisational climate rated by the staff?
- How do line managers rate the existing organisational climate?
- Which factors having a negative influence on the organisational climate are most frequently mentioned?

S 3.9 Ergonomic workplace

Initiation responsibility: Head of Site/Bldg Technical Service; personnel committee/works council

Implementation responsibility: Superiors; personnel committee/works council; staff members

In addition to the clear description of tasks, duties, rights and responsibilities, sound and effective IT operations require provisions ensuring that optimum use can be made of IT systems.

The design of the workplace must be consistent with ergonomic principles. It must be possible for the chair, table, display screen and keyboard to be adjustable so that faultless IT operations can be ensured and promoted. *Inter alia*, this implies that it must be possible to adjust the back, the height and the seat of the chair, and that it must be possible for the working materials to be arranged in a way to minimise the inconvenience involved for the respective functions.

An appropriately designed workplace will also facilitate compliance with IT safeguards. If lockable desks and cabinets are available, data media, documents and accessories can be kept there under lock and key.

S 3.10 Selection of a trustworthy administrator and his substitute

Initiation responsibility: Agency/company management; Head of Personnel Section; Head of IT Section; PBX officer; IT Security Management

Implementation responsibility: -

The operators of IT systems and PBXes (telecommunications facilities) must have great confidence in the administrators (and their deputies) of such systems and installations. Depending on the systems used, they hold far-reaching and often complete authority. Administrators and their deputies can access, and possibly alter, all stored data and allocate rights in a way that allows serious potential misuse.

The staff employed for these tasks should be selected carefully. They should be periodically instructed that the relevant powers may be used only for the required administration tasks.

As administrators play a key role in ensuring that the hardware and software used is in working order, it must be ensured that someone else performs the administrators' tasks in their absence. The appointed substitute must have the up-to-date system configuration and have access to the passwords, keys and security tokens required for the administration.

If a company or an authority has several administrators with similar IT system knowledge, they can substitute each other if they have enough free capacities. In all areas in which just one administrator has the main responsibility for IT systems, two substitutes should be trained, as experience shows that if the administrator is absent for a long period of time, the substitute may not be available to take over all of the administration.

In order to ensure that the computer utility is in working order, it must be checked whether the necessary administration activities can be dealt with by the appointed administrators and their substitutes. This is particularly important when there are impending staff changes or changes to the organisational structure.

Particularly in the case of impending moves, administration tasks at another location can cause a considerable increase in the administrator's work load. In such cases, it must also be ensured that the operation at the previous location is not impaired up to the time of the move.

Additional controls:

- How has the reliability of the administrator and of his deputy been verified?

S 3.11 Training of maintenance and administration staff

Initiation responsibility: Agency/company management; Head of Personnel Section; Head of IT Section; PBX officer; IT Security Management

Implementation responsibility: Superiors

Maintenance and administration staff require detailed knowledge of the IT components used. Therefore, they should at least receive training that will enable them

- to carry out routine administration tasks independently;
- to detect and remedy simple faults;
- to carry out data backup by themselves;
- to understand the measures taken by external maintenance staff, and
- recognise manipulation attempts or unauthorised access to the systems.

As a rule, relevant training will be offered by the suppliers of the IT systems or PBX facilities. In addition, the administrators of PBXs should be able

- to assess the operational behaviour of the PBX by means of the control messages displayed on the devices;
- to de-activate and to activate the PBX on their own initiative.

S 3.12 Informing all staff members about possible PBX warning notices, warning symbols and acoustic alarm signals

Initiation responsibility: PBX officer; IT Security Management; personnel committee/works council

Implementation responsibility: IT Security Management, Administrators

All staff members should be aware of the meaning of warning notices and/or symbols and acoustic alarms of the PBX (telecommunications facility). In particular, this includes the following:

- attention signal for direct voice calling;
- busy override warning signal (trunk offering tone);
- indication of handsfree operation;
- indication of activated direct voice calling;
- indication of automatic call-back; and
- indication/flash in case of an add-on (three-party) conference.

The use of features which are not officially authorised can be especially crucial to IT security. The warning indicators for these features should be known to all users.

Additional controls:

- Do the staff know what will happen if somebody makes a busy override call?
- Do the staff know what will be indicated visibly and audibly by a direct voice call?
- Is it possible to discern activation of handsfree operation?

S 3.13 Increasing staff awareness of potential threats to the PBX

Initiation responsibility: PBX officer; IT Security Management; personnel committee/works council

Implementation responsibility: IT Security Management, Administrators

Staff members must be advised of the risks involved in the use of a digital PBX (telecommunications facility). This could be done, for instance, by means of a short briefing or instruction sheets. It must be borne in mind that abnormal behaviour of a PBX should be reported. Since in case of manipulations of a PBX installation, involvement of the PBX operator cannot be precluded, an independent controller, such as IT Security Management or departmental data security officers, should be informed in such cases.

Additional controls:

- Is awareness training repeated in regular intervals?
- Are new employees made aware of the possible dangers involved in PBX operation?

S 3.14 Briefing personnel on correct procedures of exchanging data media

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management

Inadequate briefing and instruction of employees often causes restrictions on the forwarding of information to be ignored or neglected. Consequently, the persons involved in the exchange of data media should on all accounts be informed of specifications as to which communications partners should receive which data when (S 2.42 *Determination of potential communications partners*). Furthermore, the fundamental steps comprising the exchange of data media are to be defined (as work regulations, if required) and adherence to them made obligatory for employees.

Employees involved in the exchange of data media are also to be familiarised with threats which could materialise before, during or after the transport of data media, as well as the safeguards required to avert these threats.

If certain IT-supported procedures are used to protect data while it is being exchanged (e.g. encryption or checksums), employees involved in the exchange of data must be briefed adequately on handling these procedures.

Additional controls:

- Are all employees authorised for communication aware of the related regulations?
- Are employees familiar with encryption or checksum procedures being implemented?
- Are the persons responsible for the exchange of data media sufficiently aware of the potential threats involved?

S 3.15 Information for all staff about the use of faxes

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

All employees must be informed about the special features of fax transmissions and of the fact that the legal force of a fax message is greatly limited. Where conventional fax machines are used, a clearly written set of operating instructions should be placed by the fax machine. Where a fax server is used, users should at least be given a quick reference guide to the fax client software used.

In particular, procedures should be laid down covering the following points, possibly in the form of a standard operating procedure:

- the name of the Fax Officer responsible for the manual distribution of incoming fax transmissions and a point of contact on fax-related problems;
- who may use the fax machine or fax server;
- sending of confidential information by fax should be avoided;
- a uniform fax cover sheet should be used;
- senders and recipients should co-ordinate the exchange of confidential information by fax on the telephone prior to actual transmission;
- individual transmission receipts and transmission logs should be checked for correct transmission, added to the documentation and, if necessary, archived;
- when using a fax server with automatic distribution of incoming faxes, incoming faxes should be printed out for the files and/or electronically archived;
- outgoing faxes which are sent over a fax server should be printed out for the files and/or archived electronically;
- address books and distribution lists should be monitored regularly to ensure that faxes are not being sent out to the wrong people by accident.

Additional controls:

- Are all employees informed on the correct use of faxes, and are new staff appropriately instructed in this respect?
- Do all staff know who contact in the event of problems with faxes?

S 3.16 Briefing personnel on the operation of answering machines

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

Every person using an answering machine in his/her sphere of activities should be familiarised with its operation and capabilities. This precludes improper handling to a large extent. Furthermore, the related IT safeguards mentioned in Chapter 8.3 *Answering Machine* are to be made well known.

Additional controls:

- Has every user of an answering machine been briefed appropriately?
- Are operating and safety instructions available?

S 3.17 Briefing personnel on modem usage

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management

Employees are to be informed about possible threats, required safeguards and regulations concerning the operation of modems. Particularly the effects of different configurations on the operational security of modems are to be elucidated.

All modem users should acquaint themselves with the operation and capabilities of their modem.

Additional controls:

- Are operating and safety instructions available?

S 3.18 Log-out obligation for users

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section, IT Security Management

Where an IT system is used by several users and these persons have different access rights to the data or programs stored in the IT system, an access control system will only provide the necessary protection if every user logs off after finishing his/her task on the IT system. If it is possible for a third party to work on an IT system under the identity of another person, no form of access control is possible. Therefore all users must be obliged to log off after finishing their tasks. For technical reasons (e.g. in order that all opened files are closed), procedures should also be defined for logging off from IT systems when no access control system is in operation.

Screen lock

Where absence from the PC is likely to be of only short duration, instead of logging off it is acceptable to manually activate the screen lock (see also S 4.2 *Screen lock*). When the user is away from his/her desk for an extended period, the screen lock should automatically be activated.

Automatic logoff

Some IT systems allow a period to be specified, such that users are automatically logged off from the system when they have been inactive for a certain length of time. On the other hand, such a system can also lead to loss of data, so it should be thought about carefully. An automatic logoff system could be used, for example, in PC pools which are heavily accessed by the public since here a user who is logged on could block the workstation with the aid of the screen lock without good reason.

Depending on the workstation environment, consideration should be given to what precautions should be taken for short-term absences of users. Thus the screen lock should be automatically activated more quickly, e.g. after only five minutes, in multi-user systems than in systsems used by only one user.

Additional controls:

- Are new staff and deputies also placed under the obligation to log off once they have finished with the computer?
- Are staff reminded at regular intervals of the obligation to log off?

S 3.19 Instructions concerning the correct use of the security functions in Peer-to-Peer networks

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

Instructions concerning the correct use of security functions are particularly important in Peer-to-Peer networks under WfW and Windows 95, where the users themselves have to carry out security tasks. Each user must therefore be trained in advance regarding the following points:

Data exchange using shared directories

- The user must be trained in the correct use of the sharing of resources and the correct cancellation of directory sharing. Particular emphasis should be placed on the possibility of concealing shared directories or printers by adding the character "$" so that other users cannot see that sharing has been granted. It should be pointed out that the incentive for attacks can be reduced if share names are used which do not provide information on the contents and if resources are only shared for as long as required.
- The meaning of the options when sharing or connecting directories or printers should be made clear and the adherence to the various settings pointed out:

"share on start-up"	automatic sharing when WfW is started, without user interaction
"Connect on start-up"	automatic connection when restarting
"Save password in the password list"	Storing of the password (critical to security) so that it does not have to be re-entered when connecting the next time

Users of Windows 95 and Windows NT must take note that every enabled share must explicitly be undone, otherwise it will still apply after a restart

- The names of the access rights under WfW and Windows 95 are not self explanatory and have to be explained:

"Write-protected access"	Right to read files and execute programs
"Read/write access"	Right to read/write files, execute programs, create and delete files
"Access dependent on password"	The right to read and write files can be granted separately

Within Windows 95 all users can choose between the rights "write-protected access", "all access rights" and "user-defined" if access protection is implemented at the user level. Users must then be notified that

directories should never be approved with "all access rights". Ideally, they are user-defined with read and write privileges for other users

Awareness of security

- The user should be instructed in the security-relevant controls he must implement. He must also be informed of how the network monitor and log functions are to be used.
- The use and exchange of passwords should be explained in accordance with the security strategy.
- Under WfW and Windows 95 the user must be informed that
  - passwords for access to resources of other computers are stored in the file [*username*].*pwl*,
  - under WfW the resources of other WfW computers are entered in the file *connect.dat*, which are automatically connected when WfW is started,
  - the user's own resources are entered in the file *shares.pwl*, which are automatically shared when starting.

  These files can be deleted by users without infringing the system integrity. This is particularly sensible for the file *[username].pwl* if passwords have accidentally been saved.
- In the event that name conventions exist for the computers and users in the network, the users should be informed of these and any names which have already been allocated.

Additional controls:

- Have all users of the WfW network been sufficiently trained?
- Are certain aspects of the awareness training repeated at irregular intervals?

S 3.20 Instructions concerning the operation of protective cabinets

Initiation responsibility: IT Security Management

Implementation responsibility: IT security management, manufacturer

Following the purchase of a protective cabinet, users must be familiarised with correct operation. This should also occur when a task involving use of the protective cabinet is reassigned. As a minimum requirement, the following points must be conveyed:

- Correct procedure with the lock of the protective cabinet must be demonstrated. Typical errors should be pointed out, for example not wiping code locks. The rules governing key management, safekeeping of keys and replacement regulations must be outlined. In particular, individuals must be called on to lock the protective cabinet when not in use, even for a short period.
- The keyboard of a server must always be kept in the server cabinet so that no unauthorised console inputs can be made.
- As far as server cabinets are concerned, it should be pointed out that unnecessary inflammable materials (print-outs, surplus manuals, printer paper) should not be kept in the server cabinet.
- Data backup media of the server should be stored in another fire zone. Keeping them in the server cabinet is therefore inappropriate and only permissible if a duplicate of the data backup medium is relocated to another fire zone.
- If an air-conditioned server cabinet is used, the times the server cabinet is open should be kept to a minimum. Where necessary, sporadic checks should be carried out to determine whether there is any water condensation in the server cabinet.

Additional controls:

- Have people in charge of a protective cabinet been familiarised with its operation?

S 3.21 Training and further education of telecommuters as regards security-related issues

Initiation responsibility: Superiors, IT Security Management

Implementation responsibility: Superiors, IT Security Management

Telecommuters work partly or exclusively at home. Consequently, the security measures required in this case partly differ from those pertaining to work at the institution itself. For this reason, it is necessary to prepare a security concept for telecommuting workstations. Following the announcement of this concept, telecommuters must be briefed on the security measures to be implemented and, if necessary, trained to observe them. In addition, telecommuters must be trained to handle telecommuting workstations to the extent that they are able to perform simple maintenance tasks and solve simple problems independently.

Additional controls:

- Have special IT security concepts been prepared for telecommuting?
- Have telecommuters been trained to implement IT security measures?

S 3.22 Regulations concerning substitution of telecommuters

Initiation responsibility: IT Security Management, Superiors

Implementation responsibility: Telecommuter

In addition to safeguard M 3.3 *Arrangements for substitution*, further measures are required if a telecommuter needs to be substituted. As telecommuters work mainly outside the institution, an information flow between them and their stand-ins must be guaranteed. Documentation of the results of work performed by telecommuters is also indispensable. In addition, it might be advisable for telecommuters and their stand-ins to meet on a sporadic or regular basis.

It is also necessary to prepare regulations on how stand-ins are to access data and documents from telecommuting workstations should the need for this arise unexpectedly.

Additional controls:

- Have stand-ins for telecommuters been appointed?
- Have test substitutions been performed?

S 3.23 Introduction to basic cryptographic terms

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: Head of IT Section, IT Security management

As far as the user is concerned, the use of crypto products may mean additional effort or -- depending on the complexity of the products used – may even require a greater depth of knowledge. All staff who are supposed to make use of cryptographic procedures and products should therefore be made aware of the usefulness and necessity of the cryptographic techniques and be given an introduction to basic cryptographic terminology. This applies in particular of course to staff whose role it is to draw up a crypto concept or select, install or manage crypto products.

The following sections are intended to provide an elementary understanding of the fundamental cryptographic mechanisms. Examples are described as a means of explaining which cryptographic technique can be used in which situation.

Elements of cryptography

The term cryptographic refers to mathematical methods and techniques that can be used for protecting information against unauthorised disclosure and/or intentional manipulation. The protection of information by cryptographic methods – in contrast with infrastructural and technical safeguards – is a *mathematical-logical* form of protection.

Cryptographic procedures entail the implementation of a mathematical calculation process – an *algorithm* – through specific techniques. Their effectiveness is based on the assumption that a potential attacker will be unable to solve a certain mathematical problem - and not because of a lack of particular skills but because of not having knowledge of quite specific "key" information.

Cryptographic methods always relate to the following situation: a sender A (commonly referred to in cryptography as "Alice") sends a message via a *non-secure channel* to a recipient B (referred to as "Bob").

The sender and recipient may also be identical in this case, and the term "channel" may refer to any transport medium. When it is a matter of encrypting local data, the sender and recipient are of course identical, and the "channel" is taken to be the storage medium.

Basic cryptographic objectives

Theoretical and practical considerations lead to a distinction being drawn between four basic cryptographic objectives:

1. Confidentiality/secrecy: no unauthorised third party E (let her name be "Eve") is to gain access to the contents of the message or file.
2. Integrity: It must be possible to detect unauthorised manipulation of the message or file (e.g. the insertion, omission or replacement of parts).
3. Authenticity:

- Proof of identity (authentication of communications partners): a communicating party (e.g. a person, organisation or IT system) must be able to prove its identity beyond doubt to another party.
- Proof of origin (authentication of messages): A must be able prove to B that a message originates from A and has not been altered.

4. Non-repudiation: the emphasis here in comparison with message authentication is placed on verifiability with respect to third parties.
   - Non-repudiation of origin: it should be impossible for A to deny having sent a certain message to B after the event.
   - Non-repudiation of receipt: it should be impossible for B to deny having received a message sent by A after the event.

It is plain that there are connections between these objectives, but one fundamental understanding of modern cryptography is as follows: the guaranteeing of confidentiality and of authenticity are separate basic aims of a cryptographic system: authentication restricts the circle of potential senders of a message, while confidentiality restricts the circle of potential recipients.

The primary cryptographic method for preserving confidentiality is **encryption**, and the primary methods of guaranteeing integrity, authenticity and non-repudiation are **hash functions, message authentication codes (MACs), digital signatures** and **cryptographic protocols**. The individual cryptographic concepts are described briefly in the following.

I. Encryption

Encryption (encipherment) transforms a plaintext, in accordance with an item of additional information known as the key, into an associated secret text (ciphertext or enciphered text) that should not be decryptable for anyone who does not know the key. The reverse transformation – reclaiming the plaintext from the ciphertext – is known as decryption or decipherment. In all state-of-the-art encryption algorithms, plaintexts, ciphertexts and keys are each represented as sequences of bits.

For them to be useable in practice, encryption algorithms must satisfy the following minimum requirements:

- They should be resistant to deciphering, i.e. it must be impossible to decrypt the ciphertext without knowledge of the key; in particular, the quantity of possible keys must be "sufficiently large", because otherwise it would simply be possible to try out all keys.
- They must be easy to use.
- Encryption and decryption must be "fast enough".

The requirement for resistance to deciphering must always be considered relative to current technical and mathematical possibilities. An important factor in the assessment of encryption algorithms is that it must be practically impossible at the time of use to decrypt the ciphertext without knowledge of the key, i.e. impossible with the technology available at the time within an acceptable timescale.

When A and B want to establish a confidential connection, they proceed as follows:
1. They agree on an encryption procedure.
2. They agree on a key or a pair of keys.
3. A encrypts a message and sends this to B.
4. B decrypts the ciphertext sent from A.

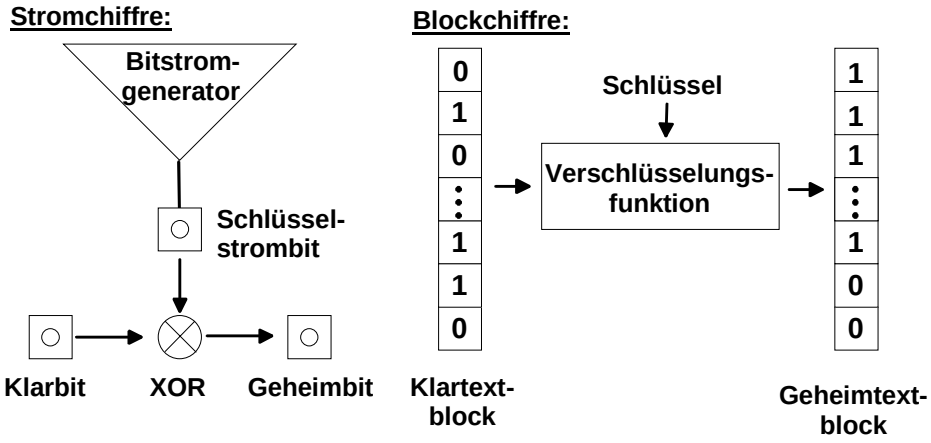
There are two major classes of encryption procedures:

Symmetrical encryption procedures use the same key both for encryption and decryption. Symmetrical techniques are therefore also occasionally referred to as "one-key" techniques, because knowledge of one key is sufficient to be able to encrypt and decrypt texts.

Well-known symmetrical encryption procedures include DES, Triple-DES, IDEA and RC5, for example.

Symmetrical procedures are further differentiated, distinguishing between stream ciphers and block ciphers.

In the case of stream ciphers, a key is used to generate a bit sequence (or bit stream) with as random an appearance as possible, which is added to the plain bit sequence (modulo 2). The plain bit sequence is therefore encrypted bit by bit (by the addition of key stream bits). It is essential for the security of stream ciphers that two (different) messages are never encrypted with the same key stream – this must be ensured with the aid of special measures (synchronisation information in the form of a message key). Examples of stream ciphers are RC4 and SEAL.



In the case of block ciphers, on the other hand, an entire block of bits is encrypted in one encryption cycle; nowadays this typically comprises 64 bits. Most symmetrical encryption methods are block ciphers; these also include DES, IDEA and RC5. A range of operating modes have been defined (and standardised) for block ciphers. These are:

- ECB (Electronic Code Book) mode, where every block is encrypted separately – independently of the other blocks
- CBC (Cipher Block Chaining) mode and CFB (Cipher Feed Back) mode; in these modes a dependence is established between the ciphertext blocks

and all preceding ciphertext blocks, depending on the choice of an additional initialisation vector

- OFB (Output Feedback Mode), a mode which can be interpreted such that the block cipher is used to generate a "block stream" that is added to the plaintext blocks bit by bit (modulo 2)

When using symmetrical procedures it must always be borne in mind that communication must be preceded by an exchange of keys between the communicating parties. This must take place via a secure channel (such as by courier or personal delivery), and both parties must subsequently keep the key secret. There are various procedures for ensuring secure key exchange. In closed systems the exchange of keys can generally be performed without difficulty, because in this case there are usually "secure channels" available. In open systems with a large number of communication partners, this is more difficult. Generally speaking, however, the problem is that if there are a large number of potential communication partners a correspondingly large number of keys have to be exchanged before the communication process itself can take place, and that the potential communication partners have to be known in advance.

Asymmetric (public key) encryption methods, on the other hand, use two different (but mathematically related) keys: one "public" key for encryption, and one "private" key for decryption. This pair of keys must have the following property: it must be practically impossible for anyone who knows only the public key to determine the associated private key or to decrypt a message encrypted with the public key.

Asymmetric encryption therefore has the nature of a "one-way" method: a message cannot be restored if the private key has been forgotten or deleted.

The name "public key" encryption comes from the fact that the public key can be made known publicly without compromising the security of the procedure. In contrast, the private key must be kept **secret**.

If we assume that Alice wants to send a message in encrypted form to Bob, Alice picks up Bob’s public key from a freely accessible file and uses it to encrypt her message. After receiving the message, Bob uses his secret key to decrypt the message he has received from Alice. If Alice and Bob are using an asymmetric algorithm for the purpose of confidentiality, they therefore do not need a secure channel for the exchange of keys, but Alice must be certain that she is indeed using Bob’s public key and not a key that has been foisted on her as being Bob’s key. If Alice were to encrypt a message with a foisted key, the perpetrator, who of course knows the matching private key, could decrypt the message. The sender normally requires confirmation from a trusted third party that the recipient’s public key really does belong to the recipient. This confirmation, the "certificate", is normally also generated by a cryptographic procedure and is enclosed with the public key.

Two well-known asymmetric encryption methods are the RSA algorithm (named after its inventors, Rivest, Shamir and Adleman) and the class of ElGamal algorithms. The latter also include the encryption procedures based on elliptic curves.

Symmetric and asymmetric encryption algorithms have advantages and disadvantages which in some cases complement each other.

Advantages of (good) symmetric algorithms:

- They are fast, i.e. they have a high data throughput.
- The level of security is largely determined by the length of the key, i.e. with good symmetric procedures there should be no attacks which are considerably better than trying out all keys (brute-force attacks).
- They offer a high level of security with a relatively short key.
- It is easy to generate keys, because usually any bit sequence of a fixed length is allowed as the key and a random number can be chosen as the key.

Disadvantages of symmetric algorithms:

- All users have to keep all keys belonging to their communication partners secret.
- They are less well suited to key distribution than asymmetric procedures, especially if there are a large number of communication partners.
- They are less practicable than asymmetric procedures for non-repudiation purposes, because when symmetric keys are used it is not easy to detect which of the two communication partners has encrypted the message. This can only be ensured by an intermediate third party, which is integrated into the message flow by means of corresponding cryptographic protocols.

Advantages of (good) asymmetric procedures:

- Every party in a confidential communication process only has to keep his own private key secret.
- They can easily be used for digital signatures.
- They offer elegant solutions for the distribution of keys in networks, because the public keys or key certificates can be stored in freely accessible form on central servers without imparing the security of the procedure.
- They are well suited for non-repudiation purposes.

Disadvantages of asymmetric procedures:

- They are slow, i.e. they generally have a low data throughput.
- Security: the following applies to all well-known public key procedures:
  - There are considerably better attacks than trying all keys one after the other, which is why (in comparison with symmetric methods) relatively long keys are required in order to achieve an equally high degree of security.
  - Security is based "only" on the presumed (but recognised among the experts) algorithmic difficulty of a mathematical problem (for example decomposing a large number into its prime factors).

- Key generation is generally complex and time-consuming, because care must be taken not to generate "weak" key pairs.

Hybrid procedures attempt to combine the advantages of both types of encryption: they use asymmetric encryption to transfer a session key for a symmetric procedure, and encrypt the bulk data with the symmetric procedure. The session key is usually used for only one session (transmission) and is then destroyed. The asymmetric key pair may be used for a long period, depending on the circumstances.

II. Protection of integrity

The objective of integrity protection is to enable the recipient of a message to establish whether he has received the message without it being corrupted. The basic principle of integrity protection is to transmit the message unencrypted and unchanged, but at the same time to send certain checking information with the message, which enables the actual message to be checked to ensure that it is uncorrupted. The prerequisite for this, however, is that the recipient must receive the check data in an unmanipulated state. The check data therefore has to satisfy the following conditions:

- The amount of check information must be kept as small a possible so as to minimise the amount of additional information to be transmitted.
- It must be possible to detect virtually any manipulation, even of only a single bit of the message, on the basis of the check information.
- It must be possible to transmit the check information in an unmanipulable form, or it must be possible to detect manipulations.

Typically there are two methods that are used for the calculation of check information: hash functions and message authentication codes.

A (one-way) **hash function** is a data transformation with the following characteristics:

- Compression characteristic: bit sequences of any length are mapped to bit sequences of a fixed, generally shorter length (typically 128 - 160 bits).
- "One-way" characteristic: for a specified hash value it must be "practically impossible" to find a message whose hash value is the specified hash value.
- Collision resistance: it must be "practically impossible" to find two messages which lead to the same hash value.

A and B can check the integrity of a message with the aid of a hash function known to both communication partners: Alice hashes her message, and transmits this and the hash value to Bob in such a way that the accuracy of the hash value is guaranteed. Similarly, Bob hashes the message he receives and compares his result with the hash value supplied by Alice. If the two values tally, he can assume that no bit of the message has been changed.

A **message authentication code (MAC)** is a cryptographic checksum for message security, in other words a data transformation in which a secret key is additionally included in the calculation, with the following characteristics:

- Compression characteristic: bit sequences of any length are mapped to bit sequences of a fixed, generally shorter length.

- Resistance to forging: for anyone who is not in possession of the key it must be "practically impossible" to calculate the MAC value of a new message, even if he has come into possession of a number of old messages with the associated MAC values.

If Alice and Bob have a MAC and a common, secret MAC key, Alice authenticates her message simply by calculating the MAC value of the message and sending it to Bob together with the message. In turn, Bob calculates the MAC value of the received message with the MAC key, which is also known to him. If this tallies with Alice's value, he can assume that the message is authentic (i.e. that it has not been altered and that it really originates from Alice). Alice has therefore authenticated her message to Bob by using the key that is known only to Bob and herself.

MACs are often designed on the basis of symmetric encryption methods. The best known variant is the encryption of a message with DES or another block cipher algorithm in CBC or CFB mode. This involves appending the last encrypted block to the message as the MAC. Apart from this, however, there are also MACs that are not based on encryption methods. The MAC value of a message can be seen as the non-forgeable, key-dependent, cryptographic checksum of the message. The use of MACs for the purpose of authentication requires that both parties reliably protect the secret authentication key.

As a side-effect of integrity protection, the procedures outlined above can be used at the same time by the recipient of the message to check that the message, which has been verified as being unmanipulated, could only have been sent by the sender who is actually known to the recipient. This conclusion can be drawn because only this sender has the necessary keys for encrypting and determining the check information.

III. Proof of authenticity

Certain criteria must be met regarding the authentication of users with respect to communication partners/IT systems or of clients with respect to servers:

- Illegitimate accesses must be detected and warded off
- Legitimate accesses must be permitted
- Sensitive data must remain protected even when transmitted across networks

To ensure this, procedures are required which allow all participants to establish the identity of their communication partners unequivocally. This includes a time aspect: Alice wants to convince Bob in real time that it is indeed she who is communicating with him. The main techniques for authentications of this nature are cryptographic challenge-response protocols.

In these, Bob sends data to Alice and requests (challenges) her to prove to him that she possesses a secret (i.e. an item of key information); Alice demonstrates to him that she has this possession without divulging the secret itself by sending him a response that is dependent on the secret and on his challenge. Bob in turn uses the response that she has sent to check that the correct secret really was used to calculate the response.

To ensure strong authentication, the challenges must not be repeated. Both symmetric and asymmetric techniques can be used with challenge-response procedures.

Example: Alice and Bob agree in advance on a symmetric encryption procedure and a common cryptographic key. For authentication purposes, Bob sends a random number to Alice as a challenge. Alice in turn encrypts this random number with the common secret key, and sends the result back to Bob. At the next stage, Bob decrypts the messages and compares the result with the random number he chose at the outset. It they are the same, it really is Alice, because only she knows the secret key.

IV. Digital signature

The purpose of the cryptographic construct of a digital signature is to allow the use of a counterpart to hand-written signatures for digital files and messages. For this, some of the cryptographic procedures explained previously, such as hash functions and asymmetric algorithms, are used in combination. The essential prerequisite for digital signatures is that every user must be in possession of a secret, known only to him, with which he can generate a digital signature to be used with any files. It must then be possible to check this digital signature on the basis of public information.

In this sense, a digital signature is a special form of integrity protection with additional special features. A **digital signature** is an item of check information which is appended to a message or file, and which is associated with the following characteristics:

- A digital signature can be used to establish unambiguously who has created the signature.
- It is possible to check, with authentication, whether the file to which the digital signature was appended is identical to the file that was actually signed.

If therefore the digital signature can be verified on the basis of the publicly accessible information, on the one hand the integrity of the signed file is assured but at the same time non-repudiation is also established, because only the person to whom the digital signature can be unambiguously attributed can have generated this signature on the basis of his or her secret information. It must be borne in mind that different files also result in different digital signatures, and that even the smallest changes to files make signatures unverifiable.

Example: One widely used procedure for digital signatures is the reverse application of the RSA algorithm. In this, every user has a secret signing key known only to him or her. Verification key certificates, in which the matching public key and the details of the owner of the matching secret signing key are linked to each other in an unforgeable way, are publicly accessible. These certificates are issued by trustworthy bodies which have previously checked the personal details of the users.

To calculate and check a digital signature for any file, the procedure used is as follows:

1. Step: Alice calculates the hash value of the selected file.

2. Step: Alice encrypts this hash value with the secret signing key known only to her. The result is Alice's digital signature for this file.

3. Step: Alice transmits the digital signature together with the verification key certificate and the file to Bob.

4. Step: Bob verifies the certificate (for example with the public key of a certification authority).

5. Step: Bob calculates the hash value of the file he has received.

6. Step: Bob decrypts the digital signature with the aid of the public verification key contained in the verification key certificate.

7. Step: Bob compares the hash value calculated in step 4 and the decrypted signature. If they are identical, the digital signature is verified. If they are not identical, Bob cannot draw any further conclusions.

8. Step: After the digital signature has been verified, Bob can rely on the following results:

   - If it is certain that indeed only Alice possesses the secret key, Bob can be sure that the digital signature was generated by Alice, who is shown in the verification key certificate.
   - The file that Bob has received is identical to the file for which Alice calculated the digital signature.

It should be emphasised that digital signatures only safeguard the objectives of integrity and non-repudiation, but in no way confidentiality. A digitally signed message is transmitted as plain text; if it is confidential, it must be encrypted **in addition**.

If a digitally signed file contains a declaration of intent from the signer, the declaration of intent can be attributed indisputably to the signer, if necessary even in a court of law, on the basis of the signature.

The verification key certificates that are used are in turn themselves files that are digitally signed by the trustworthy body; these can be checked in the same way, and provide information about the verification key and the person who holds the matching secret signing key.

It is worth noting the differences between MACs and digital signatures:

- A digital signature can be verified by anyone who is in possession of the verification key certificate, whereas MACs can only be verified by the parties who know the secret authentication key.
- Alice's digital signature on a message can only be created by Alice; the MAC value of a message, on the other hand, can be generated by both parties, Alice and Bob (and anyone else who knows the secret authentication key). It is therefore impossible for MACs to be used for the purpose of ensuring non-repudiation.

A law on digital signatures entered force for the Federal Republic of Germany in the form of Article 3 of the Information and Communication Services Act (Federal Law Gazette 1879, Part 1, 1997). This governs which security

requirements have to be satisfied by the technical components that are used for digital signatures, and what tasks are to be performed by certification authorities which issue verification key certificates. In addition it governs how the required security of the components and certification authorities is to be checked. As a result, digital signatures conforming to the Signature law are accorded a high level of security, also in court.

Key management

Whenever encryption is used, the problem arises of ensuring appropriate management of the keys. The question is raised as to how the following tasks are performed throughout the lifecycle of the keys:

- Generation/initialisation
- Agreement/establishment
- Distribution/transport
- Changing/updating
- Storage
- Authentication/certification
- Recall
- Recovery in the event of destruction or loss
- Destruction/deletion
- Archiving
- Escrow (storage in trust)

Key management can, and usually does, also make use of cryptographic techniques. It must be performed for all of the crypto modules of a cryptographically based protection system. Secret keys must be protected against unauthorised disclosure, modification and replacement. Public keys must be protected against unauthorised modification and replacement. Appropriate key management is a necessary precondition if it is to be at all possible to protect information by cryptographic methods. Key management requires its own resources, dedicated specifically to this task.

Certification bodies

Trust centres or certification bodies are required whenever it is considered necessary to use asymmetric crypto algorithms for digital signatures or for encryption and the number of users has risen so much as to be difficult to manage. These procedures require a different key for signature generation or encryption than they do for signature checking or decryption. A pair of corresponding keys is generated for this purpose on a user-related basis. One key, known as the public key, is made known publicly. The other key, known as the private key, must be kept absolutely secret. A digital signature can be generated or a text encrypted with the private key – and only with that key – and the signature can be verified or the text decrypted with the associated public key – again, only with that key. In order to ascertain whether the public keys are genuine and to check that keys are reliably allotted to individuals, it is necessary to use the trust centres or certification bodies mentioned above, which confirm the attribution of a person to a public key by issuing a certificate.

Typically, the following tasks are undertaken at certification bodies such as these:

- Key generation: pairs of keys have to be generated for the certification body and, if appropriate, for users.
- Key certification: the user data, the corresponding public keys and other data are combined to form a certificate, which is digitally signed by the certification body.
- Personalisation: the certificate and, if appropriate, the public and private keys are transferred to a signature component (generally a chip card).
- Identification and registration: the users are identified and registered on presentation of an identification document.
- Directory service: certificates are held ready for retrieval in a public directory. In addition, the directory service must provide information on whether a certificate is blocked or not.
- Time stamp service: it may be necessary to trustworthyly link certain data to a point of time. To do this, the time is appended to the data and the result is digitally signed by the time stamp service.

Trust centres can also offer the safekeeping of keys as an additional service if it is intended to use the cryptographic keys for encryption. In order to ensure that encrypted data can still be accessed if a key is lost, the owner of the key (and no-one else) can be given a duplicate key, which is stored securely at the trust centre.

Key distribution centres

The security of symmetric encryption methods is dependent on whether the commonly used secret key is only known to the users who are authorised to access the protected information. In cases where it is necessary to protect stored data to which only the data's owners are supposed to have access, this is relatively easy to guarantee because these owners merely have to protect the key in such a way that unauthorised users are unable to access it.

The situation is different, however, if it is intended to use a symmetric encryption method to protect messages that are to be transmitted from a sender to a recipient via an insecure transmission medium. In this case the secret key must be available to both the sender and the recipient, i.e. there must be a possibility of engaging a protected exchange of information between the two parties. In practice this is often achieved by the encrypted distribution of communication keys through bodies known as key distribution centres (KDCs); this involves setting up entire hierarchies of keys that are mutually interdependent in security terms. The methods used in such instances are in some cases highly complex and are dependent on a large number of components for their security, in particular on the physical, organisational, staff-related and technical security of the KDCs and on the keys agreed for communication with the KDCs.

If a secret key becomes compromised, in other words if it becomes known to an unauthorised third party, the result is that the confidentiality of all data is lost if it has been encrypted with that key or if encryption of the data is dependent on the key. This is particularly critical if one of the central keys of a key distribution hierarchy has become compromised.

Use of cryptographic methods

Provided they are used properly, cryptographic methods are excellently suited to countering the following threats:

- Disclosure of information to unauthorised persons
- Deliberate manipulation of data by unauthorised persons
- Manipulation of the authorship of information

The use of cryptography alone, however, is **not** sufficient to ward off all threats.

- The use of cryptographic methods does not make any contribution to guaranteeing the availability of data (if encryption is used inappropriately, there is even a risk that data will be lost).
- Cryptographic methods cannot achieve anything against denial-of-service attacks (see also T 5.28 *Denial of services*). They may play a part in the early detection of such attacks, however.
- They also do not help to prevent the random corruption of information (for example as a result of noise), but they can make it possible to detect corruption retrospectively.

S 4 Safeguard Catalogue - Hardware & Software

S 4.28	Software re-installation in the case of change of laptop PC users
S 4.29	Use of an encryption product for laptop PCs
S 4.30	Utilisation of the security functions offered in application programs
S 4.31	Ensuring power supply during mobile use
S 4.32	Physical deletion of data media before and after usage
S 4.33	Use of a virus scanning program when exchanging of data media and data transmission
S 4.34	Using encryption, checksums or digital signatures
S 4.35	Pre-dispatch verification of the data to be transferred
S 4.36	Blocking specific fax recipient numbers
S 4.37	Blocking fax sender numbers
S 4.38	Deactivation of unnecessary service features
S 4.39	Deactivation of answering machines for periods of absence
S 4.40	Preventing unauthorised use of computer microphones
S 4.41	Use of a suitable PC security product
S 4.42	Implementation of security functions in the IT application
S 4.43	Fax machine with automatic envelope sealing system
S 4.44	Checking of incoming files for macro viruses
S 4.45	Setting up a secure Peer-to-Peer environment
S 4.46	Use of the log-on password under WfW and Windows 95
S 4.47	Logging of firewall activities
S 4.48	Password protection under Windows NT
S 4.49	Safeguarding the boot-up procedure for a Windows NT system
S 4.50	Structured system administration under Windows NT
S 4.51	User profiles to restrict the usage possibilities of Windows NT
S 4.52	Protection of devices under Windows NT
S 4.53	Restrictive allocation of access rights to files and directories underWindows NT
S 4.54	Logging under Windows NT
S 4.55	Secure installation of Windows NT

S 4.56	Secure deletion under Windows NT and Windows 95
S 4.57	Deactivating automatic CD-ROM recognition
S 4.58	Sharing of directories under Windows 95
S 4.59	Deactivation of ISDN board functions which are not required
S 4.60	Deactivation of ISDN router functions which are not required
S 4.61	Use of security mechanisms offered by ISDN components
S 4.62	Use of a D-channel filter
S 4.63	Security-related requirements for telecommuting computers
S 4.64	Verification of data before transmission / elimination of residual information
S 4.65	Testing of new hardware and software
S 4.66	Novell Netware - safe transition to the year 200
S 4.67	Locking and deleting database accounts which are no longer required
S 4.68	Ensuring consistent database management
S 4.69	Regular checks of database security
S 4.70	Monitoring a database
S 4.71	Restrictive utilisation of database links
S 4.72	Database encryption
S 4.73	Specifying upper limits
S 4.74	Networked Windows 95 computers
S 4.75	Protection of the registry under Windows NT
S 4.76	Secure system version of Windows NT
S 4.77	Protection of administrator accounts under Windows NT
S 4.78	Careful modifications of configurations
S 4.79	Secure access mechanisms for local administration
S 4.80	Secure access mechanisms for remote administration
S 4.81	Auditing and logging of activities in a network
S 4.82	Secure configuration of active network components
S 4.83	Updating / upgrading of software and hardware in network components
S 4.84	Use of BIOS security mechanisms

S 4.85	Design of suitable interfaces for crypto modules
S 4.86	Secure separation of roles and configuration with crypto modules
S 4.87	Physical security of crypto modules
S 4.88	Operating system security requirements when using crypto modules
S 4.89	Emission security
S 4.90	Use of cryptographic procedures on the various layers of the ISO/OSI reference model
S 4.91	Secure installation of a system management system
S 4.92	Secure operation of a system management system
S 4.93	Regular integrity checking
S 4.94	Protection of WWW files
S 4.95	Minimal operating system
S 4.96	Deactivating DNS
S 4.97	One service per server
S 4.98	Restricting communication to a minimum with packet filters
S 4.99	Protection against subsequent changes to information
S 4.100	Firewalls and active content
S 4.101	Firewalls and encryption
S 4.102	C2 security under Novell 4.11
S 4.103	DHCP server under Novell Netware 4.x
S 4.104	LDAP Services for NDS
S 4.105	Initial measures after a Unix standard installation
S 4.106	Aktivation of system logging
S 4.107	Use of vendor resources
S 4.108	Simplified and secure network management with DNS services under Novell NetWare 4.11
S 4.109	Software reinstallation on workstations
S 4.110	Secure installation of the RAS system
S 4.111	Secure configuration of the RAS system
S 4.112	Secure operation of the RAS system
S 4.113	Use of an authentication server within RAS access
S 4.114	Use of the security mechanisms provided on mobile phones

S 4.115 Safeguarding the power supply of mobile phones

S 4.1 Password protection for IT systems

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

Password protection for an IT system is to ensure that only those users who establish proof of their authorisation will be granted access to data and programs. Immediately upon switching on the IT system, the required proof must be furnished. If the user is unable to do so, password protection will deny access to the IT system.

Password protection in an IT system can be achieved in various ways:

- Most BIOS variants offer installation of a boot password. If incorrect entries are made, booting will not be continued. A BIOS password is not difficult to overcome, although it does protect against coincidental culprits. It should therefore be implemented wherever better access safeguards are not available (see: S 4.84 Using BIOS security mechanisms).
- Good operating systems already contain access safeguards. However, in most cases, these must first be activated, for example by providing passwords for all users. Additional relevant information can be found in the operating-system specific modules.
- Additional hardware or software will be installed, which will, before the actual start of a computer, ask for a password and, if an incorrect password is entered, will inhibit any further use of the IT system.

As regards handling of passwords, the notes in S 2.11 *Provisions governing the use of passwords* must be observed; in particular, the password will have to be altered regularly.

Additional controls:

- Has password protection been installed on the respective computers?
- Which BIOS security options are activated?

S 4.2 Screen Lock

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT users

"Screen lock" refers to a facility enabling the concealment of information currently displayed on the screen. In order that access to an IT system is reliably prevented during a short absence of the IT user, it should only be possible to inactivate a screen lock after successful user authentication, i.e. following entry of a password.

It should be possible for the user to activate the screen lock manually. In addition, the screen lock should be automatically initiated after a predefined period of inactivity. All users should be made aware of the need to activate the screen lock when they leave their workstation for a short period. If a user is to be away from the workstation for an extended period, he should log off.

The period after which a screen lock is activated due to a lack of user inputs should be neither too short nor too long. If it is too short, the screen lock may be triggered while the user has merely paused for thought. On the other hand, if the period is too long, then a third party could exploit the absence of the user. A reasonable period to set is a time interval of 15 minutes. The IT Security Management Team should specify how the delay should be defined so as to satisfy the security requirements of the IT systems concerned and their operational environment.

Most operating systems come supplied with screen lock facilities. When these are used, care must be taken to ensure that they are configured so that input of a password is required.

A password-supported screen lock is offered in Microsoft Windows 3.x as a screen saver. However, the documentation points out that if the current application is not a Windows application, the screen saver will not be activated automatically, regardless of whether the application is executed in a window, from the MS-DOS command line or has been iconised. Under Windows 95, on the other hand, the screen saver is also automatically activated for DOS applications. Apart from Microsoft Windows, there are other products offering password-supported screen savers. Before employing such products, it is necessary to check whether the screen lock will work under all applications.

Under UNIX, a screen lock can be activated with programs such as *lock* or, while under X-Windows, the same result can be achieved with *lockscreen*.

Additional controls:

- Has a screen lock been installed on the relevant computers?
- Is the screen lock feature applied consistently?

S 4.2 Screen lock

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

Screen lock refers to the possibility of concealing information currently displayed on the screen. Such a screen lock should be activated when the user leaves the workstation for only a short time. Automatic activation of the screen lock in case of a prolonged break period should be included as an additional feature. If the software product also provides for password query, access protection for the IT system will be additionally ensured during the absence of the IT user concerned.

Password-supported screen lock is offered by *MS Windows 3.x* as a screen saver. However, its documentation points out that if the current application is a non-Windows application, the screen saver will not be activated automatically, regardless of whether the application is executed in a window, from the MS-DOS command line or as a symbol. Under Windows 95, however, the screen saver will also be automatically activated when using MS-DOS applications. Apart from *MS Windows*, there are other products offering password-supported screen savers. Before employing such products, it should be checked whether the screen lock will work under all applications.

Under UNIX, screen lock can be achieved with programs such as *lock* or, under *X Windows*, *lockscreen*.

Additional controls:

- Has a screen lock been installed on the respective computers?
- Is consistent use being made of the screen lock feature?

S 4.3 Periodic runs of a virus detection program

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

Different courses of action can be taken to afford protection against computer viruses. Programs which scan IT systems for known viruses have proven to be the most effective means of combating viruses. The advantage here is that newly-procured software and data media can be checked before they are used for the first time. Infection by known computer viruses can thus be prevented in principle. Another advantage of virus scanning programs is that they provide details on each virus detected. Known viruses have been analysed by specialists, who have ascertained whether these viruses have any damaging effects. Consequently, a good virus scanning program must not only be able to detect a large number of viruses, but also identify them as precisely as possible.

It must be noted that virus scanning programs become less and less effective in the course of time, as they are only able to detect viruses known up to the inception of the programs, and are usually not able to identify any viruses created subsequently. For this reason, it is necessary to update virus scanning programs on a regular basis, at least four times a year.

Virus scanning programs have various settings which, through parameterisation, allow users to specify which files should be tested and how thorough the test should be. It is the task of the IT security management to determine the suitable settings and inform the users of them or pass them on as pre-settings.

Like other programs, virus scanning programs can be invoked when required (transient) or run in the background (resident). The operating mode of the scanning program has a decisive influence on user acceptance and, thus, on the actual degree of protection achieved.

In transient operation, the user must start the virus scanning program and explicitly specify which data media are to be scanned. In this way, infections can only be identified afterwards. In principle, virus protection is possible, but its effectiveness depends on how careful the user is.

In the resident mode, the virus scanning program is loaded into the main memory when the computer is started, and remains active there until the computer is switched off again. It operates without requiring any intervention by users, who can continue to perform the activities assigned to them, such as writing texts. Of late, this operating mode has gained in importance as the use of Windows programs has spread. In the case of Windows, the memory management operates more efficiently than under MS-DOS, which was used mainly in the past. Rapid technical developments, accompanied by an expansion in the size of computer main memories have supported the trend toward memory-resident programs. Under MS-DOS, memory-resident virus scanning programs were often designed to have a lower performance than transient programs, in order to save memory space. The most important advantage of memory-resident operation is that the security measure (virus scanning) is implemented regardless of user action, thus increasing the level of

security. This also results in greater acceptance by users, who do not need to attend actively to the responsibility of virus protection. The users do not even notice that the virus scanning program is operating in the background, as long as no virus is detected. On detection of a virus, access to the infected file is denied, i.e. this file cannot be used any more as long as the virus protection remains active. At present, the use of memory-resident virus scanning programs under Windows operating systems constitutes the best possibility of protection against viruses, because every file can be checked before usage (opening for the purpose of editing, copying, printing, unpacking etc.) and blocked if a virus is detected.

The use of checksum programs constitutes another preventive measure. In this case, checksums of the scanned files or system areas (e.g. the boot and partition sector) are computed at regular intervals to afford protection against changes. This not only allows the detection of unknown computer viruses, but also other unauthorised modifications to files.

Procedures required in case of virus contamination are described under S 6.23 *Procedure in case of computer virus infection*.

Additional controls:

- When was the last check made? Have the results been documented?
- Have computer viruses been detected? If so, this might point to illicit use of unauthorised software.
- When was the virus detection program in use last updated?

S 4.4 Locking of floppy disk drive

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

By means of special inserts, a floppy disk drive can be locked. In this way it can be achieved that

- the PC or server can no longer be booted from a floppy disk in an uncontrolled way;
- software cannot be installed in an uncontrolled way;
- data can no longer, without authority, be copied on floppy disks.

Therefore, bootable floppy disk drives, in particular, should be locked.

When purchasing disk locks, it should be ensured that as large a number of keys as possible is offered by the manufacturer. This requires organisational steps in the area of key management.

Alternatively, it is possible to dismantle the floppy disk drives.

Additional controls:

- Has it been ensured that floppy disk drives will generally be locked and can be accessed only in case of authorised uses?
- How are the keys safeguarded?
- Has a duplicate set of keys been deposited?
- Have arrangements been made to ensure that different keys are provided for the locks used?

S 4.5 Logging of PBX administration jobs

Initiation responsibility: PBX officer; IT Security Management

Implementation responsibility: Administrators

All entries made through the PBX service ports should be logged. This may be done either through a logging printer and/or on other data media. The PBX administrator must not have any write access to the generated log files. The print-outs supplied by the printer should be serially numbered, and the individual logging messages should have sequential message numbers.

In collaboration with ZVEI, the Central Association of the Electrical and Electronics Industry, BSI has drawn up a catalogue of requirements which contains improved logging. This catalogue is to be used when purchasing new PBX systems for federal agencies. In the event that PBX systems are already in place, the extent to which manufacturers can offer improvements as updates should be reviewed.

Additional controls:

- Does logging take place?
- Is it possible to ascertain whether the logging printer has been switched off?

S 4.6 Audit of the PBX configuration (target/performance reconciliation)

Initiation responsibility: PBX officer; IT Security Management

Implementation responsibility: IT security management, revisor

After each configuration change, e.g. release of a subscriber's authorisation, this should be recorded in an *ACTUAL* inventory. That list may be kept manually or by automatic means. Periodically (not necessarily at regular intervals), e.g. every six months, reconciliation checks should, at least randomly, be made of such an *ACTUAL* inventory and of the actual status. Incongruities should be cleared by means of the listings/audit trails. In particular, it should be verified whether

- all dialling numbers not allocated have actually not been set up;
- unpermitted authorisations have indeed not been granted to anybody;
- de-activated user facilities are assuredly inactive.
- de-activated dial-in functions are assuredly inactive.

In collaboration with ZVEI, the Central Association of the Electrical and Electronics Industry, BSI has drawn up a catalogue of requirements which contains improved audit. This catalogue is to be used when purchasing new PBX systems for federal agencies. In the event that PBX systems are already in place, the extent to which manufacturers can offer improvements as updates should be reviewed.

Additional controls:

- Is it possible, by reference to the available documents, to provide information, e.g. on the rights of particular subscriber's stations/lines?
- When was the documentation last reviewed for congruity with the actual state of affairs?

S 4.7 Change of preset passwords

Initiation responsibility: PBX officer; IT Security Management; Head of IT Section

Implementation responsibility: Administrators

Many IT systems, PBXs and gateway components (e.g. ISDN routers, speech-data multiplexers etc.) are delivered with default passwords configured by the manufacturer. These should, as a first step, be replaced by individual passwords. In this respect, the pertinent provisions on passwords must be observed (cf. S 2.11 *Provisions governing the use of passwords*).

Caution: In some PBXs, changes made to the configuration are only filed in RAM. The same applies to password changes. Therefore, data must always be saved and a new backup copy made after such an operation. If this is not done, the default password will again be enforced after any "restart" of the facility. In addition, a check is required as to whether the default password has actually become invalid after the specification of a new password, and can thus no longer be used to access the system.

Additional controls:

- Does the facility still use a default password?
- Have backup copies been made after the allocation and saving of the individual password?
- Is access to the system still possible with the default password following the specification of a new password?
- Are the relevant regulations on "password handling" being observed?

S 4.8 Protection of the PBX operator's console

Initiation responsibility: PBX officer; IT Security Management

Implementation responsibility: Administrators

Where administration of a PBX is ensured by means of an operator's PC, the latter must be provided, as a minimum, with the safeguards usually furnished for PCs (cf. Part I, Chapter 5.1 *DOS PC (single user))*.

Optionally:

In the event that the PBX system does not have sufficient security functions for the management of rights and access protection, the use of conventional devices (port controllers) available on the market may be considered. Using devices of this kind, reliable identification and authentication procedures can be carried out.

Additional controls:

- Has the operator's PC been provided with password protection?
- Is the operator's PC installed in a secure environment?
- Who can access the operator's PC?
- Who has access rights to the operator's PC?

S 4.9 Use of the security mechanisms of X Windows

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: Administrators

Release 5 of the *X Window* software offers only a few features enhancing security in case of data transmission between the X server and the X client; hence use of *X Windows* software can only be recommended for secure environments.

***xhost* command**

- **Computer-specific access control:** Each X server comprises a list of approved computers, which can be altered with the *xhost* command. It is essential that this is confined to those computers which really need access to the X server; under no circumstances should universal access with *xhost +* be allowed. This can be achieved by explicitly entering computers in the *xhost* table. Moreover, it should be borne in mind that every user has unrestricted access to the X server on one of the computers that have been approved. This type of access control can therefore only be recommended when there are compelling reasons as to why none of the security mechanisms listed below can be used.

MIT-MAGIC-COOKIE
NIS authentication

- **User-specific access control:** The X server process can be configured in such a way that in case of a log-in (e.g. by means of *xdm*) a key will be generated which will be used for authentication for transmission between a client and a server. This key (*MAGIC COOKIE*) is filed in the home directory of the user in the *.Xauthority* file and can, by means of the *xauth* command, also be transmitted to the X client. Whilst, however, the *MIT MAGIC COOKIE* mechanism must be regarded only as a type of password which can be intercepted during transmission, a mechanism offered in conjunction with *NIS* and working with a form of DES encryption offers greater security and should therefore be used wherever possible.

DMA channel

- **Access control via Secure Shell:** communication between X client and X server can also take place over a protected channel of an *ssh* connection (see also S 5.64 *Use of Secure Shell*). The result is both a computer-based and also a user-based access control system. The authentication and user data is encrypted. If X Windows is to be securely operated, the use of Secure Shell is therefore recommended.

Eavesdropping of keyboard inputs

It is possible for keyboard inputs at a remote terminal to be translated into plain text and viewed under X Windows with an additional program. When using the *xterm* program forwarding of keyboard inputs by suppressing transmission of *KeyPress* events to other applications can be prevented. To ensure that only the corresponding window has access to the keyboard, the *secure keyboard* option must be enabled from the *xterm* menu.

Additional controls:

- Are steps taken to prevent users from disabling the computer-specific access control system via the command *xhost +*?

S 4.10 Password protection for PBX terminals

Initiation responsibility: PBX officer; IT Security Management

Implementation responsibility: IT-user

Terminals, especially telephones, can often be provided with password protection. When password protection is enabled, user facilities such as call diversion, follow-me call forwarding, etc. will be available only after entry of the password. Without knowledge of the password it is normally only possible to make in-house calls. Use should always be made of this form of password protection in order to prevent abuse of these facilities.

Additional controls:

- Can PBX terminals be provided with password protection?
- Have the users been briefed on the password protection option?
- If so, is use made of this option in practice?

S 4.11 Screening of PBX interfaces

Initiation responsibility: PBX officer; IT Security Management

Implementation responsibility: Administrators

The interfaces of a PBX system, through which administration activities can be carried out, are points requiring protection. Therefore, they should be specially shielded. Through unused or unprotected interfaces, unauthorised persons can, for instance, by using a laptop PC, manipulate the system. In such cases, password protection for a PBX operator's console or a PC gateway would be ineffective. Therefore, the aim is to prevent such manipulation or, at least, to provide for detection of an attempt to this effect. For this reason, the used interfaces should be tightly screwed and possibly sealed as well. Unused interfaces can be secured by screws and sealed cover plates.

Additional controls:

- Are all interfaces known through which your PBX can be configured?
- Are there any PBX interfaces which can be freely accessed?
- Have the existing connecting cables been mechanically secured at both ends?

S 4.12 Disabling of unneeded user facilities

Initiation responsibility: Agency/company management; PBX officer; IT Security Management

Implementation responsibility: Administrators

The scope of available user facilities should be confined to the required minimum. Where possible, the software for features not required should be removed from the installation. Since this often cannot be done, the only choice is to disable these user facilities. From time to time it should be checked whether these user facilities are actually de-activated.

Additional controls:

- Is the actual need for approved user facilities being checked?
- Is de-activation ensured of those user facilities which are not used and thus are obviously not required?

S 4.13 Careful allocation of identifiers

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

In UNIX systems, user IDs and group IDs of processes and files are used, *inter alia*, to establish the originators of actions and to allocate rights. Therefore, assignment of such IDs should be handled very carefully.

Every log-in name, every user ID (UID) and every group ID (GID) must be unique. Even after deletion of a user or a group, the log-in name and the UID or GID should not be reassigned for a certain period of time. On networked systems, steps must be taken to ensure that it is not possible for the same user names and IDs to be assigned elsewhere on the system more than once. This is especially important where NFS is used due to the conversion of UIDs, in order that no data can be read without authorisation.

Every user must be a member of at least one group. Every GID appearing in the */etc/passwd* file must be defined in the */etc/group* file.

Every group should comprise only those users who are absolutely required. This is particularly important in the case of system groups (such as *root*, *sys*, *bin*, *adm*, *news*, *uucp*, *nuucp* or *daemon*).

Log-ins with the UID *0* (*superuser*) may, apart from the system administrator *root*, be granted only for administrative log-ins in accordance with previously established rules (cf. S 2.33 *Division of Administrator roles under UNIX*).

It is good policy to lay down naming conventions for log-in names and UIDs/GIDs. Checks should also be made at regular intervals as to whether all the UIDs are reasonable. For example, they should consist entirely of numerals and not contain any invalid combinations such as 00 or 000.

The files */etc/passwd* and */etc/group* should not be edited using editors, as errors can greatly impair the security of the system. Only the appropriate administration tools should be used, although these are highly system-specific.

Additional controls:

- What procedures are used to allocate IDs?
- Are the */etc/passwd* and */etc/group* files regularly checked for consistency?
- Does the UID field in */etc/passwd* really contain numerals?
- Are all UIDs reasonable?

S 4.14 Mandatory password protection under UNIX

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Password protection for each account in a UNIX computer ensures that only an authorised user can log in with his log-in name, as, after entry of the log-in name, authentication is effected through entry of the password.

Use appropriate version of *passwd*

When using passwords for users and groups, the rules described under S 2.11 *Provisions governing the use of passwords* must be observed. It must be borne in mind that in some systems only a limited number of characters are considered during password verification. For implementation of these measures, appropriate program versions of *passwd* which ensure compliance with these rules or administrative measures, e.g. shell scripts and pertinent *cron* entries, should be applied.

Another possibility is to replace the UNIX standard command *passwd* with other extended functionality password programs. These include the public domain programs *anlpasswd*, *npasswd* and *passwd+*, which scrutinise new passwords chosen by users on changing their passwords and reject them if they are too weak. For example, these programs can be obtained from the FTP server at *ftp://ftp.cert.dfn.de/pub/tools/password/*.

Passwords should not be stored in the universally readable */etc/passwd* file, but in a *shadow* password file that cannot be read by the users. Newer UNIX systems come with this *shadow* option, but unfortunately it is not always activated following initial installation. Thus, for example, under RedHat Linux when the standard installation is completed, use of the *shadow* password file is activated via the command *pwconv*.

Suspend user IDs without a password

The */etc/passwd* file must be regularly checked for user IDs without a password. If such an ID is found, the user must be suspended. If mandatory password use has been agreed for groups, the */etc/group* file must be reviewed accordingly. However, assignment of group passwords is not recommended. Each group entry should contain as few users as possible. This facilitates changing from one group to another for which a user has been entered, while unauthorised changes by means of appropriate programs are precluded.

All log-ins, especially ones with UID 0, should be scrutinised regularly to ensure that there is a password and that it is of an acceptable type (see also S 2.11 and S 4.26). In addition to the programs described in S 4.26 *Regular security checks of the UNIX system*, such log-ins can also be detected, for example with

```
awk -F: '{if ($3=="0") print $1}' /etc/passwd
awk -F: '{if ($2=="") print $1}' /etc/passwd
```

Additional controls:

- Are regular checks made of password use?
- Are users prevented from selecting weak passwords (e.g. using *anlpasswd*)?
- How long do passwords remain valid?

Intentional blank page

S 4.15 Secure log-in

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Use should be made of a log-in program or the relevant options should be activated so that the following measures can be taken:

- The number of unsuccessful log-in attempts is restricted.
- After each unsuccessful log-in attempt, the waiting time until the next log-in prompt will increase. After a certain number of unsuccessful attempts, the account and/or terminal will be blocked. It should be noted that the administrator must not be locked out by this measure; his continued access from the console must be ensured (cf. also S 1.32 *Adequate siting of the console, devices with exchangeable data media, and printers*).
- When logging in, the user is informed of the time of the last successful log-in.
- When logging in, the user is advised of unsuccessful log-in attempts. This information might be repeated at the time of several subsequent log-ins.
- When logging in, the user is informed of the time of the last log-out. Here, a difference is made between log-outs to an interactive log-in and log-outs to a non-interactive log-in (log-out of background processes).
- The additional use of one-time passwords is recommended for log-in via networks with non-encrypted transmission of passwords (also refer to S 5.34 *Use of one- time passwords*).

Additional controls:

- Have the users been instructed to check the time of the last successful log-in for plausibility?
- How often are unsuccessful log-in attempts reported to the user?

S 4.16 Restrictions on access to accounts and/or terminals

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Blocking outside working hours

The account and/or terminal of a user should be blocked outside regular working hours. If this involves an unreasonable amount of time and effort (for instance in case of very irregular or frequently changing working hours), blocking should be effected at least during the standard non-working periods.

Limit to certain IT systems

If staff members are employed only on one particular terminal or IT system within the network, use of the user ID and of the associated password is to be confined to this computer so that logging-in from another computer will be precluded. In particular, the Administrator should if possible only log on from the console. It is also possible to enforce this through technical means (see also S 4.21 *Preventing unauthorised acquisition of Administrator rights*).

Granting of attributes to device files

For terminals under UNIX, the respective user must be entered as the owner of the given logical device. When he has logged out, *root* should automatically revert to being the owner. Only the respective user should have read access for this purpose. If a user wishes to receive messages from other system users (e.g. through *talk*), he must grant them write access rights to the device driver. The actual need for this must be checked.

In PC networks, the number of simultaneous log-ons under one account from several PCs can be restricted. To protect against unnoticed penetration by intruders, steps should be taken to ensure that users are prevented from logging on to more than one PC at a time.

Additional controls:

- Have time frames, i.e. temporary access restrictions, been configured for all accounts and terminals?

S 4.17 Blocking and deletion of unnecessary accounts and terminals

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Accounts which are not used over a prolonged period of time should be blocked and subsequently deleted. If any files which can no longer be assigned to an existing user entry remain after accounts have been deleted, there is a danger that these files could later be assigned to configured users without authorisation.

Find "orphaned" files

When a user is removed, under UNIX, the relevant entries in */etc/passwd*, */etc/group* and the home directory of the user should be deleted. Care should also be taken to ensure that other user entries in files such as */etc/hosts, shadows* etc. are deleted. Before this is done, the data in the home directory should be backed up. The user concerned should be informed of the blocking and, in any case, of the deletion of an account. When deleting an account, care must also be taken to locate any files of a user which are not contained in his home directory. This can be done, for example, using the program *find* with option *-uid*. Such files must be deleted or assigned to other users. Care must also be taken to delete any processes currently running and any jobs to be processed, e.g. under UNIX in *crontab*.

Similarly, terminals not used for a prolonged period of time should be blocked and subsequently removed.

Under UNIX, system-installed log-ins (e.g. *sys*, *bin*, *adm*, *uucp*, *nuucp*, *daemon* and *lp*) which are not required must be blocked in the pertinent password field in the file, e.g by entering *LOCKED* in */etc/passwd*.

If a (to be newly installed) user needs his account only for a limited period, it should be configured for a limited duration.

It can prove expedient to establish accounts initially for a limited period and extend their duration at regular intervals (e.g. annually) as required.

If the absence of a LAN user is foreseeable (e.g. due to vacation, illness, temporary assignment), his account in the network server should be blocked for that period so that working with his user ID is precluded during that time. Every user should inform the network administrator when he is going to be away for an extended period of time.

Additional controls:

- How are accounts which have not been used for some time identified?
- Are checks made of which accounts are no longer needed?
- Is the Network Administrator informed when a user will be away for an extended period?
- Are steps taken to ensure that all files and directories of deleted accounts are either assigned to other users or else deleted?

S 4.18 Administrative and technical means to control access to the system-monitor and single-user mode

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

In order to prevent activation of the monitor mode and booting to the single-user mode, the following measures should be taken:

- Where possible (depending on the UNIX variant and the respective hardware), a BIOS password must be assigned in order to protect the UNIX server. **BIOS password**
- When booting to the single-user mode, a superuser password query should be made in order to impede access by unauthorised persons to the UNIX server. **Superuser password**
- Where keyboard locks are available, they should be used for protection of the system console in order to prevent access to the monitor mode. **Keybord locks**

This measure is complemented by the following:

- S 1.32 *Adequate siting of the console, devices with exchangeable data media, and printers*
- S 4.21 *Preventing unauthorised acquisition of Administrator rights*

Additional controls:

- Is access to the console protected by passwords or other means?

S 4.19 Restrictive allocation of attributes for UNIX system files and directories

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Check programs indirectly called

The safeguards listed here apply to files and directories for which the Administrator is responsible, i.e. which are either of importance to all users or serve an administrative purpose. It is not sufficient to check the rights of one program. The rights allocation of all programs which are called up from this program must also be checked (in particular to avoid Trojan horses).

The attributes of all system files should, as far as possible, be set in such a way that only the System Administrator has access to them. Directories should provide no more than the required privileges for users.

Avoid *s bit*

The *s bit* should be set only when absolutely required. In the case of shell scripts, the *s bit* should not be set. The *s bit* may be set only by the Administrator; reasons should be given for the need to do so, which are also to be documented.

In directories to which all users must have write access (e.g. */tmp*), the *t bit* (*sticky bit*) should be set.

Check integrity

The integrity of all the attribute settings for UNIX system files and directories should be verified at regular intervals, e.g. using *Tripwire* or *USEIT* (see also S 4.26 *Regular security checks of the UNIX system*).

Additional controls:

- Is the assignment of attributes regularly checked for UNIX system files?
- Are there any lists which can be used to help carry out these checks?
- Is the *s bit* only set when absolutely required?

S 4.20 Restrictive allocation of attributes for UNIX user files and directories

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

The measures listed here apply to the files and directories of a user (including *Mail* files).

Prevent access from unauthorised outsiders

Users should set the attributes of their files and directories in a form which prevents access by other users. If other users are to be allowed access, appropriate user groups should be established.

For user-specific configuration files such as *.profile*, *.exrc*, *.login*, *.cshrc*, only the owner of the file should hold rights.

On UNIX systems, various programs have user-specific configuration files, such as *.exrc*, *.emacs* or *.mailrc*, which are automatically executed when the program is called up and which set variables and options for the user. To prevent implantation of any Trojan horses into such files, only their owner should be authorised to access them.

The file *.exrc* is read before the editors *ex* or *vi* are started. If a file with the same name is already contained in the current directory, it will be evaluated by some UNIX versions. All UNIX versions used must be checked in this regard as operating system commands can be carried out each time the editor is called up.

Avoid *s bit*

The *s bit* should be set only when absolutely required. In the case of shell scripts, the *s bit* should not be set. The *s bit* should only be set after consultation with the Administrator; reasons should be given for the need to do so, which must be documented.

umask

With *umask* (user file creation mode mask), it is laid down for each user which attributes for regulating the access rights will be contained in a file newly created by him. In the user-specific configuration files such as */etc/profile* or the *$HOME /.profile* files, *umask = 0027 (-rw-r-----)* or *umask = 0077 (-rw-------)* should be set so that the file attributes for new files will only grant access rights to the originator (and possibly to the group).

***Mail* files**

Check integrity

The attributes of *mail* files should be checked regularly to ensure that only the respective user has access to the files. The integrity of all the attributes set for UNIX user files and directories should be verified at regular intervals, e.g. using *Tripwire* or *USEIT* (see also S 4.26 *Regular security checks of the UNIX system*).

Additional controls:

- Have the users been informed about the importance of minimum rights allocation?
- Are the *umask* settings regularly checked by the Administrator?
- Is the *s bit* only set when absolutely required?

S 4.21 Preventing unauthorised acquisition of administrator rights

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Restrict access to *su*

With the *su* command, any user can obtain superuser privileges if he knows the relevant password. Since there is no upper limit on the number of unsuccessful attempts at log-on in the case of *su*, there is an increased risk that the password may be discovered by systematic try-out with the help of suitable programs. Therefore, *su* should be available only to the superuser. Alternatively, a modified *su* can be installed under which the number of unsuccessful attempts is restricted, the delay before *su* can be invoked again is longer, and, after a certain number of unsuccessful attempts, it is not possible to executability of *su* and/or the terminal as a whole is blocked. All use of the *su* command should be logged.

Where permitted by the given system, a log-in name other than *root* may be selected for the superuser. However, only Administrator log-ins should be created as additional superuser log-ins (see S 2.33 *Division of Administrator roles under UNIX*)

Administrative tasks should only be performed at the console

To prevent discovery of the Administrator's password through line tapping, he should only be allowed to work from the console. Under Solaris, for instance, this can be achieved by appropriately configuring the */etc/default/login* file.

Under BSD UNIX, *root* can only log on at terminals designated as *secure* in the */etc/ttytab* file. If this option is removed from all terminals, an Administrator can only log on at a terminal with the command *su* as *root*. Consideration should be given to setting up a user group to which execution of the command *su* is limited.

Do not designate console as *secure*

If under BSD UNIX, the console is designated as *secure* in the */etc/ttytab* file, no password is requested during start-up in the single-user mode. It is therefore essential that this entry is removed.

Block *ftp* for administrative accesses

The file */etc/ftpusers* contains the log-in names which are not allowed to log on via *ftp*. With *ftp*, passwords are transmitted over an unprotected plain text connection. Therefore administrative accesses (*root, bin, daemon, sys, adm, lp, smtp, uucp, nuucp*, etc.) should be entered in this file. Under some standard installations, *root* is not contained in this file.

Avoid *s bit*

If a user or a user program executes a superuser file (files with the owner *root* and with *s bit* set), this user or program will, during execution, obtain superuser rights. This is required for certain applications, but can in instances also be abused. Therefore, care must be taken to ensure that only essential program files are superuser files and that no extra superuser files can be added by third persons.

Automatic mounting of devices for exchangeable data media

Avoid automatic mounting

With *s bit* programs in the mounted drive, an ordinary user can acquire superuser rights. Therefore, automatic mounting (automounting) must be restricted. Some versions of UNIX offer a variant of the *mount* command

under which the *s bit* is ignored for the relevant file system. When exchangeable data media are used, consideration should be given as to whether to use this option.

When sharing directories which can be mounted by other computers, the restrictions mentioned in S 5.17 *Use of NFS security mechanisms* must be observed. In particular, no directories with *root* rights should be shared; directories with write authority should only be shared when this is necessary.

This measure is complemented by the following:

- S 1.32 *Adequate siting of the console, devices with exchangeable data media, and printers*
- S 4.18 *Administrative and technical means to control access to the system-monitor and single-user mode*

Additional controls:

- Can the *su* command be executed only by the Administrator?
- Is use of the *su* command automatically logged?
- Who has write access to the relevant configuration files?

S 4.22 Prevention of loss of confidentiality of sensitive data in the UNIX system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Restrict access to commands

With UNIX commands such as *ps*, *finger*, *who* and *last*, information can be obtained about a user (e.g. his work behaviour). Many UNIX derivatives contain additional commands which achieve the same effect under Solaris, e.g. *listusers*. Consideration should be given as to whether or not every user should be allowed to execute these commands (data privacy, unauthorised disclosure of log-in names, and the like). In case of doubt, access to these commands should be restricted.

Do not enter passwords as command parameters

When commands are invoked, no sensitive information, e.g. a password, should be entered along with them as a parameter, as other users could view this entry via *ps*.

If possible, log files such as *wtmp, utmp, wtmpx, utmpx*, should be protected against unauthorised reading through appropriate access rights, as a large amount of information about the users is contained in these files.

S 4.23 Secure invocation of executable files

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: Administrator, IT users

Steps must be taken to ensure that only approved versions of executable files and no modified versions that may have been introduced (especially Trojan horses) are called up.

Current directory not in the search path

Therefore, the current directory (.) should not be included as a path in the *PATH* variable. Executable files should only be held in the directories intended for the purpose. Only the owner should have write access to the directories contained in a *PATH* variable. This should be regularly checked. In UNIX systems with an *IFS* variable, this should be set to the default value (*space*, *tab* and *newline*) and, in particular, must not be set to *"/"*.

Additional controls:

- Are the *PATH* entries checked regularly?
- Are executable files scattered around the system?
- Are the procedures for executable files known to the users?
- Is the integrity of the relevant configuration files verified regularly (e.g. with *Tripwire* or *USEIT*)?

S 4.24 Ensuring consistent system management

Initiation responsibility: Head of IT section, IT security management, Administrator

Implementation responsibility: Administrators

In many complex IT systems, e.g. under UNIX or in a network, there is an Administrator role which is not subject to any restrictions. Under UNIX, this is the superuser *root*; in a *Novell* network, it is the *SUPERVISOR* or *admin*. Lack of restrictions will result in a particularly high risk of error or abuse.

Do not work under superuser log-in

In order to avoid errors, operations should be carried out under the superuser log-in only when this is necessary; other work should not even be carried out by the Administrator under the Administrator ID. In particular, no programs belonging to other users should be invoked under the Administrator ID. Also, routine system management (e.g. backup, installation of a new user) should be possible only via menu selection.

Agreement among Administrators

Appropriate allocation of tasks, specification of guidelines, and measures for co-ordination are required to ensure that Administrators do not perform any inconsistent or incomplete operations. For instance, a file must not be edited and modified by several administrators at the same time, as, in that case, only the version saved last would be preserved.

Use Secure Shell

If there is a risk of the lines to the terminals being tapped, then, to prevent interception of passwords, the Administrator should only work at the console. When administering UNIX systems, communications can be encrypted using the Secure Shell protocol. This enables remote workstations to be administered securely (see also S 5.64 *Use of Secure Shell*).

For all Administrators, supplementary user IDs which have only those restricted rights which the Administrators need for performing non-administrative tasks must be configured. For non-administrative activities, Administrators should exclusively use these supplementary user IDs.

Document changes

All changes performed should be documented so that they can be traced back and also to facilitate task allocation (see also S 2.34 *Documentation of changes made to an existing IT system*). To review activities performed by the Administrator, a log can be prepared of the commands input using the UNIX command *script*. This command logs the entire terminal session in an ASCII file. Such a file can then if required be appended to an electronic or hard copy administration journal.

Additional controls:

- What steps are taken to ensure that intervention by an Administrator will not lead to inconsistencies?
- Are backups made before any major intervention?
- Do all Administrators have supplementary user IDs with restricted rights?
- Are the supplementary user IDs used as default?
- Is an administration journal maintained? Are all changes documented there?

Intentional blank page

S 4.25 Use of Logging in UNIX Systems

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

The logging options offered by the individual UNIX system must be used and, where appropriate, be supplemented by programs or shell scripts.

The safeguards outlined below should be adopted.

Regular processing and evaluation

- The log files must be evaluated regularly. Such an analysis should not always be made at the same time, to prevent an aggressor from exploiting this fact. If, for instance, the administrator reviews the system activities every day at 5 p.m., an offender might get to work unnoticed at about 6 p.m.

Automatic alerting

- Depending on the type of data logged, it can be necessary to intervene as quickly as possible. To ensure that the Administrator is informed automatically of such events (e.g. log file too big, important server processes terminated, multiple attempted *root* log-ins at unusual times of the day etc.), semi-automatic log file parsers should be used to generate alerts (e.g.*swatch*, *logsurfer* or *checksyslog*).
- To the extent required, log files should be backed up before they get too big or are deleted by the system.
- Information from files like *wtmp*, *utmp*, *wtmpx*, *utmpx*, etc. should be scrutinised especially carefully as these files are easy to tamper with.
- File attributes of the log files should be set in such a way that unauthorised persons cannot make any changes to, or analyses of, the listings.
- As a minimum, the following log files should be generated and monitored: log-ins (including unsuccessful log-in attempts), *su* calls, error listing files / logging of important processes (*errorlog*), Administrator activities (especially commands executed by *root*). Further information on this subject will be found in S 4.106 *Activation of system logging*.

  The *last* command displays log-in and log-out information such as the time and terminal for each user. The Administrator should use this command to check regularly whether any users have been logging on through an unusual channel, e.g. over modem lines or via FTP.

Dedicated loghost

If log data is generated on many systems, it is recommended that a dedicated loghost which is specially secure is used. Forwarding of syslog messages on this loghost must be activated in the syslog configuration file (see S 4.106 *Activation of system logging*).

The logged data generated must only be used in order to monitor the proper use of the IT systems and not for any other purposes, especially not for the purpose of creating user performance profiles (see also S 2.110 *Data Privacy Guidelines for Logging Procedures*).

Additional controls:

- Are log files evaluated at regular intervals?
- Is logging still active and is there sufficient storage space available?
- Is the integrity of the configuration files for logging checked and logged regularly (e.g. with *Tripwire* or *USEIT*)?
- How are the log files archived and protected against tampering and unauthorised viewing?

S 4.25 Use of logging in UNIX systems

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The logging options offered by the individual UNIX system must be used and, where appropriate, be supplemented by programs or shell scripts.

The following safeguards should be taken:

- The log files must be evaluated regularly. Such an analysis should not always be made at the same time in order to prevent an aggressor from exploiting this fact. If, for instance, the administrator reviews the system activities every day at 5 p.m., an offender might get to work unnoticed at about 6 p.m.

Regular processing and evaluation

- Depending on the type of data logged, it can be necessary to intervene as quickly as possible. To ensure that the Administrator is informed automatically of such events (e.g. log file too big, important server processes terminated, multiple attempted *root* log-ins at unusual times of the day etc.), semi-automatic log file parsers should be used to generate alerts (e.g.*swatch*, *logsurfer* or *checksyslog*).

Automatic alerting

- To the extent required, log files should be backed up before they get too big or are deleted by the system.
- Information from files like *wtmp*, *utmp*, *wtmpx*, *utmpx*, etc. should be scrutinised especially carefully as these files are easy to tamper with.
- File attributes of the log files should be set in such a way that unauthorised persons cannot make any changes to, or analyses of, the listings.
- As a minimum, the following log files should be generated and monitored: log-ins (including unsuccessful attempts), *su* call-up, error listing files / logging of important processes (*errorlog*), administrator activities (especially commands executed by *root*). Further information on this subject will be found in S 4.106 *Activation of system logging*.

  The *last* command displays log-in and log-out information such as the time and terminal for each user. The Administrator should use this command to check regularly whether any users have been logging on through an unusual channel, e.g. over modem lines or via FTP.

Dedicated loghost

If log data is generated on many systems, it is recommended that a dedicated loghost which is specially secure is used. Forwarding of syslog messages on this loghost must be activated in the syslog configuration file (see S 4.106 *Activation of system logging*).

Additional controls:

- Are log files evaluated at regular intervals?
- Is logging still active and is there sufficient storage space available?
- Is the integrity of the configuration files for logging checked and logged regularly (e.g. with *Tripwire* or *USEIT*)?
- How are the log files archived and protected against tampering and unauthorised viewing?

Intentional blank page

S 4.26 Regular security checks of the UNIX system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Use tools

UNIX operating systems offer various security features as standard. However, these only work if they are used appropriately. The settings required for this purpose should be automatically checked by means of tools so that

- it is possible to detect and remedy any inconsistencies within a UNIX system and
- the System Administrator is able to manage the UNIX operating system by making optimum use of the existing security mechanisms.

Such checks can be made with programs available in the given UNIX system, individually developed shell scripts or PD programs. For some UNIX variants, commercial programs are available as well.

Examples

- **pwck**

  This is one of the standard operating system commands. With this command, a consistency check is made of the */etc/passwd* file. A check is performed as to whether all required entries have been made, whether there is a log-in directory for the user, and whether the log-in program is in existence. Similar functions are provided under Solaris by the *logins* command, which enables accounts without passwords to be located.

- **grpck**

  With this command, a consistency check is made of the */etc/group* file. This command is also one of the standard operating system commands. A check is performed as to whether all required entries have been made, whether the members of a group are actually included in the user password file and whether the group number tallies with the number given in that file.

- **tripwire**

  This program enables integrity checks of files to be carried out. Checksums of files are created and stored in a database. Various free of charge versions of *tripwire* are available.

- **cops**

  This public domain program serves to check the security of UNIX systems, for example various system settings, access rights, SUID files etc, are checked and potential security loopholes are identified.

- **tiger**

  This public domain program enables UNIX systems to be checked for security weaknesses. The program is similar in operation to *cops*.

- **SATAN**

  This public domain program enables the network security to be analysed. It checks networked UNIX systems for known deficiencies which have often not been eliminated.

- **BSI secure UNIX administration tool (USEIT)**

  USEIT was developed by the BSI to enable System Administrators to automatically check the security settings of a UNIX system with a tool. Checks of the consistency of system files and of the system itself are performed, password strength is checked and insecure processes are identified. Checksums of files and file attributes are generated and checked. Network security is reviewed and penetration testing can be performed. Insecure ports and services are checked. Logging is monitored. Checks of imported manufacturer's patches and of relevant CERT publications are performed. Further information on USEIT can be obtained from the IT baseline protection CD.

- **crack**

  With this public domain program, a check is made of whether the existing passwords are too simple and can be easily guessed.

Additional controls:

- Are the performance and results of such security checks documented?
- Which vulnerabilities are checked by means of the programs and shell scripts used?

S 4.27 Password protection in laptop PCs

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

Each portable PC (laptop) should be provided with password protection preventing unauthorised use of the PC. The rules to be observed in the use of passwords are listed in S 2.11 *Provisions governing the use of passwords*. For modern laptops, the BIOS boot password should be activated if its use is possible. The computer will only start up after the correct boot password has been entered.

If no password routine has been installed, the saving of sensitive, unencrypted data on the hard disk should be prohibited; instead, such data should be stored only on floppy disks. Such diskettes must be kept separately from the laptop, e.g. in a briefcase.

Some laptops also offer the power save option which can be activated by a specific key combination. Use of the portable PC can only be continued after entry of the appropriate password. Where a power save function is offered, it should be used for short intermissions. If it can be foreseen that there will be a longer break, the computer should be switched off.

Additional controls:

- Are passwords used for portable PCs? Are the rules for proper handling of passwords being complied with?
- When a laptop is handed over to another person, will its password be altered?

S 4.28 Software re-installation in the case of change of laptop PC users

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

In the event that the user of a laptop PC changes, it must be ensured that no sensitive data or computer viruses are present. Data can be deleted by completely overwriting these or using a special deletion program. An up-to-date virus detection program must then be used. Both processes must be carried out for all data media (hard disk, floppy disks).

It is recommendable, however, to reformat the hard disk of the laptop PC and then to add the required software and data. When formatting DOS data media, it should be ensured that the parameter */U* is used (contained in DOS 6.2) so that the formatting cannot be undone using the command unformat.

Additional controls:

- Before re-formatting, is it ensured that the former user no longer needs any data previously held in the laptop?

S 4.29 Use of an encryption product for laptop PCs

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

In order to prevent sensitive data being read from a laptop PC which, despite all precaution, has been stolen, an encryption program should be used. By means of the commercially-available products, individual files, certain areas or the entire hard disk can be encrypted in such a way that only the individual holding the secret key will be able to read and to use the data.

For secure encryption, three different requirements are of crucial importance:

- The encryption algorithm must be designed in such a way that it is impossible to reconstruct the plain text from the encrypted text without knowledge of the relevant key, i.e. the effort required to crack the algorithm or cipher should be much greater than the value of the information obtained as a result.
- A suitable key should be selected. If possible, it should be generated randomly. If a key can be selected like a password, the relevant instructions in S 2.11 *Provisions governing the use of passwords* must be observed.
- The encryption algorithm (the program), the cipher text and the keys must not be saved on the same data media. It is advisable to store the key separately. This can be done by recording it on pasteboard and then keeping it like a credit card in the purse/wallet. If the keys are stored on floppy disks, the diskettes should be kept separate from the laptop (e.g. in a briefcase).

Such encryption can be effected either online or offline. "Online" means that all data of the hard disk (or of a partition) is encrypted without any active intervention by the user. Offline encryption is explicitly requested by the user. In that case, he will also have to decide which files are to be encrypted. For the selection and use of cryptographic procedures, chapter 3.7 Crypto-concept should also be read.

For use on stationary and portable PCs, BSI can, under certain basic prerequisites, provide public agencies with an offline encryption program meeting medium-level protection requirements. A printed request form is located in the section covering Auxiliary Materials of this IT Baseline Protection Manual.

Additional controls:

- Are the users trained in the use of the encryption program?
- Are the data and keys stored separately?

S 4.30 Utilisation of the security functions offered in application programs

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

Several standard products in the PC sector offer a number of useful IT security functions; while these may be of varying quality, they discourage unauthorised persons and/or prevent potential damage. The following is a brief account of five useful functions of this type:

- *Password protection when calling up a program*: the program can onlybe started if a correct password has been previously entered. This will prevent any unauthorised use of the program.
- *Protection of access to individual files*: the program can only access a protected file if the password associated with that file is entered in its correct form. This will prevent unauthorised access to certain files by means of the program.
- *Automatic saving of intermediate data*: the program will make an automatic backup of intermediate data so that any power failure will only affect those data changes which were made after that automatic backup.
- *Automatic saving of the precursor file*: if a file is saved when a file with the same name exists in the indicated path, the second file will not be deleted but will be labelled differently. In this way, inadvertent deletion of an identically named file will be avoided.
- *Encryption of data*: the program can save a file in an encrypted form so that its unauthorised disclosure can be prevented. Thus, the contents of the file will be available only to those who have the secret key used for that purpose.
- Automatic display of macros in data files: This helps to prevent inadvertent execution of macros (macro viruses).

Depending on the software used and the existing additional security functions, it may be advisable to make use of such functions. For IT systems in mobile use, it may be particularly expedient to use password protection during program call-up and automatic backup.

Additional controls:

- Which security functions are offered by the software products used?
- Which of these functions are being regularly used?
- Are the users notified of these functions?
- Are the security-relevant instructions in manuals and certification reports adhered to?

S 4.31 Ensuring power supply during mobile use

Initiation responsibility: IT-user

Implementation responsibility: IT-user

In order to be able to maintain the power supply of a portable PC also during mobile use, the common practice is to use batteries. Depending on the capacity of the batteries and on the type of laptop PC, this will suffice for a limited period of time, e.g. several hours. To prevent loss of data held in volatile store after an operating voltage drop, some general requirements should be met:

- the warning signals (where available) of a laptop, which indicate a voltage drop, must not be disregarded; in the given cases, data backups should be made in good time;
- if prolonged mobile use can be foreseen, rechargeable batteries must be recharged in advance and, where required, charged spare batteries must be kept on hand;
- when handing a mobile IT system over to someone else, sufficient charging of the batteries must be ensured.
- optionally, the charger power pack can be carried.

In addition, it is advisable to save the processed data on a non-volatile storage medium at short intervals during mobile use of the IT system. For this purpose, also automatic storing provided by standard programs may be used.

S 4.32 Physical deletion of data media before and after usage

Initiation responsibility: IT Security Management

Implementation responsibility: IT Procedures Officer

In addition to the instructions on deletion and destruction of data carriers mentioned in measure S 2.167 Secure deletion of data media, the following items must be observed for the exchange of data media:

Magnetic data media intended for exchange should be physically erased before being written with the information to be transmitted. This is to prevent the transmission of residual data which the recipient has no authority to receive.

Physical erasure sufficient for medium-level protection can be achieved by overwriting the entire data medium or at least the used sectors with a certain pattern. Another alternative is to format the data medium, if this cannot be undone again (e.g. DOS version 5.0: *format/u*). Certain commercially available products even allow the physical erasure of individual files.

As a rule, transmitted data also requires protection by the recipient. Once the data has been received, the data medium should again be physically erased.

Optical data media (in this case: WORM) should not be used for data exchange if they bear other information which is not meant for the recipient and cannot be erased.

Additional controls:

- Are the persons responsible for the exchange of data media familiar with the process of physical erasure?
- Do these employees have access to suitable programs for physical erasure?
- Are the recipients of confidential information notified about its data protection requirements?

S 4.33 Use of a virus scanning program when exchanging of data media and data transmission

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

In addition to the instructions described in S 2.3 *Data Media Control*, a virus scan should be carried out immediately before and after data transmission as well as when floppy disks or other data media are exchanged or sent (cf. S 4.3 *Periodic runs of a virus detection program*). It must be ensured that the virus scanning program used can also to detect macro viruses.

A protocol of the sender-check should accompany data media or files sent via remote-data transmission. It is advisable to make a copy of such protocols. Recipients can use these protocols to gain a first impression of the integrity of the transferred data, but are nevertheless bound to carry out a renewed virus scan. If any complaints arise, the sender will be able to demonstrate that a virus infection probably occurred after the data was transmitted.

Additional controls:

- Is the latest possible virus scanning program being used?
- Is the data intended for transfer scanned for viruses beforehand?
- Are protocols of such checks transmitted to the recipient?
- Are received files and data media checked for virus infection before being imported?

S 4.34 Using encryption, checksums or digital signatures

Initiation responsibility: IT Security Management

Implementation responsibility: IT-users

If confidential information or information with high demands for integrity is transmitted and if there is a possibility of this data being disclosed, manipulated by unauthorised parties or changed due to technical failure, a cryptographic procedure for the protection of the data intended for transfer should be considered.

Protection of confidentiality by means of encryption

Confidential information should be encrypted before transmission. The decisive features of any encryption procedure are the quality of the algorithm and the selected key. An algorithm which has proven adequate for medium-level protection is the Triple DES, which is based on the Data Encryption Standard (DES). It is easy to implement, as example source code using the programming language C is provided in many books. For use on stationary and portable PCs, BSI can, under certain basic prerequisites, provide public agencies with an offline encryption program (Chiasmus for Windows) meeting medium-level protection requirements. An order form can be found on the CD-ROM of this manual (see appendix: Auxiliary Materials).

In order to comply with confidentiality requirements of the information to be transmitted, the recipient's and sender's IT system must provide sufficient access protection for the encryption program. Where necessary, it should be stored on an exchangeable data medium, kept under lock and key and only used/imported when the need arises.

Integrity protection using checksums, encryption or digital signatures

If only the integrity of data intended for transfer is to be protected, it should be clarified whether the protection should only be sufficient for incidental alterations, i.e. due to transmission errors, or also for manipulation. If only incidental alterations are to be detected, checksum procedures (e.g. Cyclic Redundancy Checks) or error correction codes can be used. Protection against manipulation is also offered by processes which create a so-called Message Authentication Code (MAC) using a symmetric encryption algorithm (e.g. DES) from the information to be transmitted. Other processes use an asymmetric encryption algorithm (e.g. RSA) in combination with a hash function and create a "digital signature". The resulting "fingerprints" (checksum, error correction codes, MAC, digital signature) are transferred together with the data to the recipient, who can then check them.

See S 2.46 *Appropriate key management* for the transmission or exchange of any necessary keys. Further information on the use of cryptographic procedures and products can be found in chapter 3.7 *Crypto-concept*.

Additional controls:

- Are encryption programs or checksum procedures available for protecting the confidentiality or integrity of data?
- Are those responsible for data transmission informed about correct encryption key management?
- Is the protection of confidentiality/integrity to be ensured only on the transport/transmission route or also on the receiving/transmitting systems?

S 4.35 Pre-dispatch verification of the data to be transferred

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

Before the dispatch of data media, a check must be made as to whether the required information - and only this information - can be reconstructed.

Checking transfer to the data medium for correctness can be performed by means of a program which makes a character-by-character comparison of the original file with the transferred one (e.g. with *comp* on PC's under DOS).

All files on the data medium should be listed (e.g. with *dir* under DOS or *ls* under UNIX) to ensure that it only contains files meant for the recipient.

Any data stored previously on this data medium must be physically erased (S 4.32 *Physical erasure of data carriers before and after usage*).

Additional controls:

- Are the data media intended for exchange checked beforehand as to whether the desired information on them can be reconstructed entirely?
- Are the data media intended for exchange normally checked beforehand as to whether only the desired information on them can be reconstructed?

S 4.36 Blocking fax recipient numbers

Initiation responsibility: Superiors, IT Security Management

Implementation responsibility: Fax Officer, fax mail centre

Currently, there are at least three methods of preventing the accidental or intentional transmission of information or documents via fax to undesired recipient numbers:

Settings at the fax machine or fax server

Some devices allow the (positive) exclusion of certain recipient numbers or (negative) exclusion of all recipient numbers except certain selected ones from fax communication.

Settings at the PBX

The same type of authorisation can be realised in modern PBX systems, provided that the fax machine is connected to the telephone network via such a system.

Using auxiliary devices

If a fax machine or PBX does not offer such a possibility, one alternative is to rent an auxiliary device from the operator of the public network which prevents the establishment of a connection with certain subscriber numbers (positive and negative exclusion).

Additional controls:

- Is there a requirement for blocking certain fax recipients?
- Have fax messages been sent to a wrong recipient on any occasion?

S 4.37 Blocking fax sender numbers

Initiation responsibility: IT Security Management

Implementation responsibility: Fax Officer, fax mail centre

To prevent certain fax transmissions from blocking one's own fax machine, e.g. overloading it with fax advertising campaigns, it is possible to place a block on specified fax sender numbers.

Analysis of originating call numbers by the fax machine or fax server

Some modern fax machines (Group 4) are able to evaluate sender numbers and thus prevent the reception of fax messages from particular numbers. This applies also to fax servers which are connected to the ISDN network. The Call Subscriber ID (CSID) can also be used to evaluate the numbers from which incoming faxes are sent. Unfortunately, however, it is possible for originators of faxes to suppress transmission of their numbers and for the transmitted call numbers and the originator identifier to be tampered with.

Definition of closed user groups.

Another alternative is for the telephone utility to set up a closed user group (with charges) if the sender and recipient are connected to digital exchanges. This alternative is offered by some modern PBX facilities (cf. Section 8.1 *Telecommunications System (Private Branch Exchange)).*

Additional controls:

- Is there a requirement to block certain originating fax numbers?
- Is the Fax Officer aware of the possibility of the safeguards outlined above?

S 4.38 Deactivation of unnecessary service features

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

Unnecessary service features (particularly the remote-inquiry function) should, if possible, be deactivated to prevent misuse and improper operation. To determine whether a service feature is necessary, the associated security risks should also be taken into consideration.

Additional controls:

- Are users explicitly requested to deactivate unnecessary service features?

S 4.39 Deactivation of answering machines for periods of absence

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

To prevent misuse, answering machines can be deactivated or disconnected from the telephone network for periods during which they are not required. This should be ensured particularly for answering machines with a room monitoring function.

It should be noted that, in certain cases, inactive answering machines are activated automatically if the connection is not established after a certain interval (e.g. after 10 rings).

S 4.40 Preventing unauthorised use of computer microphones

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

The microphone on a networked computer can be used by persons having access to the corresponding device file (e.g. */dev/audio* under UNIX). Under Windows NT the access right to the appropriate registry codes determine who can activate the computer microphone (*HKEY_LOCAL_MACHINE\HARDWARE*). This authorisation must therefore be granted judiciously. Access to the device file should only be possible whilst somebody is working on the IT system. If a microphone is to be prevented from being used in general, it must, if possible, be turned off or separated physically from the computer.

For microphones which are integrated into computers and can only be activated/deactivated using software, the access rights must be restricted to authorised users. Under UNIX this is possible, for example, by depriving all relevant users of the right to read the */dev/audio* device file; under Windows NT by depriving users of access to the appropriate registry codes. This prevents these users from using the microphone but still allows them to play back audio files.

On IT systems equipped with a microphone, a check must be made as to whether access rights and ownership are changed on opening of the device. If this is the case, or if every user should be able to use the microphone without the administrator having to release it individually, the administrator must provide a command which

- can only be activated once a user has logged into the IT system
- can only be activated by this user and
- withdraws the access right from this user after log-out.

If access to the microphone is not controlled by means of a secure command, the microphone must be disconnected physically from the computer.

Additional controls:

- Can the computer's microphone be turned off or disconnected physically from the computer?
- Who has access to the microphone's device file or to the entries in the registry where hardware settings may be manipulated?

S 4.41 Use of a suitable PC security product

Initiation responsibility: Head of IT Section, IT security management, data privacy officer, persons responsible for individual IT applications

Implementation responsibility: Procurement department, administrator

Provision of a PC security product must be arranged for the DOS PC with several users. The following minimum functionality may be used as a standard for procuring a product or for reviewing products already in use. The aim of this minimum functionality is to ensure that

- only authorised persons can use the PC,
- the users can only access the data in the way necessary for them to fulfil the task,
- irregularities and attempts at manipulation become apparent.

Recommended minimum functionality for PC security products for use in DOS PC's with several users:

- *Identification and authentication* of the administrator and the users. Lock-out from the system which can only be reset by the administrator should take place after 3 incorrect attempts at authentication. If a password is used, it should have at least six characters and should be stored in the system in encrypted form.
- *Administration and monitoring of rights* on hard disks and files where there should at least be differentiation between read and write access.
- Role separation between administrator and user. The administrator alone may assign or withdraw rights.
- *Logging* of logging-on, logging-off and infringement of rights procedures should be possible.
- *No system access* at operating system level (DOS) must be possible for users.
- *Screen lock* following inactivity of the keyboard or mouse for some time and re-activating by means of identification and authentication.
- *Boot protection* should make it impossible to be able to boot up the PC from floppy disk without authorisation.

Sensible minimum evaluation depth and minimum strength of mechanisms for certificates in accordance with ITSEC: E2, medium.

Additional requirements of the PC security product:

- *User-friendly surface* to increase acceptance.
- Informative and comprehensible documentation for administrator and user.

Desirable additional functionality of the PC security product:

- *Role separation between administrator, reviser and user;* only the administrator may assign or withdraw rights and only the reviser has access to the protocol data,
- *Logging* of administration activities,
- *Support of protocol evaluation* by means of configurable filter functions,
- *Encryption* of data stocks with an appropriate encryption algorithm and in such a manner that loss of data is prevented by the system in the event of malfunctions (power failure, termination of a procedure).

Implementation of this functionality may be effected in both hardware and software. Safeguard S 2.66 *Consideration of the Contribution of Certification to Procurement* should be taken into account when procuring a new product.

Temporary Solution:

An encryption product may be utilised as a temporary solution if it is not possible to purchase or implement the use of such a PC security product at short notice. When work commences, every user must use this product to decrypt the data allocated to him and must encrypt it when work ends. This makes it possible to ensure that confidentiality of the data is maintained but does not prevent encrypted data from being manipulated. Manipulation of the data is generally identified on decrypting as the result is data which does not make sense.

For use on stationary and portable PCs, BSI can, under certain basic prerequisites, provide public agencies with an offline encryption program meeting medium-level protection requirements (see appendix auxiliary materials).

S 4.42 Implementation of security functions in the IT application

Initiation responsibility: Head of IT Section, IT security management, data privacy officer, persons responsible for individual IT applications

Implementation responsibility: Application developer

There may be several reasons why it might be necessary to implement security functions such as access control, administration and checking of access rights or logging within the application programs themselves:

- If the logging facilities of the IT system, including the additional IT security products used, are not sufficient to guarantee adequate verification security, then these protocol elements must be implemented in the application program. (Example: BDSG, Appendix to § 9, Input Monitoring: "to guarantee that it is subsequently possible to check and ascertain which person-related data have been entered into data processing systems at what time and by whom".)
- If the granularity of the IT system's access rights inclusive of additional security products used is not sufficient to guarantee proper operation, then administration and monitoring of access rights must be implemented in the application program. (Example: a data base with a joint data pool. It should be assumed that access is only permissible to certain fields depending on the user's role.)
- If it is not possible with the IT system, including the additional IT security products used, to prevent the administrator from gaining access to certain data or at least to log this access and monitor it, then this must be implemented where necessary by additional security features in the application program. For example, by encrypting the data it is possible to prevent the administrator from reading this data in plain text if he does not possess the appropriate key.

These additional requirements on IT applications must be taken into account at the time of planning and development, as subsequent implementation is usually no longer possible for reasons of cost.

Additional controls:

- When developing new IT applications, is there a systematic determination of the security functions the application must provide?

S 4.43 Fax machine with automatic envelopment sealing system

Initiation responsibility: IT Security Management

Implementation responsibility: Procurer

Fax machines with an automatic envelopment system prevent unauthorised removal and reading of faxes. Incoming faxes are folded so that only the fax header remains visible and are then heat-sealed in a clear envelope. The fax then drops into a lockable box in the fax machine. Only the authorised person who has a key to this box normally has access to the envelopes. Unauthorised cognisance prior to delivery of the fax is only possible by forcibly opening the box or tearing open the heat-sealed envelope and will thus, at the very least, be noticed.

Additional controls:

- Is the purchase of such a machine worthwhile?

S 4.44 Checking of incoming files for macro viruses

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

Incoming files by means of data media exchange or remote transmission must be subjected to a virus test. This applies not only to regular program files, but also to files which have been created by means of application programs which can use a macro language. It is currently known that macros with damaging functions have been generated for the application programs listed below:

- Winword (from Version 2.0)
- Powerpoint
- Excel
- AmiPro
- Adobe Acrobat

Other safeguards may be dispensed with as long as an up-to-date virus scanning program which also recognises macro viruses is used. In addition, a test environment may be useful to check transmitted files for macro viruses using the application program. Alternatively, it is possible to process files received using an editor which converts the file into a format in which the macros are unable to run. The received files can also be opened with viewers, which are free for viewing the most common file formats and, likewise, do not allow macros to run.

If possible, documents should only be passed on in RTF format, as no macro language exists for such files and thereby no danger is posed by macro viruses. Files can usually be converted to RTF format without any particular loss in quality.

As a further precaution, users should be shown how they may be able to prevent macros present in files from running automatically. Unfortunately, this differs from program to program and version to version and is not always reliable.

Even in PostScript files there may be problems similar to those encountered with macro viruses. In PostScript display programs there are interpreters which process the PostScript language. Above level 2.0 of the PostScript specification there are also PostScript commands for writing files. As a result it is possible to generate PostScript files which, during processing by an interpreter, can modify, delete or rename other files as soon as they are displayed on the screen.

Specific problems exist in the *ghostscript (gs)* program. In the UNIX versions it is possible to switch off the write facilities on files with the *-dSAFER* option. However this is not the pre-set option. This option is similarly named in versions for other operating systems.

Use of the *-dSAFER* option is left up to the user. The result is that numerous other programs which invoke *ghostscript (gs)* internally (e.g. *mosaic, netscape, xdvi, xfig, xv,* etc.) implement it in various ways. Therefore the option should be set as a default. Descriptions of how to implement this are to be found in the security bulletins of DFN-CERT DSB-95:02 and DSB-95:03

dated August 24 1995 (see also S 2.35 *Obtaining information on security flaws of the system).*

For example, this problem affects all *ghostscript* versions of Aladdin prior to 3.22beta and the GNU versions up to and including 2.6.2. In older *ghostscript* versions there may also be further PostScript commands with which it is possible to modify files. Only *ghostscript* versions where these problems have been overcome should be used.

From version 1.5 onwards, the *ghostview* PostScript interpreter offers the *-safer* option, which activates the security functions of *ghostscript*. Versions earlier than 1.5 do not offer this protection, and should be replaced by the current version.

Similar problems can also occur in the case of PDF files. PDF files which can be read with Acrobat Reader freeware are often available in the Internet. Functions such as program calls can be embedded in PDF files, and can pose a security risk to the files of the local IT system. These embedded functions can be started when a document is opened or via *action triggers* by moving through the document, without the reader being aware of this.

To avoid this, PDF files should only be read with viewers such as *ghostscript* which are not able to process this functionality, or with the latest version of Acrobat Reader or Acrobat Exchange, which inform the user about the presence of any macros and require explicit approval of their execution.

Additional controls:

- Does the virus checker program in use also detect macro viruses?
- Was a check made to see whether the *-dSAFER* option is activated in the PostScript interpreters being used?

S 4.45 Setting up a secure Peer-to-Peer environment

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The administrator should individually authorise or block the Peer-to-Peer functions for every computer in the WfW network and thus restrict the WfW environment in a user-specific way. To do this he requires the administration tool ADMINCFG.EXE.

After calling up ADMINCFG.EXE, the security configuration file WFWSYS.CFG, in which the security settings of the respective WfW computer are stored, must first be opened. ADMINCFG.EXE cannot distinguish in this case between different users on one WfW computer.

Even if it is not intended to restrict the environment, the security configuration file WFWSYS.CFG must be provided with password protection. If the administration tool ADMINCFG.EXE is installed locally for this purpose, it must be removed afterwards.

From the point of view of security, it is possible to create the following configurations for the computer with the aid of the administration tool ADMINCFG.EXE:

The **sharing options** must be specified:

- If the computer is not intended for the sharing of directories, the option “Deactivate file sharing“ must be set. The corresponding functions are then no longer available in the file manager but it remains possible to link up with the directories of other computers.
- If the computer is not intended for the sharing of printers, the option “Deactivate printer sharing“ must be set.
- If the computer is not intended for network DDE sharing (e.g. telephony under WfW, data communication via the filing folder), the option “Deactivate network DDE sharing“ must be set.

The **password options** must be specified:

- In the case of activated password caching, all WfW network connections will be stored in a file with associated passwords if this is desired by the user in the respective connection set-up. Repeated password entries are then no longer necessary at a later date. The “Deactivate password caching“ option should always be set, at the very least, if the WfW computer does not have adequate access protection (e.g. BIOS password).
- “Display passwords in sharing dialogue fields in a readable manner“ may not be activated as otherwise the password appears on the screen in plain text when it is entered.
- “Expiration of log-on password“ should be set in the period specified in the security strategy.
- “Minimum password length“ must be set to at least 6.

- "Enforce alphanumeric passwords" should be set. Thus letter and numeral combinations become obligatory.
- The options "Request confirmed log-on in Windows NT or LAN manager domain" and "Allow caching of passcode words" are not considered at this point as the interplay of WfW with Windows NT or LAN manager was not investigated.

The **administrator settings** must be specified:

- The administrator must specify a password for the created configuration file WFWSYS.CFG, which may only be known to himself and his substitute. This password must be deposited securely (cf. S 2.22 *Depositing of Passwords*).
- Pre-set security profiles may be accepted from a server via "Update options". Furthermore, it is also possible to set them so that at the start of a client, the security configuration file of the server is checked, and, in the event of changes, the local file is updated. This makes central administration of the WfW network, simple addition of further WfW computers and changing of the password for the configuration files easier for the WfW administrator.

When configuring a Windows-for-Workgroups computer, the administrator also needs to consider the following points:

- The pre-set option "Share again on startup" must be deactivated in the sharing dialogues (file and print manager).
- The pre-set option "Store password in password list" must be deactivated in the connection dialogues (file and print manager).
- In the program group SYSTEM CONTROL under *network,* the computer name, the name of the work group and the standard log-on name should be pre-set in accordance with the name convention.
- The WfW protocol must be activated (in the program group SYSTEM CONTROL under *network*). In this case, all events should be recorded and the protocol file should be set up to be sufficiently large (e.g. 32 KB).
- In the program group SYSTEM CONTROL under *network*, an option should be set up via the button *start* indicating whether the computer's own applications or access by others should be treated with priority. If access by others is subordinate, priority in favour of more rapid execution should be selected.
- During the use of Schedule+, the right granted by default to view open and assigned time blocks must be deactivated for all unauthorised WfW users. Otherwise every user at the same post office will be able to view individual appointments in the time schedule.

If a post office is configured for use by several persons for the purpose of communications or joint appointment scheduling, a corresponding data backup should be performed at appropriate time intervals. This is required to prevent inadvertent or intentional deletion of the post office, which is not protected automatically under WfW.

Additional controls:

- Are the settings made documented in an appropriate form?
- Was any consideration given to supervising the security settings via the network? WfW offers the facility for depositing security profiles on a server which will call up the individual clients in the WfW network for updating.

S 4.46 Use of the log-on password under WfW and Windows 95

Initiation responsibility: Administrators

Implementation responsibility: IT-user

If a new user logs on to a computer under WfW or Windows 95, he will be asked whether he would like to set up a code word list (*[logonname].pwl*) under his log-on name. This list will then record all the passwords which have to be transmitted by this user on connection with the resources of others. However, this only happens if this "caching" of passwords on the computer is explicitly permitted and the user also desires it in individual cases.

The WfW log-on password serves solely to protect this password list. Only on correct entry of the password belonging to the log-on name will this be decrypted and made available.

Protection of the stored code words with respect to the users of the same computer is only guaranteed by an individual log-on password, particularly when a WfW or Windows 95 computer is utilised by several users.

The respective password must be selected appropriately, changed regularly and deposited securely (see S 2.11 *Provisions governing the use of passwords* and S 2.22 *Depositing of passwords*).

Notes:

No log-on password is necessary under WfW if no passwords are stored in the password list by the user. Therefore, if password caching is deactivated on principle by the administrator via ADMINCGF.EXE under WfW, or via the system guidelines under Windows 95, the log-on password is superfluous. Even masquerading on the PC cannot be prevented with this authentication mechanism as every password list may be renamed, the original log-on name may be re-used and the original password list may then be changed back again.

However, if password caching is permitted and also used, the administrator must set the minimum length of the log-on password to 6 using ADMINCFG.EXE under WfW, or the system guidelines under Windows 95. Then entry of the password is obligatory when logging on under WfW and Windows 95 and cannot be deactivated. In exceptional cases, e.g. if the computer is only being utilised by one user and there is adequate access protection (BIOS password, screen lock, etc.), the log-on password may be deactivated. Deactivation is possible if the minimum length of the password is set to zero.

If passwords are inadvertently stored in the password list by the user, the file *[logonname].pwl* must be deleted.

Additional controls:

- Will the WfW or Windows 95 users be told that, in addition to password protection on the PC (e.g. BIOS password), the log-on password is also necessary for protection of the individual password list under WfW or Windows 95?

S 4.47 Logging of firewall activities

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

It must be specified which events are to be logged and who will evaluate the logs. Logging must comply with the data privacy regulations. Earmarking in accordance with § 14 of the BDSG must be particularly observed for protocol data.

The packet filters used must be able to log IP number, service, time and date for every incoming or outgoing packet. Restrictions to specific packets are also possible in this case (e.g. only packets with a special source address).

Logging of the user identification, IP number, service, time and date must be carried out (application gateway) for every connection made or aborted, although restrictions to specific connections (e.g. for a special user) are also possible.

It must be possible for logging not to be carried out for certain users so that no essential information is overlooked due to too large a number of log entries. This choice may be made, for example, on the basis of the rights profile of individual users.

The log information of all components should be sent to a central point via a trustworthy route so that the log information cannot be altered prior to final storage.

Special incidents which may be set, such as repeatedly incorrect password entries for a user, identification or unauthorised connection attempts, must be emphasised in the log and should lead to the immediate alerting of the firewall administrator.

If proper logging is no longer possible (e.g. because there is no more space on the data medium) the firewall must block all traffic and pass on an appropriate message to the administrator.

S 4.48 Password protection under Windows NT

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

For each user, access to a Windows NT system must be protected by a password. User accounts without a password are not allowed to exist, as they constitute a potential weakness in the system. It is important that users too are familiar with the protective function of the passwords, since the co-operation of users naturally contributes to the security of the overall system.

Setting up a new user is performed with the aid of the utility User Manager via the command "*New User*". At the same time an initial password with a maximum of 14 characters must be entered in the fields "Password" and "Confirm Password". For passwords under Windows NT, the use of upper and lower case letters must be observed. A meaningful initial password should be allocated which is notified to the user. Always choosing the same initial password or making this password identical to the user name opens up a security gap which can be avoided with a little effort.

The option "*User Must Change Password At Next Log-On*" should be set with all new accounts, so that the log-on password is not retained. On the other hand, the option "*User Cannot Change Password*" should only be used in exceptional cases, for instance for pre-defined accounts in the training operation. The option "*Password Never Expires*" should only be used for user accounts to which a service is assigned with the aid of the system control option "*Services*" (the reproduction service, for example), as it cancels the setting "*Maximum Password Age*" in the Accounts Policy and prevents the password from expiring.

Policy for user accounts, user rights and system monitoring can be stipulated via User Manager. In the User Accounts Policy the figure 6 should be entered as the minimum password length, for higher security requirements the figure 8 should be entered (see also S 2.11 "*Provisions governing the use of passwords*").

Password history should always be activated and should include at least 6 passwords. The duration of validity of the password ("*Maximum Password Duration*") should be limited to a maximum period of 6 months. By fixing a figure for "*Minimum Password Duration*", users can be prevented from changing their password several times in a row with the object of by-passing history validation. However, a period greater than 1 day should not be chosen for "*Minimum Password Duration*", in order to enable the user to change a password at any time.

Note: The parameter "*Allow Changes Immediately*" must not be chosen under version 3.51 of Windows NT, as otherwise validation of password history is deactivated.

User accounts should be locked out following repeated invalid password entries, in order to make attempts to guess the passwords of users more difficult. The option "*Account lockout*" should in any case be activated. At the same time the option "*Lockout after*", which fixes the number (1 to 999) of

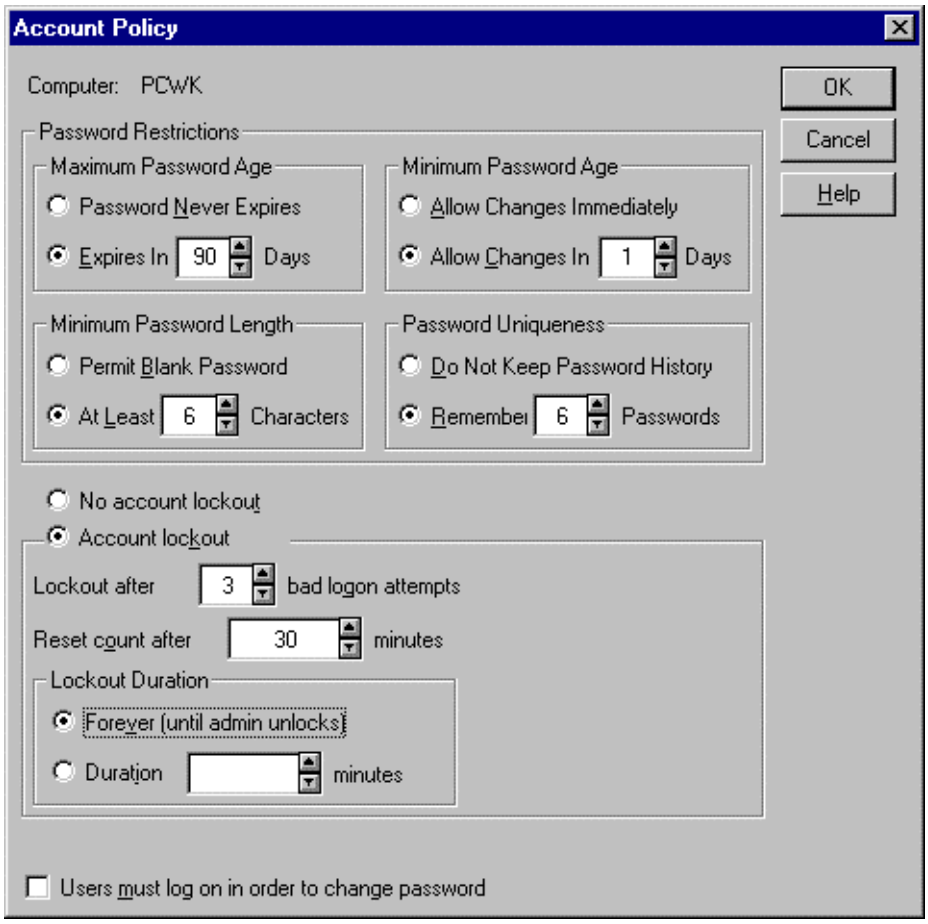
invalid log-on attempts which lead to the lockout of the account, should be set to a figure between 3 and 10. The option "*Reset count after*", which specifies the maximum number of minutes (1 to 99999) between two invalid log-on attempts, should be set at approximately half an hour. If, for example, for "*Lockout after*" the figure 5 and for " *Reset count after* " the figure 30 is specified, a lockout occurs after 5 invalid log-on attempts made within a timeslot of 29 minutes.

In general, by activating the option "*Forever*" it should be stipulated that lockout remains active until an administrator cancels it. Should this place too heavy a burden on the administrators, a suitable figure can also be specified as "*Lockout duration*", so that account lockout is only maintained for a limited period. If it is intended to investigate the causes of account lockout directly, a sufficiently long time interval, e.g. 1,440 minutes (1 day) should be specified, otherwise a figure of approximately 30 minutes should be chosen.

In order to avoid complete locking of the system (see S 4.55 *Secure Installation of Windows NT*), it should be noted that the pre-defined administrator account is not included in this automatic lockout..

The option "User must log on in order to change password" should not be activated. Together with the setting "User must change password on next log on" this would lead to new users having no access to the system.

The policy figures shown in the following diagram give adequate protection in terms of an average security requirement:



Additional controls:

- Are the specifications for the user accounts policy documented?
- Are the settings regularly checked in User Manager?

S 4.49 Safeguarding the boot-up procedure for a Windows NT system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Windows NT can only be operated securely if there is a guarantee right from the start of the system that a closed security environment is constructed, i.e. that there are no ways around the security functions of the operating system. This requires that all resources which are capable of being protected by Windows NT are under the control of the operating system and also that there is no possibility of starting up outside systems or open system environments which can circumvent the protection offered by Windows NT. In addition, the following aspects should be taken into account:

- All existing hard disk partitions must be formatted using the NTFS file system. Partitions formatted using the FAT, VFAT or HPFS file systems cannot be protected against accesses from users. On the one hand this means that the data filed on them is exposed to arbitrary accesses from any user, and on the other hand, that these partitions can be misused for the uncontrolled exchange of data between users.
- Disk drives constitute a similar risk, as disks under Windows NT can only be formatted using the FAT or VFAT file systems. For this reason disk drives on all computers which are not under strict physical control must always be locked out by fitting disk locks (see S 4.4 *Locking of disk drive slots*). On Windows NT clients, the disk drives can also be deactivated for non-privileged users via the control panel option "*Devices\Floppy*". This option should not be made use of on Windows NT servers (see S 4.52 *Equipment protection under Windows NT*).
- If the computer has an open floppy disk drive or if it is possible to boot from a connected CD-ROM drive, there is a danger that the computer could be started up with an operating system other than Windows NT. The same danger can arise if other operating systems are installed on a local hard disk. In this case, the user can by-pass the security mechanisms of Windows NT with the aid of various programs. There are now several programs which can be used to read, and partially also modify, files protected under NTFS from a DOS or Linux environment. The security attributes set by the NTFS file system are ignored both under the MS-DOS and Linux operating systems. The user therefore has access to all the computer's files from MS-DOS or Linux. For this reason, no other operating systems may be installed on the hard disk besides Windows NT. Moreover, the boot procedure must be safeguarded by a BIOS setting protected with a BIOS password in such a way that the system cannot be started up by any connected disk drive or CD-ROM drive (see S 4.1 *Password protection for IT-Systems*).
- In the context of a re-installation of Windows NT, there is an opportunity to update the current installation of the operating system or install a new version in parallel. In the case of parallel installation, the existing file structure is not changed, but the pre-defined administrator account is re-

created with a new password. This "new" administrator then has full access to all the computer's resources and thus to all data and programs. In order to prevent this possibility of re-installation, users must not be in a position to change the file *BOOT.INI* in the root directory of the first disk (see S 4.53 *Restrictive allocation of access rights to files and directories under Windows NT*).

- With the aid of the installation programs an emergency disk (see S 6.42 *Creating start-up disks for Windows NT*), can also be produced and used to carry out a system reconstruction. In the process, access protection of the NTFS partition of the operating system is cancelled. For this reason it is absolutely essential to safeguard the installation programs, an emergency disk which may already exist and the set-up disks in such a way that they are protected against unauthorised access. This specific threat can also be countered by protecting the disk drives with drive locks (see S 4.4 *Locking of floppy disk drive slots*) and safeguarding the boot procedure by means of the appropriate BIOS setting (see above).

Under Windows NT, logging-on to the server is only possible for users to whom the user right "*Local log-on*" has been given. These users are restricted to the rights and permissions assigned to them. To avoid misuse of the possibilities for logging-on to the server, provision must be made for the user rights, and the allocations to user groups, to be correspondingly restrictive (see safeguards S 2.93 *Planning of the Windows NT network* and S 4.50 *Structured system administration under Windows NT*).

Additional controls:

- Is the safeguarding of any existing disk drives checked regularly?
- Are there regular checks to ensure that no parallel installation of another operating system exists?
- Are the BIOS settings which prevent booting from media other than the hard disk checked regularly?

S 4.50 Structured system administration under Windows NT

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Under Windows NT, user groups are compilations of user accounts. Whenever a user account is added to a group, the user concerned receives all the rights and permissions which were granted to the group. In this way, designated users can easily be provided with common capabilities. If possible, the roles of employees should be reflected in groups and the access rights then allocated to these groups in accordance with their needs.

The use of groups, in place of the assignment of rights and permissions to individual users, makes administration easier, and, thanks to greater transparency, helps to increase system security. Groups should be formed even when there is a small number of employees. As a result, when there is an expansion, no fundamental restructuring of the rights structures has to be carried out.

Rights and permissions are additive. That means that for one user who is a member of several groups, the most extensive access right for a particular resource applies. However, there is an **exception** to this: If users are members of a group which has been given the access permission "No access" for a particular resource, then these users cannot access this resource, even if they are members of another group which has been granted the right "Full access" (see also S 4.53 *Restrictive allocation of access rights to files and directories under Windows NT*)

Example:

User Smith is member of groups "A" and "B". Group "A" has been granted the access permission "Read" the directory "Invoice", group "B" has been granted the access permission "Read and Write". User Smith has therefore the access permission "Read and Write" for the directory "Invoice".

The user group concept of Windows NT distinguishes between global and local groups.

Local groups

A group is called "local" if it can only be granted permissions and rights for the computer on which it was defined. On computers with the operating system Windows NT (i.e. both servers and workstations), which do not belong to a domain, all groups are local. In order to structure the allocation of rights and permissions, only this type of group is used on such computers.

If a computer under Windows NT belongs to a domain, local groups are also available. They can then contain user accounts from their own computer, global users, and global groups from their own domain or from trusted domains.

Local groups cannot receive permissions for resources of other domains. It is not possible for a local group to become a member of another local group.

Local groups are represented in the User Manager by a group symbol with a computer.

Global groups

If a computer on which Windows NT is being run belongs to a domain, there is a further type of group for which access to the workstation can be made possible. This is the "*global group*", which can be used in several places: in its own domain, on servers, on workstations of the domain and in trusted domains. If a workstation belongs to a domain, it means that permissions and rights to the local workstation and membership of local groups of the workstation, can be granted to the global groups of the domain and the trusted domains. A global group can only contain user accounts from its own domain.

Global groups can only be defined on the primary domain controller. It is not possible for other groups to become members of a global group. Global groups are represented in the User Manager by a group symbol with a globe.

To sum it up, it is recommended to structure the system administration as follows:

Rights and permissions are assigned to *local* groups. Users become members of global *groups* and the *global* groups become members of *local* groups.

In addition to the distinction between local and global groups, there is also a distinction between pre-defined user groups, special groups and freely-defined user groups.

Pre-defined user groups

The actions a user can perform depend on the group memberships of his user account. Several groups are pre-defined in Windows NT and each group is granted a particular set of user rights as standard. Where required, additional groups can be created and defined via the User Manager. With these groups, access to individually-compiled resources is made possible for the users assigned to them.

In addition to the rights, pre-defined functions are allocated to some of the pre-defined local groups. Rights and access permissions can be granted directly to the groups and user accounts and withdrawn from them. On the other hand, the pre-defined functions cannot be administrated directly. Pre-defined functions can only be provided for a user if the user is made member of a suitable local group.

On computers which are configured with the operating system Windows NT as member server (a server which does not have the function of a domain controller) or as a workstation, the following local groups are set up during installation by default.

- Administrators
- Back-up operators
- Power users
- Replication operators
- Users

- Guests

Under Windows NT, on workstations and servers which are not configured as domain controllers, the rights and functions which are granted to designated, pre-defined local groups are listed in the following table:

	Back-up operators	*Everyone*	*Guests*	*Users*	*Power users*	*Administrators*
Local log-on	X	X	X	X	X	X
Access to this computer from the network	X	X			X	
Assuming ownership of files and objects	X					
Administration of supervisory and security listing	X					
Changing the system time	X	X				
System shutdown	X	X	X		X	X
Shutdown from a remote system	X	X				
Back-up of files and directories	X					X
Restoring files and directories	X					X

	Back-up operators	*Everyone*	*Guests*	*Users*	*Power users*	*Administrators*
Generation and administration of user accounts	X	X				
Generation and administration of local groups	X	X	X			
Granting of user rights	X					
Lockout of the workstation	X	X			X	
Access to a locked-out workstation	X					
Formatting of the hard disk	X					
Generation of common groups	X	X				
Storing of local profiles	X	X	X			X
Sharing of directories	X	X				
Sharing of printers	X	X				
Loading and removing device drivers	X	X				

On servers which are configured as domain controllers under the operating system Windows NT, the following local groups are set up during installation by default.

- Administrators
- Back-up operators

- Server operators
- Accounts operators
- Print operators
- Replication operators
- Users
- Guests

In this configuration, the following global groups are also created during installation:Domain adminsDomain users

- Domain guests

The rights and functions which are granted under Windows NT on domain controllers to designated, pre-defined local groups, are detailed in the following table:

	Guests	*Users*	*Everyone*	*Back-up operators*	*Print operators*	*Accounts operators*	*Server operators*	*Administrators*
Local log-on	X	X	X	X	X			
Access to this computer from the network	X					X		
Assuming ownership of files and objects	X							
Administration of supervisory and security listing	X							
Changing the system time	X	X						
System shutdown	X	X	X	X	X			
Shutdown from a remote system	X	X						
Adding workstations to the domain	X							
Back-up of files and directories	X	X			X			
Restoring files and directories	X	X			X			

	Administrators	*Server operators*	*Accounts operators*	*Print operators*	*Back-up operators*	*Everyone*	*Users*	*Guests*
Generation and administration of user accounts	X		X					
Generation and administration of global groups	X		X					
Generation and administration of local groups	X		X				X	
Granting of user rights	X							
Lockout of the server	X	X				X		
Access to a locked-out server	X							
Formatting of the server hard disk	X	X						
Generation of common groups	X	X						
Storing of local profiles	X	X	X	X	X			
Sharing of directories	X	X						
Sharing of printers	X	X		X				
Loading and removing device drivers	X							

Note: The rights outlined above, which are allocated under Windows NT as standard, must all be reviewed separately with a view to determining whether they are compatible with the security strategy laid down (see S 2.91 *Determining a security strategy for the Windows NT client-server network*). Thus, for example, the right “Access to this computer from the network“ should be withdrawn from the group “Everyone“. Whether it is granted alternatively to the group “Users“ must be clarified in detail.

The following pre-defined groups are available under Windows NT:

- *Administrators* - The "*Administrators*" group is the most powerful group in Windows NT. The members of this group administrate the overall configuration of the system. The pre-defined "Administrator" user account is a member of the "*Administrators*" group. If a computer belongs to a domain, the "*Domains admins*" group is automatically a member of the "*Administrators*" group of this computer.

  Note: User accounts of this group should only be used for system management tasks which require full control over the system. Tasks which can be carried out under restricted rights should, if possible, be performed from user accounts which belong to one of the other groups, in order to reduce endangerment to the system from tasks with unrestricted rights. In particular, a user account which only belongs to the group "Users" or one or more freely-defined groups should be created for every administrator for performing daily routine tasks. The number of user accounts in the group "Administrators" should be kept as small as possible.

  Administrators are subject to normal access control and do not automatically have access to every file. Where required, an administrator can assume ownership of a file and thereby access it. However, in such a case the administrator cannot pass the file back to the original owner, as Windows NT does not provide a function for this purpose.

- *Domain admins* - The global group "*Domain admins*" is a member of the local group of administrators for the domain in question and of the local groups of administrators of each computer in the domain, with the result that the domain administrators can administrate the domain controllers, every server and all other computers in the domain. The pre-defined administrator account of the domain controller is a member of the "*Domain admins*" group.

- *Power users* - The local group "*Power users*" defined under Windows NT Workstation makes restricted administrative functions available to the user accounts of its members. A power user can share directories in the network, set the internal clock of the computer, install, share and administrate printers, and create general program groups. They can create user accounts and groups, change or delete the user accounts and groups that they have created, and add or remove members from the groups "*Power users*", "*Users*" and "*Guests*".

  However, power users cannot change or delete the groups "*Administrators*", "*Domain admins*", "*Accounts operators*", "*Back-up operators*", "*Print operators*" and "*Server operators*", neither can they change or delete any administrators’ user accounts.

Note: This group should be used to define sub-system administrators who relieve system administrators of the burden of certain routine tasks, especially in connection with the administration of user accounts without, however, receiving full control over the system.

- *Accounts operators* - The local group "*Accounts operators*" defined on domain controllers largely corresponds to the "*Power users*" group defined under Windows NT Workstation.
- *Users* - Membership of the local group "*Users*" offers the functions a user needs for carrying out everyday tasks. With the exception of the pre-defined administrator and guest accounts, all the workstation's user accounts belong to the "*Users*" group. If a new user account is added, it automatically becomes a member of this group. If a computer belongs to a domain, the domain users group is a member of the "*Users*" group of this computer as standard.

  Note: All users who do not require any extended rights should usually only belong to this pre-defined group and to suitable freely-defined groups which reflect the organisational structure. Allocations to other pre-defined groups should only be made in justified individual cases. This also means that users should not receive any administrator rights on their workstation computers.
- *Domain users* - The global group "*Domain users*" originally contains the built-in account of the administrator for the domain concerned. When new accounts are created, these are automatically entered into the "*Domain users*" group. As standard, this group is a member of the local group "*Users*" for the domain concerned and of the local groups "*Users*" of each computer in the domain, so that the "D*omain users*" have normal access and normal rights and permissions in relation to every computer in the domain.
- *Guests* - The local group "Guests" enables the occasional or one-time user to log on and to work with a restricted range of functions. The pre-defined guest user account is a member of the "*Guests*" group. The resource permissions granted to the "*Users*" group can be withheld from the "*Guests*" group, so that the capabilities of the members of this group can be suitably restricted.

  Note: If possible, no further user accounts should belong to this group apart from the pre-defined guest account, and the pre-defined guest account should be locked out (see S 4.55 *Secure Installation of Windows NT*). As an additional precaution it should be provided with a password to prevent unauthorised access in case it is unlocked for a short time.
- *Domain guests* - The global group "*Domain guests*" originally contains the built-in guest user account for the domain concerned. This group is a member of the local group of guests for the domain concerned.
- *Back-up operators* - The members of the local group "*Back-up operators*", which is a standard group on all computers under Windows NT, can save and restore files and directories.

Note: Data back-ups and the recovery of saved data should be carried out by a member of this group. For this it is not necessary to use an administrator account.

- *Print operators* - The members of the local group "*Print operators*" defined on domain controllers can administrate printers on the domain controllers. They can also log on to these servers and shut them down.

  Note: The administration of printers should be carried out by members of this group in order to avoid the unnecessary use of administrator accounts.

- *Server operators* - The members of the local group "*Server operators*" defined on domain controllers can administrate the printer and network shares on the domain controllers. Furthermore, they can save and recover files and directories, block and release the domain controller, format the hard disks of the domain controller and alter the system time. Finally, they can also log onto the domain controller and shut it down.

  Note: Routine tasks involved in controlling the domain controllers should be carried out by members of this group, insofar as they can be carried out with the rights of this group. Only tasks which require full control over the system should be carried out from administrator accounts.

- *Replication operators* - The local group "*Replication operators*" defined on computers under Windows NT supports the functions of directory replication. A domain user account used for logging on the replication service of the workstation should be the sole member of the group "*Replication operators*" .

  Note: No users accounts should be added to this group, and the user account present there should not have the rights "*Local log-on*" and "*Access to this computer of the network*".

Special groups

In addition to the above-mentioned pre-defined groups, Windows NT creates a number of special, internal groups which are not listed by User Manager. In a good many cases, however, they are listed in the group list, for example when permissions are assigned to directories, files, released network directories or printers.

- *Everyone* - Everyone who works on the computer. Included here are all local and remote users (i.e. the groups "*INTERACTIVE*" and "*NETWORK*" put together). They can access the network, connect with the shared network directories of the workstation and use the printer of the workstation.
- *INTERACTIVE* - Everyone who works locally on the computer.
- *NETWORK* - All users who are connected with this computer via the network.
- *SYSTEM* - The operating system.
- *CREATOR-OWNER* - The user who has created or owns the following: a directory, a file in a directory, a printer or a document that was sent to a printer.

Freely-defined user groups

With the help of freely-defined user groups, it is possible to map the organisational structure of an institution to the rights structure. For each organisational unit, e.g. for every project or every department, a group can be created which contains all the users of the organisational unit. The groups are then granted the necessary permissions to resources. If project groups are created within the institution for temporary tasks, they can be mapped to a suitable freely-defined group which contains all the members of the project group.

When freely-defined user groups are created on the primary domain controller, it must be specified whether they are local or global groups.

Additional controls:

- Has a strategy been laid down for allocating users among the pre-defined groups in accordance with the rights required by these users?
- Is this strategy documented?
- Are regular checks carried out to determine whether the allocation of the users to the groups still corresponds to the current tasks of these users?

S 4.51 User profiles to restrict the usage possibilities of Windows NT

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

User profiles are used to store user specific settings in the system environment. This includes the contents of program groups, network connections, used printers, and the colour scheme of the screen. The capabilities of users for working with Windows NT can be restricted in various respects by means of user profiles. Profiles are administrated using User Profile Editor (UPEDIT.EXE under Windows NT 3.51 or POLEDIT.EXE under Windows NT 4.0).

User profiles can be created for various usage purposes:

- in the case of single-user systems, to recover the settings originally specified following a repeated log-on,
- in the case of multi-user systems, to specify their own settings for each user,
- so that, in the case of server-stored user profiles, each user receives the same interface from each NT workstation,
- to specify uniform user environments centrally (both for stand-alone and networked systems),
- to establish a restricted user environment, for example, to prevent users from making changes to desktop settings or restrict access to the control panel.

A distinction must be drawn in principle between local and server-stored user profiles. Local user profiles are only stored on the local IT system, whereas server-stored user profiles are administrated centrally on the NT server.

If the server breaks down when using server-stored user profiles, recourse is had to the local copy.

Alongside this, a distinction must be drawn between personal and mandatory user profiles. Personal user profiles can be changed by the user at will, mandatory ones are specified by the administrator.

Mandatory profiles are maintained from one session to the next, changes made during a session are lost when logging-off. These profiles are stored in the directory which is specified in the profile entry of the relevant account, and under version 3.51 of Windows NT they carry the file name extension *.MAN*. As from version 4.0, a profile is identified as a mandatory profile by renaming the file *NTUSER.DAT* in *NTUSER.MAN*.

Personal profiles which are stored on a server can be used to provide users with the same environment, irrespective of the workstation from which they are logging on. Personal profiles are stored in the directory which is specified in the profile entry of the relevant account, and under version 3.51 they have the file name extension *.USR*.

Under version 3.51, the user profiles are stored in the directory *%SystemRoot%\system32\config* in the files allocated to the users. The following settings are stored in the user profile:

- *Program Manager:* all options which can be set by the user, including program groups, programs and their characteristics, together with all settings which can be stored
- *File Manager:* all options which can be chosen by the user, including the network connections
- *Command Mode:* all settings which can be chosen by the user
- *Print Manager:* network-wide printer connections, together with all settings which can be stored
- *Control Panel:* all settings for colours, mouse, desktop, pointer, keyboard, country settings and sounds as well as the entries for the user environment in the "System" component
- *Accessories:* all user-specific settings of the applications
- *External Applications:* all settings which are supported by these applications as user-specific options
- *Annotations in On-line Help:* all notes of the relevant user entered there

As from version 4.0, user profiles are stored as a directory tree under the sub-directory *Profiles* of the Windows directory *%SystemRoot%*, i.e. in general *\WINNT\Profiles*, as a directory with the name of the user, e.g. *\WINNT\Profiles\Smith*. In addition, the overall structure of the working interface and, in particular, the structure of the individual program groups is stored there. The following sub-directories can be featured:

- *Application data:* Application-specific data
- *Desktop:* Components of the working interface including the files and short cuts stored directly on the working interface
- *PrintHood:* Short cuts to the entries in the printer settings
- *Favourites:* Short cuts to program entries and directories with favourites
- *NetHood:* Short cuts to the entries of the network environment
- *Personal:* Short cuts to the entries in the private program groups
- *Recent:* Short cuts to the most recently-used documents
- *SendTo:* Short cuts to the entries which can be used in the Context Menu as destinations of transmission operations, such as for instance to a floppy disk drive
- *Start menu:* Structure of the overall start menu including all short cuts to programs and program groups
- *Masters:* Short cuts to document masters

Other settings, such as, for instance, the reference to the image used as the background, to the working interface or other user-specific settings of the

system control, are stored in the standing file called *Profiles* in the file *NTUSER.DAT*.

The following options can be used under version 3.51, in order to restrict the capabilities of users for working with Windows NT in various respects:

- *Settings for Program Manager*: It can be specified here whether programs may be started via “File - Execute“, whether the current settings may be stored and whether general program groups are listed. In addition, the auto-start group can be determined.
- *Settings for program groups*: Here, access to designated program groups can be locked out and for program groups which are not locked out, various amendment authorisations can be allocated.
- Users can be allowed or forbidden to connect and disconnect network printers via Print Manager.
- Waiting for the execution of the log-on script can be forced before Program Manager is started. This option should always be activated, so that the actions specified in the log-on script are performed in any event.

As from version 4.0, the following restrictions can be laid down with the aid of System Policy Editor:

- *Control Panel:* Here, access can be limited to the control panel option "*Display*". If this option was chosen, in addition the register cards "*Background*", "*Screen Saver*", "*Appearance*" and "*Settings*" can be still be masked individually, and the option "*Display*" can also be deactivated as a whole.

  Access to the control panel should be withdrawn from normal users, as unintentional changes to the system settings can cause problems. If, in addition, access to the control panel option "*Display*" and the register card "*Screen Saver*" is withdrawn, users can be prevented from deactivating the screen lock. Then, when setting up users, the administrator naturally has to activate the screen lock.

- *Shell:* Here the following restrictions can be laid down:
  - Remove "*Execute*" command
  - Remove folder under Settings in the "*Start*" menu
  - Remove "*Task bar*" under settings in the "*Start*" menu
  - Remove "*Find*" command
  - Mask drives in the "*My Computer*" window
  - Mask network environment
  - No "*Entire Network*" symbol in the network environment
  - No workgroups computers in network environment
  - Mask all desktop components
  - Deactivate "Shut Down" command
  - Do not store settings when ending

- *System:* Here the following restrictions can be laid down:
  - Deactivate programs for editing the registry
  - Only execute approved applications for Windows

  For normal users, access to the registry should not be possible, as changes to the registry can cause serious problems.

  Most users only have to discharge certain tasks with the IT system and accordingly only require certain applications. For this reason their access should also be restricted to these applications, such as, for example, a word processing program.
- *Windows NT Shell:* Here the following restrictions can be laid down:
  - Use only permitted Shell extensions
  - Remove general program groups from the "*Start*" menu

Under Windows NT, very sophisticated user profiles can be created. These should be drawn up in accordance with the security policy of the authority or the company. This can be time-consuming, as for different user groups user profiles tailored to each of the groups should also be created. All user profiles must be tested beforehand to determine whether they neither leave open loopholes nor obstruct users in carrying out their tasks. Consideration should also be given to the fact that restrictions which are too far-reaching can not only lead to user dissatisfaction even to the point of the complete rejection of the system, but can also cause the administrators a great deal of work, if the latter continually have to implement users' wishes such as, for example, setting another type size.

The Windows NT environment is determined by the values of the current user profile, even if the current user has neither a prescribed nor a personal profile or even if no-one is currently logged in. The User Default Profile is loaded under the following conditions:

- if the current user does not have his own (prescribed or personal) profile and has not yet logged in to the current computer;
- if a user logs in to the guest account.

In the first case, the current values of the user environment are stored in a newly-created local personal profile, in the second case they are lost when logging off.

If no-one is logged in, the current values for the screen background and other environment variables are determined by the System Default Profile.

Additional controls:

- Is the guest account, provided it is not locked out, restricted by a profile to the minimum functionality required?

S 4.52 Protection of devices under Windows NT

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Under normal circumstances Windows NT allows all programs access to disks and CD ROMs. You are recommended to limit this access to the user who has just logged in interactively by allocating the equipment to this user exclusively.

Under Windows NT 4.0 access to disk drives should be restricted by entering/changing the value "*AllocateFloppies*" in the key "*SOFTWARE\Microsoft\Windows NT\Current Version\ Winlogon*" of the sector *HKEY_LOCAL_MACHINE* of the registry to the value *REG_string = 1*. Note: The type "*REG_string*" used in the *Regedit.exe* program corresponds to the type "*REG_SZ*" in the *Regedit32.exe* program.

Similarly, access to CD ROM drives should be restricted where required by entering/changing the value "AllocateCdRoms" in the key "*SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon*" of the sector *HKEY_LOCAL_MACHINE* of the registry to the value *REG_string = 1*.

Note: Since the equipment is released again for general access when logging off, the data media must be removed from the equipment before log-off.

If disk drives are to be completely deactivated, this can also be done by preventing the loading of the driver program in the control panel option "*Devices*" by assigning the start type "*Deactivated*" to the "*Floppy*" device. Following the next system start-up, the disk drive is then simply no longer available for use, and it can only be made usable again by an administrator assigning the start type "*System*". On servers, it is not advisable to disable loading of the driver program for the disk drive. If the disk drive is required again for administrative purposes, for example, the "*Floppy*" device must be assigned the start type "*System*" and the server must be turned off, as the driver can only be loaded after the system has been restarted. This might disrupt the operation of services. Servers must be installed in a secure environment, and connected disk drives must be locked physically.

Furthermore, Windows NT allows all users access to tape drives, so that each user can read and write the contents of each tape. Usually this does not result in any problems, as at any given time only one user is logged on interactively. If, however, this user runs a program that is still accessing the tape drive even after log-off, this program might access a tape put on by the next user who logs on. For this reason, computers which are not located in a supervised environment should be restarted before the tape drive is used.

Note: The use of self-loading tape equipment, which can load several tapes from a reservoir, must only be permitted under very closely-supervised marginal conditions. Generally, such types of equipment should only be installed for data back-up purposes on a server. Interactive access of normal users to this server is not permitted (see also S 6.32 *Regular data back-up*).

Additional controls:

- Is the setting of the keys "*AllocateFloppies*" and "*AllocateCdRoms*" in the registry checked regularly?

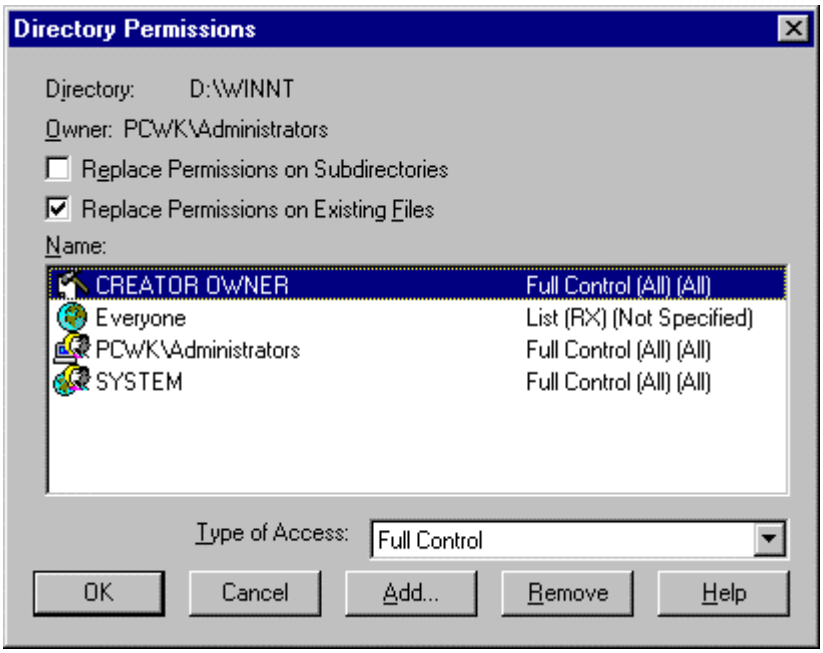
S 4.53 Restrictive allocation of access rights to files and directories underWindows NT

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Under Windows NT, a distinction is made between access rights at the share level, and access rights at the file and directory level, termed NTFS rights in the following. Access rights at the share level are described in S 2.94 *Sharing of directories under Windows NT*.

As opposed to share rights, access rights at the file and directory level are only available on data media with the NTFS file system. As a rule, these rights are assigned by the creator or owner of an object (directory or file). On servers, this is usually done by the administrator. Under Windows NT 4.0, NTFS permissions are granted typically using the Windows NT Explorer or "My Computer" desktop symbol. The menu item designated "Attributes / Security" is to be selected in the context menu of the related directory or file. The following access control list is then invoked:



Under Windows NT 3.51, the access control list is to be found under "Security / Authorisations" in the File Manager. Existing user groups and users can be added to this list; furthermore, rights can be granted to, and withdrawn from, every user group and user here. It is also possible to remove user groups and users from the access control list. By activating the option labelled "Replace permissions on existing files", the rights specified for the directory can be transferred to all the files located therein. If the option labelled "Replace permissions on subdirectories" is selected, the specified rights are also transferred to all subdirectories. This allows easy realisation of standard permission profiles.

NTFS permissions initially become effective during local access. For example, if several users need to work on a computer, file and directory access rights can be granted appropriately to ensure that each user only has access to the data intended for him/her.

NTFS permissions also become effective during access via the network. However, a prerequisite for access via a network is that the directory which needs to be accessed or which contains the required subdirectory or file must be shared and assigned a corresponding share permission beforehand (refer to S 2.94 *Sharing of directories under Windows NT*). During the interplay between share permissions and NTFS permissions, it must be noted that the more restrictive permission is conclusive in each case. NTFS permissions can be graded more finely than share permissions. In particular, it is possible to assign separate NTFS permissions for each subdirectory and file. Consequently, it is also possible to assign shares with the "full access" share permission for the user groups and domain users, and allocate the effective access rights via the NTFS permissions.

NTFS permissions are classified as specific (or individual) permissions or predefined, standard permissions which constitute combinations of the specific access permissions.

The following individual permissions are possible:

R Read
W Write
X Execute
D Delete
P Change permissions
O Transfer ownership

From these individual permissions, default standard permissions have been combined under Windows NT.

Standard permission	*Individual permissions*
No access	–
Read	RX
Change	RWXD
List	RX
Add	WX
Add and read	RWX
Full access	RWXDPO

Every owner of a file or directory has the right to grant and withdraw permissions for that file or directory. Every user who creates a file or directory automatically assumes ownership of this resource. Ownership of a file or directory can be transferred by means of the "Transfer ownership" option (O) to other users. However, this ownership only becomes effective once it has actually been obtained by the recipient. In contrast to other operating systems,

it is not possible to give away files and directories. Irrespective of the entries in the access control list, administrators can assume ownership of any file or directory.

Note:

As far as possible, users should never allocate the permission "*Full access*", but at most the permission "*Change*", so that ownership cannot be withdrawn from them and they always retain sovereignty over rights allocation.

The attention of all users must be drawn to the fact that they should check regularly with File Manager or Explorer whether they are still owners of their directories and files. This is the only way in which users can tell whether access rights set by them have been by-passed.

The safeguards mentioned in the following sections apply mainly to files and directories for which the administrator is responsible, i.e. to those which are either important for all users or useful for administration purposes. It is not sufficient to check the rights of one program. The rights allocation of all programs which are called up from this program must also be checked (in particular to avoid Trojan horses).

The attributes of all system files should, as far as possible, be set in such a way that only the system administrator has access to them. Directories should provide no more than the required privileges for users.

Directories of the operating system and the application programs

The files and directories of the operating system itself must be adequately protected against illicit accesses. Immediately following installation of the system, the standard access rights specified should be adjusted to more restrictive forms of access control for the relevant files and directories (the Windows directory, *%SystemRoot%*, e.g. *\WINNT*, the Windows system directory *%SystemRoot%\SYSTEM32* and any further program directories, e.g. *\MsOffice* and *\Programs*, and all sub-directories).

At this point, however, it should be noted that quite a number of programs, particularly 16-bit programs but also MS Winword 7.0, create initialisation and configuration files in the Windows directory and/or in the program directory. If such programs are to be used it can become necessary to give users the access right "Change" for the relevant directories and files.

Only administrators should have write access to these directories. All other users should only have read and execute permissions (RX).

User (group)	*Access right*
SYSTEM	Full access
Administrators	Full access
Users	Read

Where necessary, access to executable files (.EXE, .COM and .BAT) can be restricted still further, so that only executable (X) access to these files is possible. In a similar manner, the files which are of critical importance in starting the system, namely *\BOOT.INI*, *\NTDETECT.COM*, *\NTLDR*, *\AUTOEXEC.BAT* and *\CONFIG.SYS,* must be protected against unauthorised amendment by non-privileged users.

However, checks should also be carried out - preferably in a test environment - to determine whether all application programs are still able to run with this restrictive setting, or whether individual access controls still have to be supplemented by further access capabilities, in order to permit, for example, the storage of temporary files or configuration information in a program directory. Generally, however, access to the program files themselves (.EXE-files) and to dynamic libraries (.DLL-files) for the group "Everyone" should be restricted to read access, especially as this safeguard also offers a certain protection against the spread of viruses.

Temporary files

Temporary files, which are used by various application programs for the relocation and intermediate storage of data, are filed under Windows NT in the directory *%TEMP%* (usually *C:\TEMP*). All users also need the right to store files in this directory, but, at the same time, users must be prevented from gaining access to temporary files of other users. The access rights for the directory should therefore be changed to the following value:

User (group)	Access right
SYSTEM	Full access
Administrators	Full access
Creator/Owner	Change
Users	Add

Registration

The registry of Windows NT is located in the sub-directory *CONFIG* of the Windows system directory *%SystemRoot%\SYSTEM32*, i. e. in general in the directory *C:\WINNT\SYSTEM32\CONFIG*. The user must have access to this directory, as the registry is automatically changed by settings of the user in application programs. If the user cannot access this directory, it leads to system errors or to the crashing of the system. Under version 3.51, the standard rights set for this directory, which, as far as possible, should not be amended, are:

User (group)	Access right
SYSTEM	Full access
Administrators	Full access
Creator/Owner	Change
Users	List

As from version 4.0, the standard rights are:

(+

User (group)	Access right
SYSTEM	Full access
Administrators	Full access
Creator/Owner	Full access
Everyone	List

However, the group titled "Everyone" should be replaced by the group titled "Users". Only if guests have access to this directory, should the group titled "Everyone" be assigned the permission titled "List".

During installation, Windows NT creates the directory *%SystemRoot\REPAIR* for the purpose of storing configuration information which might be required for repairing an existing installation. These files are updated with the help of the *RDISK* utility program (also refer to S 6.42 *Creating start-up disks for Windows NT*). As these files, together with disruptive software, can be used to disable the security features of Windows NT, rights to access this directory and all the files contained therein should be set as follows:

User (group)	Access right
System	Full access
Administrators	Full access

Profiles

In order to store the data which the user interface and entries in the START menu describe from version 4.0 onwards, Windows NT creates a personal profile directory for each user of the system in the sub-directory *Profiles* of the Windows directory *%SystemRoot%* (generally *C:\WINNT\PROFILE*). Under version 3.51, profiles are stored in sub-directories of the system directory *%SystemRoot%\SYSTEM32\CONFIG* or in directories explicitly specified for individual users.

The user must have full access to these directories provided that he is supposed to be able to alter his user interface himself. However, this is not always desired (cf. S 4.51 *User profiles to restrict the usage capabilities of Windows NT*). When the user first logs on, his user profile is automatically generated by the system. The standard access rights for the directory appear as follows:

User (group)	*Access right*
SYSTEM	Full access
Administrators	Full access
Relevant user	Full access

Besides the profile directory for the individual user there is a further directory for all users (*All Users*) and a directory as a model for new users (*Default User*). Only system administrators should have write access to these directories. Access rights should be set as follows:

User (group)	*Access right*
SYSTEM	Full access
Administrators	Full access
Users	Read

These settings should only be altered if you wish to take away the user's right to alter his user interface.

User directories

The directories for the data of individual users should, in general, be protected in such a way that only the users concerned can access their files. Other users, even administrators, do not in general require access to the data of a user, unless the latter explicitly allocates additional access rights himself. Accordingly, in most cases the following pre-setting is adequate for access rights to user directories:

User (group)	Access right
SYSTEM	Full access
Relevant user	Full access

Users who want to make individual files or directories accessible to other users, should set up directories outside their base directory for this purpose. Likewise, special directories should be set up for project groups working

jointly on designated files. Again, access rights to such directories should also be explicitly limited to the users in these groups.

Lockout of access rights for guests

The access control lists described above are based on the assumption that no users of the group titled "Guests" group are to be authorised. For this reason, the group titled "*Everyone*" should be replaced by the group titled "*Users*". This safeguard effectively deprives guests of any possibility of working with the system and of accessing data. However, as this may possibly lead to a situation in which certain application software no longer runs correctly, any change of this sort should first be made on a test system and scrutinised in terms of its effects before being implemented generally.

Additional controls:

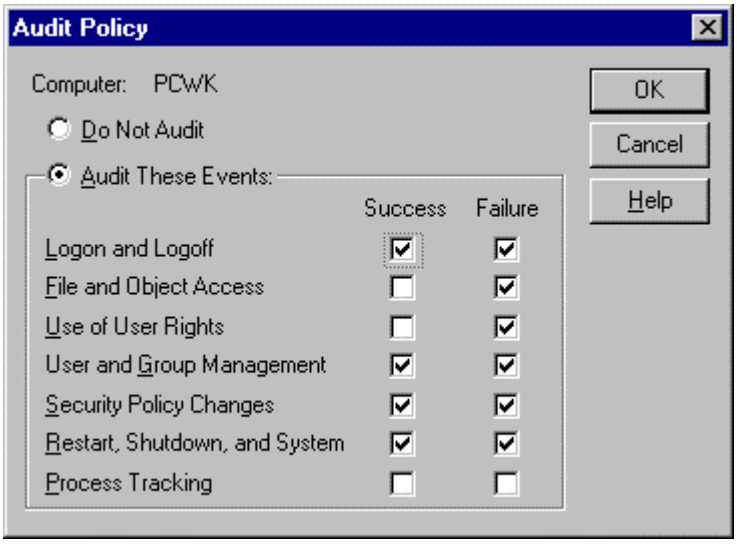
- Is the allocation of attributes regularly checked in relation to system files and the registry?
- Are the settings of the user profiles checked regularly?
- Are there lists which can be used to help carry out these checks?

S 4.54 Logging under Windows NT

Initiation responsibility: Head of IT Section, IT Security Management

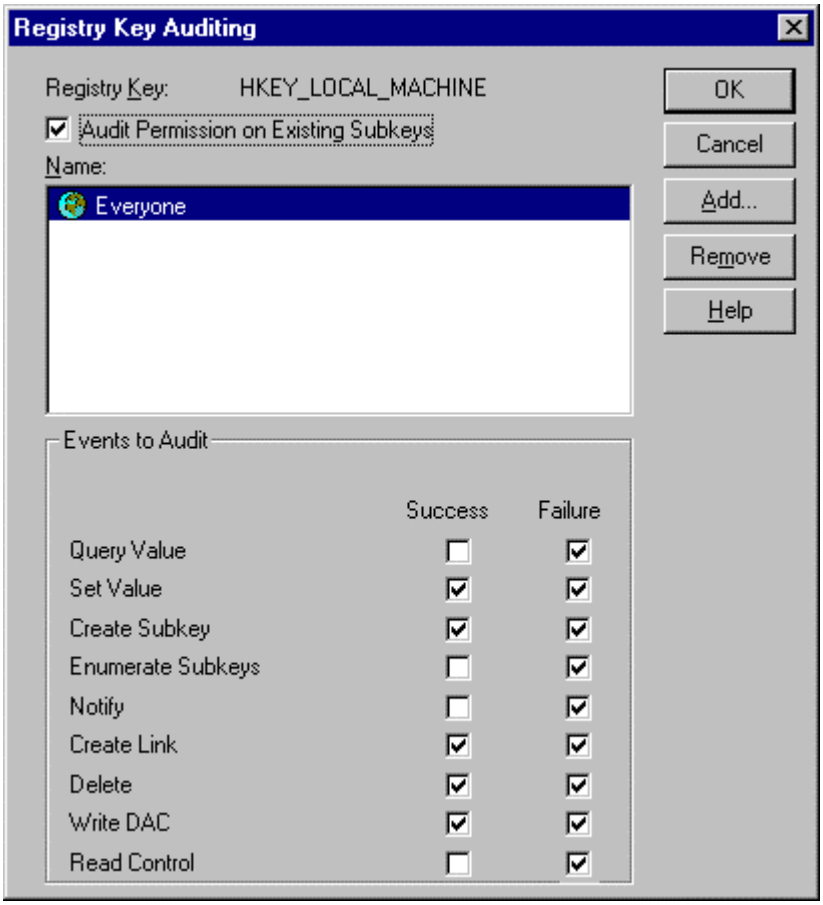
Implementation responsibility: Administrators

The regulations laid down for the logging of events relevant to security can be implemented using the "*Policy*" option of User Manager. In general, suitable regulations for average protection requirements correspond to those in the following diagram:



In addition, if data with higher protection requirements is stored and/or processed on a computer, then successful and rejected file and object accesses should still be recorded. This recording should be limited to files containing information which is particularly worth protecting, together with the programs required for processing these files, so that the log file does not become so extensive that it can no longer be evaluated at acceptable expense.

Where higher security requirements exist, accesses and access attempts to the registry, at least for the keys *HKEY_LOCAL_MACHINE* and *HKEY_USERS*, should also be recorded. In the process it is advisable to record all rejected attempts and, among the successful ones, at least the following ones which can lead to changes in the registry:



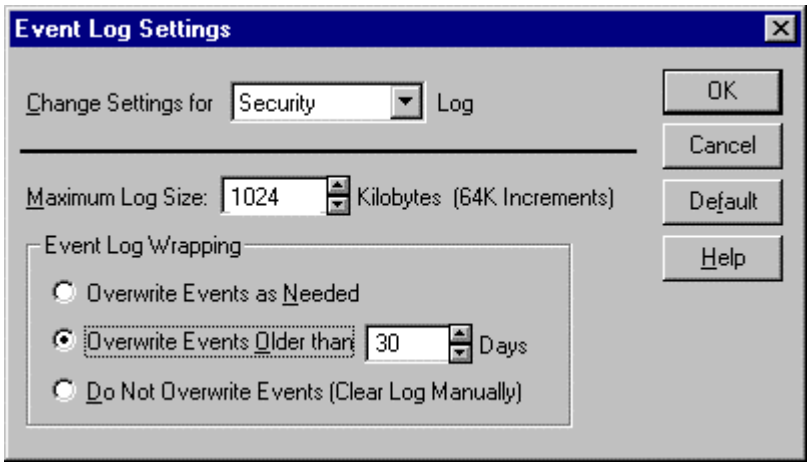
It should be noted that accesses to the registry are only recorded if the auditing of file and object accesses is activated in the General Audit Policy.

When access to the registry is monitored, a large amount of auditing data is generated which must also be evaluated. Furthermore, recording these events usually has a negative effect on the system performance. In some cases, taking the security requirements into account, the following alternative procedure is recommended. Rejected attempts to access the keys *HKEY_LOCAL_MACHINE* and *HKEY_USERS*, are recorded as described above. Successful accesses to these keys are not recorded. Rather, a suitable integrity protection program is used. In this way, changes to these keys are easily recognised. However, the disadvantage of this method is that the program does not recognise who has made the changes.

By stipulating appropriate specifications with the utility *Event display*, the log file should be created to be so large that all entries occurring within a specified period (for example, in one week) can be stored reliably. When doing this, provision should be made for a security margin, so that in general a maximum of around 30% of the log file is filled. After the specified period has elapsed, each log file should be analysed, filed and then cleared to create space for new entries.

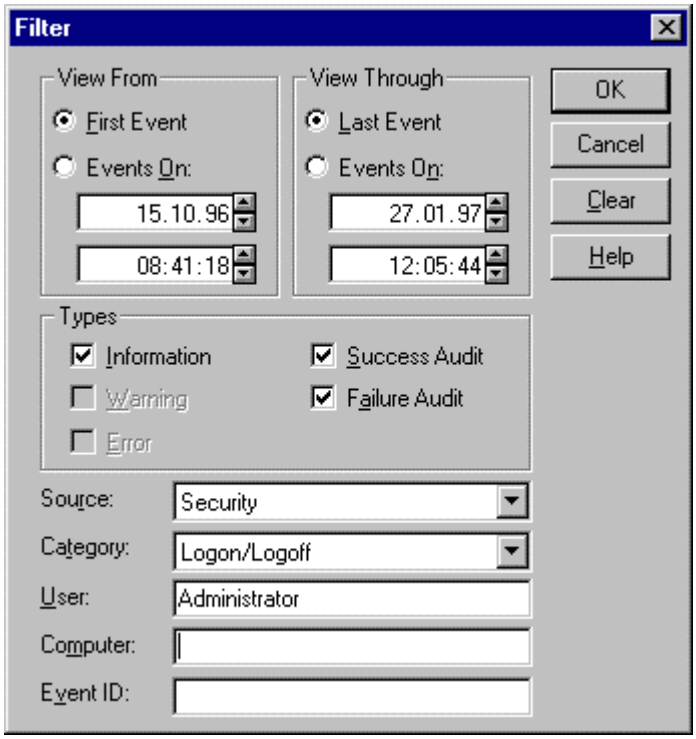
In order to avoid system failures as a result of fully writing the log file, under normal circumstances one of the options "*Overwrite events as needed*" or

"*Overwrite events older than x days*" should be chosen, choosing for *x* the length of the specified filing cycle, e.g. 30 days:



For systems where enhanced security requirements exist, the option "*Do not overwrite events (clear log manually)*" should instead be chosen. However, when the log overflows this leads to a system standstill and then causes corresponding expense.

The logs are evaluated using the management program *Event display*, which enables the specific evaluation of procedures critical to security to take place through the selection of suitable filter rules:



Evaluation of the security log should follow a suitable, generally binding checklist (see S 2.64 *Checking of log files* and S 2.92 *Performing security checks in the Windows NT client-server network*).

Additional controls:

- Are the recorded logs regularly examined?
- Are the possible consequences of log entries critical to security analysed?

S 4.55 Secure installation of Windows NT

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Before installation of Windows NT, a number of observations should be made which are briefly outlined below.

Secure system version

Even during the process of acquisition, a decision must be made as to whether the English or German version of Windows is to be run. Furthermore, to be on the safe side, Windows NT must be operated from at least version 3.51 onwards, together with the current version of Service Pack4 (also refer to S 4.xx02 *Reliable system versions of Windows NT*). If an older Windows NT installation exists, this should, if possible, be updated to version 4 or at least to version 3.51.

Partitions and file systems

Alongside its own file system NTFS, Windows NT also supports the DOS file system FAT and the OS/2 file system HPFS. A large part of the settings relevant to security are, however, only valid under NTFS. when installing Windows NT, you should ensure that no HPFS or DOS partitions are created, as no access protection applies to them, with the result that such partitions can be misused to undermine the protection of Windows NT. Instead, all partitions must be formatted using the NTFS file system or, if earlier data is to be kept, they must be converted to this file system.

However, support of the FAT file system for floppy disks is necessary as, due to its size, the NTFS file system cannot be accommodated on diskettes. For this reason, access to disk drives should be limited (see S 4.52 *Equipment protection under Windows NT*).

Configuration of the log-on procedure

At log-on, Windows NT usually displays the name of the last user who has logged in on the computer concerned. This display should be prevented by entering/changing the value "*DontDisplayLastUserName*" in the key "*SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon*" of the sector *HKEY_LOCAL_MACHINE* of the registry to the value *REG_SZ = "1"*.

In order to warn unauthorised users against illegal access to the system, before the actual log-on procedure a window containing an appropriate text should be displayed. This is achieved by inputting suitable wording into the two entries "*LegalNoticeCaption*" and "*LegalNoticeText*" in the key "*SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon*" of the sector *HKEY_LOCAL_MACHINE* of the registry.

The relevant changes can be made with the help of Registry Editor (of the program REGEDT32.EXE in the Windows system directory *%SystemRoot%\SYSTEM32*). When doing this particular caution should be exercised, as incorrect settings in the registry can lead to a situation in which the system is no longer able to run. From version 4.0 of Windows NT

onwards, these values can be specified centrally for the individual workstations with the aid of System Policy Editor.

Loading of sub-systems

The optional sub-systems POSIX and OS/2 should, in fact, only remain installed if they are also needed for executing applications. If this is not the case, their installation should not take place or, if it has already occurred, the systems should be deleted again. To do this the sub-directories *POSIX* and *OS2* of the Windows system directory *%SystemRoot%\SYSTEM32* should be deleted along with any of their sub-directories. Furthermore, the following programs and loadable libraries in the Windows directory *%SystemRoot%\SYSTEM32* should be deleted:

- OS/2:	OS2.EXE
	OS2SRV.EXE
	OS2SS.EXE
- POSIX:	PSXDLL.DLL
	PAX.EXE
	POSIX.EXE
	PSXSS.EXE

Furthermore the following values in the key *\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems* in *HKEY_LOCAL_MACHINE* of the registry have to be deleted:

- OS/2: "Os2" with the value %SystemRoot%\system32\os2ss.exe

- POSIX: "Posix" with the value %SystemRoot%\system32\psxxx.exe

Starting of services

If services which are not standard services of Windows NT are to be configured, when determining the start type of these services (using the system control option "*Services*") provision should be made, if possible, for a separate user account to start each of these services, in order to be able to restrict the authorisations of the service concerned in a suitable manner. The user account used in such cases must have the right "*Start as service*", and it should not be used except for this service, i.e. in particular it should also not allow users to log in. Services which have not been allocated in this way to a special user account, run in the context of the special user group *SYSTEM* (see S 4.50 *Structured system administration under Windows NT*), i.e. generally with the most extensive access permissions.

Device protection

If the computer has disk drives, CD ROM drives and/or tape drives, these should, if possible, be specifically protected, as outlined in Safeguard S 4.52 *Equipment protection under Windows NT*.

Emergency repair disk

At the time of installation, Windows NT offers to produce an emergency repair disk containing the most important configuration information. Use should be made of this capability and when changes are made to the system each disk should be updated (see S 6.42 *Creation of emergency repair disks for Windows NT*). It is advisable to carry out the updating of each emergency repair disk after the next system start-up, if there is a guarantee that the changed system can still be started.

Pre-defined user accounts

The pre-defined **administrator account** is a member of the pre-defined "Administrators" group. It receives the rights and permissions which were granted to this group. The administrator account is used by the person who administrates the overall configuration of the workstation or the server. The administrator has more supervisory capabilities over the Windows NT computer than any other user. This is why this account especially has to be protected (see S 4.77 *Protection of administrator accounts under Windows NT*). The pre-defined guest user account is a member of the "*Guests*" group. It receives the rights and permissions which were granted to this group. For example, a user can log on to the guest account, create files and delete them again and read files for which an administrator grants read permission to guests. The guest account is set up as a service for users who use the computer occasionally or only once, so that they can log on and work with a restricted range of functions. When Windows NT 4.0 is installed, the guest account is initially locked out, and it is installed using a blank password. The guest account should, in any event, be given a secure password, and the lockout should not be cancelled if there are no serious grounds for its use. The pre-defined guest account can be renamed but not deleted. It should be renamed immediately after installation.

The **first user account** is set up for the first user of a workstation. As it is a member of the "Administrators" group, the workstation can be administrated in its entirety with the first user account. The first user account is created when Windows NT is installed, if the workstation is added to a workgroup or if it was not configured for network operation. The system invites the input of a user name and a password. If the computer is added to a domain when Windows NT is installed, the first user account is not created, because it is expected that the user will log on using an account from the domain.

Note: If Windows NT sets up a first user account on installation, this should be used as the account for system management.

Installation in the network

Furthermore, it should be noted that when their network software is configured, all clients are configured as members of one of the previously defined domains (and not as members of workgroups). If user accounts are needed on them, they must always be defined as domain-wide accounts and not as local accounts, in order to avoid the formation of unclear rights structures.

To simplify the installation of a relatively large number of clients, scripts should be defined beforehand enabling the automatic installation and

configuration of these clients to take place. Software of all types should be made available centrally on a server and installed from there on to the appropriate computer.

Additional controls:

- Which users have been notified of the access supervision information (user name, password) to the pre-defined user accounts?
- Are regular checks carried out to determine whether the guest account is still locked out and, if it has to be used, are the access rights granted to the group "Guests" and the group allocation of the guest account regularly checked?

S 4.56 Secure deletion under Windows NT and Windows 95

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: IT users, Administrator

Windows NT

Windows NT copies all file information (name, path and attribute)to a master file table. These entries are not encrypted. Programs that can directly access the hard disk can gain access to all files by by-passing the security mechanisms of Windows NT. This applies particularly to programs that run under a different operating system than Windows NT on the same computer.

When deleting a file under the file system NTFS, the file will not be physically deleted or overwritten. Instead, access to the file will be removed, similar to MS-DOS. In contrast to MS-DOS, however, under Windows NT it is ensured that access to this deleted file is no longer possible, neither with a reconstruction program nor by direct disk access. Despite this, deleted files can be recovered under a different operating system than Windows NT by programs that directly access the hard disk.

For these reasons, Windows NT must be installed as a single operating system. Starting other operating systems from floppy disk must be prevented (see S 4.52 Peripheral protection under Windows NT and S 4.55 Secure installation of Windows NT).

Windows 95/ Windows NT

Under Windows NT version 4.0 and under Windows 95, as long as the user does not expressly execute direct deletion of a file, files to be deleted will first be stored in a user-specific area; the so-called "Recycle Bin". They will be removed from this area when the amount of deleted data exceeds the allocated memory space for the hard disk concerned, or when the user explicitly empties the Recycle Bin. The content of the Recycle Bin should be emptied regularly so that the hard disk does not become too full and the user's overview is not lost. The maximum memory space reserved for the Recycle Bin can be set to a suitable low number e.g. 2 Mbytes under "Properties" of the Recycle Bin icon. Files containing sensitive data should not be stored in the Recycle Bin. They should be directly (physically) deleted by holding down the shift key when deleting.

Under Windows 95, it is possible to reconstruct deleted files from the Recycle Bin via help programs. Therefore, files with a particularly sensitive content should be completely overwritten before being moved to the Recycle Bin (see also S 2.3 *Data media control*)

Additional controls:

- Under Windows NT version 4.0, or Windows 95 has the memory space reserved for the Recycle Bin been set to a sensible value?

S 4.57 Deactivating automatic CD-ROM recognition

Initiation responsibility: IT Security Management

Implementation responsibility: Administrator, IT users

CD-ROMs can be recognised and read automatically under Windows 95 and Windows NT 4.0. This allows programs stored on CD-ROMs to be executed directly on the computer. Automatic CD-ROM recognition should be permanently deactivated under Windows 95 and Windows NT.

Under Windows 95, this is done by deactivating the attribute "Automatic recognition when changing" on the DEVICE MANAGER card under the control panel option SYSTEM PROPERTIES.

To permanently deactivate automatic CD-ROM recognition under Windows NT 4.0, set the "Autorun" entry under the *\SYSTEM\CurrentControlSet\Services\Cdrom* key in the registration to *REG_WORD = 0* in the *HKEY_LOCAL_MACHINE* group.

If automatic CD-ROM recognition is desired in general, it can be deactivated for an individual CD-ROM by pressing Shift key when inserting the CD-ROM.

Additional controls:

- Has automatic CD-ROM recognition been deactivated?
- Have users been informed as to how automatic CD-ROM recognition can be deactivated temporarily?

S 4.58 Sharing of directories under Windows 95

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

For every computer running under Windows 95, a decision is required as to whether individual peer-to-peer functions should be enabled or disabled. For this purpose, file and printer functions can be enabled or disabled on an individual basis via the system guidelines under the menu item *Control panel / Network / File and Printer Sharing*. After that, user access to this option must be revoked.

If the file sharing is inactive, then the corresponding File Manager / Explorer functions are not available, although it is still possible to establish links with directories on other computers.

When configuring a Windows-for-Workgroups computer, the administrator also needs to consider the following points:

- By means of the system guidelines under Windows 95, unauthorised persons must be prevented from changing user names and computer names.
- The default setting "Save password in list " is to be deactivated on the appropriate menu.
- Computer and user names are to be assigned in accordance with organisational specifications. By means of the system guidelines, unauthorised persons must be prevented from changing user names and computer names.
- During the use of Schedule+, the right granted by default to view open and assigned time blocks must be deactivated for all unauthorised WfW users. Otherwise every user at the same post office will be able to view individual appointments in the time schedule.

If a post office is configured for use by several persons for the purpose of communications or joint appointment scheduling, a corresponding data backup should be performed at appropriate time intervals. This is required to prevent inadvertent or intentional deletion of the post office, which is not protected automatically under WfW.

Under Windows 95, it is possible to configure a remote administrative function which allows administrators to access individual workstations via the network. Before this option is activated, a check must be made as to whether it conflicts with the safety objectives of the organisation.

Activation of the remote administration function gives rise to the following threats:

- It is possible for unauthorised persons to try out IDs and passwords for this function
- an administrator can secretly access users’ computers at any time.

If this feature for facilitating workstation management is required, a decision must be made as to whether administrators should use the same password for

all workstations under their jurisdiction. A single password is easier to remember but, if detected, would allow intruders to access all workstations.

Additional controls:

- Is there any documentation indicating which directories on which computers have been shared for network access?
- Is the existing share profile adapted to changes in operational conditions?
- Is there any documentation indicating the computers on which remote administration has been configured?

S 4.59 Deactivation of ISDN board functions which are not required

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

A modern ISDN board and its communications software, as well as the operating system in the card's RAM, possess numerous features in addition to pure ISDN functionality. Such "convenience functions", some of which can also be used when the IT system is inactive, include:

- The reception and transmission of faxes
- Functions of a digital answering machine
- Playback of messages recorded on the answering machine
- Telephony via a microphone and earpiece included in the scope of supply of the board

Wherever possible, card functions which are not required should be deactivated, preferably by removing the related software modules. Card functions which can be configured simply through parametrisation must be checked regularly to determine whether the parameter settings are still correct.

Additional controls:

- Are checks made to determine whether available functions are actually required?
- Have functions whose use is obviously not required been disabled?

S 4.60 Deactivation of ISDN router functions which are not required

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

In addition to service functions and remote maintenance (refer to S 2.108 *Relinquishment of maintenance of remote ISDN gateways*), functions of the router operating systems can also result in security weaknesses. If the router has a Unix operating system, for example, it is possible to start a Telnet session on the router and subsequently manipulate the management information base.

Wherever possible, router functions which are not required should be deactivated, preferably by removing the related software modules. Card functions which can be configured simply through parametrisation must be checked regularly to determine whether the parameter settings are still correct.

Additional controls:

- Are checks made to determine whether available functions are actually required?
- Have functions whose use is obviously not required been disabled?

S 4.61 Use of security mechanisms offered by ISDN components

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

If ISDN cards with security functions such as those listed below have been procured for the IT system or router in accordance with S 2.106 *Purchase of suitable ISDN cards*, they should be used in an appropriate manner as described in S 5.46 *Authentication via CLIP/COLP*, S 5.47 *Callback based on CLIP/COLP*, S 5.48 *Authentication via PAP/CHAP* and S 4.34 *Use of encryption, checksums and digital signatures*:

- Capability to perform authentication via PAP and CHAP (Password Authentication Protocol and Challenge Handshake Authentication Protocol, RFC 1994)
- Use of a hardware or software-based encryption techniques (symmetric/asymmetric)
- Possibility of evaluating CLIP (Calling Line Identification Presentation) call numbers for the purpose of authentication
- Possibility of maintaining a table of call numbers for performing callbacks
- Possibility of logging unsuccessful attempts at establishing links (refusal due to incorrect authentication of call numbers or PAP/CHAP)

A prerequisite here is that all communications partners should be in possession of ISDN cards equipped with security functions which are identical to the greatest possible extent.

S 4.62 Use of a D-channel filter

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, Purchase Department

A D-channel filter is installed between the ISDN connection (S_{2M} or S_0) and the ISDN terminal device or ISDN private branch exchange (PBX). This filter acts as an ISDN terminal device facing the ISDN connection, and as an ISDN connection facing the ISDN terminal device. The D-channel filter monitors the ISDN D-channel for impermissible protocol actions and is thus capable of detecting, as well as preventing, attempts at manipulation via the D-channel. Use of a D-channel filter is particularly advisable in situations where unauthorised access by qualified persons via remote access ports is conceivable (for example, during remote maintenance and administration).

A D-channel filter also restricts performance features and services for the call numbers of certain communications partners so as to prevent the ISDN terminal device from being misused and endangered under certain operational conditions. A D-channel filter responds to an unauthorised attempt to make use of performance features and services by closing down the connection (disconnect, release) and logging the attempt.

Further details on this technology - which was initiated by the BSI - can be obtained from the IT baseline protection hotline.

S 4.63 Security-related requirements for telecommuting computers

Initiation responsibility: Agency/company management; IT Security Management

Implementation responsibility: Head of IT Section, Administrator

The security-related requirements for telecommuting computers depend on the degree of protection needed for data at remote workstations and the nature of the data which telecommuters can access from the telecommuting computer of the institution. The higher the required degree of protection, the greater the number of security measures entailed. General security objectives for telecommuting computers include the following:

- Telecommuting computers must only be used by authorised persons.

  This ensures that only authorised persons can use data and programs which are stored on the remote workstation or accessible via the communications computer at the institution. Authorised persons include administrators of telecommuting computers, telecommuters and their stand-ins.

- Telecommuting computers must only be used for authorised purposes.

  This helps prevent telecommuters from using or modifying IT for unauthorised purposes, thus avoiding misuse and damage caused by improper handling.

- Damage caused by theft or malfunctioning of a telecommuting computer must remain within tolerable limits.

  Telecommuting workstations are usually installed in an insecure environment, thus exposed to the danger of theft. In the event of a theft, the availability and, possibly, the confidentiality of the data stored on the stolen computer are impaired. The potential damage arising here should be minimised.

- Attempted or successful manipulation of remote workstations should be clearly recognisable for telecommuters.

  This ensures that remote workstations remain in an integral state even if attempts at manipulation cannot be precluded.

The following functions are useful for remote workstations:

- Telecommuting workstations must have an **identification and authentication mechanism**. The following conditions must be met, in particular:

  - Critical security-related parameters such as passwords, user IDs etc. are managed reliably. Passwords are never stored in unencrypted form on telecommuting workstations.

  - Access mechanisms respond to incorrect entries in a defined manner. For example, if an incorrect attempt at authentication is made three times in a row, access to the remote workstation is denied, or the

time intervals at which subsequent attempts at authentication are allowed become progressively longer.

- Certain minimum values can be specified for security-related parameters. For example, passwords should have a minimum length of six characters.
- After the mouse or keyboard has remained inactive for a certain period of time, a screen saver is activated automatically. This screen saver can only be deactivated following renewed identification and authentication.

- Telecommuting workstations must have an **access control mechanism**. The following conditions must be met, in particular:
  - Telecommuting workstations can distinguish between different types of users. It is possible to configure at least two separate roles on a telecommuting workstation, namely, administrator and user.
  - Access to files and programs can be regulated using differentiated allocation of rights (read, write, execute, ...).
- If a telecommuting computer is to be equipped with a **logging mechanism**, the following features might be advisable:
  - It should be possible to parametrise the minimum logging scope of the telecommuting computer. For example, the following actions and errors should be included in logs:
    - For authentication: User ID, date and time, success, ...
    - For access control: user ID, data and time, success, type of access, what was changed, read, written, ...
    - Implementation of administrative activities
    - Occurrence of operational errors.
  - Unauthorised persons must neither be able to deactivate the logging function, nor should they be able to read or edit the actual logs.
  - Logs must be clear, complete and correct.
- If a telecommuting computer is to be equipped with a **log evaluation function**, the following features might be advisable:
  - An evaluation function must be able to distinguish between the various data types contained in a log (e.g. "filtration of all unauthorised attempts at accessing any resource over a specified time period").

    The evaluation function must be capable of generating transparent, readable reports so that no critical security-related activities can be overlooked.
- Telecommuting computers should be equipped with **data backup** functions. At least the following requirements must be met by these functions:

  - The data backup program is user-friendly and fast, allowing automatic execution.
  - Specifications can be made as to which data should be backed up when.
  - An option for loading any required data backup is available.
  - It is possible to backup several generations.
  - It is possible to backup instantaneous data at specified intervals while an application is being run.

- If the telecommuting computer is to be equipped with an **encryption component**, the required functionality must first be determined: Manual encryption of selected data (offline) or automatic encryption of the entire hard disk (online). A prerequisite here is that a suitable encryption algorithm is used and that data lost on the occurrence of a malfunction (power failure, encryption error) can be restored by the system. In addition, the following features are recommended:
  - Encrypted algorithms used by government agencies should be approved by the BSI. Individual consultation by the BSI is recommended in this case. Outside government agencies, the DES is suitable for medium security requirements, while the triple DES is suitable for high security requirements.
  - Key management must be harmonious with the functionality of the telecommuting computer. In particular, fundamental differences between algorithms must be considered here: Symmetric techniques use a confidential key for encrypting and decrypting; asymmetric techniques use a public key for encrypting and a private (confidential) key for decrypting.
  - The telecommuting computer must safely manage critical security parameters such as keys. These keys (including ones which are no longer in use) must never be stored on the telecommuting computer in an unprotected - i.e. readable - form.
- If a telecommuting computer is to be equipped with an **integrity checking** mechanism, the following features are advisable:
  - Integrity checking procedures should be used which can reliably detect intentional manipulation of IT and data on the telecommuting computer, as well as unauthorised installation of programs.
  - Mechanisms should be used which can detect intentional manipulation of address fields and payload data during data transmission. Mere identification of the employed algorithms without the need for certain additional details should not suffice to perform secret manipulation of the above-mentioned data.
- Telecommuting computers should be equipped with a **boot protection** mechanism which prevents unauthorised booting from exchangeable data media such as floppy disks and CDs.

- It should be possible to **restrict** the **user environment** on a telecommuting computer. Administrators should be able to specify the programs and peripheral devices which telecommuters can use, as well as the modifications which telecommuters can perform on the system. In addition, telecommuters should be prevented firstly from making unauthorised changes to settings required for reliable operation, and secondly from installing unauthorised extraneous software.
- A **virus scanning program** must be installed on telecommuting workstations to perform regular checks for computer viruses. A virus check should be performed each time before data are copied from exchangeable data media, data media are transferred, or data are transmitted and received. As data exchange between telecommuting computers and external systems plays a significant role and individual checks prove very elaborate and time-consuming so that they are often skipped, all telecommuting computers should be equipped with a virus scanner, preferably resident in the memory.
- If a telecommuting computer is to be **administered remotely**, only authorised persons must be allowed to perform this remote administration. The process of remote administration must include authentication of the remote administration personnel, encryption of the transferred data, and logging of the administrative routines.
- The software on a telecommuting computer must be **user-friendly**. It should be simple to operate, comprehensible and easy to learn, as telecommuters require a greater degree of self-reliance than their colleagues. In particular, users should be provided with pertinent and intelligible documentation of the operating system and all the installed programs.

From the above-mentioned functions, those which fulfil the security requirements applicable in each case to telecommuting computers should be selected. A suitable operating system must then be chosen as a platform for these functions. If the operating system does not support all the functions, additional products need to be installed. If possible, all the telecommuting computers of an institution should be equipped identically in order to facilitate their care and maintenance. For security-related compatibility checks, refer to Chapter 9.1.

The whole system is to be configured by administrators such that a maximum level of security is achieved.

Additional controls:

- Does the operating system selected for the telecommuting computer provide the required functionality? Are additional security products needed?
- Which of the additionally recommended safeguards have been implemented?
- Do telecommuters accept the implemented security measures?

S 4.64 Verification of data before transmission / elimination of residual information

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

Before a file is dispatched via e-mail or placed on a WWW-server, or before a data medium is transferred to another party, a check must be made as to whether the file/data medium holds residual information not intended for public attention. Such residual information can have a variety of origins entailing a corresponding variety of measures which need to be taken. The most common sources of such residual information are described in the following.

In general, files generated with standard software such as word processing and spread-sheet programs should be checked for residual information. Some of this information is stored with, and some without the user being aware of this.

Before files are forwarded, they should at least be spot-checked for the presence of undesired additional information. For this purpose, a different editor should be used than the one with which the file was originally created.

In this process, it must be noted that not all residual information can be deleted directly without disrupting the file format. If, for example, certain bytes are deleted from a file generated with a particular word processor, the software might no longer recognise the file format. To eliminate residual information:

- The file can be stored in a different format, e.g. “Text only“ or HTML
- The useful data can be copied to another instance of the same standard software on an IT system which does not run any other applications. This is particularly advisable in the case of files with a long history of modifications.

To prevent the forwarding of information which was originally added on purpose by the creator of the document - such as text in “hidden“ format - but whose presence was later forgotten, it might prove useful to print out the file. For this purpose, all printer options for outputting hidden formats should be activated.

Residual information / slack bytes

Every operating system has a smallest possible physical memory unit of a specified size. Under DOS, this unit is termed sector and has a size of 512 bytes. Under UNIX, this unit is termed block, and its size depends on the type of UNIX system in use. Under DOS, the individual sectors of a partition are grouped logically into clusters. The number of sectors in a cluster depends on the size of the partition. When a file is opened, one or more clusters are allocated to it. The last cluster is not occupied fully, unless the size of the stored file happens to be an exact multiple of the cluster size.

This takes up memory. The average storage space required increases with the cluster size. As the cluster size, in turn, increases with the partition size, the latter should not be allowed to exceed a certain limit. Example: Given a

partition size of 1024 to 2047 MB, each cluster is 32 KB large. This results in a memory loss of 16 KB for each file.

Another problem (in the case of DOS-based systems) is that the remaining bytes of the last cluster or block are filled with old data still present in the main memory. Termed slack bytes, they can consist of unintelligible entries, information concerning file structure, and even passwords. Depending on the size of the clusters involved, a file can also be filled with slack bytes when being copied from one data medium to another.

Before files are forwarded, care must be taken to ensure they do not contain any slack bytes. This can be checked with a suitable editor (i.e. hex editor). or with the PRUNE public-domain program. Available from the BIS mailbox, this program can be used specifically to overwrite slack bytes.

In addition, many Windows applications are problematic in that they do not continuously overwrite the available memory with program data while a file is being processed. This can create gaps containing old data of the IT system.

Hidden text / comments

A file can contain text passages with a "hidden" format. Some programs also offer the possibility of adding comments which often do not show up on printouts or monitors. Such text passages might contain remarks not intended for the attention of the recipient. Consequently, this type of additional information should be deleted from files before they are transferred to external parties.

Marking of changes

In some cases, it is necessary to mark changes made to files when processing them. As such markings can be masked out on printouts and monitors, files should also be checked for these markings before being forwarded.

Version management

Microsoft Word 97 allows several different versions of a document to be stored in **one** file. This makes it possible to invoke earlier versions of a document should the need arise. However, this can also easily lead to very large files, for example, in the case of documents containing graphic objects. On no account should the option titled "Save version automatically on closing" be activated, as this would also store the entire, previous version of a file each time it is closed.

File attributes

File attributes are stored in the file information module which is meant to facilitate subsequent searches for the file. Depending on the application involved, this file information can include the title, directory path, version, creator (and editor, if applicable), comments, editing time, date of last printout, document name and document description. Some of this data is generated by the program itself, and cannot be influenced by the person editing the file. Other data needs to be entered manually. Before being transferred to external parties, files should be checked for additional information of this type.

Fast storage

Most word processing programs provide a fast-storage function which, instead of saving an entire document, only saves changes made to it since it was last saved in its entirety. This procedure thus takes less time than a full storage. However, a full storage requires less hard-disk space than a fast storage. The main disadvantage of performing a fast storage is that the file might contain text fragments which should have been eliminated during the process of reworking. For this reason, the fast-storage option should, in principle, remain deactivated.

If a user nevertheless decides to make use of the fast-storage option, he/she should always perform a full storage in the following situations:

- Once editing of document has been completed
- Before a further application requiring a large amount of memory is activated
- Before the text document is transferred to another application
- Before the document is converted into a different file format
- Before the document is dispatched via e-mail or transferred via a data medium

Additional controls:

- Have users been informed about the threats posed by residual information in files?
- Are users aware of the potential threats arising from the use of fast-storage options?

S 4.65 Testing of new hardware and software

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section, IT Security Management

Before new hardware components and software programs are employed, they must be checked on special testing systems. In addition to testing the functionality of a new product, it is of particular importance to check whether its use has any negative influence on the IT systems involved. As damaging functions cannot be ruled out before successful tests and as errors are provoked during tests, the testing systems in use should always be **isolated from the actual production environment**.

The used of isolated testing systems is also required to check self-extracting files, such as those received via e-mail, for damaging functions.

General procedures for software acceptance and release, including testing, are described in Chapter 9.1 *Standard software*. Only after passing all tests should new components be released for installation on production systems.

Additional controls:

- Has new hardware and software been tested before actual use?
- Has new software been scanned for computer viruses?

S 4.66 Novell Netware - safe transition to the year 2000

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

No patches are available from Novell for the date conversion to the year 2000 for Netware versions 2.x to 3.11 as well as 4.01 and 4.02. Although there is now a year-2000 patch for Netware 4.10, versions from Netware 4.11 still seem to be a safer solution to the year-2000 problem.

If Novell Netware versions 2.x to 3.11 are in use, early planning is required for a conversion to Novell Netware version 3.2 or Novell Netware Version 4.11 (or higher).

If Novell Netware 3.12 is used as the operating system, patches ensuring correct date conversion to the year 2000 can be obtained from Novell.

Registered customers who have acquired Novell Netware 3.12 within a certain specified time frame can obtain an update to Novell Netware 3.2 free-of-charge.

If Novell Netware 4.11 (IntraNetWare) is used as the operating system, patches ensuring correct date conversion to the year 2000 can be obtained via the Internet, for example.

Note:

During conversion to the year 2000, it is necessary to ensure - in addition to the use of these patches - that the hardware involved (BIOS) is capable of correctly processing the transition to the new millennium. (also refer to S 2.2000 *Year-2000 compatibility of products, programs and data).*

Supportive measures:

Novell's homepage

- http://www.novell.de/jahr2000/
- http://www.novell.com/year2000/)

offers a tool which determines the serial numbers of the Netware licences used in the network. These serial numbers can be forwarded to the company via facsimile or e-mail, in order to obtain information on any measures which need to be taken (date of report: June 1999).

Under the URL *http://www.novell.com/year2000/* in the Internet, Novell provides its own forum for dealing with problems concerning date conversion to the year 2000. A free mailing list distributed via this forum informs subscribers about recent developments in the "Novell Year 2000 Forum".

Additional controls:

- Have patches been downloaded from Novell via the Internet?
- Have checks been performed to ensure "year-2000 compatibility" of the IT hardware in use?

S 4.67 Locking and deleting database accounts which are no longer required

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Database accounts which remain unused over an extended period of time should, if possible, be locked and later deleted. Users of such accounts should be informed duly before these accounts are locked, and at all events before they are deleted.

If a to be newly created user only requires a database account for a limited period of time, then, if the database offers this possibility, the account should also be established for a limited period. It can prove expedient to establish accounts initially for a limited period and extend their duration at regular intervals (e.g. annually) as required.

If a user of a database is expected to remain absent for an extended period of time (e.g. due to holidays, sick leave, delegation etc.), his database account should, in order to prevent continued use of his ID over this period, be locked for this duration. The database administrator must be notified of all extended periods of user absence. It is expedient to have this done by the personnel department using standard notifications of absence.

Furthermore, the database administration should be informed as quickly as possible about user departures. The accounts of departing users should be deleted no later than on their last day of work.

Additional controls:

- Do rules on the organisation of temporary database accounts exist, particularly if the database system does not support the creation of such accounts?
- How are checks made as to which database accounts are no longer used?
- Are regular checks made as to which database accounts are no longer required?
- Is the database administration informed about users who are to depart or remain absent for extended periods?

S 4.68 Ensuring consistent database management

Initiation responsibility: Head of IT Section, IT Security Management, Administrators

Implementation responsibility: Administrators

In principle, the ID of the database administrator is not subject to any restrictions concerning the use of the database system, which increases the threat of errors and misuse. For this reason, the database administrator should receive a standard user ID in addition to his administrator ID, and only use the latter when absolutely necessary.

Appropriate allocation of tasks, specification of guidelines, and measures for co-ordination are required to ensure that administrators do not perform any inconsistent or incomplete operations. The following requirements must be met here:

- The techniques of performing and documenting modifications are to be specified.
- The type and scope of modifications, as well as their reasons, are to be described.
- In principle, changes to database objects or data must be approved by the administrator of the related IT application. Modifications to central database objects require the approval of all the administrators of the concerned IT applications.
- The times of planned changes must be specified and announced.
- A full backup of the database must be created before any changes are performed.

To avoid misuse to the greatest possible extent and preclude inconsistencies, all the database objects of an application should be managed under a user ID created specially for that application. As a result, changes to the database objects can only be performed under this special user ID, and are not possible even under the ID of the database administrator. The password of this special user ID should only be known to the database administrator responsible for the application in question.

Example:

The data of three applications, A, B and C are managed in a database. All database objects allocated exclusively to application A are configured under the database user ID apnA and managed only via this ID. The database objects of the other two applications are assigned similarly. As a result, modifications to the database objects of any of the three applications can only be performed using the corresponding database user ID (provided that appropriately restrictive access rights have been defined).

Database objects required by at least two of the three applications should be created and managed under a central database ID.

The passwords of the three application-specific IDs should only be known to the administrator responsible for maintaining and updating the database objects of the respective applications. In contrast, the password of the database ID used to manage the central database objects is not known to any of these administrators; instead it is placed in charge of a further administrator. This prevents an application-specific administrator from performing modifications to central database objects which might impair the functionality of the other applications.

Additional controls:

- What measures have been taken to ensure that actions by database administrators do not result in inconsistencies?
- Have all database administrators received an additional ID with restricted rights?
- Are the additional user IDs employed by default?

S 4.69 Regular checks of database security

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The database administrator should check the security of the database system at regular intervals, but at least once a month. All of the checks listed below should be performed; checks marked with (*) can usually be automated with appropriate scripts:

- Are the required backup and security mechanisms active and effective?
- Are there any database users who have not been assigned a password? (*)
- Are there any users who have not used the database system for an extended period of time?
- Apart from the database administrator, who has access to the files of the database software and the data files at the level of the operating system? (*)
- Apart from the database administrator, who has access to the system tables?
- Who is allowed to access the database with an interactive SQL editor?
- Which user IDs are authorised to modify the database objects of the applications? (*)
- Which user IDs have read and / or write access to the data of the applications? (*)
- Which users have the same rights as the database administrator? (*)
- Does the database system have a sufficient quantity of free resources? (*)

Note:

System tables are used to manage the database itself. The items managed in these tables include the individual database objects, database IDs, access rights and allocations of files to storage media. The system tables are generated by the database management system during the creation of the database. In principle, the contents of these tables can be modified with the access rights granted to the database IDs of the administrators. If the data of the system tables is modified with UPDATE-, INSERT- or DELETE instructions, there is a high risk that the database will be destroyed. For this reason, rights to modify the system tables should not be granted. Even read-access should be restricted, as **all** the information in the database can be viewed via the system tables.

Additional controls:

- When was the last security check performed?
- Are the implementation and results of security checks documented?

S 4.70 Monitoring a database

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Databases should be monitored regularly to ensure the availability, integrity and confidentiality of their data. The essential items which need to be observed in this respect are described briefly in the following.

The database should be checked for fragmentation at regular intervals in order to permit a timely planning and implementation of any required measures such as reorganisation of the database.

As a rule, database systems manage the memory available to them in the form of blocks having a fixed size. If data records are inserted into an empty table, new blocks are reserved for this table and filled with the data records. These newly created blocks can be utilised almost fully (with the exception of the last block).

If data records are deleted during subsequent operation, the memory blocks which were occupied by them are released. In principle, this memory space can be used by other data records. However, as the data records have different lengths, 100% utilisation of the free memory space is usually not possible. Consequently, modifications to data in the course of time result in an increasing number of gaps in the database blocks, most of which can no longer be utilised. Such gaps are created not only by DELETE- and INSERT operations but also by UPDATEs, as a data record can no longer be stored at the same location once its length has been changed.

The presence of such gaps not only increases memory requirements but also retards the operation of the database, as more disk space needs to be covered in search of data records and free memory.

The degree of fragmentation in the blocks of a table can be ascertained by comparing the quantity of data in the data records of the table with the memory space occupied by the blocks of the table. In the case of certain database management systems, an analysis of the degree of fragmentation is also supported by the accompanying administration software or add-ons.

If a database becomes excessively fragmented due to the scenario mentioned above, a reorganisation needs to be performed. This can be done manually, for example, by exporting all the data out of the database, re-computing and re-creating all the tables, and then importing the data back into the new database. Auxiliary programs for de-fragmenting tables are also available for some database management systems.

Similarly, the available space of the database files should be checked regularly in order to permit a timely planning and implementation of any required measures such as the extension of the memory capacity. Some database management systems allow administrators to prevent excessively rapid fragmentation by already defining certain parameters during the creation of the tables. For instance, it is possible to reserve a particular number of consecutive blocks for a table in advance, to save free memory for any changes required during later operation.

Example:

In an Oracle database, every table is assigned a fixed number of extents. In Oracle terminology, *Extent* designates a logical unit of magnitude. The data of a table are stored in at least one extent. Once the capacity of an extent has been exhausted, the database management system automatically creates another extent. The following values can be defined during the creation of a table:

- Size of the first extent in bytes
- Size of the second extent in bytes
- Percentage growth of all additional extents, relative to the size of the second extent
- Maximum number of extents which can be created for a table
- The PCTFREE parameter is used to reserve any required percentage of the new blocks for later modifications.

Regular checks must also be made as to whether the data volume is actually increasing at the originally assumed rate. If it increases more slowly, memory resources which could be used for other purposes are tied down unnecessarily. If it increases more quickly, bottlenecks in the memory capacity might occur.

Furthermore, the degree of utilisation of the database must be checked regularly, particularly as regards the set upper limits (refer to S 4.73 *Specifying upper limits for selectable data records*).

The information of relevance to the actual monitoring of a database depends on its mode of operation, i.e. the standard database software in use. Accordingly, individual measures must also be implemented to so modify the database configuration that it meets requirements concerning access speeds, intended transactions etc.

Scripts can be used to automate monitoring of the database. However, a prerequisite here is that the database software supplies the information in a form which can be analysed automatically.

Additional controls:

- Are database files, important tables and the utilisation of the database checked regularly?
- Have appropriate monitoring intervals been defined?

S 4.71 Restrictive utilisation of database links

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Database links allow a database to access the information in another database. To ensure adequate protection of such information however, database links should only be used when absolutely necessary.

To allow access control of users employing database links, a suitable concept of defining user IDs is necessary. In principle, a user is able to access an extraneous database if it recognises the ID with which the user logs into the local database. Additional security is provided by the possibility of establishing links with an explicit specification of the user ID and a password.

In principle, every database user is entitled to establish database links (provided that the user is able to execute the related CREATE command). In general however, only the administrator should be authorised to establish such links. This applies especially to database links which can be employed by all users (PUBLIC DB-Links). The right to establish database links should explicitly not be granted to standard user IDs.

Furthermore, the number of database links which can be employed simultaneously by a user must be restricted in order to control the loads on the database servers. Otherwise an intruder could exploit this situation to obstruct, or even completely paralyse, the operation of the database servers.

Documentation of the database links configured by the administrator is indispensable. In addition to the types of link (established via a special user ID, or given that the locally applicable database ID has also been configured, for the connected database) the documentation should also list the user groups authorised to make use of each database link. As already mentioned, database links defined as PUBLIC can be used by all database IDs.

Additional controls:

- Does a concept for defining user IDs exist, and if so, to what extent does it take the possible use of database links into account?
- Which user IDs are authorised to establish database links?
- Does a concept for employing database links exist, and if so, has it been implemented?

S 4.72 Database encryption

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators, application developers

Depending on the type of information stored in a database and the related requirements of confidentiality and integrity, it might be necessary to encrypt this data. A distinction can be made between online and offline encryption here:

- During online encryption, the data are encrypted and decrypted while the IT systems are in operation, without the involved users being aware of this process. For this purpose, tools can be used which either encrypt the entire hard disk at the operating-system level, or only encrypt the application data of the database.
- During offline encryption, the data are only encrypted after having been processed, and decrypted before undergoing further processing. In general, this is done with tools which are not part of the database system. This technique can prove particularly useful for data backups and data transmissions. In this case, it must be ensured that sufficient disk space is available, as encrypting and decrypting can only be carried out successfully if the hard disk is capable of holding both the original and the encrypted version of the database.

Furthermore, it is possible to save data as plain text in the database, but transmit it in encrypted form during access via a network. This can be realised, for example, with the *Secure Network Services* of the Oracle SQL*Net product group.

Which data should be encrypted using which techniques is best decided on during selection of the standard database software (refer to S 2.124 *Selection of suitable database software*). During this process, the requirements of data encryption should be compared with the corresponding features of the database software. However, it should at least be ensured that the passwords of the database user IDs are stored in encrypted form.

If the encryption requirements cannot be fulfilled completely by any of the standard database software available on the market, the use of add-ons should be considered for the purpose of closing the security gaps. If no add-ons are available either, a concept for implementing an encryption strategy at the corporation or authority should be prepared.

Additional controls:

- Are appropriate encryption techniques offered by the database or add-ons?
- Have the responsible persons been briefed on proper key management?

S 4.73 Specifying upper limits

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators, application developers

To allow better control of access to a database system and improve performance, it is advisable to specify upper limits for certain parameters. Particular note must be made of the following items here:

Specifying upper limits for selectable data records

Particularly for databases holding large amounts of data, it is recommended to specify a maximum number of data records which can be selected during access to the database.

If such upper limits do not exist, users can intentionally or unintentionally execute SELECTs of any scope. This not only obstructs the activities of the individual user, but also results in long waiting periods for all other users of the database. Data records which have been selected for modification remain unavailable to all other users until the transaction is complete.

The upper limits must be defined within the framework of the applications which access the database. Here, suitable controls and locks must be implemented to monitor adherence to the upper limits. In the case of applications which offer search functions, unrestricted searching should generally be disabled, and the entry of search criteria should be made mandatory.

Imposing restrictions on resources

Another option offered by certain manufacturers is the restriction of resources as regards the usage of a database. Here, it is possible to define a large number of attributes, including the number of logins per user ID, maximum permissible CPU utilisation time per login, total duration of a database session and the maximum permissible inactive period while an ID remains logged in.

Examples:

The following instruction limits the temporary tablespace "Temp" to 100 MB for database ID "Smith" in an Oracle database:

```
ALTER USER Smith TEMPORARY TABLESPACE Temp QUOTA
100M ON Temp;
```

The next instruction is used to create a profile tester which limits the number of sessions, maximum CPU utilisation time per session, maximum duration of a database link and maximum idle time (IDLE). Such profiles can be allocated to individual users.

```
CREATE PROFILE Tester LIMIT
SESSIONS PER USER       2,
CPU_PER_SESSION 6000,
IDLE_TIME               30,
CONNECT_TIME    500;
```

For example, Ingres databases allow the imposition of limits on the maximum input and output, as well as the maximum number of records for queries issued by users and user groups.

It is also possible to limit the number of users who can access the database simultaneously. The restriction of this number via parameter settings in the database management system ensures that the maximum number of licenses available for the database software is not exceeded. Simultaneous access by a large number of users might also result in an excessively high operational load on the database server, thus increasing the average transaction times. If, for some reason, an extension of the resources of the database system is not possible or desirable, limiting the number of simultaneous access attempts also helps alleviate the situation.

The related requirements should already be clarified during selection of the standard database software, to allow the preparation of a concept for imposing limitations on resources, should this become necessary (refer to S 2.124 *Selection of suitable database software*).

Additional controls:

- Have upper limits been specified for applications, and is adherence to them being monitored?
- Have unrestricted searches in the applications been disabled in principle?
- Have requirements for restricting database resources been formulated and documented?

S 4.74 Networked Windows 95 computers

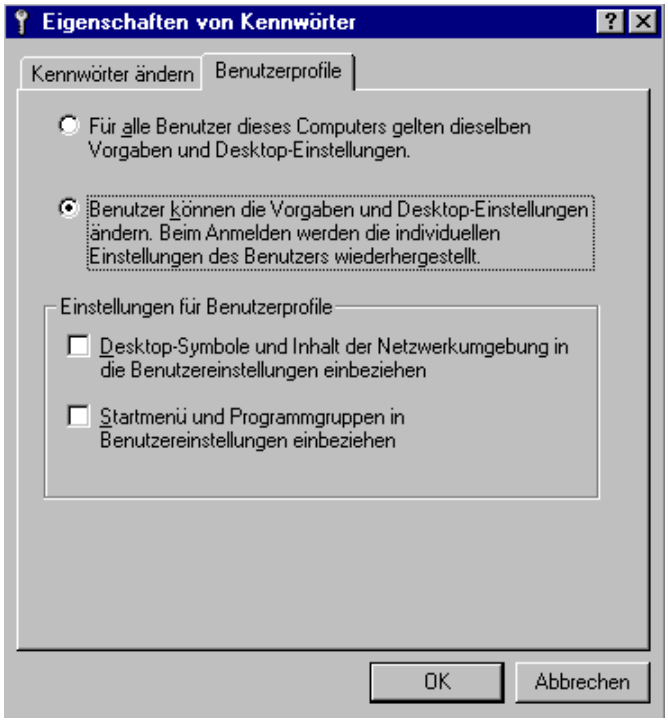
Initiation responsibility: Head of IT Section

Implementation responsibility: Administrators

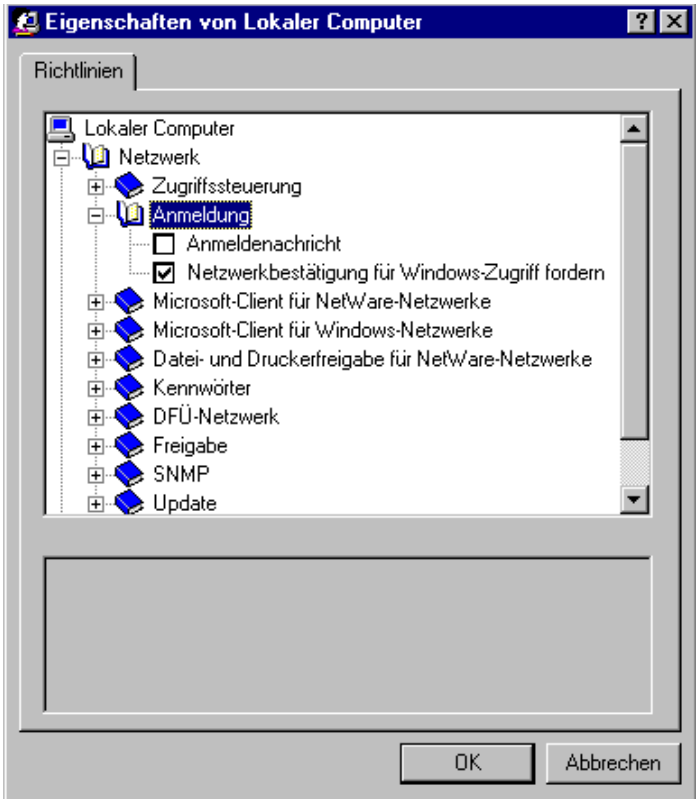
If Windows 95 computers are run in a network (Novell Netware or Windows NT), use should be made of the option of storing the applicable system guidelines on network servers and managing them centrally from there.

In this case, the primary network login, i.e. the path for the system guidelines, is specified via CONTROL PANEL under NETWORK. The user profiles on a Novell Netware server are stored by default under SYS:PUBLIC. If a primary network login is performed on a Windows NT computer, the user profiles are stored by default under NETLOGON (*%SystemRoot%\SYSTEM32\REPL\IMPORT\SCRIPTS*).

Activation of the user profiles is ensured with the help of CONTROL PANEL / PASSWORDS / USER PROFILES.



In addition, an operation of Windows 95 without network login should be disabled in order to prevent circumvention of the system guidelines on a local basis. For this purpose, the option designated *REQUEST NETWORK CONFIRMATION FOR WINDOWS ACCESS* should be activated with the help of *POLEDIT.EXE* via local computer-network login.



For reasons of standardisation, the system guidelines should be managed primarily through the configuration of user groups.

Under Windows 95, group guidelines are installed via CONTROL PANEL / SOFTWARE / WINDOWS / SETUP and located by default in the directory named ADMIN\APPTOOLS\POLEDIT\GROUPPOL.INF.

The names of the user groups must correspond to those of the user groups configured under Novell Netware or Windows NT.

Furthermore, to ensure correct IT operation, the program named *POLEDIT.EXE* must not be installed on the local Windows 95 computer, as anyone could use this program to perform persistent modifications to the valid system guidelines.

Also, the BootKeys parameter in the file named MSDOS.SYS should be changed (BootKeys=1) to prevent Windows 95 from starting in the "protected" mode. This ensures observance of the system guidelines.

Finally, the BIOS of the computer should be set to prevent a system boot from a floppy disk, and the floppy-disk drive should be furnished with a lock to discourage the use of unauthorised software.

S 4.75 Protection of the registry under Windows NT

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

All important configuration and initialisation information is stored in the registry of a Windows NT system. The registry also manages the SAM database which contains the user and computer accounts.

The registry of a Windows NT system consists of several files which are located in the directory path *%SystemRoot%\SYSTEM32\Config*. For this reason, the rights to access this directory and the files contained therein should be set as recommended in S 4.53 *Restrictive allocation of access rights to files and directories under Windows NT*.

After installation of the operating system, the following security-relevant components of the registry should additionally be protected through the explicit entry of access rights with the help of the registry editor (the program named REGEDT32.EXE in the Windows system directory *%SystemRoot%\SYSTEM32*), so that the group "*All*" only has the access rights "*View value*", "*List partial keys*", "*Report*" and "*Read access*" for these components:

- in the area HKEY_LOCAL_MACHINE:

  \Software\Windows3.1MigrationStatus (with all sub-keys)

  \Software\Microsoft\RPC (with all sub-keys)

  \Software\Microsoft\Windows NT\CurrentVersion

  under the key \Software\Microsoft\Windows NT\CurrentVersion\:

  + Profile List
  + AeDebug
  + Compatibility
  + Drivers
  + Embedding
  + Fonts
  + FontSubstitutes
  + GRE_Initialize
  + MCI
  + MCI Extensions
  + Port (with all sub-keys)
  + WOW (with all sub-keys)

- in the area HKEY_CLASSES_ROOT:

  HKEY_CLASSES_ROOT (with all sub-keys)

Care must be exercised here, as faulty settings in the registry might impair the operability of the system, thus preventing it from starting up properly the next time. Consequently, the settings mentioned here should first be used in a separate test system and checked critically for proper functionality under real conditions before being put into regular operation.

Network access to the registry

Access to the registry via the network should be disabled, unless this function is absolutely necessary. This is allowed by version 4.0 or higher, by setting the entry "*winreg*" in the key *\System\CurrentControlSet\Control\SecurePipeServers* in the area *HKEY_LOCAL_MACHINE* to the value *REG_DWORD = 1*.

Version 3.x does not allow an explicit blockage of the registry against network access. In this case, it is helpful to withdraw the right of "All" to access the root of the area *HKEY_LOCAL_MACHINE* (but not the underlying keys!), so that only administrators have access to this area. This modification must, on all accounts, be checked in a test system as it could paralyse certain applications. It must be noted that such a change only remains effective until the system is restarted.

S 4.76 Secure system version of Windows NT

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: Administrators, Procuring Department

Before the Windows NT operating system is purchased, a decision must be made as to whether the English or German version is to be used. A general recommendation cannot be made here. Consequently, this section only describes the specific advantages and disadvantages of each version.

The English version of Windows NT is used more commonly than the German version. As a result, tools, service packs and hot fixes can be obtained more quickly for the English version. In addition, there are tools which can only be used for the English version of Windows NT. Furthermore, it is possible to configure the English version of Windows NT in such a way that error messages appear in German.

However, the same applies to the availability of destructive programs. Such programs are also developed at a faster rate for the English version, and some of them are not available for the German version at all.

Windows NT can only be operated reliably if at least version 3.51 or version 4.0 is installed. Installation of the latest service pack is also recommended. Before it is actually put to use, it should be tested whether the service pack functions together with all the components in the environment concerned. It may be necessary to update other hardware and software components in addition to installing the service pack. At the time off issue of this document for Windows NT Version 3.51 service pack 5 is available and for Windows NT Version 4.0 service pack 6a. The system version installed and, if appropriate, the service pack installed are displayed when the system is started. Furthermore, Microsoft offers "hot fixes" as updates for the latest service pack versions. The current hot fixes should also be installed if they influence the functionality of the system in use. Hot fixes are created at short notice when problems occur. This also means that they are not tested as thoroughly as the service packs. Therefore, only hot fixes that are really needed should be installed on a system. The system administrator must regularly check which service packs and hot fixes are currently available for the system being operated.

A one-time installation of a service pack or hot fix is not sufficient for ensuring system integrity. Every change to the system configuration requiring access to the installation CD-ROM, or the addition of new device drivers, requires a new installation of the current service pack and the necessary hot fixes. If this is not done, there is a danger of system files originating from the respective service pack or hot fix being replaced by older versions. In the worst case, this could prevent the Windows NT system from being started up again.

After a service pack or hot fix has been installed, the start-up disks should be updated (refer to S 6.42 *Creating start-up disks for Windows NT*). Furthermore, the security configuration of the computer in question should be checked.

S 4.77 Protection of administrator accounts under Windows NT

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: Administrators

An administrator account is created each time a Windows NT system is installed. On Windows NT computers which have been installed as workstations or servers without a domain controller function, this pre-defined administrator account is a member of the group titled "Administrators". On servers installed as primary domain controllers under Windows NT, the pre-defined administrator account is made a member of the groups titled "Administrators", "Domain Admins" and "Domain Users". It is also possible to add any defined user account on a Windows NT computer to the groups titled "Administrators" and "Domain Admins".

The pre-defined administrator account and the user accounts added to the "Administrators" and "Domain Admins" groups following installation receive the rights and authorisations allocated to the group(s) of which they are members. These accounts are used by the persons in charge of managing the overall configuration of the workstation or server. Administrators possess a greater ability to control the Windows NT computer than any other user.

However, the pre-defined administrator account differs in essential respects from all other accounts under Windows NT. It cannot be deleted, and is not affected by the automatic locking mechanism which comes into effect following repeated login attempts using an incorrect password. Furthermore, it cannot be removed from the "Administrators" group on Windows NT Workstations and Windows NT Servers, unless a domain controller functionality is available. On Windows NT domain controllers, it is not possible to remove the pre-defined administrator account from both the "Administrators" and "Domain Admins" groups. However, removal from either one of these two groups is possible. This prevents an administrator from being denied access to the system on a temporary or permanent basis. On the other hand, this mechanism increases the risk of intrusion. Here, it must expressly be pointed out that all subsequently-created user accounts which have received administrative rights through admission to the "Administrators" or "Domain Admins " group can, of course, be blocked, deleted or removed from these groups by other administrators. Automatic blocking following repeated attempts at login with an incorrect password is also effective, provided that it has been defined in the account guidelines.

The pre-defined administrator account on **all Windows NT computers** should be renamed such that the new name cannot be easily guessed. The account should be assigned a secure password during installation (refer to S 2.11 *Provisions governing the use of passwords*). Wherever possible, the password should have the maximum length of 14 characters and be kept in a safe place. For daily administration, it is advisable not to use the pre-defined administrator account, but user accounts which are added to the "Administrator" or "Domain Admins" group. The passwords for these accounts should have a minimum length of 8 characters. The pre-defined administrator account should only be used if access is no longer possible via

the subsequently created accounts possessing administrator rights, for example, after these accounts have been blocked due to repeated attempts to log in with an incorrect password.

It is also advisable to subsequently create a new account named "Administrator", provide it with a password, deactivate it, and only include it in the group titled "Guests". No special system rights should be assigned to this account, as it is only meant to put potential intruders on the wrong track.

Furthermore, the security log should regularly be checked for login attempts into accounts possessing administrator rights (refer to S 4.54 *Logging under Windows NT*).

Special destructive software exists which allows a user who has logged in locally to add any number of user accounts to the group titled "Administrators". To prevent this, the hot fix "getadmin-fix" should be installed on all computers running on Windows NT 4.0 with service pack 3. This hot fix can be obtained free-of-charge from Microsoft. When service pack 4 has been installed, it is no longer necessary to install the hot fix mentioned above.

In addition, to prevent the administrator password from being extracted, the rights to access the directories *%SystemRoot%\SYSTEM32\Config* and *%SystemRoot%\SYSTEM32\Repair* should be set as recommended in S 4.53 *Restrictive allocation of access rights to files and directories under Windows NT*. Start-up diskettes and any existing backup tapes should be stored under lock and key.

Depending on the degree of protection required by the data processed on **Windows NT Workstations**, a decision must be made as to whether the same password should be used for all local administrator accounts. A general recommendation cannot be made here. However, if the decision goes in favour of using the same password for all workstations, it must be noted that an intruder who is able to crack this password will gain administrative access to all the corresponding workstations.

The following measures should also be implemented on **Windows NT Servers**. The administrator accounts on the various servers should not all be assigned the same password. Furthermore, remote administration via the network should be avoided wherever possible. This is achieved by denying the "Administrators" group the right designated "*Access to this computer from the network*". If remote administration is indispensable, for example, due to the given spatial environment, the resulting possibilities of intrusion should be minimised. For this purpose, login via the network for user accounts with administrative rights should only be allowed via Windows NT computers specified in the account guidelines. If possible, these computers should be installed in secure areas. It is vital that LAN-manager compatibility is deactivated on these computers, in order to prevent the passwords of user accounts with administrative rights from being transmitted through the network in unencrypted or only poorly-encrypted form. For this purpose, it is necessary to install the hot fix "lm-fix" if Windows NT 4.0 with service pack 3 is used. If service pack 4 has already been installed on the system, it is not necessary to install the hot fix. In the registry, however, it is necessary to add the key *HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\Lsa* by

the entry "*LMCompatibilityLevel*" of type "REG_DWORD" with the value "2".

A Windows NT computer thus modified is no longer able to access resources located on computers which do not recognise the Windows NT authentication scheme. This includes, for example, all computers running under the Windows 95 operating system.

On **domain controllers**, it is not sufficient to deny the "Administrators" group the right designated "*Access to this computer from the network*", because on such controllers, the pre-defined administrator account is automatically made a member of the "Domain Admins" and "Domain Users" groups. For this reason, the pre-defined administrator account should be removed from the "Domain Admins" group. This can be done as long as this account remains a member of the "Administrators" group. The pre-defined administrator account should also be removed from the "Domain Users" group. However, this is not directly possible, as this group is the primary group of the account. Consequently, an arbitrary, global group must first be created which does not possess the right designated "*Access to this computer from the network*". The pre-defined administrator account is to be added to this group, which should be set such that it becomes the primary group of the account. Afterwards the pre-defined administrator account can be removed from the "Domain Users " group.

S 4.78 Careful modifications of configurations

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: Administrators

All changes made to an IT system during actual operation should be considered as critical, and appropriate caution must be exercised when performing such changes.

Before any change is made to an IT system, the old configuration should be backed up, so that it is readily available if the new configuration poses any problems.

In the case of networked IT systems, users must be duly informed about impending maintenance work, so that they can plan for a temporary system shutdown and correctly localise any problems which might occur after the changes have been made.

Changes to a configuration should always be performed in individual steps. Regular checks should be made as to whether these steps have been executed correctly, and whether the affected IT system and applications are still fully functional.

If changes are made to system files, a re-start should be performed subsequently in order to check whether the IT system can still be started correctly. All data carriers required for emergency starting - such as boot diskettes, boot CD-ROM - should be kept handy in case a problem occurs.

If possible, complex changes to a configuration should not be made in the original files, but in copies. All changes which have been performed should be examined by a colleague before being incorporated into regular operations.

In the case of IT systems which need to fulfil high availability requirements, redundant systems should be maintained, or at least restricted IT operations should be ensured. Ideally, the procedures specified in the contingency manual should be followed in this case.

All changes made to a configuration should be noted down step-by-step, so that if a problem occurs, the functionality of the IT system can be restored by a successive reversal of the changes (also refer to S 2.34 *Documentation of changes made to an existing IT system*).

Additional controls:

- Have changes to the system been documented step-by-step?
- Can the changes be undone subsequently?

S 4.79 Secure access mechanisms for local administration

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Some active network components can be administered via local access. Such local access is generally implemented by means of a serial interface (normally of type V.24 or EIA-232-E). The following measures must be observed to ensure secure local access:

- The active network components and their periphery, such as connected terminals, must be installed securely (refer to S 1.29 *Adequate siting of an IT system*).
- Local access for the purpose of administering local components must be disabled by means of software and / or hardware.
- Any existing default password for local access must be modified immediately after putting the active network component into operation (for selection of a new password, refer to S 2.11 *Provisions governing the use of passwords*).
- The security features of permanently connected terminals and computers, such as automatic screen lock and auto logout, must be activated (refer to S 5.11 *Blocking the server console and active network components*).

A local administration offers the following advantages:

- The danger of intercepting passwords is reduced.
- Administration is still possible after a failure of a network segment containing the active component, or after a failure of the entire network.

A local administration has the following disadvantages:

- As a rule, active network components can be configured such that they can be administered either locally or centrally. No general recommendations can be made concerning the selection of the appropriate configuration technique. However, it must be noted that if an exclusively local administration has been configured, central administration of the active network components is no longer possible. These components must then always be administered directly on-site. This also increases reaction times in the event of a failure, as longer distances possibly need to be covered in order to reach the components.
- Local access by means of a V.24 or EIA-232-E interface is generally slower than remote access via the network.

Additional controls:

- Have the default passwords for local access been replaced by secure ones?

S 4.80 Secure access mechanisms for remote administration

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Some active network components can be administered or monitored remotely via network access. This access is performed by means of connectionless or connection-oriented protocols. Such protocols include:

- Protocols intended exclusively for the transmission of data comprising, for example, new firmware versions or configuration files such as *FTP*, *TFTP* (in general, use of the latter is not recommended) or *RCP* (also refer to S 6.52 *Regular backup of configuration data of active network components*)
- Protocols for interactive communications, e.g. *Telnet*
- Protocols for network management, e.g. *SNMP* or *CMIP*

For all types of access, measures must be taken to ensure that no unauthorised access takes place.

For this purpose, the default passwords and community names of the network components must be replaced with secure passwords and community names (refer to S 4.82 *Secure configuration of active network components*). In the case of many active network components, the coupling of community names and passwords influences the FTP, Telnet, SNMP and CMIP protocols. Some components also allow restriction of access on the basis of MAC or IP addresses. This option should be used wherever possible, in order to permit access exclusively from dedicated management stations.

Data transmission protocols (TFTP, FTP, RCP) should only be activated from the network components themselves. This applies in particular to non-authenticating protocols such as TFTP. For interactive communication protocols (Telnet), the auto-logout option of the network components should be activated.

In the case of most protocols, it must be noted that passwords and community names are transmitted in plain text, i.e. they can be intercepted in principle (refer to S 5.61 *Suitable physical segmentation* and S 5.62 *Suitable logical segmentation*).

Example: The "public" and "private" default community names in SNMP should be replaced with other names.

Additional controls:

- Have all default passwords and community names been replaced with secure, user-defined passwords and names?
- Can data transmission only be initiated from the network components?

S 4.81 Auditing and logging of activities in a network

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, auditor

Appropriate logging, auditing and review constitute essential factors related to network security.

Logging in a network management system or on certain active network components allows the storage of particular states (generally requiring definition) for the purpose of subsequent evaluation. Typical items which can be logged include faulty packets which have been transmitted to a network component, unauthorised access to a network component, or the performance of the network at certain points in time. An evaluation of such protocols with suitable aids makes it possible, for example, to determine whether the bandwidth of the network fulfils present requirements, or to identify systematic intrusions into the network.

Auditing implies the use of a service which deals, in particular, with events critical to security. This can take place online or offline. During online auditing, events are scrutinised and evaluated in real time with the help of a tool (e.g. a network management system). During offline auditing, the data are logged or extracted from an existing log file. Items monitored via offline auditing frequently include data on utilisation times and incurred costs.

During *review*, data gathered as part of offline auditing are examined by one or more independent employees (two-person rule) in order to detect any irregularities during the operation of IT systems and to monitor the administrators' activities.

The logging and auditing functions offered by a network management system should be activated to a sensible extent. In addition to performance measurements for monitoring the network load, it is particularly advisable to evaluate the events generated by the network management system, and use specific data collectors (e.g. RMON probes) which allow the monitoring and evaluation of events critical to security.

A large number of entries are usually generated during logging, so that a tool is required to analyse them efficiently. Auditing focuses on the monitoring of events critical to security. Auditing often also involves the collection of data on utilisation periods and incurred costs.

The following events are of particular interest during auditing:

- Data on the operating times of IT systems (which IT system was activated / deactivated when?)
- Access to active network components (who logged on when?)
- Security-critical access to network components and network management components, with or without success
- Distribution of network loads over an operating period of one day / one month, and the general performance of the network

The following events should also be logged:

- Hardware errors which might lead to the failure of an IT system
- Impermissible changes to the IP address of an IT system (in a TCP/IP environment)

Auditing can be performed online or offline. During online auditing, categorised events are reported directly to the auditor, who can initiate measures immediately, if required. These events must be assigned to suitable categories, so that the responsible administrator or auditor can retain a clear perspective and respond to important events immediately without being overwhelmed by a flood of information. During offline auditing, data from log files or special auditing files are prepared with the help of a tool and then examined by the auditor. In this case, measures for maintaining or restoring security can only be initiated after a time delay. Generally it is advisable to employ a mixture of online and offline auditing. During online auditing, security-critical events are filtered and reported to the auditor immediately. Events of a less critical nature are analysed offline.

Standard management protocols such as SNMP and RMON (which is based on SNMP) as well as specific protocols of the employed network management product can be used for logging and auditing.

On no account should user passwords be collected as part of auditing or logging! A high security risk would arise if unauthorised access were gained to this data. Incorrect password entries should not be logged either, as they usually differ from the corresponding, correct passwords only by one character or two interchanged characters.

A stipulation is also required as to who will analyse the logs and audit data. A suitable distinction must be made here between the originator of events and the evaluator of events (e.g. administrator and auditor). Regulations concerning data privacy must also be adhered to. Earmarking in accordance with § 14 of the BDSG must be observed in particular for all gathered data.

Log files and audit files must be analysed at regular intervals. Such files can quickly grow to large proportions. To keep the size of log files and audit files within a useful range, the evaluation intervals should not be impractically short, but short enough to allow a clear examination.

Additional controls:

- Are the recorded log files and audit files examined at regular intervals?
- Are the possible consequences of security-critical events analysed?
- Are user passwords logged?

S 4.82 Secure configuration of active network components

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

In addition to the security of server systems and terminal devices, that of the actual network infrastructure together with its active network components is often neglected. Particularly central, active network components need to be configured in a careful fashion. Whereas a faulty configuration of a server system only affects persons making use of the services offered by this system, a faulty configuration of a router can lead to a failure of large subnetworks, if not the entire network, and cause data to be corrupted unnoticed.

A secure configuration of active network components must also be defined as part of the network concept (refer to S 2.141 *Development of a network concept*). Particular attention must be paid to the following items here:

- For routers and layer-3 switching, a decision is required as to which protocols should be forwarded and which should be barred. This can be achieved through the use of suitable filters.
- A specification is required as to which IT systems are to communicate in which direction via the routers. This can also be achieved through the implementation of filter rules.
- Insofar as it is supported by the active network components, a specification is also required as to which IT systems are to have access to the ports of the switches and hubs of the local network. For this, the MAC address of the calling IT system is evaluated to determine whether the system has been granted access authorisation.

For active network components with a routing functionality, appropriate protection of the routing updates is also necessary. These are required for updating the routing tables in order to allow dynamic adaptation to the current status of the local network. A distinction can be made here between two security mechanisms:

- Passwords

  The use of passwords prevents configured routers from accepting routing updates from routers which are not in possession of the corresponding password. This protects routers against an acceptance of incorrect or invalid routing updates. The advantage of passwords in comparison with other protective mechanisms is their low overhead, which only needs a narrow bandwidth and short computing times.

- Cryptographic checksums

  Checksums provide protection against concealed modifications to valid routing updates as they pass through the network. Together with a sequence number or a unique identifier, a checksum can also provide protection against the reloading of old updates.

A suitable routing protocol must be selected to achieve a sufficient degree of protection for routing updates. RIP-2 (Routing Information Protocol Version 2, RFC 1723) and OSPF (Open Shortest Path First, RFC 1583) support passwords in their basic specification, and can also be extended to make use of cryptographic checksums in accordance with the MD5 (Message Digest 5) algorithm.

Additional controls:

- Has a secure configuration of active network components been included in the network concept?
- Has a suitable routing protocol been employed?
- How are routing updates protected?

S 4.83 Updating / upgrading of software and hardware in network components

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Updating software can eliminate vulnerabilities and extend functions. This applies, for example, to the operating software of active network components such as switches and routers, as well as network management software. An update is especially necessary on the detection of vulnerabilities which might affect the secure or reliable operation of the network, if a fault occurs repeatedly, or if a function needs to be extended for security-related or technical reasons.

Upgrading of hardware can also be advisable in certain cases, for example, if a new version of a switch provides a higher transfer and filter rate. Such measures can, under certain circumstances, increase the availability, integrity and confidentiality of data.

Before an update or upgrade is performed, however, the functionality, interoperability and reliability of the new components must be examined thoroughly. This is done best in a physically isolated test network, before the updated or upgraded product is actually put into regular operation. (refer to S 4.78 *Careful modifications of configurations).*

Additional controls:

- Are updates and upgrades checked for proper interoperability with existing components before being put into productive operation?

S 4.84 Use of BIOS security mechanisms

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

Modern BIOS variants offer a large number of security mechanisms. Users or system administrators should acquaint themselves with the options available. Untrained users should never change BIOS entries as severe damage can be the result.

- Password protection: most BIOS variants offer activation of a boot password. A BIOS password is not difficult to overcome, but it should definitely be used wherever better access safeguards are not available. In most cases it can be selected whether the password is required for booting or only for changing BIOS settings. Sometimes different passwords can be employed for these checks. The setup or administrator password should always be enabled to prevent unauthorised changes being made to the BIOS settings.

  Some BIOS variants support password protection for floppy disk drives. Unfortunately only few BIOS variants support this option. If available it should be enabled to prevent unauthorised installation of software and illicit copying of data.

- Boot sequence: the boot sequence should be set so that the first option is always to boot from the hard disk. „C,A“ should therefore be used, for example. This will protect against infection with boot viruses if a floppy disk in left in the drive by accident. It also saves time, and saves wear on the floppy disk drive.

  Rearrangement of the boot sequence is intended to prevent the boot procedure from being carried out from an external data medium. This is to ensure that the system does not access a floppy disk in the floppy disk drive during booting, which could result in a boot virus infecting the PC (see T 5.23 *Computer viruses*). Depending on which BIOS and operating system is used, it may also be necessary to prevent booting from other exchangeable data media such as CD-ROMs.

  Without rearrangement of the boot sequence it is also possible to circumvent other safeguards, such as access protection mechanisms (see S 4.1 *Password protection for IT systems*). One example is the ability to start a different operating system, with the effect of ignoring any security attributes that have been set (see S 4.49 *Safeguarding the boot-up procedure for a Windows NT system*).

  The effectiveness of the rearrangement of the boot sequence should always be checked by a boot test, because some controllers deactivate the internal sequence and need to be set separately.

- Virus protection / warning: if this feature is enabled, the computer requests confirmation every time a change is made to the boot sector or the MBR (master boot record).

Additional Controls:

- Which BIOS security options are activated?

S 4.85 Design of suitable interfaces for crypto modules

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

The design and configuration options of a crypto module should allow the entire flow of information to and from the module or even direct physical access to the data stock in the module to be controlled or restricted as necessary. Depending on the application or protection requirements, it may be advisable to use physically separate input and output ports. Whatever the case, the module interfaces should be set up such that the individual data channels are logically separated from each other, even though they may possibly share a common input or output port. In connection with the key management functions for the crypto module it must be guaranteed that the output channels are separated (at least logically) from internal key generation and the input port for manual key entry. In many cases there will be separate interfaces available for the connection of an external supply voltage or an external supply pulse and for exclusive use by repair or maintenance tasks. From the standpoint of the crypto module, therefore, it makes sense to divide these up and use them as follows:

- Data input interface, which carries all the input data for the crypto module that is to be processed or edited in the module (e.g. cryptographic keys, authentication information, status information from other crypto modules, plaintext data etc.).
- Data output interface, which carries all of the data from the crypto module that is to be passed from the module to its environment (e.g. encrypted data, authentication information, control information for other crypto modules, etc.).
- Control input interface, which carries all control commands, control signals and control data for executive sequencing and setting the module's mode of operation.
- Status output interface, which outputs all signals, indications and data to the environment in order to indicate the internal security status of the crypto module.

And finally:

- Maintenance interface, which is used exclusively for maintenance and/or repair purposes.

The documentation for a crypto component should contain a description of all components (hardware, firmware and/or software).

Furthermore, the documentation should contain the complete specification of the module interfaces as well as the physical or logical ports, manual or logical control units, physical or logical indicating elements and their physical, logical or electrical properties. If a crypto component contains a maintenance interface, the documentation should also provide a full specification of the maintenance processes that have to be performed. All physical and logical

input and output channels within the module must be explicitly declared. In addition to specific details of the way the crypto component is integrated into the intended application environment, the methods of operating and using the crypto component must also be described.

The documentation should also contain a survey of the security functionality, and if possible point out dependence on hardware, firmware or software that is not included directly in the scope of supply of the crypto component, depending on the conceptual design of the component.

The documentation about the module interfaces must be provided by the module vendor. The documentation is required in a variety of circumstances, for example by an administrator who intends integrating the crypto module into his system environment or by an evaluator who would like to carry out a security assessment of the crypto module.

S 4.86 Secure separation of roles and configuration with crypto modules

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

Many cryptographic security components offer the option of distinguishing between multiple user roles and the associated actions that can be executed by the authorised personnel. Depending on protection requirements, access control and authentication mechanisms may be necessary in this connection in order to be able to verify whether a user is in fact authorised to execute the desired service. The various roles can be sensibly subdivided as follows:

- User role, whose function is the utilisation and application of the security component (e.g. subscriber or user).
- Operator role, with responsibility for installation and crypto management (e.g. security administrator).

Plus at least one of the following:

- Maintenance role, with responsibility for maintenance and repair work (e.g. maintenance engineer, auditor).

If the crypto components offer the option of separating the user role and the administrator role, this should be done. The administration should also specify basic settings, such as the password length or key length, to ensure that it is impossible for users to select insecure settings out of convenience or lack of knowledge.

In addition to the various roles, it is also necessary in the same way to distinguish between the various actions or the services provided by the security component. A crypto module should provide the following services, at the very least:

- Status indication, for output of the current status of the crypto component
- Self-test, for the initialisation and execution of autonomous self-tests
- Bypass, for activating and deactivating a bypass by means of which plaintext information or unsecured data is transported through the crypto module

It is essential for staff to be authenticated with respect to the security component, and a wide range of different techniques can be used: passwords, PINs, cryptographic keys, biometric features etc. The crypto component should be configured such that the authentication information has to be re-entered every time there is a role change or after a specified period of inactivity. It is also advisable in this connection to set a restriction on the number of authentication attempts (for example by setting the maximum operating error counter to 3).

S 4.87 Physical security of crypto modules

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

As described in S 2.165 *Selection of a suitable cryptographic product*, crypto modules can be implemented in software, firmware or hardware. Firmware or hardware products tend to be chosen especially in cases where the crypto module is supposed to be especially resistant to manipulation.

With this in mind, the design of the crypto module should incorporate physical safeguards or corresponding material properties that provide effective prevention of unauthorised physical access to the contents of the module. This is intended to guard against the possibility of technical manipulation or other encroachments during ongoing operation. Depending on the security level of the crypto module, the techniques to be considered could include the use of passivation materials, appropriate anti-tamper measures or mechanical locks, for example. An automatic emergency deletion function, which can bring about the active deletion or destruction of all sensitive key data and key parameters stored in plain text within the crypto module after an attempted attack is identified, can also be included in this category of safeguards.

Various sensors and monitoring devices can be employed to ensure that the crypto module is always operated in its intended field of use – with regard to the power supply, timing, temperature, mechanical stress, electromagnetic interference etc.

In order to maintain its envisaged level of functionality, the crypto module should be able to initiate and perform self-tests. These tests may cover the following areas: algorithm tests, software and firmware tests, functional tests, random statistical tests, consistency tests, condition tests, and key generation and loading tests. If the result of any test is negative, an error message pointing this out must be issued to the user of the crypto module and the module should enter a corresponding error state. It should not be possible to release the module from the error state until after the cause of the error has been remedied.

When software products are used, the physical security of the crypto module must be provided by the respective IT system or its application environment. The security requirements to be met by such IT systems are described in the system-specific sections.

A software solution should be able to perform self-tests so as to be able to detect modifications made by Trojan horses or computer viruses.

S 4.88 Operating system security requirements when using crypto modules

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

Whenever crypto modules are used, the way in which they are integrated into or dependent on the operating system running on the host system is particularly significant. The interaction between the operating system and the crypto module must ensure that:

- the crypto module cannot be deactivated or circumvented (for example by manipulation or by the exchange of drivers);
- the keys used or stored by the module cannot be compromised (for example by the reading out of RAM areas);
- the data being protected can be stored on data media (including being stored without encryption) or may leave the information-processing system (for example if there is a network connection) **only** with the knowledge of and under the control of the user;
- attempts at manipulation of the crypto module will be detected.

The level of the operating system security requirements is liable to vary according to the type of crypto module (implementation in hardware or software, strategy for integration into the IT component etc.), the conditions in which it is used and the degree of protection required for the data. Where crypto modules are implemented in software, the use of a secure operating system is particularly important. Commercial PC operating systems are generally so complex and subject to such short innovation cycles that it is barely possible to verify or prove the security of data or a system. One exception may be proprietary operating systems or operating systems optimised for special applications (such as special-purpose operating systems in cryptographic devices). It is therefore important when using cryptographic products with standard operating systems for such purposes as file encryption or the safeguarding of e-mails that all standard security measures for the operating system are put in place. The security-related requirements for these IT systems are described in the respective system-specific sections, for example for clients in Chapter 5 and for servers in Chapter 6.

Crypto modules implemented in hardware can be designed so as to compensate for deficiencies in operating system security, or to eliminate them altogether. The responsibility for satisfying the requirements specified above lies solely with the crypto module. It must be able to recognise, for example, whether or not authorisation is required to write unencrypted data to data media or other device interfaces, bypassing the module. The user must decide what combination of operating system and crypto module is required, in compliance with the security policy drawn up for his particular working environment.

S 4.89 Emission security

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

Every electronic device emits electromagnetic waves of a greater or lesser strength. These emissions are known as stray radiation or radiated interference. Their maximum permissible strength is stipulated in the Law on the Electromagnetic Compatibility of Devices (German abbreviation: EMVG). In devices which process information (PCs, printers, fax machines, modems etc.), this stray radiation may also carry the information currently being processed. Information-bearing radiation of this nature is referred to as compromising emanations. If the compromising emanations can be received some distance away, for example in a neighbouring building or in a vehicle parked nearby, it is possible to reconstruct the information from the emanations. The confidentiality of the data is therefore called into question. The limiting values set by the EMVG are generally not sufficient to prevent interception of compromising emanations. Usually it is necessary to take additional steps to ensure this.

Compromising emanations can emerge from a room in different ways:

- In the form of electromagnetic waves, which are propagated through free space in the same way as radio waves.
- As conducted radiation along metallic conductors (cables, air-conditioning ducts, heating pipes).
- By cross-talking from a data cable to other cables laid parallel. The radiation propagates along the parallel cables and can be picked off from these even a long distance away.
- As acoustic radiation, for example in the case of printers. The detailed information from the printing process is disseminated as sound or ultrasound, and can be picked up with microphones.
- In the form of acoustic cross-talk to other devices. Sound is converted into electrical signals by sound-sensitive parts of equipment, which under certain conditions can function in a similar way to a microphone. The sound is then propagated further along metallic conductors, or also in the form of electromagnetic radiation.
- Compromising emanations may also be caused by external manipulation of devices. If a device is irradiated with high-frequency energy, for example, the electrical processes in the device can influence the radiated waves in such a way that they subsequently carry the processed information with them.

In all of these cases the nature of the installation, in other words the cabling between the devices and from the devices to the electricity supply system, has a substantial influence on propagation and hence on the range of the radiation.

The BSI has developed and is still developing various protective measures which effectively reduce the risk without significantly increasing costs. These include:

- Zone model

  The BSI has developed a zone model which takes account of the propagation conditions of compromising emanations in relation to particular conditions in certain buildings and on certain sites. The attenuation of the radiation on its way from the originating IT device to the potential receiver is determined by metrological means. Depending on the circumstances at the place of use, it may be possible to use devices to which only minor interference suppression measures have to be applied, or no measures at all.

- Emanation suppression at source

  Emanation suppression at source is particularly valuable when developing new IT products. This involves suppressing the compromising emanations at their place of origin within the device, or modifying them in such a way that they can no longer be utilised. This method might also allow the use of low-cost plastic housings, for example, with a negligible impact on the batch production price.

- Set of radiation criteria

  The purpose of a detailed set of radiation criteria is the graduated testing of IT devices and systems The rationale behind this concept is to adapt the scope of the protection measures as closely as possible to the threat situation assumed to exist by the user, so as in that way to achieve an optimum of emission security with the minimum of cost.

- Accelerated measurement procedures

  Devising accelerated measurement procedures and manipulation test procedures enables emission security to be ensured at as low a cost as possible after maintenance, repair or potentially unauthorised access.

- Use of low-emission or emission-protected equipment

  Manufacturers of PC monitors often make use of the term "low-emission" according to MPR II, TCO or SSI in their advertising material. However, these guidelines only take account of the possible damaging effects to health of radiation from equipment. The measuring techniques and limit values for radiation are therefore entirely unsuited to producing evidence of compromising emanations and do not allow any assessment to be made of security against the unauthorised interception of data via compromising emanations.

  In addition, special emission-protected IT systems are also offered by some suppliers. There are numerous levels of emission protection provided in this field. In order to allow the classification of IT systems with high protection requirements, in particular, the BSI developed a set of criteria known as TEMPEST (Temporary Emission and Spurious Transmission) criteria. Whether a manufacturer includes emission protected devices conforming to the TEMPEST criteria in its range of products should be clarified by asking the manufacturer or the BSI, or by checking the official product overview in BSI 7206. The statement that a device has been awarded TEMPEST approval should always be accompanied by indication of the level of approval.

S 4.90 Use of cryptographic procedures on the various layers of the ISO/OSI reference model

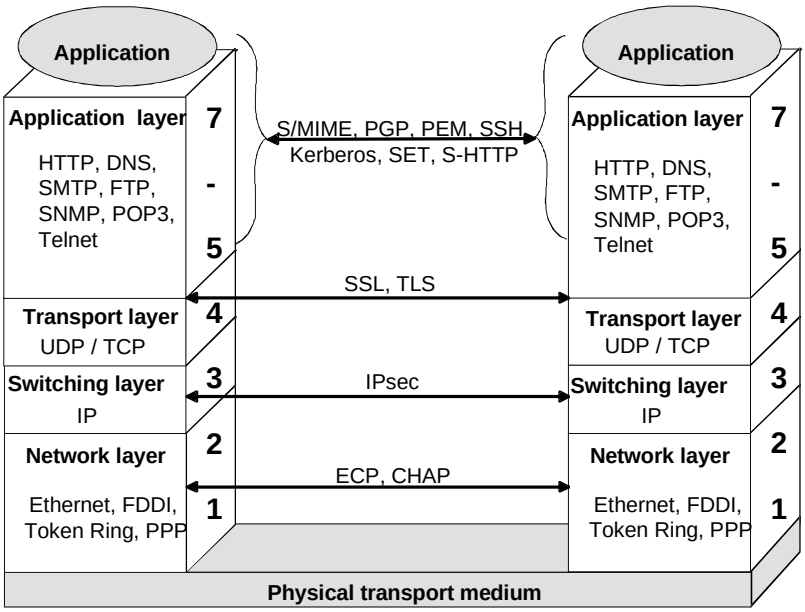
Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

The OSI reference model according to the ISO

Cryptographic procedures can be implemented on the various layers of the ISO/OSI reference model. This model, which is explained briefly in this manual in safeguard S 5.13 *Appropriate use of equipment for network coupling*, defines four transport-oriented layers and three application-oriented layers. Instances on the same layer in various systems communicate with each other with the aid of certain protocols. Each layer offers its services to the next higher layer. In addition to the usual communication services, this may also be a security service. A description of which security service should be placed in which layer of the reference model, and which mechanisms can be used to do so, is given in Part 2 of ISO 7498 (Security Architecture).

Even if particular communication systems, reference models or protocols are not always entirely in conformance with the ISO reference model, knowledge of the ISO reference model helps when assessing the security functions of products and therefore also makes it easier to assemble "secure" complete systems in a systematic manner.



The following sections aim to explain what advantages and disadvantages are associated with the use of cryptographic procedures on the respective layers.

Security services

Cryptographic procedures are used for securing a variety of information that arises in the course of communication, i.e. for encrypting information or for assigning cryptographic checksums or digital signatures to it. The data that can be secured is the data to be transmitted by the user, but also information

that is generated implicitly during the exchange of information (such as traffic flow information).

Security relationships may exist for various security services on various OSI layers simultaneously. Above the layer on which a security service is implemented, the information (relating to that service) is not secured. Cryptographic mechanisms (encryption, digital signature, cryptographic checksums) contribute to the implementation of important security services (authenticity, confidentiality, integrity, verification of communication and verification of the origin of data).

First let us look at an overview of the criteria that speak for or against the use of cryptographic procedures on the various OSI layers:

Use of cryptographic procedures on	
higher layers:	**lower layers:**
+: Makes sense if the application data is to be protected close to the application or if the "insecure channel" is to be kept as short as possible	+: Makes sense for the coupling of two networks that are classed as secure via an insecure connection, e.g. linking two properties via public networks
+: Whenever the data is not protected on the lower layers	+: For securing a network against unauthorised access
+: Makes sense if there are a large number of changing communication partners at various locations	+: Whenever traffic flow information needs to be protected, e.g. address information
+: Users can make use of them in accordance with their own requirements	+: All higher-level header information and the user information is encrypted
+: Security is provided closer to the user, and is more easily recognisable by him	+: Transparent for users, relatively low risk of operating error
-: Undermines safeguarding by firewalls	+: Easier key management
-: Often subject to operating errors	-: Protection only as far as the layer in which the security protocols are implemented
-: Often based on software; cryptographic keys and algorithms are easier to manipulate	-: Often hardware, i.e. expensive and inflexible
-: Greater dependency on the operating system or on underlying hardware	-: Often does not offer end-to-end security

Simple key management procedures are generally obtained if group keys can be used, for example when setting up secure subnetworks (VPNs) in which the access ports are equipped with cryptographic devices.

The purchase price of cryptographic products for the lower layers is usually considerably higher than that of those for higher layers, but it also has to be

said that fewer are required. Furthermore, administration and implementation costs are normally also lower, because security services do not have to be implemented in a wide variety of applications. In this way even "exotic" applications – which do not have their own security functionality – can exchange data securely.

In many cases it is a good idea to use a combination of cryptographic services on different layers. The form that this will take depends on the specific security requirements and the conditions of use, such as costs, performance and the extent to which the relevant components are available. Other crucial factors include the assumed threads which the implemented security services are intended to counteract, and the underlying system architecture.

Security terminals <-> security coupling elements

Security systems can take the form of a terminal device or part of a terminal device, or of a coupling element or part of a coupling element. Coupling elements may be active network components, for example, such as routers or gateways.

In contrast with terminal devices, security coupling elements usually have two network interfaces, which are coupled to a layer that is typical for that system via a crypto module (hardware or software). One interface is connected to the "secure" network (e.g. an in-house network), while the other interface is connected to the network considered "insecure" (e.g. a public network).

Security terminals have the advantage that the security mechanisms can be closely adapted to the requirements of the application. Typical security terminals include crypto telephones, crypto fax machines or hardware/software-based security solutions for PCs. Security terminals generally provide solutions for individual workstations. In some cases these solutions support only one service. The boundaries are fluid, however (such as in the case of telephony via an Internet PC, or a crypto telephone with a data input). In terminal devices, as opposed to coupling elements, the choice of security layer is not restricted, because terminals are generally complete – in other words they have 7 layers.

Security coupling elements are often designed with sufficient performance capability to be able to provide security for large work units, up to and including entire properties. The manufacturers of these systems try to support as many services and higher-level protocols as possible, so as to enable them to be put to universal use. The fact that they are largely independent of the operating systems on the terminals also contributes to the universal applicability of coupling elements. It is of course also possible to protect individual terminals with security coupling elements. The performance capability of the equipment, however, often results in higher costs. Coupling elements are by definition incomplete OSI systems. Consequently the implementation of security services is also limited to the layers where the coupling element is located.

There are also mixed forms in use. This relies on the precondition that security terminals and security coupling elements must be dovetailed with each other, particularly with regard to the security mechanisms and security parameters that they use (such as cryptographic keys).

User, control and management information

A user is primarily interested in the transmission of user information to remote users. Depending on the actual reference model being used, however (e.g. ISDN), control, signalling and management information is also transferred between the systems (terminal devices, coupling elements) for the purpose of setting up and clearing down connections, negotiating quality of service parameters, and configuring and monitoring the network by network providers etc.

The network concerned has the task of transmitting user information without changing it and without interpreting it; i.e. only the terminal devices must be capable of interpreting user information. In this way the information can be secured irrespective of the rest of the network infrastructure, if necessary even using proprietary security functions (closed user group). It must be possible for control, signalling and management information on the transport layers to be evaluated, modified or generated by network elements belonging to the network provider. As a result, this information largely avoids any protection provided independently of the network provider (e.g. encryption). The safeguarding of this information calls for trusting co-operation with the network provider, as well as application of the relevant standards. Threats may arise from the fact that the security functions of certain products are incorrectly assessed. When cryptographic devices are selected, it is essential to examine precisely which components of the information are secured or filtered. Likewise, looking at it the other way, it is necessary to check which information remains unsecured despite the use of crypto devices, and to what extent this can be tolerated.

Example: With ISDN, the user information is generally carried via the B channels. However, the D channel, which is primarily used for signalling, can also be used for the transmission of packetised data. If the objective is to protect all user data, it is plain that safeguarding the B channels is not sufficient in cases where packetised data is transmitted via the D channel.

Security in circuit-switched networks

In circuit-switched networks, the establishment of a connection sets up channels of a defined bandwidth, which are exclusively available to the communicating parties. After the connection has been established, the user data is transmitted, then the connection is cleared down. The network provider can set up fixed connections, in which case there is no need for the connection to be established and cleared down – usually performed by the subscriber. One example of a circuit-switched network is ISDN.

When a connection is established, user data channels are set up between the communication partners on OSI layer 1; in ISDN these are referred to as B channels. In order to ensure the confidentiality of the transferred user data, the channel can be encrypted. If it is also intended to secure the signalling channel, in the case of N-ISDN therefore the D channel (layers 1-3), it must be borne in mind that both the communication partner’s terminal and the network provider’s exchanges can appear as distant stations for a terminal transmitting data. The D channel is not normally encrypted, because this would mean imposing particular requirements on the network provider. In this case

provision should be made for monitoring and filtering the D-channel (see also S 4.62 *Use of a D-channel filter*).

Circuit encrypters: The encryption of synchronous full-duplex permanent connections must be seen as a special case, because in this case confidentiality – even confidentiality of the traffic flow – can be guaranteed. If there is no data pending transmission, filler data is encrypted, so that continuous "noise" is always present on the line. The circuit encrypter represents an alternative to installing protected circuits.

Security in packet-switched networks

In packet-switched networks it is necessary to distinguish between connection-oriented and connectionless packet switching. In connection-oriented packet switching, a virtual connection is set up during the connection setup phase, as a result of which the data path through the packet network is subsequently established. After the connection is set up, packets are routed through the network along the same path on the basis of the assigned virtual channel number. Transmit and/or receive addresses are no longer necessary for this. One example is the X.25 network.

In the case of connectionless packet switching there are no connection setup and cleardown phases. Packets are switched individually – among other things furnished with a source address and destination address. This is typical of LAN data traffic.

The choice of layer on which the security mechanisms take effect determines which information components will be protected. The lower the chosen security layer, the more comprehensive the protection of the information. When the user data passes through the instances of layers 7 to 1 (transmitter), additional control information is added to the data. If therefore it is important to protect not only the user data but also the traffic flow, it makes sense to choose a low OSI layer. On the other hand it is also the case that the lower the chosen OSI layer, the fewer coupling elements (repeaters, bridges, switches, routers, gateways) can be overcome transparently.

Coupling element	Highest layer of coupling element
Repeater	1
Bridge, layer-2 switch	2
Router, layer-3 switch, X.25 packet handler	3
Gateway	7

If it is intended that security services should take effect beyond coupling elements, they must be implemented in a layer above the highest layer (or sublayer) of the coupling elements. This ensures that the communication equipment can forward the secured information unprocessed and uninterpreted.

Examples and consequences of incorrect network configurations:

Example 1: In order to guarantee confidentiality, in particular in the sphere of public communication networks, all terminal devices in two LANS coupled

via a router and public communication networks are to be equipped with layer-2 encryption components. The router has to evaluate the addresses of layer 3 in order to forward the LAN packets via the public network. However, as all layer-3 data is hidden as a result of layer-2 encryption, evaluation of the layer-3 addresses cannot be successfully carried out. Data transmission is prevented because of this. To remedy this situation, the encryption components must be used for layer 3 (upper sublayer) or higher.

Example 2: In future, a large proportion of a certain institution's correspondence is to be sent electronically using X.400 (layer 7). In order to safeguard data integrity, the institution plans to use layer-4 crypto components in the terminal devices (in this case PCs). For security purposes, cryptographic checksums are assigned to the data packets at the sender on layer 4; these are then checked by the associated layer-4 crypto component belonging to the receiver. Only packets with correct checksums are to be delivered. However, if some MTAs (Message Transfer Agents, i.e. the intermediaries for electronic messages on layer 7) are not equipped with interoperable crypto components, the MTAs with no crypto component cannot generate valid checksums. This means that subsequent MTAs or terminal devices with a crypto component have to discard the data, in accordance with the specification.

However, even if all of the MTAs that are used are equipped with interoperable crypto components and security parameters in the same way as the terminal devices, data integrity is not assured. Although it is possible to safeguard the data transmission section by section, corruption of the data within the MTAs can occur without being noticed. Furthermore (depending on the protocol) individual layer-4 data packets could be lost, which would result in gaps in the message as a whole – and it is the integrity and completeness of this that is actually supposed to be protected. One remedy is to protect the integrity of the data on layer 7.

As the examples illustrate, it is essential to investigate precisely the nature of the network topology and to determine which network areas have to be secured, and how, so that an appropriate solution can be found with the desired (security) features.

Section-by-section security <-> end-to-end security

Users of communication systems often expect security services to be provided seamlessly throughout the system (end-to-end security), in other words from the input of information (data, speech, images, text) at terminal A through to output of the information at a remote terminal B. If there is no guarantee of continuous security service, there are other systems - apart from the terminal equipment - on which the information is present in an insecure form. For example, if there is no end-to-end encryption to safeguard the confidentiality of a communications relationship between two parties, the data is available in unencrypted form in at least one other network element. These network elements must be located, and secured by additional safeguards. Staff who have access to insecure network elements, in particular (such as administrators) must be accordingly trustworthy. In this case security services are not provided seamlessly but section by section. Care must be taken that all relevant sections are appropriately secured.

Multiple protection on various OSI layers

There is no objection to multiple protection of the transmitted information on different layers of the OSI model, provided certain rules are observed. In products that conform to the relevant standards, though, this is implicitly guaranteed. Especially with regard to encryption, it is necessary to apply bracket rules, familiar from school. Accordingly, encryption corresponds to opening a bracket, and decryption to closing a bracket. Between these brackets it is possible, in turn, to apply additional security mechanisms.

Multiple protection can also have a detrimental effect, in that data throughput may be reduced as a result of additional operations or that the amount of user data that can be transmitted is smaller, for the same reason, or that additional data has to be transmitted in order to increase redundancy (for example cryptographic checksums). Multiple protection is also obtained implicitly if data is secured by means of crypto systems before it is transferred, for example in the case of digitally signed documents. This increases the security of the data transfer with respect to the security services used.

Often it is only possible to ensure the security of an entire system by combining several security protocols or security products. If, for example, application-oriented security solutions are available but the trustworthy implementation of these solutions has not been (independently) scrutinised (e.g. by evaluation according to ITSEC or CC), and at the same time there are trustworthy transport-oriented security products available for protecting insecure network sections between remote properties, it may be possible to create an overall security solution to satisfy the requirements by combining the safeguards. Usually the increased administration expenditure and/or higher procurement costs prove disadvantageous in such cases.

S 4.91 Secure installation of a system management system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The installation of a system management system calls for extensive and careful planning. After system analysis has been performed (see S 2.168), the management strategy has been laid down (see S 2.169) and a suitable management system has been chosen (see S 2.171), installation of the product must be planned in detail and put into practice accordingly. The actual management system configuration for the local network must be drawn up in accordance with the architecture on which the management product is based, paying particular attention to the formulated management strategy.

In order to install most management systems, management software has to be installed on the computers concerned; this takes over communication between the management console or servers and the local computer. Often it is also necessary to install database systems on the central computers (servers or gateways), in which the management information is permanently stored by the management software. Depending on the product, it may also be possible to link in an existing database system for this purpose. As a rule the additionally installed software imposes extra demands on the computer's local resources. During planning, therefore, attention must be paid to what system resources are available locally. It may be necessary for some systems to be upgraded. These costs should be taken into account in the selection of the management product.

In addition to these criteria, which are essentially intended to guarantee regulated technical system operations, for security reasons the software associated with the management system and the corresponding data must be included in the determination of the protection requirements in accordance with the IT Baseline Protection Manual (see Chapter 2), and the protection requirements must be classified as "high" to "very high". Compromising the management system is liable not only to cause failure of the entire network; as well as this, unnoticed changes to the system may cause considerable damage which can very rapidly take on existence-threatening forms.

Particular attention should be paid to the following points in relation to installation:

- All computers on which management information is stored must be given special protection:
  - The measures specified in the IT Baseline Protection Manual Chapters 5 and 6 must be implemented, depending on the system on hand.
  - In particular the operating system mechanisms must be configured so as to prevent unauthorised access to locally stored management information.
  - Access to the management software must be granted only to authorised administrators and auditors.

- Physical access to the computers should be restricted.

- Communication between the management components should be encrypted – provided this is supported by the product – in order to prevent the possibility of unauthorised users eavesdropping on or gathering management information. If the product does not support encryption, special measures must be taken in order to safeguard communications (see S 5.68 *Use of encryption procedures for network communications*).

S 4.92 Secure operation of a system management system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

To ensure the secure operation of a system management system, which may consist of a number of different management tools (see S 2.171 *Selection of a suitable system management product*), the configuration of all components involved must be examined to ascertain that it is secure (see also S 4.91 *Secure installation of a system management system*). To do this it is necessary to provide appropriate security for the operating systems of the components which are administered by the system management system and which therefore have installed parts of the system in the form of software and/or data. The provision of security also includes the secure siting of the computers that perform central tasks for the management system (management servers or computers with management databases). In addition, provision must be made for secure data transmission (see S 5.68 *Use of encryption procedures for network communications*).

Particular attention should be paid to the following points during operation of a management system:

- The new hardware and software components added by the management system must be documented in the course of updating of the system documentation.
- Changes to the management system itself must also be documented and/or logged.
- Updating must be carried out in the same way for the emergency procedure manual. In particular the startup and recovery plans must be modified, because after the introduction of a management system many standard functions of the administered operating systems can only be executed with the aid of the functions of the management system. On the other hand, however, the emergency procedure manual must also include instructions on how the system can be made available without the management system (for example in the event of total failure of central components) to a sufficient degree within a short time (emergency operation regulation; see also Section 3.3 Contingency planning concept).
- Access to the components or data of the management system is generally carried out exclusively by the management system itself or by other authorised system mechanisms (such as a data backup system). Access must therefore be prohibited for normal users. In normal cases this also applies to the role of the local administrator of an individual computer. If it does become necessary in exceptional cases to access the local components of the management system on a computer (for example for crash recovery or when installing new components, assuming the management system does not support this as part of its management function), this authorisation should be granted explicitly, and only for performing this particular task.

- The relevant powers must be laid down as part of the security policy. In the field of management, too, there is a division of roles between administrators and auditors – and depending on the product also between administrators with different rights (such as workgroup administrators or divisional administrators). It is advisable to define certain roles and to set up users with the appropriate authorisations in accordance with these different roles. In that way the user accessing the system is granted only those rights to components or data in the management system that are necessary for the task in hand. Depending on the management system, users are set up either in the management system or in the user administration system for the computers. As the existing systems do not include direct provision for the definition of different roles (such as administrator and auditor), the roles must be emulated as closely as possible by creating various user accounts (e.g. "Administrator", "Auditor", "Computer Admin", "Data Privacy Officer") with the corresponding rights. Depending on the system, these roles can only be emulated incompletely and at some expense, because it may be necessary to assign and maintain the rights for individual roles explicitly for each system component (files, programs).
- Access to the management software must be protected by secure passwords. The passwords should be changed at regular intervals, in accordance with the security policy.
- Functions offered by the management software which according to the management strategy should not be used should (if possible) be disabled.
- The logging files must be checked for anomalies at regular intervals (such as the execution of functions that are not supposed to be used). It is recommended to use log analysers for this, which may either be integrated into the management product or be available as add-on software, and which can generate alarm messages (such as by e-mail or pager) as the need arises, usually under rule control.
- Integrity tests must be run on the management system at certain intervals so that unauthorised changes can be detected as early as possible. This applies in particular to all configuration data in the management system.
- If the system management system is also used to distribute software, the program data that is to be distributed must also be checked regularly for changes in order to prevent the distribution of modified software across the entire network.
- The response of the management system in the event of a system crash should be tested. Automatic restarting of the management system or of local subcomponents of the system must be ensured, depending on the management and security policies. This prevents computers that are connected to the management system from being inaccessible to management for lengthy periods (see also S 6.57 *Creation of an emergency plan for the failure of the management system*).
- In the event of a system crash, the management databases must not be destroyed or enter an inconsistent state. This prevents a potential attacker from exploiting provoked inconsistencies for an attack. To ensure this, the

management system must either make use of a database system that supports relevant recovery mechanisms or implement these mechanisms itself (see S 2.170 *Requirements to be met by a system management system*). If these mechanisms are not provided by the chosen system (for example if several management tools are used), the computers that store management information should be given the maximum possible level of security (including physical, see Chapters 4 to 6).

- The management system should include a suitable backup mechanism for backing up the management data, or interoperate with a backup system. When old data stocks are loaded from a data backup, it must be borne in mind that these usually have to be post-edited manually in order to match the current system configuration.
- Management data stocks that have been backed up by means of backup procedures must also be stored in such a way that no unauthorised third party can gain access to them. Usually the data is not stored in secure form on the backup storage medium, which means that it can be viewed by anyone who possesses the backup program and a corresponding drive.
- The validity of the division into management domains and the associated responsibilities should be examined at regular intervals. This applies in particular when internal restructuring has been carried out.

S 4.93 Regular integrity checking

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Regular checking of the file system for unexpected changes helps to detect inconsistencies. In this way it is also possible to detect attacks quickly. If an attack has indeed been made, it is important to reconstruct the attacker's approach. On the one hand this serves the purpose of ensuring that users do not have recourse to corrupted data, and on the other hand of detecting hidden back doors which an attacker may have installed to give him access to the computer at a later date.

Programs which calculate cryptographic checksums across a large proportion of the files in the file system can be used for integrity checking. Tools offering this functionality under Unix include the *tripwire* program, for example, some versions of which are also available free of charge, or the tool developed on behalf of the BSI for secure Unix administration (USEIT). Comparable programs are also available for the Windows NT operating system. Apart from the file system, it should also be possible to subject the registration keys to an integrity test.

tripwire and USEIT can detect any change to a file system because the checksums no longer match when a change has been made. They not only test whether a file has been modified, they also detect any change to access rights, or if data has been deleted and subsequently reloaded. Given a special setting, all accesses to a file, even read accesses, can be detected in most cases.

In order to prevent the possibility of the program or checksum file being corrupted by an attacker, they should be located on a data medium that optionally allows only read access. However, the checksum file also has to be changed when changes are made to the file system, so floppy disks are recommended for small file systems and removable hard disks for larger systems.

An integrity check should be performed regularly, for example every night. Notification of the outcome should be sent automatically to the administrator by e-mail, even if no changes have been detected.

Additional Controls:

- Which integrity checkers are used?
- How often are the results of the integrity checkers examined?
- How are the checksum file and the program itself protected against manipulation?

S 4.94 Protection of WWW files

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The files and directories on a WWW server must be protected against unauthorised changes, but also - depending on the security requirements - against unauthorised access.

General aspects

If scripts are attached via *cgi-bin*, it is essential to ensure that programming is secure in order to prevent the scripts from being used to circumvent the server's protection mechanisms. One possible means of making unauthorised access more difficult is to run the scripts under a user ID which only has access to selected files. It is particularly important to protect the configuration files, because otherwise it is easy to deactivate all access restrictions.

The read rights and write rights for the WWW files should allow only authorised users access, as local files.

Protection against unauthorised changes

On a typical WWW server, only the log files are subject to constant change; all other files are static. This applies in particular to system programs and the WWW pages. Although WWW pages are regularly updated, they should not be edited on the WWW server itself.

In order to ensure that no files can be modified on the WWW server without this being noticed, checksums should be formed for all static files and directories (for example with a program such as *tripwire*; see also S 4.93 *Regular integrity checking*) and should be checked at regular intervals.

In order to prevent the possibility of WWW files being modified by unauthorised third parties at all, static data can be stored on a write-protected storage medium (such as a CD-ROM or a hard disk with write protection).

Protection against unauthorised access

Access to files or directories on a WWW server can be protected in various ways:

- Access can be restricted to freely selectable IP addresses, subnetworks or domains.
- User-specific IDs and passwords can be assigned.
- The files can be stored in encrypted form and the associated cryptographic keys only made known to the target audience.

Authentication by means of addresses

Authentication by means of numerical IP addresses does not offer the protection of cryptographic procedures because it can be rendered ineffective by an attack based on IP spoofing. IP spoofing involves an attacker falsifying IP packets in order to pretend that they originate from a trustworthy IT system (see T 5.48 *IP spoofing*). However, a firewall can be used to prevent external users from pretending to be internal users. If access is not restricted to

numerical IP addresses or subnetworks but to certain computer names or domain names instead, attention should also be paid to the risk of DNS spoofing.

If the WWW browser accesses the WWW server via a proxy server, it should be borne in mind that the WWW server only finds out the IP address of the proxy. A proxy can only be considered trustworthy, however, if all IT systems and users hidden behind it are also trustworthy.

If access to WWW files is restricted to specified IP addresses, subnetworks or domains, it may therefore be advantageous to give these additional protection with a password.

Password protection

In order to protect WWW files with passwords, it is first necessary to create a password file in which the authorised users and their passwords will be entered. It is vital that this file should not be stored in areas of the WWW server which could possibly be accessed from the outside. The file must be readable for the Web server, however. It is advisable to create a separate directory for these password files. Only the owner of the file and the WWW server are allowed to access the files stored in that directory.

One problem with the protection of WWW files by means of passwords is that the authorised users have to handle their passwords carefully; for example they must not pass them on, but must keep them safely, change them regularly and select them with care (see S 2.11 *Provisions governing the use of passwords*). Another problem is whether and how passwords can be protected against interception during transmission. Passwords must under no circumstances be transmitted within a URL.

If possible it is advisable to use authentication via addresses in addition.

Encryption

Another possibility is storing files in encrypted form on a WWW server, such that only users who are in possession of the correct cryptographic key are able to read the files. This approach does require a corresponding system of key management, however, which may be complex and costly.

Procedures such as SSL or S-HTTP can be used to prevent interception of the files and passwords during transmission.

S 4.95 Minimal operating system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Computers in a security-critical environment should be designed so as to present as few targets for attack as possible. As today's operating systems provide many network services as standard, a well thought-out server service (such as an SSL-based Web server) is not sufficient for the operation of a secure server. It is also necessary to safeguard the operating system, because otherwise the security functions of the server service could be evaded via a weak point in the operating system. The characteristic feature of what is referred to as a minimal operating system is that ideally it does not provide any form of network service. A potential attacker will therefore be unable to exploit a weak point in a network service belonging to the operating system. Even if an attacker does gain access to the computer via a weak point, he will be further impeded by the minimal system. The fewer programs an attacker finds on a target computer, the more difficult it is for him to locate and exploit further weak points on that computer. Furthermore this also greatly facilitates maintenance of the server, because the patches or service packs for utility programs no longer have to be loaded if the programs are not there.

The following sections describe the configuration of an operating system using the example of an Internet server, because in this case the security requirements imposed on the operating system are generally very high.

An Internet server usually has only one task: making a certain number of services (such as the readiness to receive e-mails) available to other computers in a stable manner. The underlying operating system should not provide any other services. The following procedure should therefore be observed when installing an Internet server:

1. Basic installation of the operating system

   If it is possible to influence which packages are actually installed during installation, only the necessary packages should be loaded at this stage. It is not always easy to establish the necessity of certain packages, however, so at least those packages which are obviously superfluous should not be loaded.

2. Deactivation of unnecessary programs

   When a computer is started up, a large number of programs are launched automatically. Some of these programs are entirely irrelevant for an Internet server and should be deactivated. They can be deactivated by preventing automatic launching (start scripts under Unix, Startup and Service Manager under Windows NT) and by additionally deleting the corresponding programs. For security reasons it is recommended to delete them, because then an attacker will not be able to reactivate the services. However, it is sometimes very difficult to find and delete all of the files belonging to a particular service, so if there is any doubt the files should not be deleted.

3. Configuration of the network parameters

   The network parameters of the Internet server must be set, if this has not already been done at the time of installation. The parameters relevant to the security of the Internet server include the selection of a default gateway and a domain name server. For example, if communication between the Internet server and the Internet takes place via a proxy (see S 2.73 *Selecting a suitable firewall*), a default gateway is superfluous. Without a default gateway it is not possible to send a direct response from the Internet server onto the Internet, so that if the proxy is bypassed no communication can take place, and therefore also no attack. DNS is often also superfluous for an Internet server and should be avoided if possible, because it allows the establishment of a direct communication channel to the operating system (see S 4.96). In addition there are a great many other parameters which have a direct influence on the TCP/IP stack, for example the maximum size of IP packets. These parameters are very heavily dependent on the respective operating system, so at this stage all that can be mentioned is the deactivation of IP forwarding. Other changes could enhance stability when dealing with errored IP packets, for example, or also increase network throughput.

4. Deactivation of unnecessary network services

   Some essential utility programs provide a large number of other services (this refers in particular to *inetd* under Unix). The corresponding configuration files must be restricted to those network services that are necessary (see also S 5.16 *Survey of network services*).

5. Installation of security programs

   The operating system should be extended with additional security programs, if they are not already part of the operating system. Particularly useful additions include an integrity checking program (see S 4.93 *Regular integrity checking*) and a software packet filter (already included in Windows NT). Programs to scan for viruses and to evaluate log entries are also worth recommending. If remote administration of the Internet server is required, a security product to cope with this must be installed, for example the Secure Shell daemon (see S 5.64), and the security of the system must be checked at regular intervals (see also S 4.26 *Regular security checks of UNIX systems*).

6. Configuration and checking of network services

   Ideally, a minimal operating system should not provide a single network service, and would therefore not be vulnerable to attack from the outside. Especially in relatively large networks, this approach is not practicable for administration reasons, so remote access is in fact necessary. Under both Unix and Windows NT, the *netstat -a* command can be used to check whether the Internet server provides such services. The configuration of each of the listed services should be restricted in such a way that only authorised computers are able to access them (for example, remote access to the Internet server should be limited to the network management computer).

7. Deletion of programs that are no longer required

As soon as the installation of a minimal operating system is complete, various programs which could be helpful to a potential attacker should be deleted. In particular, any compilers which may be present should be removed, because these could be a valuable tool for an attacker. Besides, another reason why it is not advisable to have compilers on Internet servers is that these computers are production machines, and program development and tests should be carried out on other computers. It is also conceivable to delete all editors, which would make it very much more difficult for an attacker to manipulate configuration files. If the editors are deleted, though, administration is also more complicated. If changes need to be made to configuration files, an editor has to be installed on a case-by-case basis, or alternatively, and this is recommended, the configuration files have to be edited on a different computer and then transferred.

A minimal operating system should of course not be an end in itself. It goes without saying that, for an Internet server, the server service itself still has to be installed. It depends on the particular installation whether this is done at the end of the above list or between points 6 and 7, for example, or even immediately after point 1. It becomes problematical if the installation fails because of the absence of operating system packages, because in that case the missing packages have to be located and reinstalled manually. It would be better if the vendor of the server service specified the operating system dependencies, so that the minimal system could be brought into line with these from the outset.

Even a computer configured with a minimal system is not entirely protected against attacks. The most probable cause of a successful attack is no doubt the server service, but also the minimal system itself is still open to attack, in particular the TCP/IP stack, which has to forward the network packets to the application. Almost all attacks against the TCP/IP stack that have so far come to light, however, have only affected availability, with the computers concerned being caused to crash; this means that infiltration of computers has not yet been observed. In order to reduce even this risk yet further, S 4.98 *Restricting communication to a minimum with packet filters* should also be implemented.

S 4.96 Deactivating DNS

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

An Internet server does not normally need a DNS (Domain Name System) in order to provide information, unless it is used to send e-mail, but this is not advisable (see also S 4.97 *One service per server* in this connection). On most WWW servers, DNS is only used for entering computer names instead of IP addresses in the respective logging files. The conversion of IP addresses into computer names in this way could also be performed later during the analysis of the logging files. Although handling of the logging files is then a little more cumbersome, the integrity of the logging data is increased. This is because the allocation of an IP address to a computer name is neither unique nor static. Dispensing with DNS provides additional protection against DNS spoofing (see S 5.59 *Protection against DNS spoofing*) and often boosts the performance of the Internet server.

The following scenario illustrates possible negative consequences:

Let us assume that an attacker has his own domain with a test PC. At the same time, the test PC is also the DNS server for this domain. He uses the test PC to establish a connection to an Internet server. At the start of the connection request the Internet server only knows the IP address of the test PC, and tries to obtain the computer name of the test PC via DNS. To be able to do this, the operating system has to take up a connection to a DNS server, which in turn has to retrieve the data from the test PC, because the latter is the DNS server for the attacker's domain. Instead of replying to the DNS server of the Internet server, the attacker can now also send any response directly to the Internet server itself (using IP spoofing; see T 5.78). In this way the attacker is able to send data not only to the DNS server as such but also directly to the Internet server. Any flaws in the Internet server's operating system could therefore be exploited.

Note: If for example access is to be allowed to a WWW server in only one specific domain, for example only *.de, it is not possible to dispense with DNS. Access protection of this nature is very weak, however, and is therefore not recommended.

S 4.97 One service per server

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Many weak points in IT systems cannot be exploited in isolation by a potential attacker. It is often only a combination of vulnerabilities that makes successful infiltration of a computer a possibility. One recommendation for the operation of secure servers is therefore: different services should be located on different computers.

Only one service should therefore be loaded on a minimal system (see also S 4.95 *Minimal operating system*), i.e. for example either a WWW server or an e-mail server. Besides this, the security classifications of individual services also vary. Successful infiltration of a WWW server may well be very annoying, particularly if the attacker makes changes to the WWW pages that are externally accessible. The attacker does not have access to internal information in this way, however. If the WWW server is also the e-mail server, though, the attacker may be able to intercept all of the e-mail traffic, which could have much worse consequences.

The separation can even be further increased, by sharing different tasks of an individual service between different computers. For example, there could be one e-mail server (A), which receives e-mails from the Internet and forwards them to the internal network, and another e-mail server (B), which forwards e-mails from the internal network to the Internet. As communication from the Internet can only be established with e-mail server A, an attacker can only attack that server, not the other. E-mail server A is not itself allowed to send any e-mails to the Internet, and therefore this computer cannot be misused for e-mail spamming, either.

Dividing up various services between different computers has the following advantages, among others:

- Easier configuration of the individual computers
- Simpler and more secure configuration of an upstream packet filter
- Increased resistance to attacks
- Greater operational reliability

It should be possible to compensate for any negative consequences that may arise, such as higher hardware costs for purchasing several computers, by the fact that the individual computers do not have to produce the same performance and consequently all in all, with the same performance, do not have to be more expensive than one particularly powerful computer. Administration costs do not necessarily have to rise with the number of computers, either, because simpler configuration of the individual computers saves time.

S 4.98 Restricting communication to a minimum with packet filters

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Packet filters are IT systems with special software which filter the information of the lower layers of the OSI model and pass on or intercept packets in accordance with special rules (see S 2.74 *Selection of a suitable packet filter*).

The configuration of a packet filter that is used to protect Internet servers should be very restrictive, so as to maximise resistance to attacks. Although a well-configured Internet server (see S 4.95) should be able to protect itself against attacks, the software on an Internet server is much more complex and more susceptible to errors than that of a packet filter designed for security. The packet filter should only allow those communication channels through which are necessary for operation of the Internet server. In particular, it is necessary to control not only communication that is initiated from the Internet to the Internet server, but also communication which the Internet server is allowed to set up to the Internet. For many attacks it is a necessary precondition that the attacked computer must be able to establish new connections to the Internet. If this is not possible, many attacks will not be successful. In 1997, for example, an attack on a news server was very "popular", where the attacker was able to exploit an error in a news daemon to have important system information sent to him by e-mail. If the attacked computers had not had the authorisation to send e-mails, the attacker would not have received a return message. The attack would not have succeeded.

A few examples of the configuration of packet filters for various Internet servers are shown below.

1. WWW server:
   Internet has access to port 80 of WWW server TCP
   WWW server has access to Internet from port 80 TCP/ack, nothing else!
2. News server:
   Newsfeed servers have access to port 119 of news server TCP
   News server has access from port 119 to newsfeed server TCP/ack
   News server has access to port 119 of newsfeed server TCP
   Newsfeed servers has access from port 119 to the news server TCP/ack
3. E-mail server (provider makes e-mail gateway available):
   E-mail server of provider has access to port 25 of e-mail server TCP
   E-mail server has access from port 25 to provider's e-mail server TCP/ack
   E-mail server has access to port 25 of provider's e-mail server TCP
   Provider's e-mail server has access from port 25 to e-mail server TCP/ack
4. E-mail server (sending to Internet itself):
   Internet has access to port 25 of e-mail server TCP
   E-mail server has access from port 25 to Internet TCP/ack
   E-mail server has access to port 25 in Internet TCP
   Internet has access from port 25 to e-mail server TCP/ack

If these rules are implemented alone, the establishment of communication from the Internet is restricted to the enabled services. If the communication partners can be further restricted (see above examples 2 and 3), an attacker cannot set up any direct connection to the Internet server at all.

Note: The above rules may have the effect that the Internet server cannot be reached from every computer because ICMP is not let through. It is therefore advisable to let the ICMP subtype *icmp unreachable* through from the Internet to the Internet server.

S 4.99 Protection against subsequent changes to information

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators, users

Files which are passed on to third parties can generally also be edited by those third parties. This is not always in the interest of the creator of the files. A form of protection against subsequent changes, the forwarding of extracts or further processing would therefore be desirable.

A problem that is often encountered is that information is made available to third parties via the Internet or other networks, but it may not be intended that it should be printed out hundreds of times or integrated seamlessly into other documents.

There are various solutions to this, which in some cases can also be combined with each other. Examples here are:

- Using digital signatures in order to prevent changes from being made to files without this being noticed (see also S 4.34 *Using encryption, checksums or digital signatures* or S 3.23 *Introduction to basic cryptographic terms*).
- Adding copyright notices to WWW information or files. These can be formulated as follows: "This document and all of its parts is protected by copyright. Any use of the document outside the constraints of the Copyright Act without the approval of the author is inadmissible and punishable." and "Copyright (©) 7/1999 by BSI".
- The use of file formats which make it more difficult to make subsequent changes or edit extracts in any way. Postscript can be used for this, for example, or the security properties of application programs, such as in the case of PDF files.

  PDF documents can be assigned access restrictions when they are created. The opening, printing or copying of PDF files can be inhibited, for example.

  Two types of password can be assigned with Acrobat Exchange, i.e. the application with which PDF files can be created and edited. One type of password is required for opening the document, and the other for changing the security attributes. PDF documents that are protected against unauthorised opening are encrypted with RC4. The following functions can be inhibited using the security attributes:

  - Printing
  - Modifying the document
  - Selecting text or graphics
  - Adding or changing notes and form fields

In this way it is very easy to restrict rights so that no-one can take over the contents of a publication by cutting and pasting. If in extreme cases even printing is prevented, all that can be done is read the file on-line.

Unfortunately this offers only rudimentary protection, because PDF files can also be opened with programs which ignore these security attributes. As long as printing is allowed, for example, the document can even be converted back into a PDF file at any time, with no restrictions whatsoever.

S 4.100 Firewalls and active content

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

One of the biggest difficulties with the conceptual design of a firewall is how to deal with problems that arise as a result of the transmission of active content to the computers in the network requiring protection. This includes not only the detection and eradication of computer viruses, which can be carried out relatively easily, even on users' computers, but also the much more difficult problem of detecting ActiveX controls, Java applets or scripting programs with damaging functions. At present there are still no practicable programs for this purpose, none which enable the effective detection of damaging functions similar to that which is possible in the area of computer viruses.

The magnitude of the danger originating from active content for the computers in the network being protected can be illustrated with the aid of the following example. In accordance with the Java specifications, a Java applet or the browser is allowed to establish a network connection to the server from which it was loaded. This possibility, although still very rarely used at the moment, is a key prerequisite for the use of network computers (NCs) or similar equipment which have to load programs from the server without this being specifically initiated by the user. In order to be able support this property in full despite the use of a packet filter, a great many more port numbers have to be enabled or it is necessary to use a dynamic packet filter. If this is the case, Java applets can be used to enable the establishment of barely controllable IP connections.

There are essentially two approaches to countering the problems of "active content with damaging functions". Firstly, control and therefore also responsibility for execution can be shifted to the users, who have the option in their browsers of disabling the active content and only reactivating it when they are sure that individual offers are „trustworthy". The main problem with this solution is, how is it possible to establish which providers are trustworthy and which are not.

The other possible method of controlling active content is to use an appropriate filter in conjunction with a firewall. Proxy processes, by dint of their design, are basically very well suited to analysing the transmitted user data. The corresponding programs are called up within an HTML page using special tags (tag = label for structures within an HTML page). It is also conceivable to use a solution where all lines with corresponding tags are deleted from an HTML page or are replaced by output lines which indicate to the user that the required Java applet has been blocked by the firewall.

The problem with this approach is that it is not easily possible to recognise all HTML pages and, in turn, to recognise all tags that are to be deleted on those pages. For example – and this occurs frequently nowadays – HTML pages can be sent as the contents of e-mails. Intelligent e-mail programs recognise this and automatically start a browser which can display the HTML page, and which then of course also runs the Java applet or ActiveX control. It is also

not easy to detect a special tag within an HTML page, because of the complex possibilities available in the current HTML version.

Unfortunately, Java applets are not consistently sent as files with the suffix *.class*. Instead it is also possible to use compressed files, which may have the suffix *.jar* (Java archive) for example. This means that a Java filter also has to know and take account of all of the compression methods supported by the browsers that are used.

Another alternative for detecting programs with active content with damaging functions is to create a database with signatures, in much the same way as for programs designed to protect against computer viruses, and to compare every program downloaded from the Internet against these signatures. Unfortunately this procedure is still very much in the early stages of development, and it remains to be seen whether the resultant programs will be as effective as the programs providing protection against computer viruses.

Further potential danger results from the possibility of running JavaScript from within Java. The effectiveness of graduated filtering of Java and JavaScript should therefore be examined.

S 4.101 Firewalls and encryption

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

As it is impossible to predict the routes and nodes via which data will be sent over the Internet, data should always be encrypted before it is sent if at all possible. It would be useful if mechanisms to ensure that this is done were already provided in the lower layers of the protocol.

First, though, a distinction should be drawn between two approaches to encryption:

- Encryption at the firewall or on network switching elements that can be used for setting up secure subnetworks
- Encryption on the terminal equipment that is utilised by users as the need arises, for example

Encryption at the firewall

In order to exchange data with external communications partners via an open network and/or to grant these partners access to your own network, it may make sense to set up virtual private networks (VPNs). All connections to and from these partners should be encrypted, so that no unauthorised users can gain access to the connections. A large number of hardware and software solutions can be used to set up encrypted connections. If it is intended to connect only a few properties to each other, hardware solutions based on symmetric cryptographic procedures, in particular, are a simple and safe choice.

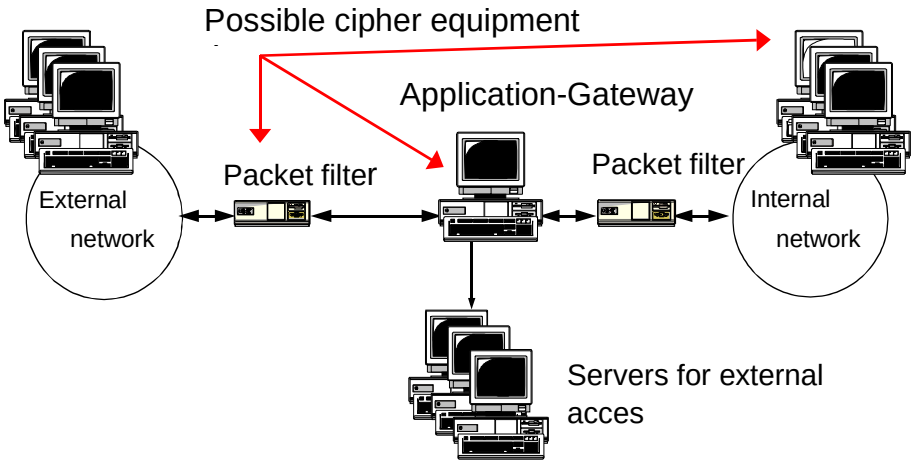


Figure: Integration of a crypto module into a firewall

Encryption and decryption can be performed on different devices. For example, a hardware solution in the packet filter could be used as the cipher equipment. This makes sense in particular in cases where no unencrypted communication is to be allowed via the device.

In contrast, the integration of encryption on the application gateway has the advantage of easier user administration. Furthermore, an attacker who has

gained control of an external information server cannot eavesdrop on the encrypted communication.

Encryption on the terminal equipment

In order to protect the confidentiality of certain data, especially when sending e-mails, another option that suggests itself is the use of mechanisms that allow end-to-end encryption. The freely available software package PGP (Pretty Good Privacy) is very often used for this, for example (see S 5.63 *Use of PGP*). To ensure trustworthy data exchange with selected partners on the Internet, modified *telnet* and *ftp* programs should be used, which support encryption of the data being transmitted.

For the foreseeable future, encryption on the end systems will still be tied to specific applications, for example through the use of SSL or PGP. On the other hand, however, the encryption of data also presents a major problem for the effective use of firewalls, i.e. the filters. If the transmission of encrypted data via the firewall is permitted (as is the case with SSL), filters on the application layer are no longer capable of checking the user data with respect to viruses or other harmful programs, for example. The logging options available are also greatly restricted by encryption. An initial ad hoc solution could take the form of allowing SSL connections to be set up from certain internal computers, perhaps only to selected destination systems. On the other hand the data is protected even if an attacker has gained control of the application gateway.

Temporary decryption on a filter component for analytical purposes is neither practicable nor desirable.

No general recommendation can be given for against the use of encryption via or at a firewall; this is dependent on the requirements applying in each individual case.

Advantages and disadvantages of various possible implementations

At firewall:		**On terminal equipment:**	
+	Central data validation	+	End-to-end security
+	Central key distribution	+	No protocol problems
+	Detailed accounting	+/-	User-dependent
-	Access from the firewall to the internal network	-	No possibilities of checking at the firewall
-	No end-to-end security	-	Public key infrastructure required

S 4.102 C2 security under Novell 4.11

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Certain standardised evaluation criteria have become established for the assessment of IT products and IT systems: the US criteria known as TCSEC (Trusted Computer System Evaluation Criteria) and the European version, ITSEC (Information Technology Security Evaluation Criteria), which in the meantime have been further developed to become the CC (The Common Criteria for Information Technology Security Evaluation). In the autumn of 1997 Novell Netware 4.11 received a certification in accordance with functionality class C2 of the TCSEC from the *National Computer Security Center* (NCSC); this corresponds to ITSEC class F-C2/E2.

The use of a certified product provides a guarantee that the security functionality of the product has been independently tested and does not fall below the standard specified in the evaluation level (see also S 2.66 *Consideration of the contribution of certification to procurement*).

Frequently encountered standard cases are grouped together as functionality classes in these security criteria. The requirements of functionality classes F-C2 are essentially intended for operating systems. They include definitions of the following features, for example:

- Adoption of the C1 specifications
  - Existence of mechanisms for restricting access by users to certain documents
  - Identification of users
- Refinement of access rights
- Auditing of all security-related events with time stamp, user name, object and message indicating whether successful or unsuccessful
- Administration of audit files (access protection, control of size, etc.)
- Delimitation of resources (access protection)
- Delimitation of data from different processes with respect to other processes even after sharing

The observance of these specifications is checked with special test procedures.

However, acquiring a C2-certified product is not sufficient in itself to achieve C2 security. The key factor for actually putting a C2 system into practice is the precise implementation of the specifications of the certification report.

The security options necessary for achieving C2 security with Netware 4.11 were summarised in the file named SECURE.NCF. The following sections look more closely at the SECURE.NCF file and explain the individual options.

The SECURE.NCF file and its options

To enable a Novell Netware 4.11 server to utilise the extended security mechanisms, attention should be paid to the following points:

- The SECURE.NCF file must be stored on the server in SYS:SYSTEM.
- The SECURE.NCF file is an executable file similar to a batch file under DOS, and should therefore only be edited with an ASCII editor (e.g. EDIT.NLM).
- The line "SET ENABLE SECURE.NCF=ON" must be inserted into AUTOEXEC.NCF to call the SECURE.NCF file. Alternatively, the command "SECURE" can also be inserted into AUTOEXEC.NCF or this command can be issued on the server console.

The extract from the SECURE.NCF file given below shows only the commands contained in the file. The original file contains a brief explanation of each command.

```
SET ALLOW UNENCRYPTED PASSWORDS = OFF

SET ALLOW AUDIT PASSWORDS = OFF

SET AUTOMATICALLY REPAIR BAD VOLUMES = ON

SET REJECT NCP PACKETS WITH BAD LENGTHS = ON

SET REJECT NCP PACKETS WITH BAD COMPONENTS = ON

SET IPX NETBIOS REPLICATION OPTION = 0

SET ADDITIONAL SECURITY CHECKS = ON

# SET CHECK EQUIVALENT TO ME = ON

# SET NCP PACKET SIGNATURE = 3

# SECURE CONSOLE

## DISPLAY NCP BAD COMPONENT WARNINGS

## DISPLAY NCP BAD LENGTH WARNINGS
```

All command lines that are commented out with "#" are additional security parameters and are not necessary for observance of the C2 or F-C2/E2 provisions. Command lines that are identified by "##" do not form part of the standard scope of the SECURE.NCF file, but they represent a meaningful benefit in everyday use.

The commands in detail

All commands and SET statements can also be issued at the console or be set using the SERVMAN.NLM or MONITOR.NLM program.

All SET parameters in the SECURE.NCF file are described below, and the default values are also specified.

SET ALLOW UNENCRYPTED PASSWORDS = OFF (Default=OFF)

The purpose of this parameter is to ensure the compatibility of Netware 2.x clients and print servers. The consequence of setting the parameter to ON is

that a password that is necessary for authentication can be transmitted to the server without being encrypted. This favours unauthorised infiltration into the system concerned. The default value of OFF ensures that each password has to be encrypted during the login procedure. Unencrypted passwords are not accepted.

SET ALLOW AUDIT PASSWORDS = OFF (Default=OFF)

This parameter is connected to the auditing mechanisms of the Netware operating system. During auditing, changes to (or manipulations of) objects are recorded in accordance with the specifications of the configurations by means of the AUDITCON.NLM program. Given the appropriate authorisations, which can be set individually for each auditor in the general assignment of rights for the operating system, an auditor can be put in a position to read the auditing file. The authorisation in each case restricts the scope of what can be read. The effect of the default value OFF is that the auditor does not have to identify himself with an additional password.

SET AUTOMATICALLY REPAIR BAD VOLUMES = ON (Default=ON)

This parameter instructs the operating system to repair a volume that cannot be mounted on system startup by invoking the VREPAIR.NLM program. This ensures that after an uncontrolled system crash and the subsequent restart, possible errors on volumes (data areas in the disk packs) will be rectified without additional intervention by the system administrator.

SET REJECT NCP PACKETS WITH BAD LENGTHS = ON (Default=OFF)

The effect of this parameter when set to ON is that NCP packets with the incorrect length will be rejected. This may lead to errors with older applications (utilities).

SET REJECT NCP PACKETS WITH BAD COMPONENTS = ON (Default=OFF)

The effect of this parameter when set to ON is that NCP packets with incorrect components will be rejected. In this case, too, there may be errors with older applications (utilities).

SET IPX NETBIOS REPLICATION OPTION = 0 (Default=2)

This parameter specifies the procedures that the IPX router is to use for dealing with NetBIOS broadcast messages. The following values are available for selection:

0 = No replication of type 20 IPX packets

1 = Replication of type 20 IPX packets to all available network adapters

2 = Replication of type 20 IPX packets with two special filter functions
a) Reverse Path Forwarding: type 20 IPX packets from the same source are forwarded only once to all available network cards, even if the packets have been received via different network adapters.
b) Split Horizon: type 20 IPX packets are not routed back into the network from which they were received.

3 = Replication as for option 2, but not via long-distance links

SET ADDITIONAL SECURITY CHECKS = ON

This parameter activates additional security checks which are incompatible with earlier NDS versions.

The parameters listed above are absolutely mandatory for observance of the security certification in accordance with class C2 and class F-C2/E2. The parameters in the following can be used for extending the security functions.

SET CHECK EQUIVALENT TO ME = ON (Default=OFF)

This parameter forces checking of the NDS attribute "Equivalent To Me" on the server. If the value for extended security is set to ON, the attributes "Equivalence" and "Equivalent To Me" must be synchronised with the DSREPAIR application. Activating this option may possibly have detrimental effects on the system's authentication speed.

SET NCP PACKET SIGNATURE = 3 (Default=1)

Communication between a Novell Netware client and a Novell Netware server is controlled by the Netware Core Protocol (NCP). The client and server exchange individual packets which contain data. A potential attacker can monitor these packets by using special programs (see T 5.58 *"Hacking Novell Netware"*) and can manipulate packets belonging to users with higher privileges.

The packet signature was developed to counteract this threat. When a user logs on to the network, a secret key is determined. Whenever a workstation then sends an inquiry to the network using NCP, it is provided with a signature formed from the secret key and the signature of the previous packet. This signature will be attached to the relevant packet and sent to the server. The server will verify the packet signature before dealing with the actual inquiry.

The packet signature can be activated on the server with this parameter. The following NCP packet signature levels are possible:

0 = There are no NCP packet signatures.

1 = The Novell Netware server uses NCP packet signatures at the request of the client.

2 = The Novell Netware server requires an NCP packet-signature from the client. If the client cannot supply one, communication between the client and the Novell Netware server is nonetheless allowed.

3 = The NCP packet signature is mandatory.

To guarantee security, the value for the NCP packet signature should be set to 3. The Novell Netware server and the client sotware on the workstations must be configured accordingly. However, as use of the NCP packet signature increases network load, it should be clarified beforehand whether performance will be reduced unacceptably as a result.

SECURE CONSOLE

This command triggers several functions. It should therefore only be executed on security-sensitive systems. The functions are:

1. All search path extensions are reversed. Only the search path to the SYS:SYSTEM drive is then available for invoking NLMs.
2. A search path extension with the SEARCH ADD command is no longer possible.
3. Changing various server parameters with the SET command is no longer possible.
4. Changing the system time and system date is no longer possible.
5. The system debugger can no longer by called using the special key combination.

Note: because SECURE CONSOLE reduces the search paths to the system minimum, considerable problems may arise with server applications which require a special search path extension.

DISPLAY NCP BAD COMPONENT WARNINGS

This parameter instructs the server to display a warning message on the console when NCP packets are received with invalid content or parts of the content. This could indicate that attacks have taken place.

DISPLAY NCP BAD LENGTH WARNINGS

This parameter instructs the server to display a warning message on the console when NCP packets are received with an invalid length. This could indicate that attacks have taken place.

S 4.103 DHCP server under Novell Netware 4.x

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Setting up TCP/IP protocols involves considerable effort if the IP address, the subnetwork mask, the default gateway etc. have to be assigned manually for each workstation. If it is intended to change only the default gateway entry in a particular segment, for example, this requires a great deal of work and also increases the risk of incorrect inputs being made. These tasks can be centralised and automated through the use of a DHCP (Dynamic Host Configuration Protocol) server.

In order to ensure reliable handling of the DHCP server from Novell Netware 4.x, it is necessary to know the structure of the TCP/IP network whose addresses are to be administered with the aid of the DHCP server. The important features here, apart from the address class (TCP/IP network class A - C), are also the subnet masks that are used and the addresses of the default gateways, so as to allow cross-segment data traffic on the basis of TCP/IP.

The following sections examine certain aspects relating to the configuration of the DHCP service under Novell Netware 4.x that are of particular relevance to the security of the system as a whole.

Configuration of TCP/IP segments

The TCP/IP segments that are to be managed by the server are defined using the SUBNETWORK PROFILE option. Values such as the subnetwork name, address range and type of assigment are read out automatically from the configuration menu of the DHCP server when it is started up. If the DHCP server is supposed to take care of several IP segments, it is advisable to delete the values that are read in automatically and to replace them with "meaningful", manually configured values. For example, if "3CX9_1_EII" is read out as the subnetwork name, it is easier for troubleshooting and for subsequent configuration work on that segment if this entry is replaced manually by an entry that describes the segment better, such as the name "EthernetII". It is also possible to use other descriptive naming conventions, which designate a segment according to its topological arrangement, for example (Building A, 2nd floor or Management).

Automatic assignment of IP addresses

One of the key services of the DHCP server is the automatic assignment of IP addresses. The AUTOMATIC IP ADDRESS ASSIGNMENT parameter identifies the address range from which the DHCP server dynamically distributes the addresses to the network nodes that request an address. This range should be chosen such that the addresses for servers, printers and routers are not included within the range of dynamic allocation. The general rule is that servers, printers, routers and the network nodes with dynamic address assignment should be assigned clearly distinguishable IP address ranges. This ensures that it is obvious from the address range alone which type a network node belongs to, if problems arise in the IP area.

Static assignment of IP addresses

For certain components in the network it is advisable to link the required IP address permanently to the MAC (Medium Access Control) address of the network node by means of static address assignment. Such components include network printers and routers, for example. The advantage of static assignment by a DHCP server in comparison with local manual configuration at the network node is the ability to carry out central administration of the assignments with the DHCP server configuration tool. Although static assignment of their IP address is also mandatory for servers, these addresses are not assigned via the DHCP server. The IP addresses of Netware servers are always assigned manually.

Configuration of the static address assignments is carried out with the IP ADDRESS ASSIGNMENT option. The node is added to the menu using any required name, and the IP address is linked directly to the network card (MAC address) of the node. When choosing the name, Novell recommends using the login name of the user who works at that workstation.

Lease time

The lease time determines how long a network node that receives its TCP/IP address from the DHCP server dynamically can retain that address. The assignment of the IP addresses is implemented on booting of the network node. A period of at least 24 hours should be chosen for the lease time, because otherwise the following problems may occur:

- Programs whose access rights are granted on the basis of TCP/IP addresses may no longer be executable after the computer is rebooted because the IP address of the computer accessing it has changed. The new address may not have the authorisation to execute the program.
- If workstations are unstable in operation and have to be restarted several times per day, an unnecessary burden is imposed on the network after every restart as a result of the assignment of a new IP address.
- During access to the Internet, intermediate proxy servers log the Internet pages that have been opened from the workstations. In the resultant logging files, the DNS names of the opened Internet pages are usually assigned to the IP addresses of the computers from where the pages were requested. If these IP addresses constantly change, in the event of a problem it is very difficult to track back to determine which workstation was assigned the corresponding IP address at what time.

It is necessary to designate a lease time when using DHCP servers if a network contains more nodes than there are IP addresses available. Through the use of an appropriately chosen lease time, an IP address that has become free because the node no longer needs it (the PC has been switched off) can be assigned to a different node that requests an address from the DHCP server. In networks that have at least as many IP addresses available as nodes are installed, the configuration of a lease time can be dispensed with. For some time it has been possible to work in LANs with "private" IP addresses (see RFC 1597). The problem of having more nodes than IP addresses can therefore be avoided. The assignment of private IP addresses according to these specifications may be advisable for auditing reasons, for example, for

networks which implement an Internet access. Attention must be paid to aspects of data privacy law and the right of co-determination.

At present it is not yet possible to deactivate lease time in the Netware 4.x DHCP server. It is therefore recommended to set it to the maximum value of 10,000 days and 23 hours.

Exclusion of specific network nodes from address assignment

The assignment of an IP address can be prevented for certain network nodes. To do this, the same steps have to be carried out under the EXCLUDED NODES menu item as described for the static assignment of IP addresses. This has the effect that certain programs based on TCP/IP cannot be invoked from those workstations. This "block" is easy to infiltrate, however, by assigning an IP address manually to the "blocked" network node (provided the TCP/IP protocol stack has been loaded on that node). As soon as a free IP address is found in the course of manual assignment, communication is just as possible with this computer via TCP/IP as with nodes which have received their IP addresses from the DHCP server. The method of excluding network nodes from the assignment of an IP address using EXCLUDED NODES therefore offers only a relative degree of security.

In addition, blocking MAC addresses for assignment by the DHCP server can also be used to control load balancing in networks with several DHCP servers. It is also possible to prevent nodes which have their own DHCP server in their segment from requesting an IP address from a DHCP server located in another segment. It should be borne in mind that in this case in the event of failure of the local DHCP server no IP address can be assigned to local clients. Use of the EXCLUDED NODES option therefore calls for careful planning.

DHCP service in routed networks

An intermediate router located between the segment of the DHCP client and the segment of the DHCP server may in some cases suppress the DHCP request. Routers which are RFC 1542-compatible have an agent known as the DHCP/BOOTP relay agent. This agent ensures that DHCP relay packets are routed further as required. In the case of routers that are not RFC 1542-compatible, separate DHCP servers must be defined in every network segment. An IP address is then assigned by the DHCP server in the same way as in non-routed networks. Forwarding of the DHCP relay packets does not mean, however, that all broadcast packets are automatically forwarded. "Normal" broadcast data packets are still filtered out by the router.

Use of multiple DHCP servers in networks

In networks of a sufficient size, in certain circumstances it may be appropriate to work with multiple DHCP servers. In some operating systems the administration of 10,000 IP addresses per DHCP server is considered to be the upper load limit. This figure can be exceeded by the Netware DHCP server many times over. In addition, when considering how many DHCP servers are required in the network, account should be taken of the positions of the routers.

Irrespective of the structure of the IP network, whenever multiple DHCP servers are used it is essential to prevent two (or more) network nodes that are

"supplied" from different DHCP servers from being assigned the same IP address. This risk applies if every DHCP server in the network (or in the segment) each administers the entire IP area that was set up for dynamic assignment, because the DHCP servers are not synchronised with each other under Netware 4.x. Each individual DHCP server stores its configuration data in a separate DHCPTAB file. However, as this file is not part of NDS under Netware 4.x, it is not distributed to other servers using its replication mechanisms, either, nor is it compared with other DHCPTAB files. If multiple DHCP servers are used, therefore, each server should be assigned its own IP address range which it administers exclusively.

S 4.104 LDAP Services for NDS

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The Lightweight Directory Access Protocol (LDAP) has become the de facto standard for accessing directory information based on the X.500 standard via the Internet or an intranet. Novell Directory Services (NDS) is one of the LDAP directories whose main task is to be able to process a multiplicity of search operations at the same time. With the aid of NDS the administrator is able to create and manage all company employees and all resources available in the network as objects in a hierarchical directory tree. For example, users can be assigned access rights to Unix, Microsoft Windows NT or Novell Netware servers or other resources, such as access to the mailing system and printers. Previously, information had to be maintained in application-specific lists and consolidated beyond the various system boundaries. If directory-capable applications are used, a single point of administration is created, i.e. all information is maintained from one location.

All directory services based on X.500 use a Directory Access Protocol (DAP) to synchronise the directory information and to provide a communications interface between the various network components.

LDAP is a Directory Access Protocol whose primary task is the high-speed extraction of information, based on a lower protocol overhead. In this case not the whole of the OSI protocol stack is implemented; instead, LDAP is based directly on the TCP/IP protocol. As a consequence, the LDAP clients are far less complex than the DAP clients. As the implementation of LDAP is founded on the Internet standard RFC 1777, developers are able to use platform-independent application program interfaces (APIs). There is therefore no need to pay attention to manufacturer-specific notation, because the LDAP server takes care of converting an LDAP request to the necessary format.

LDAP version 2 is implemented in LDAP Services for NDS for Netware 4.11; this deals with client-to-directory communication. Version 3 of LDAP contains specifications on directory-to-directory communication, for example on replication and the synchronisation of directory information in the network. To date, though, the standard (RFC 2551) has not been definitively adopted. An implementation of LDAP version 3 is used under Netware 5.

LDAP Services for NDS assumes the role of an intermediary between NDS, which of course has to be installed, and the LDAP client. The client sends an LDAP request to the server on which LDAP Services is running. The request is accepted and converted into an NDS request by LDAP Services for NDS. NDS evaluates the request and returns the requested information to LDAP Services for NDS. In turn, this uses the NDS response to generate an LDAP response, and forwards it to the client.

Novell itself does not offer an LDAP client. Currently the most common clients are browsers, such as Netscape Communicator, which have a corresponding LDAP interface. There are however also other, freely available LDAP clients in the Internet. Certain things have to be taken into

consideration before using these clients, though. For example, Netscape Communicator is not able to grant access to LDAP servers which require a user name and a password. LDAP Services for NDS therefore recognises a user who uses this browser as a client as an anonymous user, and by default makes him a trustee of [Public], which typically comprises only a browse right for NDS. If additional rights are required, a proxy user must be set up who has the corresponding NDS rights. As well as this, the proxy user feature must also be enabled in the LDAP group object.

As LDAP Services for NDS is fully integrated into NDS, an extension of the NDS scheme must be set up at the time of installation. This can only be done via an account with supervisor rights for the [Root] object. During installation of the first LDAP server in an NDS tree, the database scheme of NDS is extended so as to make two new NDS objects *LDAP Server* and *LDAP Group* available. LDAP Services for NDS is configured with the aid of these two objects. If additional LDAP servers are installed in this NDS tree, it is not necessary to install the scheme extension again because NDS already has the current database scheme.

The configuration of LDAP Services for NDS is stipulated in the properties of the two objects, *LDAP Server* and *LDAP Group*. The settings must be made in accordance with the security strategy that has been devised. Some of the properties that are particularly relevant to the security of the system are examined below.

Log file size limit (*LDAP Server* object)

This property can be used to set the maximum size of the log file specified in the *Log filename* property. When the log file reaches the size specified here, the information in the *Log filename* file is copied to the file specified under *Backup log file*. All new log data is written to the *Log filename* file.

Default: 1.000.000

Minimum: 0 (unlimited file size)

Maximum: 4.294.967.295

If the size is set to zero, there is no size limit for the log file. In this case the file should not be stored on the SYS volume because the file is liable to grow to such an extent that the available storage space on the volume will be fully taken up. Inconsistencies within the NDS may occur as a result, and the availability of the server is reduced.

In the *LDAP Group* object the following properties are particularly relevant to security:

Suffix

The *Suffix* box is where the subtree is defined that is made available to the LDAP clients. If this box is blank, the clients are granted access to the entire NDS tree, in other words from the [Root] object. If a client sends a request to the server relating to an object outside the defined subtree, an error is returned, unless a value is entered in the *Referral* box.

Referral

A uniform resource locator (URL) of an alternative LDAP server can be entered in this text box. If for example a client sends a request to the server which the latter cannot reply to because the *Suffix* was set, this URL is returned to the LDAP client. The client is then able to forward the request to the specified server.

Enable NDS User Bind

If this check box is activated, a user has to authenticate himself with his NDS password when issuing a bind request. The passwords are not encrypted between the LDAP client and the LDAP server, however, i.e. they are transmitted across the network as plain text. Given a suitable network monitor (LANalyzer), an attacker is therefore in a position to spy out these passwords in this way. For security reasons this setting should not be used, unless you are using accounts that have been set up specifically for LDAP accesses and apart from that have no further rights in NDS nor with respect to the Netware file system.

Proxy Username

The proxy user is an NDS account that does not require a password, nor a password change. When an anonymous bind is requested (a connection setup without a user name or password), the LDAP server authenticates this request with the *Proxy Username* in NDS. Typically, the rights of these proxy users will be heavily restricted. If no *Proxy Username* has been defined, however, these anonymous binds will be validated as a user [Public] and will therefore also be given the corresponding rights.

LDAP Services for NDS obtains an additional security feature via the Access Control Page: the **Access Control List** (ACL). The LDAP ACL defines the access rights to the LDAP object properties for users and groups. The LDAP server uses the ACL to establish whether a user request is forwarded to the NDS or rejected. If a user has the appropriate rights, the request is forwarded to the NDS. In turn, NDS checks on the basis of the NDS rights whether the request will be processed or rejected.

Rights can be assigned to the users via the LDAP ACL dialog window. The following levels are possible:

None

If this option is activated, the user is granted no rights of any kind to the NDS tree.

Search

This right allows the user to search for LDAP object properties. These must be defined in the *Access To* list, however. Access to properties can be explicitly enabled by clicking on the Add button.

Compare

Assignment of this right enables the user to compare LDAP object property values with the corresponding NDS object property values.

Read

If a user has the *Read* right, he is permitted to view the LDAP property values defined in the *Access To* list. The *Read* right includes the *Search* right and the *Compare* right.

Write

If a user has the *Write* right, he can write the LDAP property values defined in the *Access To* list. The *Write* right includes the *Search*, *Compare* and *Read* rights.

Over and above these five security access levels, access can be restricted yet further. For example, an entry can be made in the *IP Address* field to specify that a request can only be accepted from one IP address or a group of IP addresses.

S 4.105 Initial measures after a Unix standard installation

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

Most Unix systems do not satisfy the system security requirements after a standard installation. Often too many sensitive services and configurations are activated by the vendors or else these are provided with access rights which are not sufficiently restrictive.

This section is intended to show by way of example how to make the system secure following a standard installation.

- Prior to installation the administrator should be given appropriate training, especially as regards the security aspects. This should include informing him of all the potential security weaknesses of the IT system (see also S 2.35 *Obtaining information on security weaknesses of the system*). Subscribing to appropriate mailing lists should also be covered.
- After the installation has been completed, the System Administrator's account should be assigned a good password (see S 2.11 *Provisions governing the use of passwords*).
- A review should be made of which services are running on the IT system. It is possible to check this e.g. by entering the command *netstat -a | grep listen*. Services which are not needed should be disabled or removed (see S 5.72 *Deactivation of unnecessary network services*).
- If the system does not function as a mail server, the mail daemon should be deactivated as a network service. If mail is to be delivered **locally** on the system, *sendmail* can be started with the option *-q15* or as a *cron* process:

  ```
  1 * * * * /usr/sbin/sendmail -q 2>&1 >/dev/null
  ```

  The mail queue is emptied at regular intervals and the mail is delivered locally.
- The latest version of the vendor's *sendmail* should be installed (see also S 4.107 *Use of vendor resources* and S 5.19 *Use of the sendmail security mechanisms*). Alternatively, public domain mail programs such as a *qmail* can be used. The version number of the installed version of *sendmail* can be identified with the command *telnet localhost 25*.
- After the standard installation, the security patches provided by the vendor should be installed (see also S 4.107 *Use of vendor resources*). It is extremely important then to check that no unnecessary services have been activated as a result of the patch installation.
- The file systems should be imported or exported only to the necessary extent. Care must be taken to ensure that file systems are not exported in such a way that anyone can write to them.
- If there is no alternative to using *NIS*, then *NIS+* should be used as additional security mechanisms are incorporated into this.

- If it is necessary that *tftp* is available, then the system should be started with the option *-s* in order to prevent every file in the system being copyable (see also S 5.21 *Secure use of telnet, ftp, tftp and rexec* and S 5.72 *Deactivation of unnecessary network services*).
- The *inetd* logging function should be enabled with *-t* so as to ensure that every attempt to establish a connection is logged (cf. S 5.72 *Deactivation of unnecessary network services*). It is helpful to install the public domain tool *xinetd* or TCP Wrapper. With these tools it is possible amongst other things to log all connection attempts promptly, and before the daemon addressed has been started via *inetd*.
- Log files should be examined on a daily or weekly basis. Analysis programs such as *swatch*, *logdaemon* or *logsurfer* should be installed in order to have the data processed and interpreted semi-automatically (cf. S 2.64 *Checking the log files*).
- Security checks using *USEIT*, *COPS*, *Tripwire* or *Tiger* should be carried out at regular intervals.
- It is important that *rshd*, *rlogind*, *rexecd* are deactivated as well as all the other unnecessary services (cf. S 5.72 *Deactivation of unnecessary network services*). To convert RPC program numbers to port addresses, most vendors supply the program *rpcbind*. If the daemon *portmapper* is available for the existing platform, then it should be used either as an addition or as a replacement.

  All clients which use these services should be non-executable for normal users. Any other authentication procedures which are based on host names should be completely removed.
- *Telnet* should be replaced by *ssh*. With *ssh* it is possible to have a strongly encrypted and authenticated interactive connection between two systems. *ssh* should be viewed as a substitute for *telnet*, *rsh*, *rlogin* and *rcp*. It also enables X-Windows traffic to be passed securely (see also S 5.64 *Secure shell*).
- *Xauth* is to preferable to *xhost* - "xhost +" should never be used (see also S 4.9 *Use of the security mechanisms of X-Windows*).
- All entries which are not required should be removed from the configuration file */etc/inetd.conf* (see S 5.72 *Deactivation of unnecessary network services*).
- The configuration file */etc/syslog.conf* must be modified so as to activate the log functions (see S 4.106 *Activation of system logging*).
- A list of all world-writable files and directories can be created with the following commands:

  find / -type f -perm -22 -exec ls -l {} \;

  find / -type d -perm -22 -exec ls -ld {} \;

  The results should be compared regularly with the installation status.
- Either *Tripwire* or *USEIT* should be installed before the system goes live in order to obtain a checksum summary of the installed system on

commencing actual operation. The summary created should be stored on a write protected data medium.

- To ensure that malicious generation of log data cannot bring the Unix system to a halt, */var* should be a large partition.

All changes carried out should be carefully documented and be agreed among all the system administrators. This documentation can be in paper form or in a file that is maintained on the system concerned. However, it must be possible for the documentation to be inspected and updated at any time (see also S 2.34 *Documentation on changes made to an existing IT system*).

Additional controls:

- What services are enabled on the IT system?
- Have all the available security patches been installed in the correct manner?
- Are all changes documented promptly and agreed among all the system administrators?
- Are all changes made to the operating system configuration documented and easy to follow after a new installation?

S 4.106 Activation of system logging

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

The native Unix logging tool *syslog* is used to record information which is generated by the operating system or by application processes. It is important that security-relevant events, such as attempted logins and execution of the command *su*, are logged and available for processing and interpretation at a later time.

The required daemon *syslogd* is normally started automatically and configured via file */etc/syslog.conf*. The granting of rights must be performed in such a way that only system administrators can change this file and that the log files contained in */var/log* and */var/adm* can only be read by system administrators. All changes made to */etc/syslog.conf* must be documented. When making modifications to the existing IT system, at first everything should be logged. After that, individual areas can be deactivated in stages as required. The */var* partition must be sufficiently large to accommodate the log files. The example of a configuration file set out below is based on a SunOS configuration and specifies a detailed logging procedure in various files.

```
#ident  "@(#)syslog.conf        1.3     93/12/09 SMI"   /* SunOS 5.0 */
#
#
# All messages are sent to a loghost which has to be defined in the
# /etc/hosts file.
#
#
# TAB must be used as separator!
#
# Test: . Start syslogd with the option "-d"
#       . Start syslogd with kill –HUP after each change to this file.
#       . The log file must already exist prior to start-up / reboot.
#       . Test messages can be generated for each facility and
#         priority with /usr/ucb/logger.
#
#


*.err;kern.warning;auth.err;daemon.err          /dev/console
*.alert;kern.err;daemon.err                     operator
*.alert                                         root


# Displays emerg messages on terminals (uses WALL).
*.emerg                 *
#
```

```
#
kern.info               ifdef(`LOGHOST', /var/log/kernlog, @loghost)
user.info               ifdef(`LOGHOST', /var/log/userlog, @loghost)
mail.info               ifdef(`LOGHOST', /var/log/maillog, @loghost)
daemon.info             ifdef(`LOGHOST', /var/log/daemonlog, @loghost)
auth.info               ifdef(`LOGHOST', /var/log/authlog, @loghost)
lpr.info                ifdef(`LOGHOST', /var/log/lprlog, @loghost)
news,uucp.info          ifdef(`LOGHOST', /var/log/newslog, @loghost)
cron.info               ifdef(`LOGHOST', /var/log/cronlog, @loghost)
#

## All other "local" messages, for own programs
local0,local1.info         ifdef(`LOGHOST', /var/log/locallog, @loghost)
local2,local3,local4.info  ifdef(`LOGHOST', /var/log/locallog, @loghost)
local5,local6,local7.info  ifdef(`LOGHOST', /var/log/locallog, @loghost)

#
# All alarms and above are written to a separate file:
*.err                   ifdef(`LOGHOST', /var/log/alertlog, @loghost)

#
# Example of log levels:
# -----------------------------------
# 'su root' failed for ..       auth.err
# ROOT LOGIN REFUSED ON ...     auth.err
# 'su root' succeeded for..     auth.notice
```

Additional controls:

- Are changes to */etc/syslog.conf* documented?
- Is the system administrator the only person who is able to change the configuration?
- Is the system administrator the only person who is able to read the log files contained in */var/log* and */var/adm*?

S 4.107 Use of vendor resources

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

All vendors of IT systems or IT components offer various forms of support and information for purchasers of their products. These include, for example, assistance in dealing with problems (support, hotline, updates, patches etc.) and access to information on security solutions (www sites, news groups, mailing lists etc.). Some of these are free of charge, others are not.

Already when purchasing IT systems or products, consideration should be given to the question of which forms of support provided by the vendor should be taken up, especially when these incur ongoing costs.

Steps should be taken to ensure that for **all** IT systems and products used regular checks are made as to whether new information regarding security problems and possible solutions is available from the vendor. This is especially important for all server operating systems as a security weakness on the server can cause significantly more damage than one which affects only a single IT system.

Security-specific updates, when these are not supplied directly from the vendor on CD-ROM, should only be obtained from trustworthy sources, e.g. from CERTs (see also S 2.35 *Obtaining information on security weaknesses of the system*). Updates should be checked to ensure they are intact using cryptographic methods (e.g. MD5, PGP) if they are offered appropriately encrypted and digitally signed.

To ensure that security-relevant advice from the vendor can be accessed at any time, a summary should be maintained for all operating systems and all major IT products used. This should show clearly the www addresses where security-specific updates and patches and information provided by the operating system vendor can be found.

A table like the one set out below, which provides a summary of the relevant links to known server operating systems, can be used for this purpose. The lines marked with **U** contain the URLs for **(security-specific) updates and patches** for the vendor concerned, while the lines marked with **I** contain the addresses from where **security-specific information** can be obtained.

Berkeley Software Design, Inc. - BSD/OS	
U	ftp://ftp.bsdi.com/bsdi/patches/
I	http://www.bsdi.com/services/support/
Caldera OpenLinux	
U	ftp://ftp.caldera.com/pub/openlinux/updates/
I	http://www.calderasystems.com/support/security/
Deban Linux	

U	http://cgi.debian.org/www-master/debian.org/security/ (German) http://cgi.debian.org/www-master/debian.org/security/index.en.html (English)
I	http://www.debian.org/security http://www.debian.org/security/index.en.html
Digital Equipment Corporation - DEC	
U	http://www.service.digital.com/patches/
I	http://www.unix.digital.com/
The FreeBSD Project – FreeBSD	
U	ftp://ftp.FreeBSD.org/pub/FreeBSD/
I	http://www.freebsd.org/security/security.html
Hewlett Packard – HP	
U	http://europe-support.external.hp.com/ http://us-support.external.hp.com/ ftp://ftp.hp.com/pub/security/patches/
I	http://europe-support.external.hp.com/ http://us-support.external.hp.com/
IBM	
U	http://service.software.ibm.com/aixsupport/
I	http://www.ers.ibm.com/tech-info/index.html
The Open BSD Project – OpenBSD	
U	http://www.openbsd.org/errata.html
I	http://www.openbsd.org/security.html
RedHat Linux	
U	ftp://www.redhat.com/pub/updates/ http://www.redhat.com/download/mirror.html http://www.redhat.com/corp/support/errata/index.html
I	http://www.redhat.com/LinuxIndex/Administration/Security/
S.u.S.E. Linux	
U	ftp://ftp.suse.de/pub/suse_update/
I	http://www.suse.de/de/support/security/index.html (English also)
Santa Cruz Operation – SCO	
U	ftp://ftp.sco.com/SSE/
I	http://www.sco.com/security/
Silicon Graphic Inc. – SGI	

U	ftp://sgigate.sgi.com/patches/
I	http://www.sgi.com/Support/security/security.html
Sun MicroSystems Inc. – Sun	
U	http://sunsolve.sun.de/pub-cgi/us/pubpatchpage.pl http://sunsolve.sun.com/pub-cgi/us/pubpatchpage.pl (depending on address of the local SunSolve server)
I	http://sunsolve.sun.de/sunsolve/securitypub.html http://sunsolve.sun.com/sunsolve/securitypub.html (depending on address of the local SunSolve server)
NT	
U	http://www.microsoft.com/security/
I	http://www.microsoft.com/security/
Novell	
U	http://support.novell.de/ http://support.novell.com
I	http://www.novell.com/corp/security/

Unfortunately, experience indicates that links frequently change so it is important to check the list regularly to ensure that it is correct and, if necessary, to update it. For this reason no responsibility can be accepted for the material to be found on the links listed above, which has been provided for illustrative purposes.

Additional controls:

- From which source are vendor patches obtained?
- What steps are taken to ensure that information about the latest patches is always available?
- How is the patch level status of systems verified?
- Is the integrity of patches verified using cryptographic techniques (e.g. PGP, MD5)?

S 4.108 Simplified and secure network management with DNS services under Novell NetWare 4.11

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

Link between IP addresses and host names

A unique address must be assigned to every IT system in a TCP/IP network. The Internet Protocol (IP) specifies this address as four decimal numbers separated by a dot, each with a value range of between 0 and 255. As many numeric addresses are difficult to remember, meaningful host names can be assigned to the IT systems as well, e.g. *www.bsi.bund.de*. Resolution of host names into IP addresses can be performed using two different mechanisms. Under the first, an ASCII text file called HOSTS, which is stored in the SYS:ETC directory, can be manually created. From a security and administrative viewpoint this method should only be used in small networks as the HOSTS file has to be stored individually on each server and each workstation to enable local resolution. Special routines (e.g. login scripts) can be used to automate distribution of the HOSTS file.

The second mechanism entails using a DNS server. Some of the aspects of setting up and configuring a DNS server under Novell NetWare 4.11 which require especial consideration in relation to system security are considered below.

Function of the DNS components

The two main components of DNS are the *name server* and the *resolver*, which is loaded on the client and queries the name server.

- **Primary name server**

  One primary name server per zone

  The primary name server obtains the DNS entries for the zones for which it is authorised from a file on its hard disk. "Authorised" here means that the primary name server does not need to cross-check the DNS information with any other name server for a given zone. At the same time the primary name server is also the *single point of administration* for the domain. Only one primary name server exists for each zone.

- **Secondary name server**

  Load distribution, reduction of network traffic and redundancy

  The secondary name server possesses a write-protected copy of the DNS database of the primary name server. This copy is updated within a set period of time which is specified in the record type SOA (Start of Authority). Record types define the *resource records* which form the entries in the DNS database. The copy operation is known as "zone transfer" and forms the basis for updating the distributed DNS database of a domain. Secondary name servers take on load distribution tasks, enable the DNS database to be made available close to the resolver and create redundancy of the DNS domain information. To ensure that the system is fail-safe, at least one secondary name server should be configured for each zone.

- **Resolver**

  The resolver is the program which sends the DNS queries to one of the defined name servers. A name server which is unable to perform name resolution can also act as resolver, sending the query to a name server outside the domain. Similarly the resolver interprets the responses received from the name server and sends information back to the programs which have requested it.

Querying of the DNS server and interpretation of the responses

DNS server configuration - initial steps

With a NetWare 4.11 server, DNS is configured via UNICON.NLM. First of all *DNS Client Access* needs to be activated. This is done via *Configure Server Profile - Manage Global Objects*. At least one name server which performs address resolution must be listed. A maximum of three name servers can be entered. To speed up entry of a large address area and ensure that name resolution can be performed, the entries for the three name servers should be utilised. The sequence in which the name servers are listed determines the query sequence and should be determined in the manner which results in the fastest name resolution.

Register three name servers

The first name server can be the main DNS server of the authority or company. Even if this server cannot resolve every host outside its own domain, it allows host names to be resolved rapidly within the organisation.

The second name server can belong to the Internet Service Provider (ISP), enabling access to a wider data pool of host names. This has the effect that due to the higher utilisation, the remoteness and the available bandwidth, resolution is usually somewhat slower than with the local name server. If redundancy of the local domain is a priority, then the server with the write-protected copy of the DNS database (secondary name server) should be registered as the second name server.

The third name server defined can be a so-called *root server*. This type of server holds the data for all the registered domains. A list of root servers can be obtained from *ftp://rs.internic.net/netinfo/root-servers.txt*.

Configuration of the DNS server

The configuration and administration functions for the Domain Name System are accessed by selecting *Manage Services - DNS* from the UNICON.NLM main menu. To set up a master database or a write-protected replica database, the *Administer DNS* menu option should be selected.

The domains and zones for which the primary name server is authorised are entered by selecting *Manage Services - DNS - Administer DNS - Manage Master Database - Delegate Subzone Authority* from the UNICON.NLM main menu.

Enter all the secondary name servers in the database

The DNS database entries are entered via *Manage Services - DNS - Administer DNS - Manage Master Database*. With a standard implementation of DNS, the *Start of Authority* (SOA), which identifies the starting point for the authority of a zone within the DNS hierarchy, and the record type *Name Server* (NS) must be entered. The primary name server must receive entries for all the secondary name servers of the zone. Linking of this zone with the DNS hierarchy is achieved through name server entries for primary name

servers which possess authority for superordinate and subordinate zones. To ensure name resolution for the hosts in the zone, record type *Address* (A) must be entered for every terminal device to be addressed.

The entries needed in record type SOA include the name and address of the *zone supervisor*. The default setting for this address is *root.<domain_name>*. The settings for the synchronisation behaviour of the secondary name servers are also made in record type SOA.

The *refresh validity period* determines the time within which a secondary name server continues to reply to queries from hosts after it has tried unsuccessfully to contact the primary name server. The shorter this time is set to, the lower the likelihood that the secondary name server will send invalid DNS entries and thus prevent name resolution. To make the system fail-safe, this time should not be set too short since, if the primary name server should fail, the Domain Name System for this zone will then no longer work. A compromise must be found for this parameter between the probability of being unable to resolve individual host names and - if too short a period is set - the probability of being unable to address any terminal devices by individual host names.

The *minimum caching interval* determines the time for which information from queries is retained in the cache of the primary name server. If too short a time is selected, this can increase the load on the network where the same hosts are queried frequently and delay resolution of the host names into IP addresses. On the other hand, if too long a *minimum caching interval* is defined, this can result in out-of-date information being passed on.

Connection to the external DNS hierarchy

Direct connections to speed up name resolution

Queries involving host addresses outside the local domain are automatically executed as long as the DNS server is running. The DNS server receives information about the DNS hierarchy from the file SYS:ETC\DNS\ROOT.DB, which contains a list of name servers of the US Top Level Domains. *Manage Services - DNS - Administer DNS - Link to existing DNS Hierarchy* provides access to two different methods of building a direct connection to other domains, namely *Link Direct* and *Link Indirect via Forwarder*. If certain domains are accessed frequently, these procedures can speed up host name resolution.

Checking of name servers

The menu option *Manage Services - DNS - Administer DNS - Query Remote Name Server* allows checking of what information is held on other name servers as well as allowing one to determine whether a particular name server is responding to queries. In either case, the name or IP address of the server must be entered. The resource record type which is being interrogated and the domain from which the information is required must also be specified.

Backing up the DNS database

The DNS database should be backed up at regular intervals. Such backups can be used, for example,

- to restore a DNS database which has become unusable,

- or to move the database to a different server.

The menu option *Manage Services - DNS - Save DNS Master to Text Files* is used to save the database to *SYS:ETC/DBSOURCE/DNS/HOSTS*.

Use of UNICON.NLM

Restrict access

The Domain Name System settings are entered with UNICON. For administrative and security reasons, it is sometimes necessary to split up tasks and restrict access. When a NetWare product that is controlled via UNICON is installed, group objects which control certain task areas within UNICON are created in the NDS directory tree. Users who are required to perform particular tasks with UNICON are made members of the relevant group.

Group name	**Area of responsibility**	**Available UNICON menu options**
UNICON MANAGER	Full functionality of UNICON	Access to all menu options
UNICON SERVICES MANAGER	Starting, stopping and managing services	Start/Stop Services und Manage Services
UNICON HOST MANAGER	Changing host entries	Manage Global Objects - Manage Hosts

Compatibility with *bind* (Berkeley Internet Name Domain)

TCP/IP networks were developed from the Unix environment. The most widely used DNS program for Unix is *bind*. It is therefore important that other DNS products are compatible with *bind*. The Novell DNS service is fully compatible with *bind* version 4.8.3.

S 4.109 Software reinstallation on workstations

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

Problems with the operating system or the applications which can only be resolved through user support occur relatively frequently on workstations. These can be caused, for example, by software errors, configuration changes, installation of new software or computer viruses.

Restoring standard configuration

To avoid administrators having to spend a lot of time troubleshooting on workstations in connection with the problems described above, a software reinstallation of the standard configuration should be performed.

Identification of the IT system

First of all the computer must be uniquely identified. Starting from this identification, it is then necessary using appropriate documentation or a program to establish precisely what software is installed in what configuration on this computer. It is helpful here if the IT systems are very similar, at least in areas with similar assigned tasks.

It is recommended that the workstation hard disk is re-formatted and the required software and data is then reinstalled.

Time-critical reinstallation

A software reinstallation can be performed in various ways. For example, there are special programs which will export a predefined configuration from a server onto the workstations which are to be reinstalled. It should be noted that this kind of work is generally doubly time-critical: on the one hand it is desirable that reconfiguration is effected as quickly as possible so as to make the IT system available once more, while on the other hand the network loading must be minimised. This is especially important in the case of training computers or PC pools.

It is of course also possible to perform the reinstallation "manually". To do this, a standard installation should be performed first of all. The special features of the individual computers, such as special device drivers, additional configuration files or special software, are then copied. However, this requires that these are available preconfigured, e.g. on the network or on mobile data media. An up-to-date anti-virus program must then be run.

S 4.110 Secure installation of the RAS system

Initiation responsibility: Head of IT Section, IT Security Management Team

Implementation responsibility: Administrators

After the hardware and software necessary for implementation has been purchased as part of the organisational preliminary work, the individual components must be installed and operated. Generally a RAS system can only be securely operated if care has previously been taken over the installation. A pre-requisite to secure installation is the selection of suitable hardware and software for RAS access (quality, interoperability, compliance with existing standards) through the previous decision process (see S 2.186 *Selection of a suitable RAS product*). This goes to show once again how important it is for the decision process to be thorough and systematic.

The physical components of a RAS system consist of conventional IT systems: generally there are at least one server and several clients, network switching elements, modems or other technical devices. The physical security of these items must be assured as for all other components of a computer network. Hence at the outset the general safeguards for each of these components must be implemented, as described in Chapters 3 to 9.

The following additional points should be considered specifically with reference to installation:

- It must not be possible either for users or external third parties to access either the RAS system or any part of it during the installation phase. No connections to the productive LAN or to the telecommunications systems should be active.
- The installation must be performed by appropriately skilled personnel.
- The installation should follow the procedures specified during planning of the RAS system.
- The installation and configuration must be documented. This can take the form of either separate installation documentation or a confirmation that the installation agrees with the planning premises.

Meticulous documentation of installation

- If during installation any departures from the planning premises (e.g. different cable arrangement, additional equipment) occur, these must be documented and a note should be entered in the planning documents explaining why the change was made. This documentation is especially important as a means of improving future planning.
- The correct functioning of each individual component must be established (e.g. through function testing or self-test).
- For every security-relevant setting, a function test of the security mechanisms must be carried out. For example, encryption of communications should be tested using a network analyser.
- Once the installation work is complete, the correct functioning of the entire system must be verified (acceptance and approval of installation).

System test before approval

Normally this should entail the use of predefined acceptance configurations and simulated operational scenarios. During testing care must be taken to ensure that only the persons authorised to participate in testing can access the RAS system.

Upon completion of installation of a RAS system, the system should have a secure starting configuration which initially allows access only to the authorised administrators (see also S 4.111 *Secure configuration of the RAS system*). These persons should then convert the RAS system to a secure operating state. Once this is achieved, continuous operations can then commence.

Example

Under Windows NT the installation of RAS servers and clients is very simple and is virtually identical as the Windows NT Remote Access Service contains both client and server functions.

The following applies to a RAS client running under Windows NT:

- The server functions of the Remote Access Service must be disabled. This is done by allowing only outgoing calls on all devices which can be used for remote access (e.g. modem, ISDN card, VPN adapter). The relevant dialogue boxes are reached by selecting the following sequence of options: *Control Panel, Network, Services, Remote Access Service, Attached Device, Configure*.
- For the RAS client only the protocols that are permitted for remote access should be enabled. This is done by selecting *Control Panel, Network, Services, Remote Access Service, Attached Device, Network.*
- The characteristics of a RAS connection are specified in Windows NT through *Dial-Up Networking*. Here the parameters required under the RAS security concept should be set (e.g. "Require data encryption").

The following applies to a RAS server running under Windows NT:

- The client functions of the Remote Access Service must be disabled. This is done by allowing only incoming calls on all the devices which can be used for remote access.
- For the RAS server only the protocols that are permitted for remote access should be enabled.
- The parameters required under the RAS security concept must be set for incoming RAS connections. This is done by selecting *Control Panel, Network, Services, Remote Access Service, Attached Device, Network.*
- Only authorised users should be allowed to dial in. This can be specified under Windows NT through either RAS Manager or User Manager.

Additional controls:

- Have all deviations from the planning premises for the RAS system been noted in the planning documentation?
- Have the security mechanisms been function tested (e.g. has encryption of communications been tested using a network analyser)?

S 4.111 Secure configuration of the RAS system

Initiation responsibility: Head of IT Section, IT Security Management Team

Implementation responsibility: Administrator

The functioning and security of a RAS system are essentially determined by the configuration parameter settings. However, since a RAS system does not consist of only one component which has to be configured, the overall configuration is naturally a lot more complex. Due to this complexity, configuration errors which could reduce the security of the system as a whole can easily occur. Uncoordinated changes of one configuration parameter on a component can thus interact with the other components in such a way as to prevent error-free operation. In extreme cases the security of the LAN could even be impaired.

Since the configuration of a RAS system is generally subject to changes over time (e.g. due to changes in personnel, new operational scenarios, system enhancements etc.), it cannot be assumed that there is only one secure (and static) configuration which is defined once and never changed afterwards. On the contrary, the configuration is likely to undergo a series of version changes. It is the job of the administrators who are responsible for the RAS system to ensure that only secure versions of the system configuration are defined and that when the system configuration settings are changed, the new configuration is also secure.

In general, the following configuration categories may be distinguished:

- The *default configuration* comprises the default parameter settings defined by the vendor. This will normally not be secure enough and should therefore not be used.
- After installation and prior to initial operation, the default configuration must be converted to a secure *initial configuration* by the administrators. Here the settings should be as restrictive as possible so that only authorised administrators can effect changes in order, for example, to define an initial operational configuration which implements the planned security concept.

Default settings must be modified

- The secure *operational configurations* are the result of configurations made during ongoing operations. Regular checks must be made here to see whether any new security weaknesses which have come to light inflict modifications (see also S 2.35 *Obtaining information on security weaknesses of the system*).
- Finally, secure *fallback configurations* should be defined and documented as part of contingency planning. These are also used to maintain security where operational capability is reduced. Normally several emergency situations are defined during contingency planning. It is recommended that an appropriate fallback configuration is specified for each of the defined situations. In the simplest case the fallback configuration simply means that access to the RAS system is blocked.

To ensure that the configuration is secure, the following points should be noted when making the configuration settings.

- On top of the RAS system configuration, dividing the network into subnets can also be useful for access control. For reasons of IT security it can therefore be appropriate to set up access networks (see also S 5.77 *Creation of subnets*).

Setting up access networks

- The routing settings of the network switching elements within the RAS system should be used to restrict the flow of network traffic. Network packets should only be forwarded on permitted connections. In addition, the latest network switching elements allow selective forwarding of packets within permitted network connections (packet filter function). In this way it is possible, for example, to ensure that only connection requests are forwarded to the HTTP service of a server.

Routing settings

- Restricting access to RAS clients is especially difficult to implement with mobile computers. With mobile RAS clients it is therefore especially important that users adhere strictly to the defined rules (e.g. to protect against theft; see also module 5.3 *Laptop PCs*).

- The secure configuration of the RAS server software requires that the security settings which are offered by the software and are appropriate in the existing operational scenario are also enabled and can be used. The use of certain security settings may presuppose that other components of the RAS system also possess corresponding functions and/or can be correspondingly configured. Thus, for example, when the Calling Line Identification Protocol (CLIP) is used, it is important to ensure that this is also enabled for the selected connection. For example, user identification on access over the Internet using X.509 certificates requires that the storage location of the user certificates is known to the RAS system. So the RAS software must either support external authentication servers or else offer a certificate management module of its own.

  It is therefore necessary to check in advance whether all the security mechanisms offered can also be used or whether different and/or additional hardware or software is necessary for this. Once the RAS system is up and running, regular checks must then be made in order to verify that the settings are correct.

Use of existing security mechanisms

- The requirements which apply to the secure configuration of the RAS client software are similar to those which apply to the server software. In addition, care must be taken to ensure that passwords required for RAS access are not stored within the software, even though this option is frequently offered. If this cannot be technically prevented, all users must be forbidden from making use of the option. Moreover, all users must be informed of the problem.

Client configuration

- In order that clients and server can communicate in a secure manner, care must be taken to ensure that the components involved are configured in a consistent manner (e.g. as regards the method used to protect communications).

- The secure and consistent configuration of client and server can be supported by specifying a standard configuration for RAS clients (hardware and software) in the RAS concept and implementing it through appropriate organisational measures. The result of doing this is that only a

Setting up standard IT systems

fixed number of different client configurations are in use. This simplifies the overall job of configuration and also helps to maintain a secure and consistent configuration.

- Changes to the RAS system configuration should undergo an organisational process which ensures that the RAS system only operates with tested configurations. All changes should be documented and approved. Note: the addition of new RAS users or deletion of existing ones generally does not require any change to the RAS system configuration as these changes are often effected using the user administration facilities of the operating system (e.g. Remote Access Service under Windows NT) or an authentication server (e.g. RADIUS, TACACS+).

Change management

- The RAS configuration should be checked regularly. Care must be taken here to ensure that all the requirements contained in the RAS security guidelines are implemented and that the settings do not have any weak points.

Regular checking of the RAS configuration

Although the task performed by RAS systems is quite simple, their configuration and operation are as complex as, for example, those of a firewall system. The topics listed here should therefore always be elaborated, expanded and modified as part of RAS system planning and RAS operation.

Examples

- Under Windows NT RAS access authorisation should be restricted after installation of the RAS, but this can only be performed at user level and when there are many users this is no longer efficient to administer via the User Manager. However, the RAS administration tool under Windows NT also allows dial-in permission to be taken away from all users at once.
- Only dialling in should be allowed on a RAS server. Outgoing connections from the RAS server itself are generally not necessary and should therefore be prohibited. Under Windows NT this can be configured for each device which is suitable for remote access (e.g. modem, ISDN card, VPN adapter) from the Properties dialogue within Remote Access Service. The relevant data entry fields are accessed by selecting the following sequence of options: *Control Panel, Network, Services, Remote Access Service, Attached Device, Configure*.
- When remote access services are used, only the protocols which are actually necessary should be allowed over RAS access. Any unnecessary protocols should accordingly be disabled. This is achieved under Windows NT by selecting *Control Panel, Network, Services, Remote Access Service, Network, Server Settings.* The configuration of the required protocols must comply with the security guidelines, for example as regards authentication, encryption, IP address area, local or network-wide access.

Additional controls:

- Is the RAS client software configured so that passwords used for access are not stored?
- Are measures in place to ensure that all RAS components are consistently configured?
- Is the RAS configuration regularly checked?

S 4.112 Secure operation of the RAS system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

For the secure operation of a RAS system it is essential that the hardware and software components of the system have been securely installed and configured. Safeguards S 4.110 *Secure installation of the RAS system* and S 4.111 *Secure configuration of the RAS system* must therefore have been performed before the RAS system goes live. In addition, all the organisational processes must have been defined and implemented (e.g. reporting channels and responsibilities). It should also be noted that the desired level of system security can only be assured if the physical security of the hardware components which make up the RAS system is also assured (see also S 4.110 *Secure installation of the RAS system*).

The security of a RAS system can be roughly broken down into three areas:

1. the security of the RAS server,
2. the security of the RAS client and
3. the security of data transmission.

Whereas the desired level of security of the RAS server can be controlled through implementation of local security guidelines, the RAS client is typically not under the complete control of the IT personnel who are responsible for the LAN. The security of data transmission media is generally completely out of their control. For this reason, protection of communications between client and server must be secured by additional means.

In the environment of the **RAS server** the following recommendations for secure operation should be considered:

Monitoring of RAS access

- RAS access should be continuously monitored using logging and management tools.

Regular analysis of log files

- The information collected in the course of monitoring should be regularly reviewed by a trained administrator. This person should if possible be supported with a log file analysis software tool. The data protection regulations must be considered (see also S 2.110 *Data privacy guidelines for logging procedures*).
- If any security incidents are detected, the measures previously specified must be implemented immediately. The identified security incidents should be documented in an incident report (see also module 3.8 *Handling of security incidents* on this point).
- In order that a controlled user authentication procedure (e.g. Remote Access Service under Windows NT, RADIUS, TACACS, TACACS+, SECURE-ID) is possible for RAS access, the consistency of the authentication data must be assured. This can be effected either through central administration of the data (using an authentication server) or else through periodic synchronisation.

- User authentication must be performed via the chosen mechanism **every** time that a connection is established. In particular use of the CLIP mechanism (transmission of call numbers) on its own is not sufficient to ensure reliable authentication.
- Protection of communications using one of the methods permitted in the RAS security concept must be enforced for **every** connection in order to ensure that the transmitted data is protected.
- The *additional* security mechanisms (use of call number transmission, callback to a preconfigured phone number for non-mobile RAS clients or for RAS clients connected over a mobile phone) provided by the access technology should be used.
- The RAS system should be audited at regular intervals. The roles of Administrator and Internal Auditor must not be assigned to the same person.

Auditing

- A mobile IT system can be connected to a LAN over GSM (see also ### S 5.x5 *Secure transmission over mobile phone*). When RAS is used over a mobile phone network, it should be noted that the CLIP mechanism (transmission of call numbers) is generally only suitable as an *additional* authentication feature as the mobile phone identified over the call number can easily fall into unauthorised hands.

Connection over mobile phone

As RAS clients are generally operated in environments that are not under full control, special mechanisms, procedures and safeguards must be employed to ensure protection of the client. In particular, mobile RAS clients are exposed to a special danger here in that their physical design makes them especially easy to attack (e.g. theft, vandalism). Once a RAS client is compromised, there is a danger that the security of the LAN could also be impaired as a result.

For the secure operation of **RAS clients**, the following aspects must therefore be considered:

- The basic security of the IT system must be assured (see also modules 5.3 *Laptop PCs*, 7.2 *Modems*, 8.6 *Mobile phones* and 9.3 *Telecommuting*).
- As mobile RAS clients are exposed to greater risks than stationary clients, they need to be protected through additional safeguards. One such safeguard is to encrypt the hard disk in order to ensure that in the event of the device going missing it is not possible for any data to be read or for unauthorised RAS connections to be established.

Encryption of hard disks

- Especially where RAS clients are linked using Internet connections, it is essential to have anti-virus software installed on them (see also module 3.6 *Computer virus protection concept*).

Up-to-date anti-virus program

- Consideration should be given to installing PC firewalls on the RAS clients so that they are protected against unauthorised access from the Internet by third parties. Like conventional firewalls (see module 7.3 *Firewalls*), PC firewalls filter the packets of network communication protocols. However, the filtering rules can generally be dynamically generated by the user. For every access for which no rule currently exists, a selection of possible responses is offered (e.g. allow, reject, conditional processing), enabling

PC firewalls

the user to define a new rule. However, as it is often difficult for the user to distinguish between permitted and unauthorised accesses, the ruleset should be pre-installed by an Administrator.

- RAS clients too should be included in the system management as far as is possible. Firstly this permits monitoring of the clients within the framework of maintaining ongoing operations. And secondly it enables software updates (e.g. virus databases, applications programs) to be imported over a controlled route. Remote computers, however, place higher requirements on system management as they are not permanently linked to the network, so that the computers must regularly be examined for (non-permitted) configuration changes. Here, depending on the management product, the "Discovery" function can be used to ascertain the current status of the computer. It should be noted that capturing this information places a load on the RAS client and the data has to be transmitted over the RAS connection. If the RAS connection has a low bandwidth, as is the case for example on a mobile phone, this can result in response times which are unacceptable to users.

Include RAS clients in system management

- If TCP/IP is used as the protocol, consideration should be given to the possibility of using fixed IP addresses for RAS clients rather than assigning addresses dynamically. This procedure does carry high administrative penalties (e.g. the necessity to maintain the assignment tables), but it does allow unique network addresses to be assigned to individual computers. The disadvantage of dynamic assignment of network addresses is that a record must be made of which RAS client was given a certain network address when. Otherwise it is generally not possible to establish which RAS client executed a particular action.

Unique assignment of IP address and computer

The **communications link** between RAS client and RAS server is generally established over third-party networks. The network components used here are generally not under the control of the operator of the LAN with which the connection is to be established. It must also be assumed that the data will not only be transmitted over the telecommunications network of a provider but that the networks will also be used by partners of the telecommunications provider. This applies especially where a LAN is accessed from abroad. To satisfy the protection requirements of the data thus transmitted, security measures must be taken which, for example, assure the confidentiality of data. The following therefore applies to data transmission:

- It is imperative for secure operations that all data transmitted is encrypted.
- Signature mechanisms should be employed to safeguard the authenticity and integrity of the data.

A number of security mechanisms can be used for RAS connections in order to satisfy these data protection requirements. These include the following:

- The communication can be encrypted at a low protocol level (so-called tunnelling - see S 5.76 *Use of suitable tunnel protocols for RAS communication*). This requires selection of a suitable procedure. Conventional RAS systems offer such methods as standard, though in different number and form.

Tunnelling

- SSL can also be used for encryption if it is not possible for particular reasons to use encryption at a low protocol level. This applies especially to access on Web servers or e-mail servers via Web browsers, which support SSL-protected communication as standard. In this connection see also S 5.66 *Use of SSL*.

SSL encryption

- As well as software protection of communications, the use of network switching elements such as routers and modems which encrypt data should also be considered. These are especially advisable for stationary use and where several computers are to be connected, as the encryption process is transparent and no extra load is placed on clients and server. However, it should be noted that the devices must be carefully configured and maintained.

Encryption through network switching elements

- Where e-mails are to be exchanged over insecure channels it may be appropriate to use e-mail encryption (see also S 4.34 *Using encryption, checksums or digital signatures*).

E-mail encryption

Security with remote access over a RAS connection can only be assured if all the components of the RAS system are correctly and consistently configured. However, it should be noted that, depending on the access procedure, a large proportion of the components used are not under the direct control of the local RAS administration. Therefore RAS access to a LAN must be monitored especially carefully and thoroughly.

Example

As Windows NT comes with RAS support as standard, the Remote Access Service of Windows NT will be used as an example. The functionality offered and the available security mechanisms are, however, generally only suitable for a small number of RAS users and for data which has a low protection requirement. Where there are large numbers of users and the protection requirement is high, additional RAS products should be considered as well.

The following applies to **RAS clients running under Windows NT**:

- For RAS clients, the option of saving user names and passwords so as to allow automatic connections should be disabled. This requires that the "Save password" option in the Dial-Up Networking dialogue is disabled. If the password has been saved by mistake, it can be deleted again by clicking the "Unsave password" pushbutton on the "Security" tab of the properties dialogue.
- Automatic establishment of a dial-up connection should only occur after confirmation by the user. This is ensured by selecting the "Always prompt before auto-dialing" option on the "Settings" tab of "User preferences" in Dial-Up Networking. However, it is best that auto-dialling should be completely disabled. This is ensured by disabling the option "Enable auto-dial by location" for all locations on the "Dialing" tab of "User preferences" in Dial-Up Networking.
- Care should be taken to ensure that no incoming connections are allowed. For the "Port Usage" setting under *Control Panel, Network, Services, Remote Access Service, Attached Device, Configure* the option "Dial out only" should be enabled.

- To ensure that communications are protected (using MPPE encryption), in the "Security" tab of Dial-Up Networking, the options "Accept only Microsoft encrypted authentication" and "Require data encryption" should be enabled. Care must be taken to ensure that the RAS server is correspondingly configured.
- Assignment of a fixed IP address to each RAS client should be considered. This makes it easier to trace activities performed over the RAS connection. The IP address can be entered in the TCP/IP properties of Dial-Up Networking under *Phonebook, Server, TCP/IP Settings* in the field "Specify an IP address".

The following applies to **RAS servers running under Windows NT**:

- RAS dial-in should only be permitted for authorised users. For all other users, the option "Grant dialin permission to user" must be disabled. This can be performed either through the User Manager or the RAS Manager.
- The option of callback by the RAS server should only be enabled for those users for whom this is explicitly allowed. If possible, a fixed callback number should be used.
- In order that RAS clients can request a fixed IP address, the option "Allow remote clients to request a predetermined IP address" under *Control panel, Network, Services, Remote Access Service, Attached Device, Network, TCP/IP settings* must be enabled.
- If use is to be made of MPPE encryption, then the relevant option must be enabled. This is achieved by selecting the following sequence of menu options: *Control Panel, Network, Services, Remote Access Service, Attached Device, Network, Encryption settings.*
- It is possible to specify for a RAS server under Windows NT whether RAS clients should only access the resources of the RAS server or whether they should be able to access the network to which the RAS server is connected as well. Depending on the intended purpose (e.g. export of local resources, RAS access server for a network), the appropriate access restrictions should be set. This is performed by selecting the option "Allow remote TCP/IP clients to access" under *Control Panel, Network, Services, Remote Access Server, Attached Device, Network, TCP/IP settings*.

Additional controls:

- Are all security breaches identified documented?
- Is user authentication performed for every connection established using the specified mechanism?
- Is protection of communications enforced for every connection through one of the procedures permitted in the RAS security concept?
- Can mobile RAS clients be protected through additional safeguards (e.g. encryption of hard disks)?

S 4.113 Use of an authentication server within RAS access

Initiation responsibility: IT Security Management Team

Implementation responsibility: Administrator

For RAS systems with a lot of users, consideration must be given to the question of how user administration for RAS access can be carried out efficiently. As a rule, every RAS user must also either be given a system identity (user account of the operating system) or else be identified via such a user account. Some operating systems (e.g. Windows NT) offer direct integration of the RAS functionality and a common user administration facility. For medium-sized and large networks, most of which are organisationally split into several subnets (domains, administration areas), in many cases there is often the problem that administration of user data is performed separately in each administration area. If such users are also to be able to log on to outside subnets, cross permissions (cross certificates, trust relationships) or a central directory service must be set up and maintained. Another alternative is that the users are given another user account in the other subnet; however this complicates administration of the user data. In particular, in the RAS context special authentication systems have been developed which can also be used for the "normal" authentication process during system logon. Typical examples of such systems are RADIUS, TACACS, TACACS+, SecureID, SafeWord etc.

These systems always operate as follows:

- Users' authentication data is administered through a central server.
- The system logon program refers to the authentication server to check the authentication data entered by the user.
- A secure protocol is generally used for communications between the logon process and the authentication server.

The logon process must support the use of external authentication servers and the network address of the authentication server to be used must be correctly entered in the configuration data for the logon process. If a user now wishes to log on to the system, irrespective of whether he is using a RAS connection for this or is directly inside the LAN, the following rough simplified sequence of events occurs:

- If a connection is established during the system or RAS logon process, the logon process contacts the authentication server and informs it that the user has requested a connection. If the Challenge-Response procedure is being used, the authentication server sends back a Challenge to the process, which then passes this on to the user.
- The user enters his secret authentication data. Depending on the system used, this can be a password or one of several types of one-time password (numbers, text).
- The logon process passes the data to the authentication server, generally transparently to the user.

- The authentication server verifies the user data and passes the results of the validation process to the logon process.
- If the user has been successfully authenticated, access is now granted to the (access) network.

Through the use of central authentication servers it is possible to ensure on the one hand that the authentication data is consistently administered and on the other hand that better authentication mechanisms can be used than are supported as standard by the operating systems. In particular, smart card and token-based mechanisms should be mentioned here. Depending on the system, these generate, for example, one-time passwords which are shown on a display and which the user must specify as password.

For medium-sized and large networks the use of authentication servers is especially recommended in the RAS area as these offer a significantly higher degree of security during user authentication. However, it should be noted that these servers also have to be administered and maintained. An authentication server must be positioned in the network in such a way that performance is good while at the same time protection is provided against unauthorised accesses.

Additional controls:

- Is the external authentication system supported by the operating system and the RAS system?
- Does the RAS client software allow use of a smart card reader for smart card-based authentication systems?
- What security mechanisms are offered by the external authentication system?

S 4.114 Use of the security mechanisms provided on mobile phones

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Users

Mobile phones and related services offered can be protected at various points by means of PINs and passwords. The facilities offered include the following:

Access to the SIM card

The SIM card can be protected against unauthorised access with a four- to eight-digit PIN. The subscriber identifies himself to the card using this PIN. If an unauthorised person gains possession of a SIM card, he cannot use it without also knowing the PIN. To prevent misuse of the SIM card, it is therefore essential that the option on the phone requiring entry of this PIN is activated so that once the mobile phone is switched on the PIN has to be entered. The PIN should not be kept with the mobile phone or SIM card.

Usually new mobile phones come with this PIN entry requirement disabled and a PIN is preconfigured. It is essential that the first time the phone is used the PIN is changed and activated. The PIN selected must not be a trivial number or a number that is easy to guess (e.g. 1111, date of birth etc.).

Note: On most mobile phones, underneath the numbers on the keypad there are also letters. These can be used to choose passwords for oneself instead of PINs. Passwords are easier to remember, but of course once again they must not be too simple. For example, "4EYES" corresponds to the PIN "43937".

After three failed attempts at entering the PIN, the SIM card is blocked. To lift this block, an eight-digit unblock code must be entered. This is frequently referred to as the PUK (PIN Unblocking Key) or Super PIN. After ten entries of an incorrect PUK, the card is invalidated. This unblock code normally comes in a PIN notification letter together with the SIM card. It should be kept with the utmost care and protected against unauthorised access. Under no circumstances should the PUK be kept together with the mobile phone.

As well as the PIN, there is also a PIN2, an additional secret number which can be used to protect access to certain functions on the SIM card. It is often used when changes need to be made to the configuration of the SIM card but the user himself cannot make these changes, for example restrictions on use of the phone. For example, there might be a corporate telephone directory which can only be modified after entry of PIN2. PIN2 has its own unblock code (PUK2).

Access to the mobile phone

In addition, there is generally also a security code for the mobile phone (device PIN) which is used to protect access to certain functions. Once again, this code should be changed to a user-defined value at the earliest opportunity. It should be written down and protected against unauthorised access. However, the device PIN does not have to be entered every time the mobile

phone is switched on. For example, this PIN can be used to prevent the mobile phone being used with a different SIM card (anti-theft protection).

Access to mailbox

The network provider can set up a mailbox for every subscriber which amongst other functions serves as an answerphone. As the mailbox can be interrogated from anywhere and also from any terminal device, it must be protected against unauthorised access with a PIN. When the mailbox is first set up, the network provider issues a predefined PIN. It is important that this is changed immediately.

Other passwords

As well as the various personal identification numbers listed above, there may be additional passwords for various types of use. For example, a password will be required to access the user data held by the network provider. Thus, a password may be required when the user rings the hotline to query a bill. Services which incur additional charges, such as retrieval of information or getting the network provider to perform certain configurations are generally protected through additional passwords. Like all other passwords, these should be chosen carefully and kept securely.

As a general rule, all PINs and passwords should be handled with care (see also S 2.11 *Provisions governing the use of passwords*).

Note: There have been a number of cases recently in which criminals have attempted to obtain the PIN or PUK of mobile phone users over the phone by posing as staff of a network provider and pretending that there is a technical defect. Information on personal identification numbers should **never** be given out over the telephone.

There are many different security mechanisms available with mobile phones. Which of these are available and how they can be activated depends on the particular mobile phone used, the SIM card and the selected network provider. Therefore the network provider's operating instructions and security instructions should be evaluated carefully. Where company phones are used, it is recommended that the most important security mechanisms are preconfigured and also documented in a well laid out leaflet.

S 4.115 Safeguarding the power supply of mobile phones

Initiation responsibility: Administrators, users

Implementation responsibility: Administrators, users

Normally rechargeable batteries are used as a means of maintaining the power supply to mobile phones. Depending on the capacity of the batteries and the design of the mobile phone, a single battery will last for a limited time, normally several hours. To ensure that a mobile phone is available at any time in case of need and that no data held in temporary storage is lost, certain precautions should be adhered to:

- Warning displays on the mobile phone that the battery is low should not be ignored.
- If it is foreseeable that the phone will be used over a relatively long period, then the battery charger should be taken along with the phone.
- When charging a mobile phone, the instructions contained in the manual which comes with a mobile phone should be observed; in particular, care must be taken to avoid impairing the life of the battery.
- Steps should be taken to ensure that when a mobile phone is issued, the battery is in a charged state. The state of charge of the battery should be regularly checked as a battery discharges over time even when it is not being used.

Check state of charge regularly

It is also recommended that any data stored on the mobile phone, such as telephone directory, short messages etc, is saved to a different medium at regular intervals.

If it is foreseeable that prolonged use will be made of the mobile phone, e.g. on business trips, a charged spare battery should be taken along as well. The spare battery should be kept in a protective case as damage can occur through overheating or fire if the battery contacts come into contact with conductive materials. This can be caused by many objects in everyday use such as keys or chains.

Avoid short-circuiting the battery

To avoid damage to the memory, a mobile phone should be switched off before the batteries are changed.

A mobile phone should not be exposed to any extreme temperatures. Otherwise, the battery in particular, but also the display, could suffer a loss of functional performance. Therefore neither mobile phones nor batteries should be left in parked vehicles.

Danger of extreme temperatures

S 5 Safeguard Catalogue - Communications

S 5.1 Removal, or short-circuiting and grounding, of unneeded lines

S 5.2 Chosing a suitable network topography

S 5.3 Selection of cable types suited in terms of communication technology

S 5.4 Documentation on, and marking of, cabling

S 5.5 Damage-minimising routing of cables

S 5.6 Mandatory use of a network password

S 5.7 Network management

S 5.8 Monthly security checks of the network

S 5.9 Logging at the server

S 5.10 Restrictive granting of access rights

S 5.11 Blocking the server console

S 5.12 Setting up an additional network administrator

S 5.13 Appropriate use of equipment for network coupling

S 5.14 Shielding of internal remote accesses

S 5.15 Shielding of external remote accesses

S 5.16 Survey of network services

S 5.17 Use of the NFS security mechanisms

S 5.18 Use of the NIS security mechanisms

S 5.19 Use of the sendmail security mechanisms

S 5.20 Use of the security mechanisms of rlogin, rsh and rcp

S 5.21 Secure use of telnet, ftp, tftp and rexec

S 5.22 Compatibility check of the transmission and reception systems

S 5.23 Selecting suitable types of dispatch for data media

S 5.24 Use of a suitable fax cover sheet

S 5.25 Using transmission and reception logs

S 5.26 Announcing fax messages via telephone

S 5.27 Acknowledging successful fax reception by telephone

S 5.28 Acknowledging a correct fax sender

S 5.29 Periodic checks of destination addresses and logs

S 5.30 Activating an existing call-back option

S 5.31	Suitable modem configuration
S 5.32	Secure use of communications software
S 5.33	Secure remote maintenance via modem
S 5.34	Use of one-time passwords
S 5.35	Use of UUCP security mechanisms
S 5.36	Encryption under UNIX and Windows NT
S 5.37	Restricting Peer-to-Peer functions when using WfW, Windows 95 or Windows NT in a server-supported network
S 5.38	Secure integration of DOS PC's into a UNIX network
S 5.39	Secure use of protocols and services
S 5.40	Secure integration of DOS-PCs to a Windows NT network
S 5.41	Secure configuration of remote access under Windows NT
S 5.42	Secure configuration of TCP/IP network administration under Windows NT
S 5.43	Secure configuration of TCP/IP network services under Windows NT
S 5.44	One-way connection setup
S 5.45	Security of WWW browsers
S 5.46	Installing stand-alone-systems for Internet use
S 5.47	Configuration of a Closed User Group
S 5.48	Authentication via CLIP/COLP
S 5.49	Callback based on CLIP/COLP
S 5.50	Authentication via PAP/CHAP
S 5.51	Security-related requirements for communications links between telecommuting workstations and the institution
S 5.52	Security-related requirements for communications computers
S 5.53	Protection against mail bombs
S 5.54	Protection against mail overload and spam
S 5.55	Checking of alias files and distribution lists
S 5.56	Secure operation of a mail server
S 5.57	Secure configuration of mail clients
S 5.58	Installation of ODBC drivers
S 5.59	Protection against DNS spoofing

S 5.60	Selection of a suitable backbone technology
S 5.61	Suitable physical segmentation
S 5.62	Suitable logical segmentation
S 5.63	Use of PGP
S 5.64	Secure Shell
S 5.65	Use of S-HTTP
S 5.66	Use of SSL
S 5.67	Use of a time stamp service
S 5.68	Use of encryption procedures for network communications
S 5.69	Protection against active content
S 5.70	Network address translation (NAT)
S 5.71	Intrusion detection and intrusion response systems
S 5.72	Deactivation of unnecessary network services
S 5.73	Secure operation of a fax server
S 5.74	Maintenance of fax server address books and distribution lists
S 5.75	Protecting against overloading the fax server
S 5.76	Use of suitable tunnel protocols for RAS communication
S 5.77	Creating subnetworks
S 5.78	Protection against mobile phone usage data being used to create movement profiles
S 5.79	Protection against call number identification during use of mobile phones
S 5.80	Protection against bugging of indoor conversations using mobile phones
S 5.81	Secure transmission of data over mobile phones
S 5.82	Secure use of SAMBA
S 5.83	Secure Connection of an External Network with Linux FreeS/WAN

S 5.1 Removal, or short-circuiting and grounding, of unneeded lines

Initiation responsibility: Head of Site/Bldg Technical Service

Implementation responsibility: Administrator; Site/Bldg Technical Service

It is advisable to remove unnecessary lines. If this is not feasible due to the resulting disruption of operations (opening of ceilings, window-sill and floor ducts), the following measures are useful:

- marking those lines which are not needed in the review documentation and deleting the entries in the documentation kept in the distributor;
- opening of all strap connections and crosscuts of free lines in the distributors (to the extent possible);
- short-circuiting the free lines at both cable ends and in all affected distributors;
- grounding of free lines (ground connection) at both cable ends and in all affected distributors. If this causes ground-induced ripple pickup, single-end grounding will be sufficient;
- ensuring that lines no longer needed will be removed when other relevant work is carried out.

Additional controls:

- Who decides on the need for lines and on the required reserves?
- Who verifies proper short-circuiting and grounding?

S 5.2 Selection of an appropriate network topography

Initiation responsibility: Head of IT Section

Implementation responsibility: Network planner; Head of Site/Bldg Technical Service

The topography of a network is the purely physical structure of the network as it is visible with cables. In contrast to this, the topology of a network is the logical structure as it appears to network components. The topography and topology of a network are therefore not necessarily identical. By nature, topography mostly relates to the spatial environment of the building. These are amongst others:

- locations of the network subscribers
- available space for cable routes and cables (S 1.21 *Sufficient dimensioning of lines*)
- required cable types (S 1.20 Selection of cable types suited in terms of their physical/mechanical properties)
- specifications regarding cable protection (S 1.22 *Physical protection of lines and distributors*)

The advantages and disadvantages of various possible topographies are discussed in the following. Other conceivable topographies which are not mentioned in this chapter can be considered as special cases of the structures described here.

In general, a distinction can be made between two basic types of configuration, star and bus, which can also be extended to form the tree and ring configurations respectively. These four types are described briefly in the following:

Star

All subscribers in a star network are linked with a central node via a dedicated line. The cabling of the frequently-used Token-Ring architecture topographically results in a star configuration, but functions topologically as a ring.

Advantages:

- Impairment of a line will only affect the operations of the system connected to it.
- Changes in the allocation of network subscribers to connection points at the central node and separation of individual subscribers can be performed centrally.
- A topographical star configuration can serve as a basis for forming any conceivable topology.

Disadvantages:

- Failure of the central node will result in the failure of all connected IT systems.
- Extensive cabling is required due to the separate linkage of each subscriber to the central node.
- With an increasing number of individual lines, the risk of cross-talk will increase.
- Cabling in star configuration might restrict the communications range, depending on the cable type and communications protocol in use (refer to S. 5.3 *Selection of cable types suited in terms of communications technology*). Repeaters can be used to solve this problem, although they prove very expensive if a large number of lines is involved. Furthermore, it is not possible to insert any required number of repeaters into a line. The maximum number here also depends on the protocol in use. Another alternative is to convert the network to a tree configuration.

Tree

A tree structure is formed by linking together several star networks. In this case, the network subscribers are assigned to groups which are connected in star configuration to decentral network nodes. These decentral network nodes are linked mutually via one line or several dedicated lines. In certain cases, all the decentral nodes are also routed to one central network node.

Advantages:

- As concerns a linkage of the systems to the decentral network nodes, the same advantages apply here as in the case of the star network.
- For new subscribers, new cabling is required only in the area of the corresponding decentral network node.
- Given an appropriate configuration of the decentral network nodes, an exchange of data between the subscribers of any particular node is possible even if the other nodes fail.
- Connecting the decentral nodes to each other via a single line reduces the cabling requirements.
- Amplification on a single line is sufficient for bridging large distances between the nodes (cost saving).
- It is advisable to link the nodes by means of (usually more expensive) high-quality cables, which can also bridge large distances without the need for additional amplification. As compared with the repeater option which would otherwise be required, this offers advantages in terms of reduced costs and increased reliability.
- A tree structure allows the establishment of redundant links through the meshing of the individual nodes.

Disadvantages:

- Failure of a transition from one decentral network to another will disrupt the operations of all the connected subscribers.

Bus

In the case of a bus, all network subscribers are connected to a common line. This line usually consists of a central cable, to which the individual subscribers are connected via breakout cabling.

Advantages:

- Cabling is reduced to just one cable and any breakout cabling which might be required.
- A subsequent installation of new subscribers generally requires only minimal cabling: the subscribers are simply connected to the existing bus cable.
- A bus can be easily extended through the use of repeaters. However, it must be noted that such extensions are restricted in length in accordance with the type of cable and protocol used (refer to S 5.3 *Selection of cable types suited in terms of communications technology*).
- Resources can be connected to almost any point on the bus.
- Due to the central cable, the bus cabling takes up much less space than a comparable star configuration with a TP cable.

Disadvantages:

- Interferences in the cable line affect the entire bus.
- An interruption in the bus cable completely paralyses data communications.
- From a certain bus length and number of subscribers onwards, the bus can no longer be extended easily.
- Depending on the type of cable in use, restrictions need to be observed when connecting new subscribers (e.g. the minimum distance between two subscribers).

Ring

Topographically, a ring is a bus whose two ends are connected together. One special type of ring consists of a double-ring like that used with FDDI, for example.

Advantages:

- If a line is interrupted, a ring can continue operation to a limited extent. The type of limitation depends on the network access protocol used for the ring and can involve, for example, losses in bandwidth..
- The optional, double-ring design provides additional redundancy and failure tolerance.

Disadvantages:

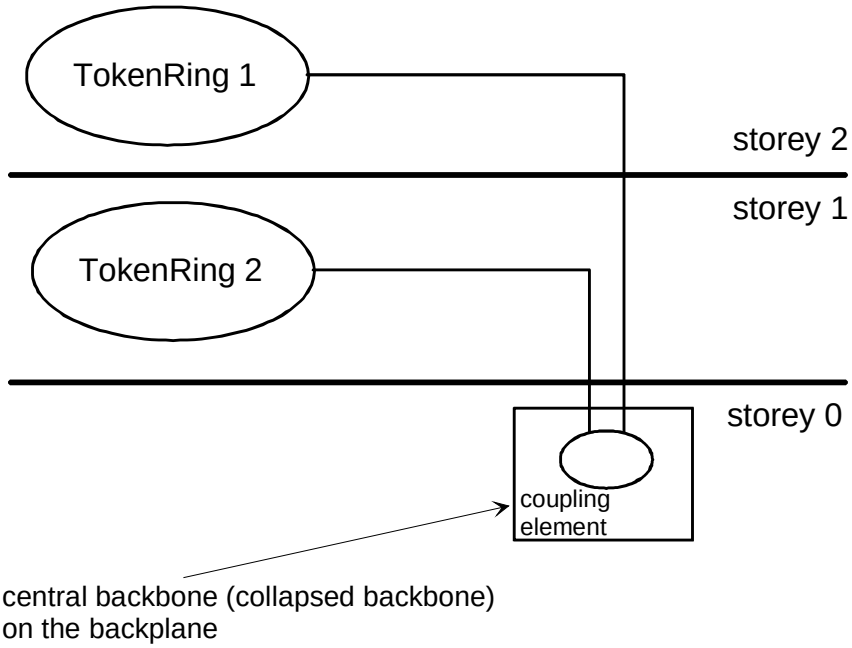
- A restricted number of protocols is available for the ring and double-ring systems, i.e. not all protocols can be used on these systems. This can prove disadvantageous for the future development of a network.

Collapsed and distributed backbone

A **collapsed backbone** is a special variant of a network node whose backplane (a local, high-speed link within a device) incorporates one of the above-mentioned structures or a combination thereof. In the case of a collapsed backbone, all cables are routed centrally to one network node, thus comprising a star configuration in principle. A large variety of structures can be supported within the network node. In the case of a tree structure, for example, very short connection lines within the network node are used to establish the required links between the decentral stars.

Advantages:

- All cable connections can be controlled and managed centrally.
- High transmission rates are generally achieved in the backplane. Depending on the product in use, this results in the availability of the full network bandwidth between the segments. Disadvantages:
- If the collapsed backbone fails, so do all network access ports.



In the case of a **distributed backbone**, the individual network components belonging to the backbone are spatially distributed and coupled via the standard network infrastructure. Topographical trees, for example, are generally realised by means of a distributed backbone.

As mentioned above, no general recommendations can be made as regards the selection of a suitable network topography. One of the factors which decisively influence any such selection is the structural environment. In general, newly installed networks today are wired in star or tree configuration. Here, it is advisable to use optical fibre cables in the backbone areas (primary and secondary areas) and twisted-pair cables from category 5 or higher for the

storey cabling (tertiary area). The primary area contains the cabling which links buildings together, whilst the secondary area contains the cabling which links together the active network components of individual sections within a building (e.g. linkage of individual storeys).

From today's perspective, the selection of these media for the individual areas ensures cabling which has a guaranteed future and which also fulfills high requirements concerning the bandwidth, particularly in the backbone area. In each case however, a check must also be made as to whether a hybrid installation consisting of star and ring configurations is practical or necessary. Here, it is often useful to install primary cabling between buildings as a FDDI double ring, and secondary as well as tertiary cabling in star or tree configuration, as mentioned above.

S 5.3 Selection of cable types suited in terms of communication technology

Initiation responsibility: Head of IT Section

Implementation responsibility: Network planner; Head of Site/Bldg Technical Service

From the communications technology standpoint, the choice of cable is determined by, among other things, the required data transfer rate (bandwidth) and the distances to be covered without repeaters. The requirements arising from the structural conditions at the installation location also have to be taken into account when making the selection. In the following, the respective advantages and disadvantages are described from an IT security point of view.

At present there can be considered to be two types of transmission media for cable (as opposed to wireless) communications: copper cable or an optical medium (optical fibre (FO)). Both of these types of media can be further divided into various subcategories. The most important of these for the medium of copper are the coaxial cable (one centre conductor with overall screening) and the multi-core copper cable with the wires twisted in pairs (twisted-pair cable, TP cable). These are explained in more detail below.

Twisted-pair cable

Twisted-pair cables are available in many different forms. These differ on the one hand according to the nature of their shielding and on the other according to their potential bandwidth. The current shielding classes are as follows:

- unshielded (UTP)
- unshielded but with overall screening (*screened-unshielded*, S/UTP),
- shielded, where the individual pairs of wires are shielded (*shielded*, STP)
- shielded TP cable with additional overall screening (*screened-shielded*, S/STP).

In addition to their shielding designations, TP cables are divided into categories according to their bandwidth and other electrical properties, currently categories 1 to 5. A draft standard has been drawn up for categories 6 and 7. The rule here is: the higher the category, the higher the possible bandwidth. The bandwidth is determined by various physical properties of the cable. The commonly used UTP or STP cables in categories 3 to 5 can be used to transfer between 10 and 100 Mbit/s over a maximum length of 100 m with Ethernet or Fast Ethernet, while up to 155 Mbit/s can be transferred on category 5 cables with ATM. Cables in category 6 will have a bandwidth of 600 MHz and therefore allow data transfer rates of up to 1 Gbit/s.

TP cables are at present mainly used for star-type cabling and in some cases also for ring-type cable configurations.

Advantages:

- TP cables, and in particular the methods of preparing them for installation, are relatively cheap in comparison with optical fibres if bandwidth needs are low.

- TP cables up to category 5 are relatively easy to install and prepare.
- TP cables can be considered to be universal cables, because other services (such as telephony) can be used via these cables without major technical investment. If bandwidth needs are relatively low, existing telephone networks based on TP can also be used as data networks.
- It is easy to measure and test existing installations.

Disadvantages:

- Depending on the type of cable used (UTP to S/STP), the cable is surrounded by an electrodynamic field of greater or lesser strength. As a result of this, there is both a risk of interaction with other fields (for example from an adjacent cable or from power installations) and the possibility of data interception.
- The maximum cable length given the requirements commonly encountered today is limited to 100 m (including the necessary connecting cables and patch cables; cf. table below).
- In the case of unshielded installation cables (UTP) with a large number of pairs, there may be cross-talk between individual pairs.

Coaxial cable

Coaxial cables are mainly used for bus cabling or for connecting the network nodes in tree structures, for example. Thanks to the overall screening of the centre conductor, it can generally be assumed that the electromagnetic compatibility (EMC) of these cables is good.

Advantages:

- The bandwidth and unamplified transmission range are greater than in the case of TP cables. For both types of cable which can be used for the Ethernet protocol the upper limits, depending on cable type, are 185 and 500 m respectively (thin and thick Ethernet cable).
- The risk of cross-talk is lower with coaxial cables that with TP cables.

Disadvantages:

- Coaxial cables are generally more expensive than TP cables.
- Despite the coaxial design, the cables can be tapped and are sensitive to interference.
- Depending on the type of coaxial cable used, they have relatively wide bending radii and are therefore more difficult to install than TP cables, for example.
- Only a few network access protocols have been defined for coaxial cables. Fast Ethernet, for example, cannot be run on coaxial cables.

Optical fibres (FO)

Optical fibre cables use light in the visible to far infrared range for the transmission of signals. The structure of an optical fibre cable is similar to that of a coaxial cable. The actual optical fibre in the centre is surrounded by cladding, the optical properties of which are different from those of the core.

Around the whole of this is another sheath to provide protection against mechanical and optical influences. Optical fibres are available in two versions: multimode and single-mode optical fibres. These two types differ primarily in terms of the possible bandwidth and the maximum length that can be attained without additional repeaters.

Optical fibre cables are generally used for bridging long distances (for example connections between buildings or floors) in a backbone, and in some cases in dual ring systems.

Advantages:

- The bandwidth and the unamplified range is greater than with copper cable.
- Tapping can be achieved only with substantial technical effort.
- Inadmissible rewiring/changes of line assignment can be easily identified by means of the available technology.
- Optical fibre cables are insensitive to all non-destructive ambient conditions, in particular to electromagnetic fields.
- Optical fibre cables require relatively little space.
- There is no cross-talk or interference between various optical fibres or an optical fibre and TP cables.
- With optical fibres the fire load is lower in comparison with copper cables, because they have less or different sheathing and also because as a rule less cable material is required over a given route.

Disadvantages:

- The installation costs for optical fibre cables are very much higher than for copper cables, mainly due to the splicing work required.
- The coupling components for the operation of optical fibres, especially for single-mode optical fibres, are more expensive than those for copper cables.
- Laying and preparing optical fibre cables requires special knowledge, special tools and special additional components (e.g. splice boxes).
- Optical fibres cannot be bent through just any radius, as required. This may make installation more difficult, as a result of the need to take account of possible and necessary cable routing options.

An overview of the length restrictions on cables for some of the common protocols (Ethernet, Fast Ethernet, FDDI and CDDI; cf. S 5.60 *Selection of a suitable backbone technology*) is given in the table below:

Network access protocol		**Cable type**	**Max. length**
Ethernet	10Base2	Coaxial	185 m
	10Base5	Coaxial	500 m

	10Base-T	TP	100 m
	10Base-FL monomode	FO	2 km
	10Base-FL single-mode	FO	5 km
Fast Ethernet	100Base-TX	TP	100 m
	100Base-FX	FO	412 m
FDDI	Monomode	FO	2 km
	Single-mode	FO	60 km
CDDI		TP	100 m

It should be noted that the lengths stated above are the maximum lengths in each case. This is often made up of the installation cable itself and the connecting cables (patch cables). For 10Base-T, for example, the length of the installation cable should therefore not exceed 90 m so as to leave sufficient length for patch cables. With some procedures (such as 100Base-FX) the length is reduced by the use of repeaters, depending also on the type of repeaters.

When installing new networks it makes sense to use optical fibres in the primary and secondary areas because they will be able to satisfy future requirements thanks to the high available bandwidth. For the tertiary area it needs to be examined whether the use of TP cables or optical fibres is possible and/or necessary according to technical and security criteria, and also whether it is justifiable from the economic standpoint (cf. also S 5.2 *Selection of an appropriate network topography*).

S 5.4 Documentation on, and marking of, cabling

Initiation responsibility: Head of IT Section; Head of Site/Bldg Technical Service

Implementation responsibility: Site/Bldg Technical Service

Good documentation and clear marking of all cables are required for any protective measure, for maintenance, fault location, repair and for successful checking of cable layout. The quality of such review documentation depends on the completeness, up-to-date status and readability of its contents.

A l l facts concerning the network must be included in this documentation (also referred to as "master plan"):

- precise type of cable;
- application-oriented marking of the cable(s);
- location of exchanges and distributors, with precise designations;
- precise routing of cables and ducts on the premises (plotting on dimensioned floor plans and location plans);
- dimensioning and allocation of lines;
- allocation plans for all connectors and distributors;
- use of all lines; listing of the network users connected to them;
- technical specifications of connection points;
- danger spots;
- protective measures that are in place and to be reviewed.

Based on this documentation, it must be possible to get an accurate overview of the cabling easily and quickly.

Since, with increasing size of networks, it is not possible to include all information in a single plan, it is advisable to subdivide such information. Actual location information is always to be plotted on full-scale plans. Other information can be listed in tables. An important point is to ensure clear cross-referencing of all listed elements.

To keep the documentation up to date, it must be ensured that the person keeping the documentation is promptly and completely notified of all work carried out on the network.is For instance, consideration might be given to requiring this person's co-signature for the issue of material, for the placing of outside contracts or for allowing access to protected areas.

Since this documentation contains sensitive information, it must be stored safely and access to it must be regulated.

Additional controls:

- Who is responsible for the documentation on cabling?
- Is up-dating of the documentation sufficiently prompt?
- How is the review documentation protected against unauthorised access?

S 5.5 Damage-minimising routing of cables

Initiation responsibility: Network planner; Head of IT Section; Head of Site/Bldg Technical Service

Implementation responsibility: Site/Bldg Technical Service

When planning cable routes, attention must be given to avoiding perceptible danger spots. As a general rule, cables should be routed only in areas which can be accessed exclusively by the user. Control will be facilitated by a clear layout of lines. Routes and individual cables should always be laid out in such a way that they will be protected against direct damage caused by persons, vehicles and machines.

When selecting a site for equipment, it should be ensured that the cables are not run in walking or driving areas. If this cannot be avoided, the cables must be protected by adequate duct systems in the light of the anticipated mechanical loads.

As a general rule, attention must be given, in the case of appliance cords (flexible cables), to sufficient pull relief of the cables in the connector(s). In instances, it may be expedient to do without the screwing of the connectors. In case of tensile load, only the plug-in connections, and not the connector/cable or connector/device soldering points will be torn apart.

Underground car-parks pose a major problem as regards damage-minimising routing of cables. Due to the automatic operation of control devices and on account of the long periods during which entrance gates are open, access by outsiders to underground car-parks can never be precluded. On account of the normally low height of ceilings, simple means suffice to obtain access to the lines located there. When lines are located in the driving area, there may not be enough space left for the permissible height of vehicles. In that case, damaging or destruction of ducts and cables by vehicles cannot be precluded.

When buildings are used jointly with third parties, it must be ensured that cables are not run in floor ducts in areas occupied by those parties. Floor and window-sill duct systems must, by mechanical means, be tightly shielded against the areas of external users. The preferable solution is to confine such ducts to the user's own area.

Areas with a high fire hazard must be avoided. If this is not possible and the operating state of all cables run on a cable route is to be maintained, fire sealing must be provided for that route. If only individual cables are to be kept in an operative condition, an appropriate cable must be selected for this purpose.

In production plants, high inductive loads and the resultant interference fields are to be expected. These must also be taken account of in the layout of ducts and cables. For cable protection, an approach similar to that of fire sealing is to be taken.

In the case of underground lines, warning tapes must be laid approx. 10 cm above the line. For individual cables (without conduit), it is advisable to provide cable covers.

S 5.6 Mandatory use of a network password

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

As a standard feature, a user password should be provided for every user (as well as for administrators) in a local network. For correct handling of such passwords, the provisions of safeguard S 2.11 *Provisions governing the use of passwords* must be observed.

Additional controls:

- Has every user been provided with a password?
- Have users been informed on how to handle passwords correctly?

S 5.7 Network management

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section

Networks can be managed centrally or locally at the various nodes. This will depend on the technical possibilities and administration of the network nodes. In any case, central co-ordination of all network activities of an agency/company is required in order to avoid redundancies. The following should be controlled centrally:

- selection and layout of cables;
- selection of the IT systems and applications in order to avoid incompatibilities;
- central allocation of network addresses and user IDs;
- the organisational allocation of network components, e.g. to departments.

Local management of the various network nodes and the connected IT systems is also possible.

In this respect, the functions and responsibilities of system administrators must be clearly specified and regulated (cf. also S 2.26 *Designation of an administrator and his substitute*).

S 5.8 Monthly security checks of the network

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The network administrator should perform at least monthly security checks of the network. Some network operating systems offer programs which automate these checks. One example is the program SECURITY in the directory SYS:SYSTEM within Novell 3.11. The parameters checked include the following:

- Are there any users without a password?
- Are there any users who have not used the network for some time?
- Are there any users whose passwords do not meet the prescribed requirements?
- Which users have the same rights as the supervisor?

UNIX systems also come with programs which enable such checks to be performed automatically. A large number of public domain and commercial programs offer additional test capabilities. Some of these programs are described in S 4.26 *Regular security checks of the UNIX system.* The secure UNIX administration tool developed by the BSI (USEIT) also offers extensive facilities for checking the network security of a UNIX system. The tests performed include the following:

- checking for log-ins without passwords or with only weak passwords,
- checking of preconfigured minimum password length,
- checking of network services and their configuration,
- penetration testing in the local subnetwork,
- inconsistency checks of system files and the system,
- checking for insecure ports and services.

Additional controls:

- Are the performance and results of such security checks documented?

S 5.9 Logging at the Server

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

The logging possible on the network server should be activated to a sensible degree. The Network Administrator must review the network server log files at regular intervals. All security-relevant events should be logged. In this context, the following occurrences are of particular interest:

- entry of an incorrect password for a user ID through to blocking of the user ID when the maximum permitted number of unsuccessful attempts has been reached,
- attempts to gain unauthorised access,
- power failure,
- data on network utilisation and network overload.

How many other events are logged will depend to a certain extent on the protection requirements of the IT systems concerned. The greater the protection requirement, the more information should be logged.

As log files can become very long over time, the intervals at which they are evaluated should kept short. To enable appropriate analysis of the data, every protocol entry should include the user ID or process number, terminal device ID, date and time.

Additional controls:

- Who analyses the log files and at what intervals?
- Are the evaluations documented?

S 5.9 Logging at the server

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

The logging possible on the network server should be activated to a sensible degree. At regular intervals, the network administrator must screen the log files of the network server. In this context, the following occurrences are of particular interest:

- entry of a wrong password for a user ID, to the barring of the user ID when the limit of unsuccessful attempts has been reached;
- attempted violation of access rights;
- power failure
- data on capacity utilisation and network congestion.

As, in the course of time, these files can become very voluminous, the intervals between analyses should be short enough to allow efficient analysis.

Additional controls:

- Who analyses the log files at what intervals?
- Are the analyses being documented?

S 5.10 Restrictive granting of access rights

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Access rights to data held on the hard disk of the network server must be allocated on a restrictive basis: Each user will be authorised to have access only to those files needed for the performance of his tasks. In turn, the access rights will be confined to the required type of access.(See also S 2.5 *Division of responsibilities and separation of functions*, S 2.7 *Granting of (system/network) access rights* and S 2.8 *Granting of (application/data) access permissions*). (On this point, see also S 2.5 *Division of responsibilities and separation of functions*, S 2.7 *Granting of system/network access authorisations* and S 2.8 *Granting of (application/data) access rights*) Thus, for instance, it will very rarely be necessary to grant write access to programme files.

In most cases, it is possible to have access to files in sub-directories if such rights exist for parent directories (inheritance). This implies that access rights at the highest level (volume level) should be granted only on a very restrictive basis. Particularly when installing new software products, the granting of rights should be revised.

If the PCs are provided with floppy disk drives, particular importance should be attached to the restrictive allocation of rights.

If little storage space is provided on a network server, the maximum memory capacity which a user may occupy on the network server can be restricted (disk quota).

Additional controls:

- Is it possible, on the basis of the documentation on the rights structure, to verify that only the minimum rights required have been granted?

S 5.11 Blocking the server console

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

From the server console, it is possible to control the network server. If the server console is not blocked during network operation, anybody obtaining access to the server room can exploit this opportunity for illicit manipulations. Therefore, the server console should generally remain blocked and only be released with a special password.

This measure can be replaced or, preferably, be complemented by S 1.23 Locked *Doors*.

Additional controls:

- Is default blocking of the server console provided?

S 5.12 Setting up an additional network administrator

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Arrangements must be made for the possible situation that both the network administrator and his deputy are not available. In such cases, an additional user must be established who shares the rights of the network administrator. The user ID and the pertinent password must be deposited in a sealed envelope. Use of the password must be documented and be controlled according to the two-person rule.

Additional controls:

- Has a user substituting for the network administrator and his deputy been designated?

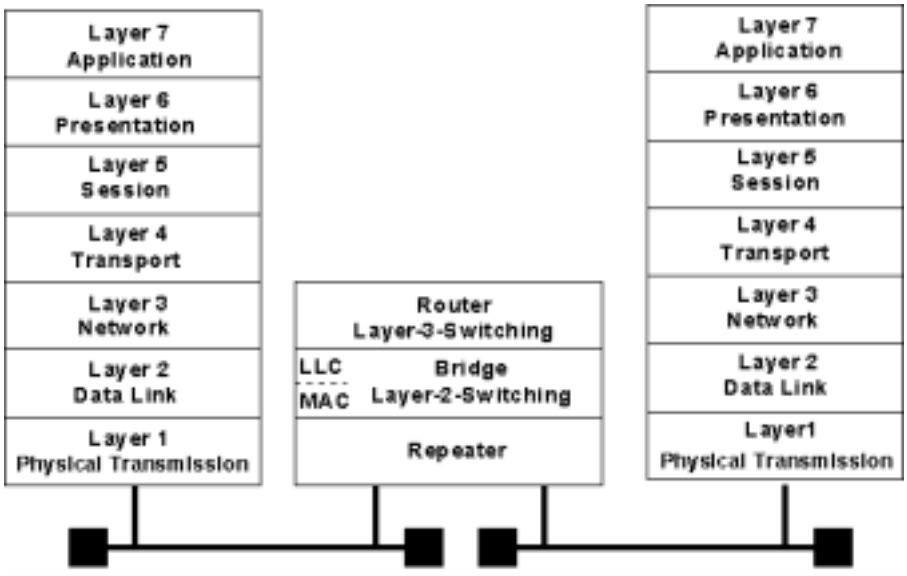
S 5.13 Appropriate use of equipment for network coupling

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section, Administrator

Devices used for network coupling such as routers, bridges or gateways not only connect networks, but can also be used for the physical or logical segmentation of networks. Availability can be enhanced by segmenting large networks into sub-networks, as a failure then affects only a limited part of the network and can be located more quickly. With an increasing number of network stations, response times can become unacceptable, and the need may arise to establish sub-networks for load balancing. Protection of sensitive information may be another reason for segmentation of networks so as to ensure that such information is not available throughout the network. For protection against external perpetrators, it may be advisable to allow transfer of packets only from a secure to a non-secure network; on the other hand, for protection of confidential data it may be advisable to bar transfer of packets from a secure to a non-secure network.

A segmentation or coupling of networks can be performed on various layers in accordance with the OSI model. In this model, network coupling elements comprise, for example, repeaters on the physical layer (layer 1), bridges on the data link layer (layer 2), routers on the network layer (layer 3) and, in general, gateways on the application layer (layer 7). The illustration below is intended to provide a clearer understanding of the OSI model.



The OSI/ISO reference model

Connection with another network on a higher layer (from layer 3 onwards) of the OSI model allows, for example, the data flow to be regulated in

accordance with security requirements, and thus achieves a controlled linkage between insecure networks and networks requiring protection.

On the other hand, it might become necessary to separate two networks if one needs to be protected against access from the other and vice versa, if the network availability in the event of a failure needs to be increased, or if the load on the individual network segments needs to be decreased.

To prevent manipulation, all network coupling devices must be installed so that only authorised persons have physical access to them.

Repeaters

Repeaters operate on layer 1 of the OSI model, and simply comprise signal amplifiers. As a result, they allow the maximum cable length of an existing network segment to be increased, or several network segments to be linked together. In an Ethernet network based on coaxial cables, for example, repeaters can be used to extend the maximum cable length to more than 185 m and 500 m respectively (for thin and thick Ethernet cables). Observance is required here of the configuration rules for repeaters, which impose constraints on the number and arrangement of repeaters.

In the case of twisted-pair cabling, repeaters are often used as central or decentral network nodes for the purpose of linking individual network subscribers. As several repeaters need to be connected together in one device for this purpose, such a device is termed multi-port repeater. Multiport repeaters are often also identified as hubs or mini-hubs.

The separation thus achieved on layer 1 of the network restricts electrical errors to just one segment. However, this does not apply to errors occurring on higher layers (e.g. excessively frequent collisions or broadcast storms). Some manufacturers now also offer multi-port repeaters which evaluate information from layer 2 (but do not act as bridges), thus allowing the implementation of access restrictions. With such devices, for example, it is possible to grant network access only to certain network users.

Bridges

Connection of networks on layer 2 of the ISO/OSI reference model is performed using bridges. A bridge connects two networks which generally use the same logical link control protocol (LLC), but different medium access control (MAC) protocols. For instance, a bridge can connect an Ethernet with a Token-Ring network. Such a bridge is termed translation bridge or T-bridge.

This results in three essential advantages:

- The bridge separates collision domains, i.e. performance-reducing collisions occurring in one segment of a CSMA/CD-based network do not impair other segments.
- A bridge only routes data packets to another segment if the destination address of the packets is located in that segment. This restricts the data traffic to the required segment in each case, thus lowering susceptibility to eavesdropping.

- For this reason a bridge also raises the data throughput in each segment, as data can be transmitted independently on either side of the bridge, thus achieving a separation of loads.

Switches (Ethernet, Token-Ring, ATM)

A *switch* is a variant of a bridge which links several logical LAN segments (multi-port bridge), and operates on layer 2 of the OSI model. Some new products also implement a switching functionality on layer 3 of the OSI model, thus allowing segmentation on this layer.

An Ethernet switch consists of several bridges connected together internally in an appropriate manner (e.g. via a switching matrix).

An Ethernet switch provides the advantages of a bridge for several ports (8 to 32 ports per switch are standard at present), i.e. every subscriber and every segment at a switch port comprises a separate collision domain, and connections are established on demand. This allows every connected segment to communicate with any other segment, irrespective of the network traffic and load, provided that it is not already busy. Switches are particularly suitable for load separation and as central coupling elements for several sub-segments. Cascading switches, i.e. connecting secondary switches to a central switch, allow the formation of extremely high-performance networks, given that an appropriate, logical network structure has been selected.

Ethernet switches which operate in accordance with the IEEE standard for bridges use the store-and-forward technique. With this technique, the entire Ethernet packet of the source port is first read in and checked for correctness. Only packets which have been received correctly and completely are forwarded to the target segment. Such switches generate relatively long delay times, but also guarantee that no faulty packets are routed to other segments. The use of such store-and-forward switches is advisable in situations where maximum availability and integrity are of greater importance than bandwidth.

In contrast, alternative techniques which have also been developed increase the throughput of an Ethernet switch, i.e. shorten the delay times involved in the processing of data packets. One such technique, termed on-the-fly or cut-through, does not read in and check entire data packets; instead, it just evaluates the target address of a packet and then sends the whole packet immediately to this address. On-the-fly switches are thus up to 20 times faster than store-and-forward switches. However, they can also route faulty packets to other segments, thus impairing the bandwidth and, under certain circumstances, the availability of the segments in question. For this reason, on-the-fly switches should be used in networks characterised by an infrequent occurrence of faulty packets and requiring the maximum throughput. Most manufacturers now offer switches which incorporate both technologies and can thus be configured as required.

Some products now also support switching on layer 3 of the OSI model. In this case, network subscribers are no longer distinguished by their MAC address (layer 2 switching), but by the addresses on layer 3 (for the TCP/IP protocol stack, this is the IP address). Layer-3 switching can further enhance performance; for this though, the switch must be able to process the protocols used on layer 3, similar to a router.

In terms of their function, switches for ATM and Token-Ring are very similar to Ethernet switches, i.e. a switch for these protocols also allows two network subscribers or segments to communicate with each other, independently of the remaining subscribers / segments. In fact, the underlying design of an ATM network makes the use of switches mandatory in such a network.

During the selection of switches intended to realise a collapsed backbone, the available port density must be taken into account. A collapsed backbone should not involve the use of several switches, if these switches do not have a common (high-speed) backplane (refer to S 5.2 *Selection of an appropriate network topography*).

Routers

Routers separate or link networks on layer 3 of the OSI model. Routers thus do not operate independent from network protocols (like repeaters and bridges do, for example), but need to process the protocols in use on the network layer too. As a result, routers significantly retard the flow of data between two connected subnetworks, as they need to evaluate every packet on layer 3.

Due to their ability to process protocols, routers are used mainly for LAN-LAN and LAN-WAN coupling. For example, a router can link two LANs via an ISDN line. In this case, the LAN protocol is encapsulated in its original form in the WAN protocol and then transferred. Another protocol which can be used here is the X.25 protocol. In large networks consisting of many subnetworks which are linked together via routers, one important task performed by these routers is *routing* between the subnetworks, i.e. forwarding of data packets between these subnetworks. A fundamental distinction can be made between two techniques here:

- Static routing, which involves manual specification of routes.
- Dynamic routing, which involves automatic discovery and regular updating of routes by the router. For this purpose, several algorithms and protocols are available which also ensure synchronisation between the individual routers. The most familiar protocols are RIP (Routing Information Protocol), OSPF (Open Shortest Path First) and IGRP (Interior Gateway Routing Protocol). For the selection of a suitable routing protocol, also refer to S 4.82 *Secure configuration of active network components*.

Filters can also be used to ensure access control, i.e. to specify which systems are allowed to communicate with each other via the router in which directions using which protocols.

Concentrators and hubs

A *Hub* is an element which incorporates one or more active network coupling components and allows these components to communicate with each other via an internal backplane (also refer to S 5.2 *Selection of an appropriate network topography*). Hubs which can incorporate several network coupling components, if required, are termed *modular hubs*. Accordingly, hubs which can only incorporate one coupling component are termed *non-modular hubs*. If it is possible to connect the backplanes of several hubs together, these hubs are termed *stackable hubs*. The use of a hub or concentrator results - at least to

a partial extent - in a star-shaped wiring of the terminal devices; for this reason, hubs and concentrators are also termed star couplers.

As already mentioned in the case of repeaters, the smallest form of a concentrator or a hub is a *multi-port repeater*. In contrast, modular hubs allow the integration of various coupling elements (e.g. repeaters, bridges, routers) which, in turn, can operate on several layers. This concentration of network coupling components at a single point gives rise to advantages which facilitate the administration of the network, although a failure of such a central hub would affect the entire network. Appropriate precautionary measures, e.g. redundant arrangement of the network components, should be taken for such a contingency (refer to S 6.53 *Redundant arrangement of network components*).

Gateway

A gateway links two networks on the application layer (layer 7) of the OSI model. For this reason, a gateway not only converts network protocols, but also transports data on the application layer and, if necessary, modifies this data and evaluates it from the perspective of security. One typical application of a gateway is communications between systems in a TCP/IP network and a SNA host. In this case, the gateway consists of a combination of hardware and software. However, there are also gateways based purely on software. These include, for example, mail gateways which can recognise and convert different mail formats.

S 5.14 Shielding of internal remote accesses

Initiation responsibility: PBX officer; IT Security Management

Implementation responsibility: Administrators

The remote accesses in case of PBX equipment are used for remote maintenance, remote administration and network management tasks. Furthermore, remote accesses can also exist for system users (dial-in options).

A distinction can be made between

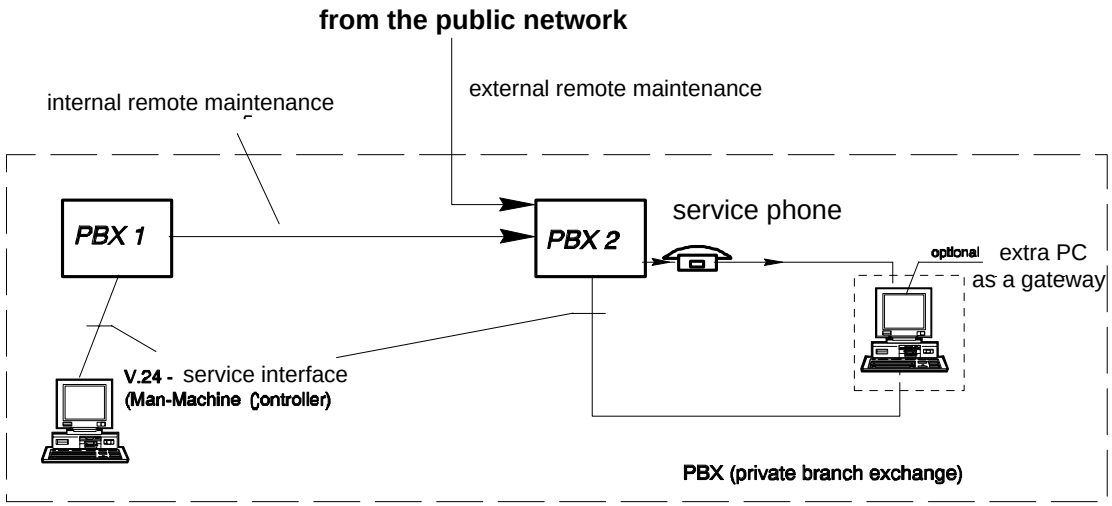
- a remote access in the local interconnected PBX system (internal access) and
- a remote access from other networks (external access).

In the case of internal remote access, consideration is given to measures for the protection of remote maintenance within a telecommunications (PBX) network. Such a network is understood to mean an overall installation comprising several separate facilities interconnected with private lines. Where such a link is provided over public switching systems, the measures described under S 5.15 *External remote maintenance* must be implemented as well. In case of networking via closed user groups within public networks or via virtual private networks (VPN), the measures for internal remote access **and**, if possible, the items marked * in the measures for external remote accesses should be implemented.

The most important aspect when securing the internal "remote access" is being able to effectively prevent and detect penetration attempts from external networks. Furthermore, the accesses from the internal network should be limited to the authorised points **and** persons. There are various methods of doing this, depending on the type of access technology.

Securing an internal remote access via modem

The following illustration shows a typical scenario of an internal remote access to a remote administration port via modem. The PBX 1 system is administered by the service point directly via the V.24 service interface. The PBX 2 system is administered by the service point via modem 1 - PBX 1 - PBX 2 - modem 2 - V.24 service interface.



Structure of a remote maintenance unit

Diagram: Modem

In this case, the following measures can be taken to **protect against accesses from external networks:**

- No direct-access extension for the modem connection

  The modem connection through which the administration port of the installation is accessed should in any case **not** be a **direct-access** extension! This minimum requirement should be checked first. Thereby itcan be preventedfor the modem to be called directly from outside.

- Confidentiality of the call number of the service port (modem)

  In order to discourage misuse from the very start, the call number of the service phone should not be listed in telephone directories. It should be known exclusively to the persons having a direct need for it.

- Use of dedicated lines (optional)

  The use of dedicated lines for the remote connections which do not run via switching equipment is one of the most secure methods of preventing external access to the remote accesses. As this system is generally very expensive, it can only be used in exceptional cases.

In order to ensure that **only authorised bodies** within the internal network can gain access to remote accesses, the following steps must be taken:

- **Creation of Closed User Groups (CUG)**

  CUG's which operate on a supra-system basis can be set up in some PBX systems. These closed user groups represent a type of network within a network. All required remote accesses should thus be combined with the various authorised bodies in such CUG's.

- **Automatic call-back**

  The call-back option of the modem should be used (c.f. S 5.30 *Activating an existing call-back option)*. If a PC gateway is used, the call-back should be started from there.

- **Limitation of the rights of the remote port (optional)**

  In the event that the PBX system is to manage the rights for various ports, this can be used to prevent security-critical actions via remote access and only to allow this on-site. Many PBX systems do not have this option, however. In such cases, additional products, e.g. port controllers, can limit the transactions executed by a particular port.

In order to ensure that **only authorised persons** within the internal network can gain access to remote accesses, the following steps must be taken:

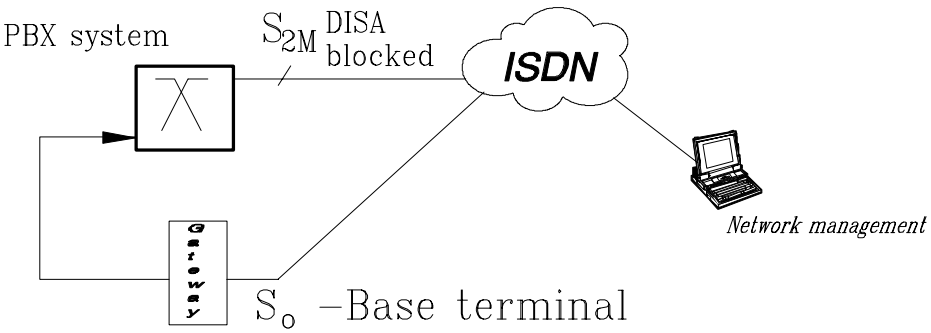
- Identification and authentication,
- Challenge response procedures for authentication (optional).

Securing an internal remote access via ISDN networks

For practical reasons, it is recommended to equip the PC's used for network management tasks with ISDN cards. In this instance, a closed user group should be created. Here, the number of the calling party can be used (Calling Line Identification and Presentation CLIP). This could be implemented by the terminal itself using the number of the calling terminal (CLIP) provided by the network.

Securing Direct Inward System Access (DISA)

If possible, direct system accesses should be blocked. If this is not possible, the authorisation should be set in such a way that the direct system access can only take place via a dedicated port. In this way it is possible to run the DISA access via a gateway. An example of this is shown in the following illustration:



Menu diagram: Securing a direct system access

Establishment and accommodation of a network management centre

The advantage of a central network management is, that besides being a convenient method of system administration, physical access to the PBX is no longer needed for everyday administration work.

If the installation of central network management is being considered, it should be located in a secure area. Access to this centre should be controlled using organisational measures. For the relevant provisions, c.f. Chapter 4.3.2 *Server Room*. The management computers from which work can be carried out should be protected by suitable safeguards. See Chapter 5.1 *DOS PC (single user)* and 5.2 *UNIX system.*

Logging of maintenance work

It must be possible at all times to get a picture of the current plant configuration, i.e. allocated call numbers and rights, activated and de-activated user facilities, established follow-me groups, etc. For this purpose, the changes made must be logged. A neat solution is forced logging by means of a PC gateway.

Additional controls:

- Has external remote maintenance been disabled?
- Is it ensured that the remote access is not switched on a direct-access line?
- Who can, from where, call the remote access?
- Who has access to the remote-maintenance centre?
- Is the remote maintenance centre accommodated in a protected area?
- Are all instances of remote-maintenance access and all related entries being logged?

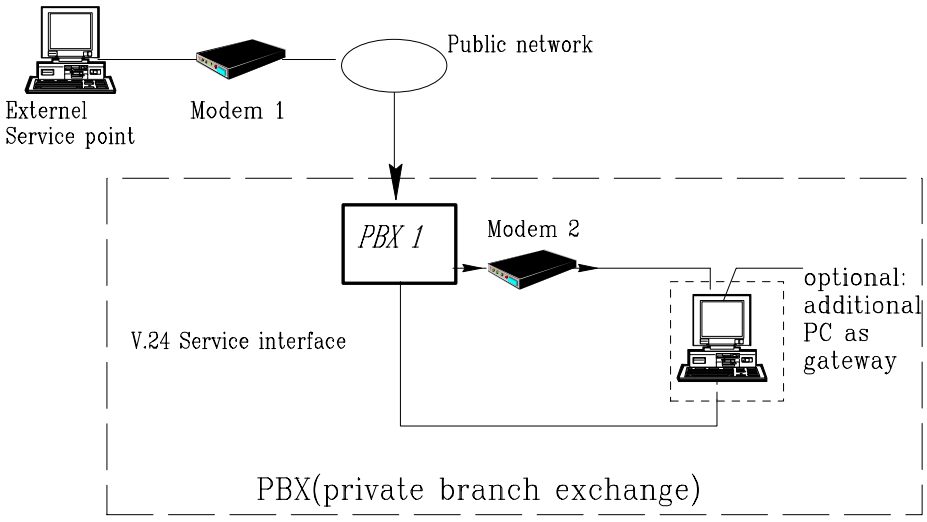
S 5.15 Shielding of external remote accesses

Initiation responsibility: PBX officer; IT Security Management

Implementation responsibility: Administrators

Here external remote access is understood to mean any access through the maintenance port of the telecommunications (PBX) system via public switching systems. The reasons for such access may be either that the individual installations of the PBX network are not, or not exclusively,[1/] connected through dedicated lines or that, in emergencies, reliance on quick assistance by the manufacturer is indispensable. In such cases, the service port (modem) must have full direct-access rights.

The following illustration shows a typical scenario of an external remote access to a remote administration port via modem. The PBX system is administered by the external service point via modem 1 - public network - PBX 1 - modem 2 - V.24 service interface.



Menu diagram: Configuration of external remote administration via modem

For security reasons, it is advisable to operate without external remote maintenance. Where this is not possible, apart from the measures for internal remote access, additional safeguards are unavoidable.

PC-Gateway*

A PC gateway should be switched between the service port and the modem. This should provide the following security functions:

---

[1] Some installations offer the option to process only the basic traffic load through dedicated lines and to route peak loads automatically through the public network. This fact is not signalled to the user.

* Diese Maßnahme sollte auch bei interner Fernwartung über virtuelle private Netze angewandt werden.

- identification and authentication of the operator;
- disconnection in case of critical security incidents;
- automatic call back; and
- logging of all activities.

In addition, other functions can be implemented as well:

- Activation of a time lock on invalid access attempts.
- De-activation of remote maintenance during normal operation and explicit release for a clearly defined period of time. This is an expedient measure which, in an emergency, will enable the manufacturer or another service contractor to intervene.
- Restrictions on the rights of maintenance staff. By means of additional software installed on the service PC, the users' scope for action can be restricted in order to achieve gradation of the administration of rights.
- "Forced log-out" in case of line interruption. If the connection between the remote-maintenance unit and the PC gateway is interrupted in any way, access to the system must be stopped by a "forced log-out".

Physical de-activation of the remote-maintenance ports

If remote maintenance is normally not required and is to be provided only if required, physical shut-off of the port is recommended. If required, it can be re-activated at short notice, possibly after consultation over the telephone with the manufacturer or the service contractor.

Closed User Group (CUG)

It is possible to create a CUG in public ISDN and X.25 networks. Here, the network operator provides the user with a virtual "network within a network". The closed user groups can be obtained from the network operator against the appropriate fee.

Alternatively, it can be considered realising the closed user groups by using the ISDN Calling Line Identification and Presentation (CLIP) and Connected Line Identification and Presentation (COLP). If possible, this can also be done by appropriately configuring the PBX system or the PC gateway.

Avoiding or controlling direct dial-in

Direct dial-in, e.g. from other networks by suffix dialling in dual tone multifrequency signalling, into the PBX system should be disabled, if possible. This is often used for access to server services. If it is not possible to prevent direct dial-in, it is recommended to activate all available protective mechanisms and regular controls to detect possible abuse.

Additional controls:

- Is remote maintenance normally *physically* de-activated?
- From where can remote maintenance be performed?
- Is a call-back procedure installed?
- Has a PC gateway been implemented?
- Are the inputs made via remote maintenance logged?
- Is access to the protocol files provided for remote maintenance?
- Is it possible to de-activate the logging printer through remote maintenance?
- Are invalid log-in attempts logged?
- Is the connection terminated after such attempts?
- Is an automatic log-out effected on line interruption?

S 5.16 Survey of network services

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: Administrators

Before starting the security check of individual network services and processes under UNIX, a survey should first be made of the services required and those which may already have been installed. For the latter, it is useful to generate a list of all network processes by means of the *ps* command and relevant options. Then information should be obtained on the function of each one of these processes and on where a process is started with which options. Often this is done in the */etc/rc*, */etc/rc.net*, */etc/rc.local* files which are read during system bootup.

Of particular importance is the *inetd* daemon since it can initiate all processes listed in the */etc/inetd.conf* file. Configuration files such as */etc/services*, */etc/protocols*, */etc/hosts*, */etc/gated.conf*, and others, must also be checked.

S 5.17 Use of the NFS security mechanisms

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: Administrators

NFS (*Network File System*) allows common use of files on a server from all computers (clients) which are integrated in the same network and have obtained the pertinent rights on the server. Every server can also be operated as a client, and *vice versa*. It has to be ensured that every computer works only with the function assigned to it. Thus, for instance, it is not necessary to start the mount daemon *mountd* or the NFS daemon *nfsd* on an NFS client.

- On an NFS server every file system or directory which can be mounted by other computers must be entered in a file (e.g. */etc/exports* or */etc/dfs/dfstab*). The following requirements apply in this case:
  - Only file systems absolutely required should be exported.
  - With the key words *root=* and *access=*, it is possible to precisely define the computers to which data systems are to be released for export. If no specific computers have been designated, the respective data system is approved for use by all computers, and this must be precluded at all events!
  - For read-only file systems, and these include all executable files, the *ro* option (*read only*) should be used.
  - Normally, the user ID of the system administrator (UID *0*) will, for NFS queries, be reset to the number of the user *nobody* (UID -2 or 65534) so that files with the UID *0* cannot be accessed through NFS. This does not apply to files belonging to other privileged users, such as *bin* or *daemon*, a fact that will also have to be borne in mind in the context of the division of administrator roles (S 2.32 *Establishment of a restricted user environment*), i.e. file systems comprising files of these users must not be exported. Since any computer within the network can assume any ID and, for instance, any PC user has *root* privileges under DOS, mapping of *root* to *nobody* should not be disabled, and it should be ensured that the entry *nobody:*:-2:-2:anonymous users::* exists, and is effective, in the */etc/passwd*. In this context, it must also be borne in mind that any user having *root* privileges on a networked computer (e.g. as a PC user) can, through NFS, also assume any group ID so that consequently no exported directory and no exported file should have group write-access rights and, moreover, only have read and execute rights to the extent absolutely necessary. In addition, attention should be paid to the fact that not only individual files, but all higher-level directories must be protected!
  - The *anon=-1* option should be used to prevent anonymous queries. *anon=0* (*root*) should never be used as this makes it possible for any user to access files with *root* privileges.
- In files such as */etc/fstab* or */etc/vfstab*, those file systems are listed which can be mounted by a command such as *mount -a* or *mountall*. This might

also occur even without a query during booting. Therefore, an early check for correctness must be made of such a file.

- The */etc/exports* and */etc/fstab* files (or similar files on other systems) are system files to which only the system administrator may have access.
- File systems to be exported should be installed on a separate disk or partition so that, for instance, a user will be prevented from filling the system disk by writing without authorisation.
- For mounting of exported file systems, the *nosuid* option must be used in order to prevent execution of *suid* programs on the client.
- Where possible, the NFS daemon should be configured in such a way that it will automatically carry out a check of the port numbers in order to ensure that only packets from the privileged ports 0 - 1023 will be accepted.
- For identification of files, so-called *file handles* are used between client and server, which can be guessed easily. Therefore, they should be randomised by means of the *fsirand* programme.
- Where available, *SECURE NFS* should be used to ensure that data will be transmitted in encrypted form. In this respect, the following steps are important:
  - - generation of keys for all NFS users;
  - - deletion of the *public key* for the user *nobody*;
  - - *rpc.ypupdated* must not be run on the NIS master server;
  - - transfer of the *public key map* to all computers before *SECURE NFS* is started;
  - - use of *keylogin* and *keylogout* for the generation and deletion of *private keys* when logging in and out;
  - - the *keyserv* daemon must be run on every client;
  - - the *secure* option must be used for mounting;
  - - the clocks in all computers must be synchronised since the transmitted packets are provided with timing marks in order to prevent replay of messages.

S 5.18 Use of the NIS security mechanisms

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: Administrators

NIS (*Network Information Service*) cannot be operated without serious security shortcomings and should therefore be used only in a secure environment.

The following requirements apply to a NIS server:

- The password file */etc/passwd* must not contain the entry *+::0:0:::* since otherwise access with the name ´+´ without a password is possible. Should the entry be necessary, the password must be replaced by ´*´ (you must check whether access has actually been blocked!). Nevertheless, there still will be the risk that, in case of inadvertent deletion of the first column (i.e. ´+´), privileged access will be possible without a password and without a user name!
- The situation is similar as regards the group file */etc/group* and all other security-relevant files which are to be made accessible network-wide through the NIS, e.g. */etc/hosts*, */etc/group* or */etc/bootparams*.
- The *ypserv* server process should respond only to queries made by computers which have been designated in advance.

The following requirements apply to a NIS client:

- The entry *+:*:0:0:::* in the password file */etc/passwd* should be documented (cf. S 2.31 *Documentation of authorised users and authorisation parameters*), and in any case there should be an entry in the password field so that access with the user name ´+´ without a password will not be inadvertently provided in case of (intentional or unintentional) failure to use the NIS.
- Similar provisions apply to the group file */etc/group* and all other security-relevant files to be made accessible network-wide through the NIS.
- The *ypbind* client process should only accept data coming from a privileged port since otherwise it might obtain data (including passwords!) from any process whatsoever claiming to be a server.
- In order to prevent the NIS system administrator from having *root* rights on all NIS clients, a local user with the UID *0* should be established on each NIS client.
- It must be borne in mind that NIS will, as a first step, search the local files for matching entries so that, for instance, the entries

  root::0:0::::

  +:*:0:0:::

  in the */etc/passwd* file have the effect that the first entry without a password, instead of the *root* password from the NIS map, will be used.

S 5.19 Use of the sendmail security mechanisms

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: Administrators

Since *mail* transmission would appear to be the application most frequently used in networks, the pertinent processes are of particular importance and are one of the most common targets in a system. A further aspect is the fact that these processes often have set the *suid* bit and belong to a privileged user (e.g. *root* or *bin*). For instance, a fault in *sendmail* was one of the reasons for the propagation of the *Internet* worm.

- As regards the starting of *sendmail*, many options can be listed which would lead to security problems if they were run with *root* privileges. Therefore, if *sendmail* can be called up by any user, a check should be made to see whether, when being started with any of these options, it disregards the set *suid* bit and is run with the user's UID. In order to avoid security problems, the administrator should ensure that *sendmail* can be started only with the following options with the set *suid root* bit by non-privileged users: *7, b, C, d, e, E, i, j, L, m, o, p, r, s*, and *v*.
- On account of the security shortcomings of the *sendmail* programme which have been discovered in the past, the most recent programme version must always be used. Information on the current versions is provided by the agencies listed under S 2.35 *Obtaining information on security flaws of the system*, such as BSI, CERT, DFN-CERT.
- It should not be allowed to run the *sendmail* process in the debug mode as in that case it would be possible to obtain *root* privileges. This can be tested by entering the command

  telnet localhost 25,

  where *localhost* can be the name of the computer to be checked, and *25* the port number for addressing the *sendmail* process. The computer or the *sendmail* process will then respond with

  Trying 123.45.67.8...

  Connected to xxx.yy.de.

  Escape character is '^]'.

  220 xxx Sendmail 4.1/SMI-4.1 ready on Wed, 13 Apr 94 10:04:43 +0200

  If you now enter the command *debug*, *showg* or, for very old versions, *wizard*, the process should repudiate this with

  500 Command unrecognised

  You can then exit with the *quit* command.
- The commands *vrfy* and *expn* must not be available since they give the matching log-in name for a *mail* name so that the pertinent password might then be found out by trial. For *sendmail* Version 8, these commands can be disabled during starting, e.g. by the *p* option (*privacy*). As described under

the preceding point, the availability of these commands can be verified, e.g. by entering the *vrfy useralias* command.

- The configuration file *sendmail.cf* should belong to *root*, and read and write access should also be confined to *root*. The same goes for the higher-level directories since, otherwise, by simply renaming these directories, it is possible to generate a new *sendmail.cf* file.
- Identification of executable programmes or of files as valid addresses for a recipient or sender must be prevented by the configuration of *sendmail.cf* or, by appropriate measures, be confined to certain safe programmes and files.
- The *F* command (that is, for instance, *FX/path [^#]*) which serves to define classes should be used in the configuration file (*sendmail.cf*) only to read files which anyhow can be read system-wide, as, otherwise, relevant security information from protected files might become generally available. The programme format of the *F command* (e.g. *FX***Fehler! Es wurde kein Textmarkenname vergeben.***/tmp/prg*) should not be used!
- For definition of the delivery agent (e.g. *Mlocal*), only absolute paths may be indicated (e.g. *P=/bin/mail*). Also the *S* (*suid*) flag should be set only when any security problems involved have been resolved.
- For any file to which *sendmail* could write, e.g. *sendmail.st* for statistics, only *root* should have write access, and it should also only be listed in the directories belonging to *root*. The same goes for files used by *sendmail*, such as *:include:* in mailing lists
- Privileged users like *bin* or *root* should not have a *.forward* file. If the user or group write-access rights for this file are set incorrectly, or if a user manages to get into a privileged group, he can generate a shell with the privileged user ID.

  In the case of normal users, only the owner should have write access to the *.forward* file, and this must be located in a directory belonging to the owner.

  In case asystem-wide write access to a home directory needs to be available, e.g. *uucp*, creation of a deleterious *.forward* file can be prevented in the following way: A directory with the name *.forward*, the rights *000* and the owner *root* and, under this directory, a file also having the rights *000* and the owner *root* must be created so that nobody else but *root* can modify or delete these files. In this case, the home directory of *uucp* should also belong to *root* and be provided with the sticky bit (*t*). A similar approach is recommended also for other configuration files (e.g. *.login*, *.cshrc*) in directories which can system-wide be written to.
- Any executable programme, including *uudecode* in particular, should be removed from the alias file. Moreover, the alias file and the pertinent database should belong to *root*, and only *root* should have write access to them.
- It must be borne in mind that any received mail might be corrupt. Corruption can occur either in the mail queue or through log-in on port 25. The first situation can be avoided if the mail queue directory belongs to

root and has the rights *0700*. The queue files should have the right *0600*. Modification of mail during its transport cannot be avoided so that users must be made aware of the fact that, for instance, a mail message from *root* requesting them to alter their passwords may be faked.

S 5.20 Use of the security mechanisms of *rlogin, rsh* and *rcp*

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: Administrators

With the *rlogin* program and/or the associated daemon *rlogind* it is possible to log in on another computer through a network connection; in that case, however, only the password will be requested since the user name will be passed on directly. With the commands *rsh* or *rcp* and the *rshd* daemon, it is possible to execute a command on another computer. Both commands use trusted hosts which are defined either user-specifically in the home directory *$HOME/.rhosts* file or system-wide in the */etc/hosts.equiv* file. Any computer entered in one of these files will be considered trusted so that neither logging on (with *rlogin*) nor command execution (with *rsh*) require entry of a password.

Do not use .rhost* and *hosts.equiv

Since it is very easy, especially from a PC, to impersonate any computer name, steps must be taken to ensure that there are **no** *$HOME/.rhosts* and */etc/hosts.equiv* files or that if there are, they are empty and cannot be accessed by ordinary users. To achieve this, users' home directories should be regularly checked, or it should not be possible to start up the daemons *rlogind* and *rshd* (for further information, see the */etc/inetd.conf* file and safeguard S 5.16 *Survey of network services*). If use of the */etc/hosts.equiv* file cannot be avoided, steps must be taken to ensure that no "+" entry exists as that would result in every computer becoming a trusted one.

Use Secure Shell as a substitute

Secure Shell (*ssh*) can be used as a substitute for the *r* services. It makes use of extensive functions designed to ensure secure authentication and to maintain confidentiality and integrity (see also S 5.64 *Use of Secure Shell*). If *ssh* is used, then if possible the *r* services should be disabled to ensure that the security safeguards cannot be circumvented. However, this presupposes that all communication partners have suitable implementations of *ssh*.

S 5.21 Secure use of *telnet, ftp, tftp* and *rexec*

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: Administrators

Passwords in plain text

With the *telnet hostname* command it is possible to log into the *hostname* computer after entry of a user name and associated password. With *ftp*, sizeable quantities of data can be copied, and *rexec* allows execution of a command on another computer without previously logging on. For all of these three programs, the entered user names and passwords are transmitted unencrypted over the network; so they should only be used when one can be certain that the network cannot be intercepted (cf. T 5.7). All calls to *telnet*, *ftp* and *rexec* must be logged. Particular attention must be paid to unsuccessful connection attempts by external IT systems.

Security weaknesses in *ftpd*

When using the *ftpd* daemon, it must be borne in mind that, as in the case of *sendmail* (cf. S 5.19 *Use of the sendmail security mechanisms*), new, serious security flaws are constantly coming to light which may make it possible to gain Administrator privileges without a password (on this point, see CERT notice CA-94-08. 14 April 1994). *ftp* versions that are older than those described there should not be used.

Restrict *ftp* access

In addition, all user names for which *ftp* access is not to be permitted should be entered in the */etc/ftpusers* file. These include, for example, *root*, *uucp* and *bin*. When configuring new users, care should be taken to ensure that these are entered in */etc/ftpusers* if their profile does not permit them any *ftp* access (see also S 2.30 *Provisions governing the configuration of users and user groups*).

With *.netrc*-files, automatic FTP accesses to remote IT systems are permitted as *.netrc* files contain the necessary passwords. Steps must therefore be taken to ensure that there are no *.netrc*-files in the user directories or else that they are empty and the user is unable to access them.

Restricted file access with *tftp*

Use of the *tftpd*, *rexd* and *rexecd* daemons must be prevented (e.g. by deleting the corresponding entry in */etc/inetd.conf*) or, as a minimum, steps must be taken to ensure that, when using *tftp*, users only have restricted access to files from the log-in directory (see also S 2.32 *Establishment of a restricted user environment*). This can be verified by making the following entries:

```
tftp hostname
tftp>get /etc/passwd /tmp/txt
```

If the *tftp* daemon does not respond with an error message, its use must be prevented.

If notwithstanding *tftp* is still used for the start-up process of active network components or X terminals, it is essential that this is documented and the underlying rationale is explained. Again, if *tftp* is used, steps must be taken to ensure that the *tftp* daemon is started with the option *–s directory*. The *directory* entered here must be the only directory which is visible to the daemon.

Use Secure Shell as a substitute

Secure Shell (*ssh*) can be used as a substitute for *telnet* and *rexec*. It makes use of extensive functions designed to ensure secure authentication and to

maintain confidentiality and integrity (see also S 5.64 *Use of Secure Shell*). It is also possible using tunnelling to operate *ftp* with secure encryption. If *ssh* is used, then if possible these services should be disabled to ensure that the security safeguards cannot be circumvented. However, this presupposes that all communication partners have suitable implementations of *ssh*.

Additional controls:

- Is the */etc/ftpusers* file updated regularly?
- Are access attempts via *telnet*, *ftp* and *rexec* logged?
- Is *ssh* used to provide protection?
- Is *tftp* disabled?

Intentional blank page

S 5.22 Compatibility check of the transmission and reception systems

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Procedures Officer

The reliability of data exchange depends on the compatibility of the sending and receiving systems involved. The necessary compatibility, in turn, depends on the complexity of the data to be exchanged. Before establishment of a regular exchange of data media, the following characteristics must therefore be examined in order to determine any incompatibilities and eliminate them if possible.

- Physical storage medium:

  One prerequisite is that both the transmission and reception systems must have **identical physical storage media**. However, mechanical equivalence alone is not enough, as differences in parameters like tape speed or disk capacity can also lead to problems.

- Character set (e.g. ASCII or EBCDIC):

  If the transmission and reception systems have identical **character sets**, physical reading allows the interpretation of individual sectors/blocks in the text which can be distributed sporadically on the data carrier. If the character sets are not identical, the transmitted data is interpreted incorrectly.

- Formatting the operating or file system of the data medium:

  If both systems also have the **same operating and file system**, or the reception system is capable of reading the formats of other operating systems (some UNIX operating systems can read DOS diskettes), then all files can be reproduced in the form in which they were present at the sender. This proves adequate for information not requiring any further formatting as carried out by most application programmes (e.g. word processors).

- Application software:

  If application programmes were used for generating the data to be transferred, these programmes must be checked for their respective **version**, as the file formats might be different. The versions need not be identical in case of upward/downward compatibility.

- IT security software and IT security parameters:

  If IT security products or the protective mechanisms of certain application programmes are used (cf. S 4.30 *Utilisation of the security functions offered in application programmes*), the compatibility of these products must be ensured. The sender and recipient must reach an agreement on the **keys** and **passwords** used.

In case of incompatibilities, additional measures or products must be provided to achieve the required conversion, or the transmission and reception systems must be identically configured.

Additional controls:

- Do the transmission and reception systems use the same IT products (hardware/ software)?
- Do the sender and recipient have compatible versions of application programmes?
- Does the recipient know the keys and passwords required for reading the information?

S 5.23 Selecting suitable types of dispatch for data media

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

In addition to the instructions in *2.3 Data carrier Control*, the type of dispatch of data media should be selected in accordance with the respective threat potential. As regards availability, timely delivery should be guaranteed by the selected type of dispatch. The bigger the number of persons involved in dispatch and the longer the periods for which the data medium remain unsupervised, the more difficult it is to ensure confidentiality and integrity. Appropriate types of dispatch should therefore be selected.

Some of the types of dispatch available are:

- The Postal Service
- Federal Railway
- Courier services
- Personal couriers and
- Personal delivery

Additional controls:

- Are the types of dispatch for data media selected in accordance with their respective protection requirements?
- Are reliable transport agencies and couriers available?

S 5.24 Use of a suitable fax cover sheet

Initiation responsibility: Head of General Services Section

Implementation responsibility: Fax Officer, IT users

A standard fax cover sheet should be used to allow orderly and efficient exchange of fax information. In particular, this makes it possible to check whether fax messages have been received and printed out successfully.

The fax cover sheet should contain the following:

- Subscriber number of the fax machine
- Name of the sender (with subscriber number of the fax machine, telephone number and complete address)
- Telephone number of a contact person in case of transmission problems
- Name of the recipient (with subscriber number of the fax machine and complete address, where possible)
- Number of pages including the cover sheet
- Degree of urgency
- Sender's signature

It is advisable to request incorrect deliveries to be re-routed or the sender to be informed in such cases.

Additional controls:

- Does the fax cover sheet include all the required items?
- Is the fax cover sheet used regularly?

S 5.25 Using transmission and reception logs

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management, Fax Officer, Fax Office

When fax services are used, a distinction must be made as regards the use of transmission and reception logs between conventional fax machines and fax servers.

Use of a conventional fax machine

Check transmission and reception logs regularly

Lists of completed transmissions (journals) which are compiled automatically by the fax machine must be printed out regularly. Who is responsible for these printouts, how long they are kept for, and in what form sample checks for irregularities are made on them must all be specified. The requirements of the *Federal Data Privacy Protection Act* must be observed here. In particular, access by unauthorised persons must be prevented.

Maintaining a fax journal

A fax journal listing the senders and recipients of fax messages should also be kept. Optionally, a log of incoming faxes can be kept as well.

Another means of checking is available where the fax machine is connected to a modern private branch exchange, in which case it is possible, for example, to evaluate the call charge data records for the fax subscriber number in the PBX (cf. S 2.40 *Timely involvement of the staff council / works council*).

Use of a fax server

Evaluate log files regularly

It is also possible to log transmissions on fax servers. These logs should be evaluated and archived regularly. It is especially necessary to define the basic requirements and responsibilities for processing, interpreting and archiving of the logs.

Thus, for example, one option is that the fax mail centre is responsible for these activities but that the logs can only be evaluated in the presence of a member of the works council or staff council or a member of the audit or data privacy team. Once again, the requirements of the *Federal Data Privacy Protection Act* must be observed and access by unauthorised parties must be prevented.

When fax servers are used, it is inappropriate to keep manual fax journals. Instead, it should be sufficient to archive the transmission and reception logs in their entirety.

It may sometimes also be possible to use the data records of charges incurred for outgoing fax transmissions from the fax server to pass on these costs based on usage.

Additional controls:

- What procedures apply to the checking of transmission and reception logs?
- Where are the logs archived and who can access them?

S 5.26 Announcing fax messages via telephone

Initiation responsibility: IT Security Management, Superiors

Implementation responsibility: Fax sender

Important fax messages of a confidential or financial nature (e.g. tenders) or involving deadlines must be announced to the recipient before dispatch (e.g. via telephone). This allows the recipient to pick up the fax message from the fax machine before other parties are able to do so.

Superiors should instruct users to announce confidential and important fax messages.

Additional controls:

- Are important fax messages announced beforehand?
- Are users instructed to do so?

S 5.27 Acknowledging successful fax reception via telephone

Initiation responsibility: IT Security Management, Superiors

Implementation responsibility: Fax sender

Recipients should be asked whether important fax messages have been received/printed completely and viewed by them. Employees should be instructed to observe this measure. The receipt confirmation of such fax messages can also be requested by furnishing the fax cover sheet with a distinct and appropriate mark.

It is facilitated on some fax machines by a service feature which consists of the output of individual reports indicating the error during dispatch.

Additional controls:

- Does the agency/company transact fax messages whose correct reception is of particular importance?
- Is the recipient requested to acknowledge the arrival of such fax messages?

S 5.28 Acknowledging correct fax origin via telephone

Initiation responsibility: IT Security Management, Superiors

Implementation responsibility: Fax receiver

Consideration must be given as to whether the source of important or extraordinary fax messages should be confirmed by the sender to preclude forgeries by third parties. This acknowledgement can be provided easily via telephone. The relevant subscriber number should generally be documented on the fax cover sheet. It should, however, be verified as it could be forged.

Additional controls:

- Is the sender requested for confirmation via telephone in the case of important or unusual fax messages?

S 5.29 Periodic checks of destination addresses and logs

Initiation responsibility: IT Security Management

Implementation responsibility: Fax Officer

Programmable keys for abbreviated dialling and destination addresses should be periodically checked to determine whether the programmed fax numbers still coincide with the actual ones and whether they are still required. This prevents incorrect fax numbers input by strangers from being used instead of the correct numbers for extended periods and allows modifications to the desired destination number to be recognised at an early stage.

Additional controls:

- Are the stored subscriber numbers checked periodically?

S 5.30 Activating an existing call-back option

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: IT users, Administrator

Many modems offer an automatic call-back function. If this option is active, the modem disconnects the line immediately on receiving a call, and then calls a preset number back. This prevents unauthorised users from misusing the modem as long as they are not reachable at the preset number. Callback should be used whenever a specific communications partner needs to dial in automatically. It should be noted that automatic callback also accepts the costs of data transfer.

The required command is described in the operating instructions; AT%S is normally used. Before the call-back option is activated, the relevant subscriber number should be determined.

Some modems also allow automatic call-back to be used with a password. After establishment of a connection, the called modem prompts the calling modem for a password. The validity of this password is checked by the called modem. Every valid password is assigned a subscriber number which is called back. A list of call-back numbers can normally be stored in the local modem and used to establish connections with it from various remote points.

Note that automatic call-back is only active one side, otherwise the mechanism would generate an endless loop. Call-back should be activated on the passive side, i.e. from which data are requested or on which data are imported. A typical example involves an employee on external duty who wants to establish contact with an IT system within his organisation. This requires activation of the call-back function on the modem inside the organisation.

The preset call-back numbers must be checked and updated periodically.

A call-back can take place either by the modem or by the application. If the application used offers this option, the call back should be carried out by the application and not by the modem. If the modem causes the call-back, an attacker can attempt to call the modem when it is about to start the call-back and thus intercept the call-back. If the application causes the call-back, it is considerably more difficult for an attacker to judge the correct moment.

Additional controls:

- Has payment of costs in the callback mode been clarified?
- When were preset call numbers last checked?

S 5.31 Suitable modem configuration

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: IT users, Administrator

Most modems operate with the Hayes standard (also termed AT standard, as the commands start with "AT"). This is a manufacturer-dependent standard. The basic instruction sets of the various modems largely correspond. Considerable deviations are found in the extended instruction sets. It is important to check the instruction set of the employed modem to determine how the functions described in the following have been realised and whether incorrect configuration could result in security shortcomings.

The selected settings should be stored in the non-volatile memory of the modem (cf. S 1.38 *Suitable installation of a modem*). Furthermore, they should be printed on paper to allow a comparison with current settings whenever required.

Some security-related configurations are described in the following:

Auto-answer

The S0 register can be used to set the modem to automatically accept an incoming call after a preset number of rings. The setting S0=0 prevents this and requires calls to be accepted manually.

This setting should be selected if connections are to be prevented from being established covertly by an external source. Otherwise a call-back mechanism is to be employed. (cf. S 5.30 *Activating an existing call-back option*).

Remote configuration of a modem

Some modems can be set to allow their configuration from remote modems. Ensure that this feature is inactive.

Refer to S 5.33 *Remote maintenance via modem* for problems concerning remote maintenance via modems.

Password-protected storing of (call-back) numbers

Many modems allow the password protection of telephone and call-back numbers stored in the non-volatile memory. If this feature is available, it should be used, and the password should be selected in accordance with S 2.11 *Provisions governing the use of passwords*. With some modems, the entry of a certain command causes a list of the numbers to be displayed **together with** the related passwords. Access to such modems must therefore be limited to authorised persons (cf. S 1.38 *Suitable installation of a modem*).

Additional controls:

- Are the employees responsible for modems familiar with their entire instruction sets?
- Are the modem configurations documented?

S 5.32 Secure use of communications software

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: IT users, Administrator

The security of computer access via modem is decisively influenced by the computer software used.

Almost all communications software allows storage of the telephone numbers and other data of communications partners. Such person-related data must be protected appropriately.

Passwords for access to other computers and modems should not be stored in the communications software, even if this appears convenient; every person having access to the IT system and the communications software can then access other systems under a different user name (cf. S 1.38 *Suitable installation of a modem* and S 2.8 *Granting of (application/data) access rights*).

Several communications programmes allow data transfer to take place unobserved in the background, e.g. within Windows. This feature should only be used with trustworthy communication partners, as it is possible to interrupt data transmission and transfer data of a different, unauthorised nature from/to the local computer. In this manner, for example, viruses could be smuggled into the local computer or confidential data could be copied. Protocols allowing full-duplex transmission, i.e. simultaneous transmission and reception, are also available. Such transmission protocols must only be used with a trustworthy communications partner, as they are equivalent to background transmission of data.

If the communication software includes password protection or protocol features, these should be activated.

Additional controls:

- Are passwords being stored in the communications software?
- Are IT users aware of the risks associated with the background transmission of data?

S 5.33 Secure remote maintenance via modem

Initiation responsibility: IT Security Management

Implementation responsibility: Administrators

The remote maintenance of IT systems via modem involves particularly high security risks. For security reasons, it is advisable to operate without external remote maintenance. If this is not possible, additional safeguards must be implemented.

The IT system to be maintained, including the modem used, must incorporate the following functions:

- The establishment of a connection for remote maintenance should also be initiated from the local IT system. This can be achieved by calling the remote maintenance point of the IT system requiring maintenance or by automatic call-back.
- External maintenance personnel must authenticate themselves before commencing maintenance. If passwords are transferred unencrypted, they should be one-time (cf. S 5.34 *Use of one-time passwords*).
- All activities during remote maintenance must be logged on to the IT system being maintained.

The following additional functions can be implemented on the IT system to be maintained:

- Activation of a time lock on invalid access attempts.
- Disablement of remote maintenance during normal operation and explicit allowance for a specified time period.
- Restriction of permissions for maintenance personnel. The maintenance personnel must not possess full administrative privileges. On DOS PC's, gradation of the administration of privileges must be realised by means of additional software. Observe S 2.33 *Division of administrator roles under UNIX* for UNIX systems and S 2.38 *Division of administrator roles in PC networks* for PC networks.

  The maintenance personnel should only have access to those data and directories actually requiring maintenance.
- The IT system should provide the maintenance personnel with their own user ID under which all maintenance should be carried out, if possible.
- If the connection to the remote maintenance point is interrupted for some reason, access to the system must be terminated through automatic log-out.

The remote maintenance must be monitored locally by IT experts. Even if remote maintenance is implemented due to lacking internal know-how or capacity, the maintenance personnel must not be left unobserved (cf. S 2.4 Maintenance/repair regulations). If there are any doubts concerning procedures, the local IT expert should enquire immediately. It must, at any time, be possible to interrupt remote maintenance locally.

If data or programmes are stored on the local IT system during maintenance, this must be made clearly noticeable and comprehensible; e.g. such processes must only take place in marked directories or under certain user ID's.

In accordance with S 3.2 *Commitment of staff members to compliance with relevant laws, regulations and provisions*, contractual provisions should also be laid down as regards the commitment of external maintenance personnel to the secrecy of data. In particular, data stored externally during maintenance must be erased meticulously after work has been completed. The obligations and responsibilities of the external maintenance personnel must also be carefully specified.

Additional controls:

- From where can remote maintenance be performed?
- Is a call-back procedure installed?
- Have the described security functions been implemented?
- Are the inputs made via remote maintenance logged?
- Is access to the protocol files provided for remote maintenance?
- Are invalid log-in attempts logged?
- Is the connection terminated after such attempts?
- Is an automatic log-out effected on line interruption?

S 5.34 Use of one-time passwords

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: Administrators

It is relatively easy to intercept passwords which are transferred in uncoded form through networks. Implementation and logging errors in the operating system and application software might even threaten the security of encrypted passwords as well.

For this reason, it is advisable to use one-time passwords which are changed after first usage. Both hardware and software-aided generation of one-time passwords is possible.

Users must generate one-time passwords on the local IT system or via a token, or read them from a list which is generated by the remote IT system and must be kept in a safe place. One-time passwords must be verified by the remote IT system.

Public-domain programmes, e.g. OPIE or S/Key, can be used for one-time passwords. OPIE (one-time passwords in everything) is a public-domain advancement of S/Key, which is now marketed as a commercial product.

As opposed to OPIE, S/Key still uses the MD4 algorithm as standard for generating and verifying one-time passwords. Due to the recognised weaknesses of the MD4 algorithm the MD5 algorithm supplied should be used.

The OPIE and S/key programmes consist of a routine on the server for verifying entered passwords and a routine on the user's IT system. After logging into the remote system and entering their name, users obtain a display of the sequential number of the password to be entered and an ID. Using these two items and a confidential password, OPIE or S/Key calculate the one-time password for this session on the local IT system. If no local programme is available to the user for the purpose of calculating one-time passwords, the remote system can generate a list of one-time passwords which must then be kept in a safe place.

Non-recurrent passwords can also be generated via tokens which provide the generation and which can consist of chip cards or devices similar to pocket calculators. The token first requires authentication by the user. After that, the token either authenticates itself automatically to the server, or provides the user with a display of the one-time password to be entered on the client.

The greater the amount of sensitive information which needs to be protected against unauthorised access simply through the use of passwords, the greater the importance of one-time passwords and hardware-based authentication methods. Hardware-based systems should be used in situations where the use of software-based one-time password systems such as OPIE are not readily accepted. In addition, many hardware-based systems also offer the possibility of configuring a ”single sign-on” option. With this option, users no longer have to employ a different password for each individual IT system, even in large, heterogeneous networks. Instead, they only need to authenticate

themselves to the first IT system to be used, and this system subsequently passes on the information to all other IT systems.

Hardware-based one-time password systems also eliminate the need for observing many of the rules specified for users in S 2.11 *Provisions governing the use of passwords*, as these rules are then observed implicitly.

Additional controls:

- Are unencrypted passwords transferred through the networks being used?
- Are one-time passwords being used?

S 5.35 Use of UUCP security mechanisms

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: Administrators

The UUCP (UNIX-to-UNIX Copy) programme package is present as a standard feature in UNIX systems and is also available for other operating systems allowing the exchange of data between IT systems as well as the invocation of commands on remote IT systems. The only prerequisite for this is the compatibility of the *uucio* programmes on the two systems involved. UUCP is extremely widespread, although it has decreased in significance, e.g. due to the capability to connect computer via ISDN by means of TCP/IP.

As a rule, UUCP is used to exchange Email and news between computers. It also allows log-in *(cu)* and execution of programmes *(uux)* on remote computers.

Different UUCP versions exist: In addition to the implementation by Peter Honeyman, David Nowitz and Brian E. Redman from 1983 (HoneyDanBer UUCP), frequent use is made of the original UUCP system from the AT&T UNIX Version 7, whose second variant is currently available (and called Version 2 UUCP) or the Tahoe UUCP (delivered with BSD 4.3).

The UUCP variant being employed can be identified through the files in the */usr/lib/uucp* directory (*/etc/uucp* on some systems): Version 2 UUCP contains the file *L.sys*, HoneyDanBer contains the file *Systems*.

Version 2 UUCP poses major security problems (errors in *uucico*, risk of incorrect configuration due to the complexity of the security-related administration files). For this reason, the HoneyDanBer UUCP should be used instead.

The following security aspects should generally be considered when UUCP is used:

- The administration of UUCP requires intensive treatment of the configuration possibilities and the related files. Note that differences might exist between the UUCP packages of the various UNIX derivatives, even if these are all based on the HoneyDanBer UUCP.
- The same requirements apply to the administration of UUCP files, programmes and directories as to the administration of system files and directories (cf. S 2.25 *Documentation on the system configuration*, S 2.31 *Documentation of authorised users and authorisation parameters*, S 4.19 *Restrictive allocation of attributes for UNIX system files and directories*).
- A user named *uucp* exists on most systems. The UUCP files, programmes and directories belong to this user. It must be ensured that this account has a password in accordance with the specifications in measure S 2.11 *Provisions governing the use of passwords*.

  The home directory of the *uucp* user must not be the public directory */usr/spool/uucppublic*, but a personal one accessible only by this user.

- For every IT system which needs to log into the local IT system via UUCP, a separate user ID and password must be entered in */etc/passwd*. The *uucp* user's UID must not be selected for this; instead, each remote IT system must have its own, individual UID.
- UUCP passwords are transferred in the uncoded form during communication requests, and stored uncoded in the corresponding UUCP configuration file for requests to remote computers. Depending on the application and environment (particularly in the case of long-distance networks), appropriate safeguards must be taken, e.g. use of one-time passwords.

Various configuration files must be set up to allow the use of UUCP. All settings must be documented, and deviations from the settings recommended in the following must be explained to allow an understanding of these modifications at a later stage.

The following files must be administered very carefully as they contain critical information for security. The files are located in the */usr/lib/uucp* and */etc/uucp* directories. Only the *uucp* user must have write access to these directories.

- *Systems*: This file contains information required for establishing connections with remote IT systems. The time periods over which UUCP transmission is allowed can be specified here for every IT system. These time periods must be as short as possible. This file also contains the telephone numbers and log-in sequences for the IT systems with which UUCP connections can be established. Only the *uucp* owner must have read access to *Systems*, as passwords for remote IT systems are also entered here.
- *Permissions*: Access rights for remote systems are specified here. No IT systems are listed in *Permissions* on its delivery, i.e. no access is possible via UUCP. For every computer that can call and log-in, and for every computer that can be called, settings must be made to specify the respective access rights and other conditions. The access rights for IT systems called by the local one are specified in the entries listed under MACHINE, and under LOGNAME for the calling IT system. Security can be increased considerably through the use of these configuration possibilities.

  The *uucheck -v* command should be regularly used to check the options set in the *Permissions* file. These options should be set as follows:

  REQUEST

  This option should be set to NO (default setting) to prevent remote systems from reading local data.

  COMMANDS

  On no account should ALL be entered here; only required commands like *rnews* or *rmail* should be allowed. The commands should be stated with the full path name.

  WRITE/READ

If this option is not specified, write/read access is only possible to the */usr/spool/uucppublic* directory.

Directories to which access is allowed by means of this option must be documented together with the reasons for access. On no account should the root directory or the one containing the UUCP configuration files be entered here.

NOWRITE/NOREAD

This specifies exceptions to the WRITE/READ option. Directories containing sensitive information should generally be listed here. This prevents access to such directories by remote IT systems resulting from negligence to impose restrictions if higher-level directories are released with READ/WRITE.

PUBDIR

This can be used to specify a public UUCP directory in place of */usr/spool/uucppublic*. For UUCP communication involving several IT systems, a separate UUCP directory must be stated here for each of these systems.

CALLBACK

If CALLBACK is set to YES. the local IT system must call back the calling IT system before data exchange can be commenced. Of course, this is only useful for LOGNAME entries. The communication partners should agree on who is to activate a CALLBACK:

MYNAME

If MYNAME=*name* is set, the local system identities itself with *name* instead of the computer designation when a UUCP connection is established with a remote system. This feature should be used for identification with a name which is intended exclusively for this connection and is thus difficult to ascertain.

VALIDATE

If VALIDATE=*name* is set, only IT systems listed under *name* can establish a connection via the systems listed under LOGNAME. This option must, on all accounts, contain an entry, otherwise remote IT systems will be capable of masquerading by impersonating another computer name using MYNAME:

SENDFILES

The default setting (SENDFILE=CALL) should be retained here, so that jobs in the local queue are only transferred outside on establishment of a connection by the local IT system.

- The */usr/lib/uucp/remote/.unknown* file of the HoneyDanBer UUCP is invoked if an unknown IT system - i.e. one not entered in the *Systems* file - attempts to establish a connection. Such attempts are repudiated and logged. If *remote.unknown* cannot be executed, the local IT system grants all requests for connection by remote IT systems. It must therefore be ensured that *remote.unknown* can always be executed. Depending on the UNIX system being used, *remote.unknown* exists in the form of an executable shell script or a C programme. If *remote.unknown* exists as a shell script on the local IT system, it should be replaced by a programme for security reasons. If this is not done, there is a danger of a calling IT system entering a command like "cat</etc/passwd" as a system name which is then capable of being executed.
- For UUCP, several cleanup shell scripts are available which can be executed automatically by means of *crontab* daemon. This must not be initiated by *root*, as is the case for many systems, but by the *uucp* user.

When UUCP is used, various protocol files are created. In the case of HoneyDanBer UUCP, these files are located in subdirectories of */usr/spool*. Successful and invalid requests for connection, transmitted and received quantities of data, error messages and data transfer statistics are listed here. These protocol files must be evaluated regularly (cf. S 4.25 *Use of logging in the UNIX system*).

Additional controls:

- Has the administrator been trained to use UUCP?
- Are manuals on UUCP available?
- Which UUCP variants are used?
- Are the settings in the configuration files documented?
- Are the UUCP protocol files evaluated regularly?

S 5.36 Encryption under UNIX and Windows NT

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: IT users, Administrator

Encryption and/or digital signatures

Where messages are transmitted over a network, all communication partners should be aware that unencrypted messages can be read, altered or intercepted unnoticed at any point along the transmission route. For this reason, consideration should be given to whether messages should be encrypted and / or signed digitally.

Many UNIX systems provide encryption programs like *crypt*; other systems are stripped of their encryption programs on being exported from the USA

Use public domain programs

Various encryption programs which will run under Windows NT and UNIX are available from commercial software providers. Furthermore, many public domain programs for UNIX, DOS and Windows, such as PGP mentioned below, can also be installed under Windows NT.

Several public-domain encryption programs covering different operating systems are available for encrypting messages.

DES is a simple encryption program based on an algorithm of the same name. To decrypt a message, the recipient has to use the same key that the sender used to encrypt the message.

PGP (Pretty Good Privacy) is a widely used encryption program based on the RSA (for key management) and IDEA (for data encryption) algorithms. With PGP it is possible both to encrypt messages and to protect them from alteration by means of a digital signature (see also S 5.63 *Use of PGP*).

UNIX sources of PGP can be obtained, for example, from the FTP server *ftp.de.uu.net* (192.76.144.75) or the mail server *archive-server@de.uu.net*.

Do not pass keys as a program argument

The UNIX standard editors *ed*, *ex* and *vi* can be used in an encryption mode, allowing text to be encrypted immediately on creation. The *crypt* encryption program is generally used here. Note that the key must never be used as an argument for command invocation, otherwise it could be detected, for example, with the *ps* command.

Avoid encryption algorithms which are easy to crack

Many mail programs also contain options for encrypting messages. Here, a check must be made as to exactly which encryption algorithms are used. Often the encryption techniques can easily be cracked. Although the use of such encryption mechanisms always increases the degree of protection of the message, the use of stronger algorithms such as DES or RSA should be considered here.

The security of an encryption mechanism depends on three factors:

It must be impossible to reconstruct plain text

- The encryption algorithm must be designed in such a way that it is impossible to reconstruct the plain text from the encrypted text without knowledge of the relevant key, i.e. the effort required to crack the algorithm or cipher should be much greater than the value of the information obtained as a result.

- A suitable key should be selected. If possible, it should be generated randomly. If a key can be chosen like a password, the relevant instructions contained in S 2.11 *Provisions governing the use of passwords* must be observed.

Choose suitable key

- The encrypted text and keys must not be stored together on a single data medium. This can be implemented by writing the key down on a piece of card and then storing it like a credit card in one's wallet. If the keys are stored on floppy disks, these should be kept separate from the IT system.

Keep ciphertext and key separate

Additional controls:

- Are users trained to use encryption products?
- Which encryption algorithms are used?
- Are the data and keys stored separately?

S 5.37 Restricting Peer-to-Peer functions when using WfW, Windows 95 or Windows NT in a server-supported network

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

If Windows for Workgroups, Windows 95 or Windows NT are used as the user interface in a server-supported LAN, alongside the server-supported network, a Peer-to-Peer network can be operated. This creates new communications possibilities apart from those provided in the client-server (CS) network. These are not logged on the server (CS).

With this kind of configuration, operating the two network structures in parallel is often not advisable as the required functionality can generally be provided by the server-supported LAN. Therefore, Peer-to-Peer functions should not be installed in a server-supported LAN. The administrator should, in individual cases, decide if certain connected WfW, Windows 95 and Windows NT computers should activatethe Peer-to-Peer functions ”File sharing” and "Network-DDE-support". In some cases "Printer sharing" can be a sensible addition.

Under Windows NT only administrators can share resources for network access (by using File-manager or Explorer). Before sharing a resource, it should be examined whether the share is in accordance with the established security strategies (see also S 2.67 *Determining a security strategy for the Peer-to-Peer network* and S 2.91 *Determining a security strategy for the Windows NT Client-Server-network*).

Additional controls:

- Who decided whether Peer-to-Peer functions should be used in a server-supported network?

S 5.38 Secure integration of DOS PC's into a UNIX network

Initiation responsibility: Head of IT Section, IT Security Management, Administrators

Implementation responsibility: Administrator, IT users

DOS PC's can be integrated into UNIX networks in various ways. In general, PCs have weaker security mechanisms than UNIX systems. Everyone with access to a PC can administrate it, thus being able, for example, to change settings or install software.

By installing the appropriate software, a networked PC can be used to eavesdrop the network. Therefore only authorised users may have access to a PC (see also S 1.23 *Locked doors* and S 2.6 *Granting of site access authorisations*). Moreover, measures must be taken to ensure and regularly monitor that software cannot be loaded without supervision (see also S 2.9 *Ban on Using Non-Released Software* and S 2.10 *Survey of the software held).*

In addition, it is easily possible by changing the configuration of a PC, to fake any computer ID and thus carry out a masquerade. This means that when using RPC on the UNIX server no trusted hosts must be defined. Trusted hosts are systems which are regarded as trustworthy and from which you can log in (using *rlogin*) or perform a command (using *rsh*) without giving a password. This is set in the *$HOME/.rhosts* and */etc/hosts.equiv* files on the UNIX server. It must be ensured that the *$HOME/.rhosts* and */etc/hosts.equiv* files are **not** available or are empty and that the user does not have access permission to them (see also S 5.20 *Use of the security mechanisms of rlogin, rsh and rcp*).

If PC's are connected to a UNIX network via NFS, the following points should be noted:

- On an NFS server every file system or directory which can be mounted by other computers must be entered in a file (e.g. */etc/exports* or */etc/dfs/dfstab*). The access rights of the NFS clients to the released file systems are also set in this file. When using NFS, care must be taken on the UNIX server that directories are only released for mounting where absolutely necessary.
- In order to avoid *root* rights being acquired through NFS, no *root* access must be granted for exported file systems on the UNIX server as would be possible using the "*root=*" option. Under no circumstances may *root* access be given to a PC in this way.
- When copying files from a PC to a UNIX system via NFS or *ftp* it can happen that the attributes are set too freely. You must always check whether this is the case and change the *umask* if necessary.

Computer viruses occur mainly on DOS PC's. When PC's are networked with UNIX systems, viruses can spread by infected programmes passing from PC to PC. The same measures should therefore be taken here as when exchanging programmes using data media or remote data transfer (see also S 4.3 *Periodic*

runs of a virus detection programme). Whereas file viruses only represent a threat within a DOS emulation system, viruses which change the boot sector of Intel-based systems like PC's can also be a threat to UNIX systems on Intel platforms; and the greatest danger to UNIX systems from computer viruses comes from PC's which have mounted a UNIX system using NFS. Viruses which delete or alter files or directories on a PC can also access mounted directories and destroy them. So when opening directories for mounting, the access permissions must be allocated as restrictively as possible, in particular read-only access should be given for directories using the *ro* option (*read only*). Apart from this, users on UNIX should set the attributes for their files and directories as restrictively as possible, so that other users cannot access them, or so that no writing access is possible for files which are not regularly changed. This should be pre-set using an appropriate *umask*.

Additional controls:

- Are the permissions associated with NFS directories too wide-ranging?
- Are network access points sufficiently protected (organisationally or technically)?
- Are the RPC configuration files correctly set?

S 5.39 Secure use of protocols and services

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

The following short descriptions of the protocols and services most commonly used on the Internet explain what information is carried by these protocols and what is therefore eligible for filtering by a firewall. It also describes other points which should be borne in mind when using the various protocols and services.

With a TCP/IP communication, a connection is normally established by a client process from a random port with a port number > 1023 to a server process with a port number < 1024 (well known port). The ports with numbers < 1024 are also known as privileged ports, because they may only be used by processes with root privileges. However, the restriction that ports < 1024 may only be used by processes with root privileges, is only a convention and it may be circumvented. No security strategy, therefore, may assume that the IT systems really do protect their privileged ports in this way. Even if FTP is used, for instance, to access ports 20 or 21, this cannot be regarded as a secure connection.

IP

The Internet Protocol (IP) is a connectionless protocol. An IP header includes two 32 bit addresses (IP numbers) for the target and source of the computers communicating with each other.

As the IP numbers are not protected by cryptographic procedures, they may only be used for authentication in very specific topographies, i.e. only when it is certain that the addresses cannot be changed. For example, packets coming from outside but whose source address is an address from the network to be protected, may not be admitted by the firewall.

ARP

The Address Resolution Protocol (ARP) is used to find the correct 48 bit hardware or Ethernet address for a 32 bit IP address. If it cannot find the corresponding entry in the computer's internal table, an ARP broadcast packet is sent with the unknown IP number. The computer with this IP number then returns an ARP response packet with its hardware address. As the ARP response packets are not tamper-proof, they can only be used in very specific topographies (see above).

ICMP

The Internet Control Message Protocol (ICMP) is a transport layer protocol whose purpose is to transport error- and diagnostic information for the IP protocol. It is initiated and processed internally by IP, TCP or UDP and may be applied at user level by the command *ping*.

If a computer or network is not accessible, a message such as *Destination Unreachable* is generated, and this can be misused to interrupt all connections between the participating computers.

The message *Redirect* is broadcast if a gateway recognises that the packet can be sent direct to another gateway, in other words that a detour has been used. The shorter route is then entered in the sender's routing table. This can be misused to configure unwanted routes.

The firewall must ensure that these messages are not admitted through the filters. In the case of the other messages, consideration needs to be given as to whether the information sent out can be misused for the purposes of an 'invasion'.

Routing protocols

Routing protocols like RIP (Routing Information Protocol) or OSPF (Open Shortest Path First) are used to pass route changes between two networked systems to the systems involved, thus permitting a dynamic change of routing tables. It is quite easy to create false RIP packets and thus configure unwanted routes. Dynamic routing should therefore only be used in very specific topographies (see above).

TCP

The Transmission Control Protocol (TCP) is a connection-based protocol of the transport layer. Accuracy of transmission is ensured by sequence numbers, check sum generation with receipt acknowledgement, acknowledgement with timeout and segment retransmission after acknowledgement timeout. The header includes two 16 bit port numbers which are used to identify the communication terminals and are associated with the application layer services using *well known ports*. As they are not protected by cryptographic procedures, they can only be used for authentication in very specific topographies (see above).

The first packet transmitted when the connection is established is normally the only one transmitted without a set confirmation flag (ACK). This makes it possible to distinguish between connection set-up and data transfer phases. The firewall must be able to distinguish between ACK and non-ACK packets, i.e. whether a connection setup is taking place or an existing connection is being used.

UDP

The User Datagram Protocol (UDP) is a connectionless protocol of the transport layer which provides no transport acknowledgements or other security measures for ensuring transmission accuracy. The header includes two 16 bit port numbers (see TCP) which are independent of those used with the TCP protocol. As they are not protected by cryptographic procedures, they may only be used for authentication in very specific topographies.

As the protocol definition makes no distinction between a call connection and data transfer, this distinction must be made by the firewall. It must be possible to check the status of the connection and it must be possible to identify clearly to which connection a packet belongs.

This can be achieved, for instance, when making a UDP connection by storing the target port and temporarily marking it so that the response packets are only admitted at this port and blocking the port again after the connection is terminated.

Telnet

The Telnet protocol allows a user to create a terminal session on a remote computer and defines for this purpose virtual input and output units (network virtual terminals) between which connection parameters have to be negociated.

To get access to another computer using the Telnet command, the other computer must be running the Telnet Daemon. The standard port for a Telnet session is Port 23. Other port numbers may be set as parameters, allowing a connection to be made to other server processes.

As Telnet allows full access to a remote host for a user, this access must be protected by strong authentication.

A distinction is often made between simple and strong authentication. Simple authentication uses simple password procedures where the password is transmitted as plain text and is therefore not protected from eavesdroppers. Strong authentication, on the other hand, uses more complex procedures based, for example, on the use of one-time passwords or smart cards.

There is the risk with Telnet that an 'invader' may cut into an authorised Telnet connection during transmission, e.g. to tap classified information or enter his own commands in the Telnet connection. For this reason encrypted transmission should be possible.

FTP

The File Transfer Protocol (FTP) allows exchange of files between remote computers.

When using FTP, two connections are established whereby the commands are transmitted through port 21 and the data through port 20. To allow the exchange of commands between computers with different operating systems, FTP defines a set of standard commands which are not the same as the user interface commands. The FTP client translates the user interface commands into the corresponding standard commands. For the firewall it is the standard commands which are relevant, because these are the only ones actually transmitted over TCP/IP.

While the client establishes the command connection to the server port 21, the server is responsible for establishing the data connection from his port 20 to a client port (> 1023). This constitutes a security weakness, since 'invaders' could pretend to be servers. The connection should, therefore, be set up the other way round and the client should use the standard command *PASV* instead of *PORT*. This forces the server to decide on a random port number and await the data transfer at this port. The client can then set up a connection to this port, so that the TCP connection is made from the protected network into the external one.

All commands which manipulate or read files or directories (*CWD, CDUP, RETR, STOR, DELE, LIST, NLIST*), must be linked to a corresponding authorisation administration. This restricts access to certain files for untrustworthy users or blocks it altogether. This assumes that a strong authentication mechanism is in place.

The command SYST, with which a client asks for the operation system version of the server, should be linked to an authorisation administration and blocked for untrustworthy users.

Moreover, it must be possible to encrypt the transmission of files, directory information and passwords.

SMTP

Simple Mail Transfer Protocol (SMTP) is a simple protocol for transmitting electronic mail on the Internet consisting of only a few commands.

The commands *VRFY* and *EXPN* can call up internal information, so the use of these commands should only be allowed within the protected network. For untrustworthy users, *VRFY* and *EXPN* must be blocked. The firewall should be able to encrypt SMTP connections between trustworthy users, although this is only advisable if a strong authentication mechanism is used.

DNS

Domain Name Service (DNS) is used to convert computer names into IP numbers and vice versa and provides information on computer systems using the network. The information transmitted is not protected by cryptographic procedures, so spoofing attacks are possible using forged data. This should be taken into consideration especially in the event of DNS responses from the Internet.

To gain access to computers on a network, an intruder first needs their addresses which he can either get by random searching or more simply by analysing the DNS information. Once he has the address the intruder can, for example, forge an address (IP spoofing) by pretending that his computer belongs to the network to be protected and sending packets to it.

It must always be remembered that all information made available by DNS can be misused. How a firewall must be configured in order to provide risk protection when using DNS is described in Safeguard S 2.77 *Secure Arrangement of Further Components*.

NNTP

Network News Transfer Protocol (NNTP) is used for transmitting news articles.

The firewall must be able to prevent the transport of certain news groups entirely or only admit them for certain computers. There must be a guarantee that when sending news, no information percolates via the network to be protected (e.g. computer names) into the external network.

HTTP

Hypertext Transfer Protocol (HTTP) is used for transmitting data between WWW clients and WWW servers. It supports four operations: *Connection, Request, Response,* and *Close*.

The firewall must be able to analyse the commands of an HTTP packet and restrict it with filters. It must, for instance, be possible to prevent implementation of the *POST* command and the associated file change during a

Request operation. The filters must be distinguishable both by individual users (by means of strong authentication) and by computers.

It must be possible to distinguish the type of data transmitted and to search special file types for specific information. Should other processes be necessary for processing the data transmitted (e.g. an external viewer or a shell), it must be possible to let the user confirm implementation of these processes first.

Other services: X11, BSD "r services", NFS, NIS, TFTP

These services should not be used through a firewall (see also T 4.11 *Lack of authentication possibilities between NIS Server and NIS Client, T* 4.12 *Lack of authentication possibilities between X Server and X Client* and Safeguards

- S 5.17 Use of the NFS security mechanisms
- S 5.18 Use of the NIS security mechanisms
- S 5.19 Use of the sendmail security mechanisms
- S 5.20 Use of the security mechanisms of rlogin, rsh and rcp
- S 5.21 Secure use of telnet, ftp, tftp and rexec

S 5.40 Secure integration of DOS-PCs to a Windows NT network

Initiation responsibility: Head of IT section, IT security management, Administrator

Implementation responsibility: Administrator, IT users

DOS-PCs can be integrated into Windows NT networks in different ways, for example via TCP/IP or the Peer-to-Peer functions of Windows for Workgroups. In contrast to Windows NT systems, DOS-PCs contain less security mechanisms. Everyone with access to a PC can administrate it, thus being able, for example, to change settings or install software.

By installing the appropriate software, a networked PC can be used to eavesdrop the network. Therefore only authorised users may have access to a PC (see also S 1.23 *Locked doors* and S 2.6 *Granting of site access authorisations*). Furthermore, it must be ensured that software is not installed without supervision; this should regularly be checked. (see also S 2.9 *Ban on using non-approved software* and S 2.10 *Survey of the software held*).

In addition, it is easily possible by changing the configuration of a PC, to fake any computer ID and thus carry out a masquerade.

Computer viruses occur mainly on DOS PC's. When PC's are networked with Windows NT systems, viruses can spread by infected programmes passing from PC to PC. Therefore, the same safeguards must be implemeted here as for the exchange of programmes via data-media or Remote Data Transfer (see also S 4.3 *Periodic runs of a virus-detection programme*). File-viruses only pose a threat if they are in a position to change executable files under Windows NT in such a way that they can still be executed. However, under certain conditions computer-viruses that threaten to change the boot sector of Intel-based systems such as PCs, can also pose a threat to Windows NT systems on an Intel platform by leaving them in a non-bootable state. This can be avoided by changing the boot sequence (see S 4.*3 Periodic runs of a virus-detection programme*).

The largest threat that computer-viruses pose for Windows NT systems are on PCs that have access to shared directories on the Windows NT system. Computer-Viruses that change or delete files or directories on a PC can also access shared directories of a Windows NT system and destroy them. Therefore, access rights for directories shared for network access should be restrictively provided. In particular, only read access should be provided for shared directories wherever possible.

Generally, users under Windows NT should restrict the attributes of their files as much as possible so that, for example, other users cannot gain access to them or so that no write-access is possible to files that are not regularly changed. The appropriate settings should be made beforehand via the functions of access control (see also S 4.53 *Restrictive allocation of access rights to files and directories under Windows NT*). With this safeguard all files stored on the server will have sufficient protection; DOS-PCs cannot by-pass this protection.

If Windows for Workgroups or Windows 95 is installed on the PC, the threats that can be posed by the use of Peer-to-Peer functions must also be considered (see chapter 6.3 *Peer-to-Peer Network*). The particular problem of stored passwords must be emphasised. Passwords are stored in files with the name [*log-on name*].*pwl*. They are stored encrypted but can still be read with various programmes. It is absolutely necessary that a user logging on to a Windows NT system from WfW or Windows 95, observes the notes in safeguard S 4.46 *Use of the log-on password under WfW and Windows 95*. In any case, administrators must ensure that a list of passwords is not created.

Additional controls:

- Have shared directories been provided with too many permissions?
- Are network access points sufficiently protected (organisationally or technically)?

S 5.41 Secure configuration of remote access under Windows NT

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Users can connect to local Windows NT systems from remote IT systems via RAS (Remote Access Service). For this, the RAS-client must be installed on the remote IT system and the RAS-server on the local IT system which accepts the remote connection. Using RAS, these users can work as if they were directly connected to the network. The remote clients use standard programmes to access resources. With the help of the File-Manager or Explorer, network drives and printers are, for example, connected. These connections are permanent, i.e. users do not have to recreate connections to network resources during one session. As clients, the systems Windows NT, Windows 95, WfW, MS-DOS and OS/2 are supported.

The user creates the connection to the RAS-server with a local modem, X.25 or ISDN-card. The RAS-server, which is run on the Windows NT server, authenticates and serves the user until either he or the administrator terminates the session. The RAS connection provides all the services (file and printer sharing, database access and notifications) that are normally available to a user connected via a LAN.

Access to the RAS is provided for the whole pool of Windows NT user accounts. With the User-Manager, permission to dial in to the local network can be provided to single users, user groups or all users. Furthermore, RAS administration offers an option which allows access either to all resources which the RAS host can access within the network, or only to the resources available on the local computer. The users then use their domain log-on to create a connection via RAS. Once the user's access permission has been checked by the RAS, he can use the local resources or, if he has been granted the appropriate permission, the resources in the whole domain as well as in trusted domains.

Via the *Challenge Handshake Authentication Protocol* (CHAP) the Remote Access Server provides the securest form of encrypted access permission which is supported by the server as well as the client. CHAP allows the RAS server to systematically make a selection from the securest encryption mechanism to the most insecure procedure of plain-text transmission and it protects transmitted passwords in the process.

CHAP allows the employment of diverse encryption algorithms. RAS in particular uses the cryptographic algorithm MD5. RAS refers to DES encryption for authentication if the client and the server work with RAS. For data communication, Windows NT, Windows for Workgroups and Windows 95 select among themselves the DES encrypted confirmation of authenticity. When connecting to external RAS servers or client software, a confirmation of authenticity is possible with SPAP or unencrypted text, if the external product does not support an encrypted confirmation of authenticity.

MD5, an encryption scheme installed by diverse PPP implementations for encrypted confirmations of authenticity, can be selected from the Microsoft RAS-Client if a connection to other RAS servers exists.

PAP works with simple, unencrypted passwords, thereby offering little in the way of responsible protocol for confirmations of authenticity. This protocol will normally only be selected if the external workstation and the server cannot agree on a form of encryption that offers more security.

Depending upon which level of protection is required, the RAS encryption protocol should be selected according to the following table, so that at least the relevant protocol given below is deployed. This can mean that, if the security demands are high, the use of clients not supporting the required protocol must be ruled out.

Protection requirement	*Type of encryption*	*RAS encryption protocol*
High	One-sided	CHAP, MD5
Moderate	Mutual	SPAP
Low	Unencrypted Text	PAP

Data encryption protects data and ensures a secure dial-up connection. The RAS administrator can set up the RAS server in such a way that the transmission of data always takes place in encrypted form. Users connected to this server automatically encrypt all data sent.

Note: This option requires that all connected clients know how to encrypt data. In this case as, for example, in a homogeneous Windows NT network, this option must in any case be activated.

The start options for RAS are set under the control panel option "*Services*", and the configuration takes place via the control panel option "*Network*", where the choice of authentication procedure also takes place. By choosing the option "*Only Microsoft-encrypted confirmation of authenticity*", the choice of CHAP can be forced by MD5; the encryption for data can additionally be activated. Under the german version of Windows NT transmitted data is then not encrypted with DES but with RC4.

RAS supports the security-hosts of other manufacturers, whereby the security-host switches between the remote user and the RAS server. A security host is an additional computer in the network, which offers security services such as support for chip cards. A security host of this type generally offers an extra security level by demanding an identity card for confirmation of authenticity, or by supporting similarly strong authentication procedures, before allowing access to the RAS Server.

Access supervision via call-back is an additional safeguard offered by RAS. With this function the system administrator can demand that a certain remote user dials from a previously determined place (e.g. private telephone line) or that this user can be dialled from anywhere. With access supervision via call-back, the user initialises a call and makes a connection with the RAS server. The RAS server then hangs up and momentarily calls the previously-given call-back number. When using an analogue telephone network call-back modems must be installed, where during transmission via ISDN or X.25 (e.g. Datex-P), the features of these networks can be used. However, it must be borne in mind that the security of the partner identification is no longer

ensured when changing the X.25 carrier, i.e. with data transmission crossing country borders.

Under RAS the system administrator controls remote access to the network. Further to the service programmes that are delivered with the Windows NT server package, the service programme RAS-Administration offers the administrator the possibility to remove or provide access permissions for single users and/or groups. This means that access to the network must be explicitly provided for every user accessing the network via RAS, although RAS is running on a Windows NT server computer. This process ensures not only that remote access must be explicitly permitted, but also allows call-back restrictions to be defined.

RAS offers an additional security level. RAS-Administration offers an option which allows access to all resources that the RAS host detects, or to the available resources on the local computer. The administrator can thus control which data is available to a remote user. If possible, permission for access to further computers in the network should either be provided restrictively or not at all, in order to limit possible damage when security barriers have been broken.

Note: If RAS is used in a domain, changes to RAS permission will not immediately take effect on all servers. It can take up to 15 minutes for a change to be replicated on all servers in the domain. If required, the domains can be explicitly synchronised anew, to ensure that a user whose permissions have been removed, no longer has access to the network until the change has been replicated.

Additional controls:

- Are the functions of encrypted authentication and call-back security used for all external accesses?
- Is access activated only for the RAS server, but not for the rest of the network?
- Is the list of authorised users for RAS access regularly checked and brought up-to-date?

S 5.42 Secure configuration of TCP/IP network administration under Windows NT

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

When integrating Windows NT systems into a computer network, correct configuration of the installed network services is particularly important. Notes are given in the following paragraphs regarding the most widely-used services; these notes, however, do not replace a detailed examination of security requirements and the necessity for exact knowledge of the system documentation.

DHCP (Dynamic Host Configuration Protocol)

To reduce the effort involved in administration of IP address information, IP addresses, and the data belonging to them, can be dynamically configured under DHCP.

A Windows NT computer becomes a DHCP client if it has been configured for automatic DHCP-configuration when installing TCP/IP. After starting a DHCP client a connection to a DHCP server will be established in order to obtain the necessary TCP/IP configuration data. This configuration data contains at least one IP address, a subnetwork mask and the current validity length of the address.

Installation of a DHCP server is part of the installation of Microsoft TCP/IP and can only be carried out by a member of the "Administrators" group.

Note: To avoid a possible conflict, it must be ensured that other DHCP servers do not already exist in the network before installing a new DHCP server.

Automatic configuration of a new DHCP server cannot be carried out under DHCP as a computer cannot simultaneously act as a DHCP client and a DHCP server.

Note: »All entries in the registry concerning the DHCP server can be found under the path

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

DHCPserver\Parameters.«

With the service programme DHCP-Manager the following fundamental tasks can be performed:

- Creating one or more DHCP areas, so that DHCP services are available.
- Defining the properties of an area including length of usage time and IP address pools which should be allocated by servers to possible DHCP clients.
- Determining standard values for options like Standard-Gateway, DNS server or WINS server, which should be allocated together with an IP address and the addition of personal options.

A DHCP area is a group of computers, which execute the DHCP client service in a subnet. The area is used to define parameters for every subnetwork. Every area has the following properties:

- A unique sub-network mask is used to establish a subnet which is in turn assigned to a particular IP address.
- An area name assigned by the administrator when the area was created.
- Values for the length of usage time of dynamic addresses which are allocated to DHCP clients.

Each subnetwork can only have one single area with a continuous IP address pool; these addresses must be valid for the subnet. If many address pools areto be created in one subnetwork, a continuous area should be created which encompasses all these address pools and the addresses between the desired pools can be excluded. If more addresses are needed, the area can be extended at a later stage.

Configuration parameters which a DHCP server assigns to a client will be defined as DHCP options under the DHCP-Manager. Most options are pre-defined on the basis of standard parameters which have been determined in the Internet standards RFC 1541 or RFC 1542. Such types of options can be assigned to a configured DHCP area which regulates all configuration parameters.

Additional to IP address information, further DHCP options which are to be passed on to DHCP clients must be configured for every area. These options can be globally defined for all areas, specifically defined for single areas or defined for single DHCP clients with reserved addresses. Active global options are valid as long as they are not deactivated by area options or DHCP client settings. Active types of options for one area are valid for all computers in this area as long as they are not deactivated for a single DHCP client.

Note: Any change to the preset values should only be made if the effects of this change are completely known. The values to be used have to be determined within the guidelines of a specific security analysis.

A particular IP address can be reserved for a client. As a rule, this is necessary in the following cases:

- for domain controllers, if the network also works with *LMHOSTS*-files which define IP addresses for domain controllers,
- for clients working with IP addresses which were assigned for TCP/IP configuration via a different procedure,
- for allocation by RAS servers to clients that do not use DHCP,
- for DNS servers.

If multiple DHCP servers distribute addresses in the same area, the client reservations must be identical on every DHCP server otherwise - depending upon the answering server - the reserved client will receive different IP addresses.

Note: The IP address and the static name entered in WINS take priority over the IP address allocated by the DHCP server. In this case a client reservation is generated for the client which will be established in the WINS database.

The following files are stored in the directory *%SystemRoot%\SYSTEM32\DHCP*, which is established when setting up a DHCP server:

- *DHCP.MDB* is the DHCP database file.
- *DHCP.TMP* is a temporary file, which DHCP installs for temporary database files.
- The files *JET.LOG* and *JET*.LOG* contain protocols with the complete transactions that have been executed with the database. With the help of these files, DHCP can reproduce possible lost data if required.
- *SYSTEM.MDB* is used by DHCP to save data regarding the structure of its database.

Note: The files *DHCP.TMP*, *DHCP.MDB*, *JET.LOG* and *SYSTEM.MDB* should neither be deleted nor changed in any way since this can lead to faulty DHCP functions. Access to these files may only be granted to administrators as, otherwise, unsupervised changes to DHCP configuration are possible.

WINS (Windows Internet Name Service)

Via WINS, NetBIOS-computer-names can be allocated to IP addresses. Installation of a WINS server takes place as part of the installation of TCP/IP on Windows NT servers. To achieve a better availability of servers and a balanced workload, several WINS servers should be set up. Each WINS server must be configured in such a way that it functions as a reproduction partner for at least one other WINS server.

Information regarding the reproduction of database entries for the partner is part of a WINS server configuration. A Pull-Partner is a WINS server that obtains copies of database entries from its partner by first sending a request and then receiving the desired copies. A Push-Partner is a WINS server that sends its partner a renewal message, if something has changed in the WINS database. If its partner then replies with a request for reproduction, the Push-Partner sends a copy of the up-to-date WINS database to the reproduction partner. To ensure that the databases on the primary WINS server and the back-up server always correspond to one another, both servers must act as Push and Pull-Partners. It is always advisable for reproduction partners to take both roles, i.e. Push and Pull-Partner.

A particular point in time, length of time or number of data sets must be determined for every WINS server as a threshold value. If this value is reached, the reproduction of the databank will be performed. If a certain point in time is determined for the reproduction, this will be carried out once. On the other hand, if a certain length of time is established, reproduction will be repeated according to the appropriate intervals. Within a geographical region this could lie, for example, between ¼ and ½ an hour, whilst over larger distances, intervals of a few hours can be selected.

Note: All registry entries concerned with the configuration of the WINS server can be found under the path

HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\WINS\Parameters

WINS servers communicate with one another in order to achieve a complete reproduction of their databases and to ensure that a name registered in one WINS server will eventually be reproduced in all other WINS servers within the combined network. All assignment changes will be collected for the complete WINS system within the so-called reproduction period (maximum length of time for transmission of changes to all WINS servers). All freed names will be passed on to all WINS servers as soon as they are obsolete according to the relevant intervals defined in the WINS-Manager.

Reproduction takes place under a reproduction partner and not between one server and the other servers. Finally, complete copies are requested from the other WINS servers within a combined network, but the WINS servers transmit start signals to draw attention to the fact that a reproduction should be initiated. For a reproduction to take place, every WINS server must act as the Push or Pull-Partner for at least one other WINS server.

Note: All registry entries concerned with the WINS reproduction can be found under the path

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services\WINS\Partners.

Static assignments are fixed lists in which IP addresses are assigned to computer names. These classifications may not be questioned or deleted unless the administrator removes a particular assignment. Via the command "*Static Assignments*" in the WINS-Manager, static assignments can be added, edited, imported or deleted for clients in the network for whom the WINS service is not activated.

Note: If DHCP is also in operation on the network, a reserved (or static) IP address will deactivate all the settings of the WINS server. Static assignments should not be assigned to a computer if WINS is active on the computer.

The following files are stored in the directory *%SystemRoot%\SYSTEM32\WINS*. This directory is automatically created when configuring a WINS server.

- *JET.LOG* is the log file for all transactions carried out in the database. If required, WINS uses this file to recreate data.
- With the help of *SYSTEM.MDB,* WINS records information concerning the structure of the database.
- *WINS.MDB* is the WINS database file.
- *WINSTMP.MDB* is a temporary file created by WINS. It can remain in the directory \WINS following a system failure.

Note: The files *JET.LOG*, *SYSTEM.MDB, WINS.MDB* and *WINSTMP.MDB* should neither be deleted nor changed in any way since this can lead to faulty functions under WINS. Access to these files may only be granted to the

administrator as, otherwise, unsupervised changes to the WINS configuration are possible.

SNMP (Simple Network Management Protocol)

SNMP is used for supervision and administration of a TCP/IP-based network. The SNMP service is installed if the appropriate options are selected when installing Windows NT TCP/IP. Following installation the SNMP service must be configured with valid information for SNMP to be operational.

Only members of the administrator group of the local computer may configure SNMP. During configuration, Communities and Trap-Targets will be defined:

- A *Community* is a group of hosts to which one server belongs which executes the SNMP service. The Windows NT system on which SNMP has been installed will send Traps to one or more entered Communities. The name of the community will be recorded in the SNMP packet when sending Traps. If the SNMP service receives a request which does not contain the correct Community name and does not correspond to any of the accepted hosts, the SNMP service can send a trap to the Trap-Target(s) drawing attention to the fact that the confirmation of authenticity failed.
- *Trap-Targets* are the names or IP addresses of hosts to whom the SNMP service will send traps, i.e. messages of pre-defined events, with the selected Community names.

Note: In principal, SNMP should be configured in such a way that it only accepts requests from the defined Communities (and if possible not the pre-defined Community *public*).

SNMP security allows Communities and Hosts to be defined from which a computer accepts requests. Furthermore, it can be defined whether a confirmation of authenticity Trap is sent if a Community or Host requests information without authority. These determinations must be carefully planned and the possibility to send Traps must be used. The resulting logs must be checked regularly.

Additional controls:

- Are only the minimal necessary network services installed / activated?

S 5.43 Secure configuration of TCP/IP network services under Windows NT

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

TCP/IP

When installing the TCP/IP protocol, properties can be set with the control panel option "*Network*". Given that the computer concerned has more than one network card and/or remote access via RAS is installed (Remote Access Server, see S 5.41 Secure configuration of remote access under Windows NT), attention must be paid here, that routing between these cards, i.e. between the remote access interface and the network card, can be switched on via the "*Enable IP-Forwarding*" option under the register card "*Routing*". As a rule, this option should not be activated on computers which have a connection to an external network such as the Internet, since this will allow external computers transparent access to the local network.

In version 4.0 filtering of data traffic via TCP/IP can be achieved to a certain extent. This can be done by choosing the "*Advanced*" option under the register card "*IP address*" and selecting the "*Enable Security*" option in the opened window. By choosing the "*Configure*" option the permitted or, as the case may be, locked TCP and UDP ports and IP protocols for single network cards can be selected. The values to be entered here should be selected according to the necessary function and the given security requirements. A security concept for the use of Internet services should exist for computers with external connections. Considerations to be taken here should be similar to those taken when installing a firewall (see Baseline Protection module 7.3 *Firewall*, in particular S 2.76 *Selection and Implementation of suitable filter rules*).

FTP (File Transfer Protocol)

An FTP server will be set up during installation of TCP/IP under version 3.51; in version 4.0 the FTP server can be installed as part of the installation of Peer-Web-services. If the FTP server service is executed on a Windows NT system, other IT systems can create a connection with this Windows NT system as clients via the FTP service programme and thus transfer files. Users who create a connection with the FTP server are authenticated under Windows NT via their user account and are granted access dependent upon their user profile. For this reason, it is necessary to install the FTP server on a NTFS partition so that files and directories made accessible by FTP can be protected.

Following installation the FTP server must be configured before it can be operated. The configuration settings can lead to one of the following situations:

- No anonymous FTP connections are permitted. In this case, each user must enter a username and password valid under Windows NT.
- Anonymous users as well as users under Windows NT can make a connection. In this case a user can choose between an anonymous port and a connection via username and password under Windows NT.

- Only anonymous FTP connections are permitted. In this case a user cannot create a connection by entering a username and password under Windows NT.

Note: As standard, FTP transmits user passwords across the network unencrypted. Therefore, with the help of a network analysis programme, a user can find out user passwords for remote accounts during the FTP authentication procedure.

Whether anonymous FTP connections should be permitted is dependent upon various factors:

- In a pure NT network there are more secure forms of data transmission, therefore FTP should not be permitted.
- In a heterogeneous LAN with NT computers, FTP can be necessary for data transmission between different systems. To prevent tapping of NT user names including passwords, for example with Sniffers, only anonymous FTP should be permitted on NT computers.
- When installing FTP in WANs the local network must also be protected with a firewall. Anonymous connections should only be allowed on systems specially designed for this purpose; information other than that offered by FTP may not be stored on these systems.

The username "Anonymous" must be entered for anonymous connections. A password is not required although the user will be asked to supply his E-mail address. A local user account must be set up for anonymous connections under Windows NT. As standard, this account is called "guest". As soon as data transmission occurs via an anonymous connection, Windows NT examines the username supplied in the dialogue field and, based on this username, determines which accesses are permitted.

The user deployed for anonymous connections should be a member of the "*guests*" group. It should, under no circumstances, be a member of the "*users*" group, since extensive access possibilities may then exist.

When first installing the FTP server, access rights for this service must also be configured. Drives and partitions for which access rights should be configured must be selected. Depending upon the security required for the partition, read or write-access or both may be activated. Permissions granted are valid for FAT and HPFS partitions for all files on the complete partition. With the help of this setting, read or write-protection (or both) for NTFS partitions can be locked for the complete partition.

All restrictions defined in this way are additional to the security safeguards which are a part of the file system. This means that an administrator can remove permissions for certain data-media using this dialogue field, but cannot grant any permissions beyond those contained in the file system. If, for example, only read access has been provided for a partition, nobody can write to this partition via FTP, no matter which permissions have been defined for this partition.

Under version 3.51 of Windows NT, it is possible to record incoming FTP connections in the system-event log by setting the values for *LogAnonymous* and *LogNonAnonymous* in the registry code *HKEY_LOCAL_MACHINE\SYSTEM*

CurrentControlSet\Services\ftpsvc\Parameters to 1. These values are not provided in the registry as standard. To log incoming connections, these values must be entered anew. It can be stated whether entries in the event-log should be made, be it for anonymous or non-anonymous users creating a connection to the FTP server.

In version 4.0 of Windows NT, the appropriate settings for security of the FTP server can be carried out with the help of the Internet service Manager; direct changes to the registry are no longer necessary.

Telnet

Windows NT does not provide a Telnet-server; this system can only act as a Telnet client. The Telnet client is installed together with TCP/IP. If a Telnet server is required, the one provided as a part of the Windows NT Resource Kit version 4.0, or the product of another manufacturer, or shareware can be used.

Note: Since Telnet transmits the user password in plain-text when logging on, the installation and use of Telnet should only be allowed if the computer network is protected against eavesdroping. Therefore, the use of Telnet should be completely avoided if possible.

NFS (Network File System)

Windows NT itself provides neither an NFS client nor an NFS server. Given that NFS should be used, products provided by third parties must be installed.

Regarding the configuration of these products, no general entries can be made. Given that this is supported, the appropriate entries for NFS configuration under the UNIX operating system should be implemented.

Additional controls:

- Are only the minimal necessary network services installed / activated?

S 5.44 One-way connection setup

Initiation responsibility: IT Security Management

Implementation responsibility: Administrators

In most cases there is exactly one telephone line for one modem. The modem receives incoming calls and sends outgoing calls via this telephone line. To prevent an attacker from gaining unnoticed access to the connected IT system, at the very least one call-back mechanism should be installed (see also S 5.30 *Activating an existing call-back option*).

Despite an activated call-back mechanism, an incoming connection might not be terminated unless the caller hangs up. The public exchange switchboard only terminates such a connection after a certain amount of time has elapsed. The problem arises particularly if a PBX unit does not also terminate the connection.

Therefore, an attacker can initiate a call-back, but simultaneously keep the line open so that the modem correctly dials the stored call-back number but remains connected with the attacker as before.

To prevent this, it should first be checked whether an incoming connection is terminated if the caller does not hang up. If this is not the case, and if it cannot be ensured that every modem connection is observed by one person, working with separate telephone lines and one-way connections should be considered, i.e. with one socket for incoming calls and one socket for outgoing calls. This requires a modem for every socket and the initiation of the call-back via the application. It must be ensured that the modem does not automatically receive any calls for outgoing connections (*S0=0*, i.e. no Auto-Answer). To prevent the receiving modem from creating any external connections, the modem socket should either be locked at the internal PBX unit or the relevant lock from the telephone provider should be applied for.

S 5.45 Security of WWW browsers

Initiation responsibility: IT manager, network planner

Implementation responsibility: Administrator, IT users

When accessing the World Wide Web (WWW) various security problems can arise on the computers at the workstation. This can be due to faulty operation on the part of the user, insufficient browser configuration (i.e. the program being used to access the WWW), or weaknesses in the security of the browser.

Local data can be under threat if, for example, programs are downloaded from the Internet and executed without confirmation on the local computer (e.g. ActiveX programs or Java-applets). Documents or pictures may also contain commands which will automatically be executed when viewed and can thus lead to damage (e.g. macro viruses in Winword or Excel documents). To avoid such problems, the safeguards described in the following should be implemented.

Downloading files and/or programmes

When files and/or programmes are downloaded, a considerable number of security problems can arise, the most well-known amongst these being viruses, macro-viruses and Trojan horses. Users should never rely on the fact that the downloaded files or programmes come from trustworthy sources.

When the browser is configured, it must be ensured that the applications associated with files which may contain macro viruses are not started automatically (see also S 4.44 *Checking incoming files for macro viruses*).

Every user must be reminded that he himself is responsible for taking the relevant precautions when downloading files. Even if the downloaded data is automatically tested for viruses by a firewall, the responsibility for the cleanliness of the files or programmes is still with the user. In principle, the internal security regulations of the organisation must naturally be observed during the installation of programs. In particular, only tested and approved programmes may be installed. Before installation, stand-alone computers should act as a testbed for the cleanliness of their programs.

In case of doubt contact IT administration.

Plug-ins and additional programs

Not all browsers can process all file formats directly. This generally means the files cannot be displayed, and in some cases they cannot be played back. For some file formats, plug-ins or additional programs are also needed.

Plug-ins are library files (e.g. DLL files) which are downloaded by installation programs into the plug-in directory and are executed with the invocation of the corresponding file format.

Additional programs, such as viewers, are independent programs which are able to process certain file formats. The invocation of such an additional program is controlled using one of the browser's configuration files, in which the file extension and program are linked.

When adding plug-ins or additional programs to a WWW browser, the same safeguards should be observed as for loading files and/or programmes. No program should be installed which is not absolutely trustworthy.

Of course, plug-ins also take up memory space and increase the time required to start the browser. All plug-ins that are not required should, therefore, be removed, which is not always easy. Many uninstallation routines do not recognise plug-ins and not all browsers offer a list of the plug-ins that are installed. This means that all the files belonging to a plug-in must be deleted manually in the browser's plug-in directory.

Cookies

Information concerning loaded WWW-pages, passwords and user-conduct is stored in so-called cookie files on the user’s computer. Next time the respective user pays a visit, WWW providers can offer him special information or make certain services available to him via password. However, WWW providers can also create user profiles with this technique, for example, to address particular target groups with advertisements.

To prevent this, creation of cookie-files should be prevented or, if this is not possible, they should be regularly deleted. Cookies can usually be found in the configuration directory of the WWW browser in files such as *cookie.txt* or directories such as *cookies*. For example this file is called *$HOME/.netscape/cookies* in Netscape Navigator 2.02 under UNIX. Preferably, browsers should be installed with which the storage of cookies can be avoided. If this is not possible, browsers should be installed which at least warn the user of the acceptance of cookies. This option must always be activated. Users can then accept or deny the reception of cookies in every situation. If reception is denied, some WWW pages become partly or fully incapable of transfer, but this happens very rarely. If the function warning against the acceptance of cookies is activated, warnings are accompanied by an indication of the contents of the cookies, so that clarification is obtained as to which provider collects which information about the user.

To prevent the creation of cookie-files, an empty cookie-file can be created and provided with write-protection. The extent to which this is effective depends upon the browser version and the operating system installed. In particular, it must be ensured here that the browser can neither undo the write-protection nor create crashes when doing so.

Otherwise, it can be helpful to control regular deletion of the cookies via a batch-file. The batch-file deletes the old cookie-files for example with every system start or every user log-on.

Data collections

Data regarding various users' access to the Internet are collected externally as well as locally. In this context it must also be ensured that only authorised personnel have access to this data. This applies in particular to the files created by the browsers regarding History, Hotlists and cache. Users must be informed where such data is stored on their local computer, and how this data can be deleted.

These files are particularly sensitive on proxy-servers, because on such servers, every external WWW-access attempt by all staff is logged, including the IP number of the client which started access and the requested URL. Therefore, a badly administrated proxy-server can lead to severe violations of data protection regulations.

Most browsers gather a lot of information on users and their utilisation profiles: Firstly, users might not want these details to be disclosed, and secondly, superfluous information of this nature can block the available storage space on the computer. These data include:

- Favourites
- WWW pages which have been invoked
- News-server visits (see below)
- History database (see below)
- URL list (list of the last URLs which have been called)
- Cookie list
- Information on users who are stored in the browser and whose details might be forwarded (see below)
- Information in the cache (see below)

Information on news-server visits

Most browsers are able to directly access news servers.

In this process, Netscape notes the sequential numbers of the news items which have been read. This allows the determination of user profiles which also indicate the newsgroups and news items accessed by a user.

Microsoft's Internet Explorer goes a step further and stores the entire contents of all accessed news items.

History database

The history database of the Internet Explorer contains a complete collection of all activities performed with this browser, i.e. details on pictures which have been viewed, addresses, internal confidential documents which have been read, etc.

As a result, the history database quickly takes up a lot of storage space, so that it needs to be cleared on a regular basis. The files in the history database should not simply be deleted; instead, they should be replaced by prepared copies of an empty history database, as certain entries need to be retained.

Information on users

Browsers also store, and sometimes forward, various details concerning users, e.g. real name, e-mail address, organisation. To prevent flooding by e-mail advertisements, it is advisable to use the browser under an alias name.

Information in the cache

Internet Explorer, Netscape and other browsers generate large numbers of files in a cache directory. These files contain the text and pictures from all Web pages visited since the last time the cache was deleted.

The cache is intended to avoid a multiple loading of pages during a **single** session. However, the Internet Explorer does not independently delete these data, which are of no use in subsequent sessions, so that tens of megabytes of garbage accumulate in caches which are not deleted regularly. These data can also be used to generate user profiles.

For this reason, the cache should be deleted regularly, just like the history folder.

Unfortunately, it is not always easy for users to find out how to empty the cache. In the case of the Internet Explorer under Windows 95 for example, the cache is emptied by selecting the option *Empty folder* under *View/Options/Advanced/Temporary Internet Files/Settings*.

When WWW sites secured with SSL are accessed, this can, amongst other things, be used to transmit sensitive information such as credit card numbers over the Internet in encrypted form. Such pages should, therefore, not be stored in the cache in the first place. In the Internet Explorer, for example, this can be deactivated with "Do not save encrypted pages to disk" under *Tools/Internet Options/Advanced/Security*.

Access to client hard disk

With some browsers (e.g. Netscape or Microsoft Internet Explorer) the WWW servers will be given the opportunity to actively access the hard disk of the client (ActiveX, Java).

Rather than being executed on the server, Java and ActiveX programmes will be executed on the client site via the browser. However, this transfers the security risk from the server to the client. Therefore, various safeguards have been built into Java and ActiveX to prevent misuse. Many security pitfalls have nevertheless been discovered so far.

Certain security risks exist when using browsers which allow access to the files of the client in connection with ActiveX and Java. Under certain conditions ActiveX allows local resources to be used. Access of this kind is also possible with Java, but only if the user explicitly allows it. The ActiveX security concept is based upon the user having confidence in the content provider and in an authentic third party in the World Wide Web. This confidence is problematic if the web-pages of unknown or new providers are called up.

Due to the existing problems with ActiveX, Java and JavaScript, these should, as a general rule, be deactivated.

If ActiveX, Java and JavaScript absolutely must be used, they should only be allocated to computers separated from other internal computers in such a way that security-relevant data cannot be impaired.

Breaches in the security of WWW browsers

Considerable security breaches have already been found in most browsers. For example in February and March 1997 many weaknesses in the security of different versions of the Microsoft Internet Explorer were discovered.

These mistakes can all be put down to Microsoft attempting to connect WWW with local Windows components, thereby granting WWW-sites as much confidence as local data. With the appropriate software it became possible to execute harmful programmes on the local computer of the WWW-user simply by calling up low-key WWW-sites without the user realising.

Encryption

Since all data is transmitted across the Internet in plain-text, sensitive data should be encrypted before transmission. It is sensible, as long asthe appropriate mechanisms are already provided in the sub-areas of the protocol. For safe transmission of data across the Internet it must be considered whether more recent protocols such as IPv6, S-HTTP or SSL can be used.

More recent browsers support the use of diverse security protocols. At least SSL should be supported.

Using available security functions

In every case, the available security functions of the browser should be used (confirmation before execution of programmes, access to restricted file systems only, no possibility to change local data).

When surfing in the Internet, automatic execution of programmes should be prevented (e.g. via the Disable Java option) and only reactivated for trustworthy servers.

News-Reader and Mail-Clients frequently offer the possibility of reading any type of data in MIME format. Commands can also be contained in this data which lead to automatic execution of programmes on the local computer. The appropriate possibilities should therefore be removed from the configuration files or confirmation should be required before programmes can be executed.

Gathering information about security breaches

Since new gaps in security are constantly discovered in WWW browsers, information should regularly be gathered regarding these gaps and how to eliminate them. Procuring the most up-to-date version of the product should not be a priority as new programme additions can mean new security problems. By installing patches it is at least ensured that acknowledged security breaches are eliminated.

Regulations

The user is responsible for the majority of the safeguards listed above, since their implementation as, for example the activation of certain options, cannot be consistently checked by administration. Every user should therefore be required, via the appropriate instructions, to observe the listed security guidelines before using Internet services. It is advisable to commit users to compliance with an operating pattern before allowing them to access Internet services. A training course should be held to impart the contents of the Internet security guidelines and the operating pattern to users.

This operating pattern should contain a brief description of the available communication services and a list of all the relevant regulations. Every user should confirm with his signature that he has acknowledged the regulations and will observe them when using communication services.

It should be brought to the attention of every user that the use of Internet services can be expensive. Consequently, it is important that the information gathered in the Internet is made available to other staff so that they do not access the same external Web pages repeatedly. For this purpose, a separate area of the internal network should be set aside where such information can be stored in a structured manner.

Furthermore, users must be aware

- that the configuration of WWW programmes may not be changed without authorisation,
- which data is logged
- who should be contacted when security problems arise.

S 5.46 Installing stand-alone-systems for Internet use

Initiation responsibility: Head of IT Section

Implementation responsibility: Administrators

To reduce the threat of attacks from the Internet on local data or a computer in a LAN, it is wise to install computers that are only networked with the Internet and do not possess any further network connection to a LAN.

Different operating systems offer various possibilities for the confidentiality and integrity of data on this computer as regards respective threats.

It is important to observe that no unnecessary programmes are installed when installing Internet-access software. Some products and operating systems offer the possibility of converting the computer into a complete Internet-server via the installation of server-programs. The installation of TCP/IP software allows a complete two-way connection, via which data can be sent into the Internet as well as collected from it.

Under UNIX, for example, it must be observed that daemon processes do not get started. This normally happens when booting or with the help of *inetd*. The appropriate entries must be removed from the configuration files (*rc*.* and *inetd.conf*). The software (PPP, SLIP) must be installed in such a way that a connection from the Internet cannot be established.

S 5.47 Configuration of a Closed User Group

Initiation responsibility: IT Security Management, PBX officer

Implementation responsibility: Administrators

Integrated Services Digital Networks (ISDN) allow the configuration of Closed User Groups (CUG). Such groups are characterised by the fact that all the subscribers in a CUG can communicate with each other via the public ISDN network; however, requests by external subscribers for establishing links with CUG subscribers can be rejected, just as requests by CUG subscribers for establishing links with subscribers in the public ISDN network.

Mode of operation:

All communications partners here are members of a Closed User Group configured by the network operator (e.g. Deutsche Telekom AG). Authorisation to communicate is checked by the digital exchange of the communications partner via an interlock code which is uniquely assigned to the CUG. To start with, the calling communications partner sends a call request to the digital exchange assigned to him. The digital exchange appends to this call request the ISDN number of the calling partner as well as the unique interlock code of the related Closed User Group. The digital exchange of the called communications partner uses this interlock code to identify whether the call request can be accepted. If identification is positive, the call request is forwarded to the communications partner being called.

The advantage of this function is that unauthorised attempts at access can be rejected already by the digital exchange of the network operator, so that they do not reach the gateways of the communications partner.

A disadvantage of this function is that changes in the membership of a CUG always need to be reported to the network operator, as only this party is capable of making the required modifications to the authorisation parameters. This also means that the network operator is in full control of the membership profile of a CUG and any changes made by the operator cannot necessarily be monitored by the users of a CUG. Furthermore, the configuration and operation of a CUG by a network operator generates one-time as well as running costs.

The configuration of a Closed User Group by the operator of a public network is advisable wherever

- Hardware and software for other processes (e.g. S 5.48 *Authentication via CLIP/COLP*) first need to be procured
- The membership of a CUG rarely changes
- The network operator is sufficiently trustworthy

Additional controls:

- Is clear and comprehensive documentation available on CUGs which have been configured? Is this documentation up-to-date?
- Are regular checks made as to whether the CUG function - which usually costs money - is still required?

S 5.48 Authentication via CLIP/COLP

Initiation responsibility: IT Security Management, PBX officer

Implementation responsibility: Administrators

Integrated Services Digital Networks (ISDN) allow the signalling of call numbers not only to public exchanges but also directly to the participating communications partners. This ISDN function is termed:

- CLIP = Calling Line Identification Presentation and
- COLP = Connected Line Identification Presentation or, more generally,
- Call number display

The call number display can be evaluated by each communications partner for the purpose of authentication.

Mode of operation:

To start with, the calling subscriber sends a call request to the digital exchange assigned to him. The digital exchange forwards this call request, together with the number of the calling subscriber, to the called communications partner in the ISDN. The digital exchange on the other side then forwards the call request to the ISDN communications unit of the called subscriber. On the basis of the forwarded call number, the communications unit (e.g. an ISDN router or PBX) can then identify the calling subscriber (CLIP). On positive identification, the call request is accepted and the exchange of data can be commenced.

An advantage of this function is that identification is performed by the equipment (ISDN router, PBX) of the communications partner, who is thus in full control of the identification process.

A disadvantage of this function is that call numbers transmitted via the D-channel of an ISDN are always vulnerable to manipulation (refer to T 5.63 *Manipulation via the ISDN D-channel*). Simple authentication using forwarded call numbers is thus only possible in conjunction with a callback function (refer to S 5.49 *Callback based on CLIP/COLP*) or a D-channel filter (refer to S 4.62 *Use of a D-channel filter*) which detects attempts to manipulate protocols.

Additional control:

- Can the installed ISDN equipment make use of the CLIP and COLP functions, as well as maintain sufficiently large tables of call numbers?

S 5.49 Callback based on CLIP/COLP

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: Administrators

Many communication cards offer an automatic callback function. If this function is active and the communication card receives a call, it waits for a connection to be established successfully, then closes it down again immediately, and calls a preset number back. This prevents unauthorised callers from misusing a remote port as long as access is not possible via a preset number. Callback should be used whenever a specific communications partner needs to dial in automatically. It should be noted that automatic callback also accepts the costs of data transfer.

ISDN offers a variant of callback to a specific subscriber number: Using Calling Line Identification Presentation (CLIP), the addressed ISDN card identifies the source of the call request and compares the forwarded subscriber number with a table of subscriber numbers. If a valid subscriber number was forwarded via CLIP, the corresponding number stored in the table is called back.

An advantage here, compared with authentication exclusively via CLIP/COLP (refer to S 5.48 *Authentication via CLIP/COLP*), is that even if an unauthorised subscriber feigns an authorised call number, the call request is refused because the unauthorised subscriber cannot be accessed via the specified callback number.

Additional controls:

- Has payment of costs in the callback mode been clarified?
- When were preset call numbers last checked?

S 5.50 Authentication via PAP/CHAP

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: Administrators

Many ISDN cards support communications via a Point-to-Point Protocol (RFC 1661) after an ISDN switched connection has been established. This Internet standard also offers authentication protocols such as the Password Authentication Protocol (PAP) and the Challenge Handshake Authentication Protocol (CHAP) (RFC 1994). If the ISDN card in use provides these functions, authentication should be performed with the Challenge-Handshake Authentication Protocol instead of the Password Authentication Protocol, because in the case of the latter, the password used for authentication is transmitted in plain-text form.

As a rule, the passwords used by PAP and CHAP are stored in the IT systems, so that they do not have to be entered by the user each time authentication is required. To allow continued use of these processes following a re-installation, the required passwords should be noted down and kept in a safe place (refer to S 2.22 *Depositing of passwords*).

Mode of operation:

CHAP always distinguishes between two types of communication partner: authenticator and peer. The authenticator is the communication partner requesting authentication, while the peer is the communication partner needing to submit authentication. In general therefore, the authenticator comprises the server which users need to log into as peers from their respective IT systems.

CHAP checks for the recognition of a common secret (password) on both communicating sides. This password is not transferred as plain text through the communications lines, and is protected against replay by integrating random numbers.

A Challenge-Response-Protocol is sequenced as follows:

To start with, the authenticator computes a random number. The hash value of the computed, random number is then formed using a hash algorithm. A hash function is a computing instruction which converts inputs of any length into outputs of a fixed (usually shorter) length. A one-way hash function only works in one direction, i.e. it easily allows hash values to be calculated from inputs, but makes it very difficult, if not impossible, to calculate inputs corresponding to hash values.

In the next step, the authenticator transfers the challenge, i.e. the random number just calculated, to the peer. As the authenticator and peer both possess the same hash algorithm, the peer is able to form the hash value of the transferred random number in a fourth step. The peer calculates the hash value using three parameters: the identifier (user ID), secret (password) and the transferred random number. It then transmits the hash value as a response to the authenticator. The authenticator checks the correctness of the password by also calculating the corresponding hash value and comparing it with the received one. If the comparison is positive, the peer has been successfully

authenticated by the authenticator and the communications link can be established.

Authentication using this technique should also be repeated several times while a communications link is in use, in order to prevent intrusions into active links. This can be triggered by the authenticator at sporadic intervals, without the need for user intervention.

Additional controls:

- Does the installed ISDN card and communications software allow the use of authentication protocols such as PAP and CHAP?
- Is use being made of available authentication protocols?

S 5.51 Security-related requirements for communications links between telecommuting workstations and the institution

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: Administrators , Telecommuters

The exchange of business data between a telecommuting workstation and the communications computer at the institution normally takes place via public communications networks. As neither the institution nor the telecommuter can fully guarantee the confidentiality, integrity and availability of their information in such public communications networks, additional safeguards might be required if the networks do not offer a sufficiently high level of security.

In general, data transmission between home workstations and the institution must meet the following security requirements:

- *Ensuring the confidentiality of transmitted data*: A sufficiently reliable encryption mechanism must be used to prevent the contents of data from being recovered even if these data are intercepted during transmission between the home workstation and the communications computer at the institution. In addition to a suitable encryption technique, this also requires appropriate key management and a change of keys at regular intervals.
- *Ensuring the integrity of transmitted data*: The employed transfer protocols must be able to identify and reverse coincidental changes to data during their transmission. If required, an additional error detection mechanism can be used to identify intentional manipulation during data transmission.
- *Ensuring the availability of data transmission lines*: If time delays during telecommuting are very difficult to tolerate, the selected public communications network should provide redundant routes which prevent a complete breakdown in communications should one of the routes fail. Under certain circumstances, redundant network links between the interfaces of the telecommuting workstation and communications computer at the institution can be dispensed with.
- *Ensuring the authenticity of data*: During the transmission of data between telecommuters and the institution, it should be possible to reliably determine whether communications are taking place between the correct parties, in order to preclude masquerading. This means that the indicated source of data should be identical to the actual source of the data. In addition, it should be possible to clearly establish whether data apparently transmitted by the institution actually originated from that institution.
- *Ensuring the reproducibility of data transmission*: To render data communications reproducable, logging functions can be used to subsequently ascertain which data were transmitted to which location.
- *Ensuring the reception of data*: If the correct reception of data is of importance during telecommuting, acknowledgement routines can be used to determine whether transmitted data have been received correctly.

The performance of the mechanisms needed in each case depends on the degree of protection required by the data.

Additional controls:

- Do the communications protocols in use meet the above-mentioned requirements to a sufficient extent?

S 5.52 Security-related requirements for communications computers

Initiation responsibility: Agency/company management; IT Security Management

Implementation responsibility: Administrators

Access by telecommuters to data at an institution differs in accordance with the type of telecommuting and the tasks to be performed. In some situations, only e-mail might be exchanged between telecommuters and the institution. In other cases, it might be necessary for telecommuters to access servers at the institution. Regardless of the type of access procedure being used though, the communications computer at the institution needs to meet the following security requirements:

- *Identification and authentication*: All users of the communications computer, i.e. administrators, employees at the institution and telecommuters, must identify and authenticate themselves before gaining access to the computer. If attempts of identification and authentication fail repeatedly, access is to be denied. Preset passwords are to be changed.

  If necessary, the communications computer should be able to prompt for renewed authentication from the telecommuter or remote workstation during the process of data transfer in order to preclude unauthorised interventions.

  As part of user identification and authentication, the remote workstation should also be identified (for example, by means of subscriber numbers and call-back procedures).

- *Role distinction*: The roles assumed by the administrator and users of the communications computer must be separated. Only the administrator should be able to allocate permissions.

- *Rights management and monitoring*: Access to files on the communications computer must only be granted in accordance with the rights allocated in each case. In particular, access to computers installed at the institution and the data stored on them must be regulated. Data and system access should be restricted to the bare minimum. The time periods during which access by telecommuters is possible, can also be restricted.

  In the event of a system failure or irregularities, the communications computer must assume a stable state, in which access to it might no longer be possible.

- *Minimisation of services*: Services provided by the communications computer must follow the principle of minimisation: Everything not explicitly allowed is prohibited. The services themselves must be restricted to the scope absolutely necessary for telecommuters to fulfill their duties.

- *Logging*: Data transmissions from, to and via the communications computer must be logged with details of the time, user, address and type of service.

Tools for evaluating log data should be available to administrator and auditor. Any irregularities which are detected should be reported automatically.

- *Automatic scanning for computer viruses*: Transferred data must undergo automatic scanning for computer viruses.
- *Encryption*: Confidential data maintained on the communications computer for telecommuters are to be encrypted.
- *Disabling or securing of remote administration*: If the communications computer does not require remote administration, all related functions should be disabled. If remote administration is unavoidable, it must be secured adequately. Every remote administration routine should only be allowed to take place following successful identification and authentication. Administrative activities are to be logged and administrative data are to be transmitted in encrypted form. Preset passwords and cryptographic keys must be changed.

Additional controls:

- Which functions does the communications computer offer?
- At which time intervals are checks performed as to whether the selected settings and allocated rights still conform with actual requirements?

S 5.53 Protection against mail bombs

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

Mail bombs are e-mails which have been intentionally equipped with disruptive functions. For example, a mail bomb can consist of a compressed file which is sent along as an attachment and which, when unpacked, creates a countless number of subdirectories or takes up a lot of hard-disk space.

Archives, i.e. with zip programmes compressed files, should never be unpacked without being checked beforehand. To protect one's IT systems against Trojan horses and other disruptive functions possibly harboured by compressed files, it is advisable to view a list of the archived files together with their size before unpacking them. Archive files should also be scanned for computer viruses before being unpacked.

Self-extracting executable programmes with the extension *.exe should never be opened on regular workstations, as the contents of such programmes cannot be examined before unpacking.

New programmes should always be tested beforehand on IT systems which are isolated from the production system (refer to S 4.65 *Testing new hardware and software*).

In the case of UNIX systems and other server-based operating systems, the following points should also be observed:

- Unfamiliar archives should never be unpacked under super-user authorisation, but only under a user ID with as little write access as possible.
- A file system with disk quota should be used to restrict the amount of disk space which a disruptive programme could occupy in the worst case.

Additional controls:

- Have users been informed about the potential threats posed by mail bombs?

S 5.54 Protection against mail overload and spam

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

A flood of advertisements or intentional overloading via incoming e-mails can not only block mail systems but also give rise to considerable expenses for the recipient. To protect IT systems against "spamming" - or e-mail with irrelevant contents - every user should make careful decisions as to when to disclose one's e-mail address to whom.

The following safeguards can be implemented against advertisement mail and spamming:

- Anonymous remailer services are available on servers for the purpose of de-personalising e-mail. A remailer makes it possible to send contributions to newsgroups and dispatch e-mail without the recipient being able to identify the address of the sender. A disadvantage here is that e-mail is often rejected if the sender cannot be identified.
- The mail server or firewall should be equipped with e-mail filtering programmes which only allow the passage of e-mail from/to specified communications partners and restrict the influx of spam by means of other header entries. Caution must be exercised here to prevent desired e-mail from being filtered out as well.
- Every organisation should decide whether to allow its employees to post articles in newsgroups and, if so, which form and which topics may be involved. In this context, users must be instructed to observe Netiquette and, in particular, refrain from distributing information of irrelevance to the general public.
- It might be advisable to use e-mail addresses which are not easy to guess (also refer to S 2.122 *Standard e-mail addresses*).
- On no account should attempts be made to retaliate with mail bombs or similar measures in response to spam. In fact, senders of spam should not receive any response at all. Sender details in a lot of spam mail are forged. In such cases, responses are routed to innocent parties or returned as undeliverable. At any rate, responses to spam further increase the volume of e-mail traffic and, in the worst case, confirm the correctness of e-mail addresses to advertisers.
- One effective measure against molestation by spam is to inform one's own mail provider and the mail provider of the sender so that they can take appropriate action against the sender.

It must be noted that not all of these measures are advisable under all circumstances, as each of them impose certain restrictions. On one hand, it might be advisable to refrain from basing e-mail addresses on user names in order to protect one's IT systems against undesired advertisements. On the other hand, abstract e-mail addresses can render communications with external parties difficult, as such addresses are harder to memorise. The form of an e-mail address should always comply with internal organisational rules.

A high volume of e-mail traffic can also result from subscriptions to a correspondingly large number of mailing lists. In general, regular checks should be made as to whether the subjects discussed in a mailing list are still worth reading. If not, subscription should be cancelled. Users must be instructed to make regular (i.e. daily, if possible) checks of mail influx related to subscriptions to mailing lists. In large organisations, mailing lists of professional interest should only be subscribed to by one staff member (e.g. the mail administrator) and then made available centrally to all other employees.

Additional controls:

- Have all users been informed about the threats posed by spam?
- Who subscribes to which mailing lists?

S 5.55 Checking of alias files and distribution lists

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

Alias files and distribution lists are often used to facilitate the addressing of e-mail. If alias files are maintained on mail servers as well as mail clients, clarification is required as to which entries have priority, i.e. if an alias is duplicated on both servers, which address should be accepted on the selection of this alias. Aliases on the mail server should be decisive when e-mail is received, aliases on the mail client should be decisive when e-mail is dispatched. Users must be notified of aliases which are resolved by the mail server, so that they can take this into account when passing on e-mail addresses.

Users must have read-access to alias files on the mail server to be able to make use of these files. Only the mail administrator should have write-access to the files.

To prevent e-mail from being transmitted to the wrong parties as a result of incorrect, outdated or manipulated distribution lists, these lists must be checked regularly for correctness and validity.

Additional controls:

- At which locations have alias files and distribution lists been stored?
- Who has access to alias files and distribution lists?
- When were alias files, distribution lists and stored e-mail addresses last checked for validity?

S 5.56 Secure operation of a mail server

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Secure operation of a mail server requires secure local communications as well as secure communications through public networks. The mail server receives e-mail from other mail servers and forwards it to connected clients and servers. The mail server also forwards e-mail transmitted by local users to external mail servers. Here, the mail server must ensure that local e-mail transmitted by connected users is only forwarded internally and not allowed to reach the public network.

A mail server temporarily stores e-mail until it is forwarded. Many Internet providers and administrators also archive incoming and outgoing e-mail. The mail server must be protected appropriately to prevent unauthorised persons from gaining access to messages on it. For this purpose, the server must be located in a secure area (server room or server cabinet). One administrator and one substitute should be trained and placed in charge of the proper functioning of the mail server as well as its operating system. A postmaster account must be configured to receive all undelivered e-mail and related error messages (also refer to S 2.120 *Configuration of a mail center*).

Only locally connected users should have access to their mailboxes. However, these local users should not be allowed to access areas where e-mail is stored temporarily prior to forwarding (e.g. spool files).

Regular checks must be made of the stability of links with neighbouring mail servers, particularly that of the mail provider. Furthermore, regular checks are required to determine whether there is still sufficient hard-disk space for the temporary storage of mail, otherwise the exchange of messages might be impeded.

Logging of the mail server's activities should be defined with respect to scope and contents.

The mail server should never be part of a production system. In particular, no other services should be dependent on the availability of the mail server. Quick deactivation of the server should be possible at all times, e.g. in the event of a denial of service or if manipulation is suspected.

To make unauthorised access to user accounts more difficult, user names on the mail server should not be directly inferable from the e-mail addresses.

Incoming e-mail should be checked by the firewall or mail server for computer viruses and other disruptive as well as active components (e.g. Java applets).

Filtration rules can be used to block the transmission and reception of e-mail for specific addresses. For example, this can prove useful for protection against spam mail. Other header entries can also be filtered to exclude spam. Caution must be exercised here to prevent desired e-mail from being filtered out as well. For this reason, the filtration rules should be defined very precisely, for example, by deriving a new, dedicated set of rules for every

newly received consignment of spam mail. Appropriate filter lists are available in the Internet and can be obtained from various manufacturers of communications software.

Authorised protocols and services on the mail server must be specified. For example, it is advisable to authorise SMTP (TCP port 25) for outbound and inbound links, but only authorise POP3 for internal links.

The mail server must be protected against use as a spam relay. For this purpose, the mail server should be so configured that it only accepts e-mail intended for the organisation and only transmits e-mail originating from the staff of the organisation. The mail server should only accept incoming e-mail if the IP address of the transmitting mail server is located in an IP network authorised explicitly by the administrator, or if the mail server holds an MX entry for the recipient. All other e-mail must be rejected with a corresponding error message.

In spite of these safeguards, authorised users can continue to send/receive e-mail to/from any required party. However, the filtration of incoming e-mail described above prevents the mail server from being misused as a spam relay by external parties.

If IP networks from which e-mail is to be accepted have been inadvertently omitted from the list mentioned above, the administrator of the mail server must be informed duly so that he/she can include these networks subsequently in the list.

If, instead of operating its own mail server, an organisation accesses the mail server of a provider via one or more mail clients, clarification by the provider is required as to the rules and security measures applicable on that server (refer to S 2.123 *Selection of a mail provider*).

S 5.57 Sichere Konfiguration der Mail-Clients

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, IT-Benutzer

Die E-Mail-Progamme der Benutzer müssen durch den Administrator so vorkonfiguriert sein, daß ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann. Die Benutzer sind darauf hinzuweisen, daß sie die Konfiguration nicht selbsttätig ändern dürfen.

Insbesondere die folgenden Punkte sollten bei der Konfiguration der E-Mail-Clients berücksichtigt werden:

- Das E-Mail-Paßwort darf keinesfalls dauerhaft vom E-Mail-Programm gespeichert werden. Dabei wird das Paßwort auf der Client-Festplatte abgelegt, u. U. sogar im Klartext oder nur schwach verschlüsselt. Jeder, der Zugriff auf den Mail-Client hat, hat so die Möglichkeit, unter fremden Namen E-Mails zu verschicken bzw. das E-Mail-Paßwort auszulesen.
- Als Reply-Adresse ist die E-Mail-Adresse des Benutzers einzustellen, um sicherzustellen, daß keine internen E-Mail-Adressen weitergegeben werden.
- Um die Netzbelastung niedrig zu halten, sollte der Mail-Client nicht zu häufig den Mail-Server auf neu eingetroffene Nachrichten überprüfen. Ein automatischer Abholversuch alle 30 Minuten (= 1800 Sekunden) wird als Standardwert empfohlen und ist im allgemeinen ausreichend. Sollten Benutzer eine dringende Nachricht erwarten, sollten sie das E-Mail-Programm manuell dazu veranlassen, in ihrer Mailbox nachzusehen.
- Nachrichten, die vom Mail-Server abgeholt wurden, sollten dort auch gelöscht werden. So kann ein mehrmaliges Abholen derselben Nachrichten verhindert und Speicherprobleme am Mail-Server vermieden werden.

S 5.58 Installation of ODBC drivers

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

ODBC (Open Database Connectivity) creates an additional layer between a database application and the related database protocol, and thus does not constitute a database protocol as such. The installation of an ODBC driver matching with a database creates a standard interface between the application and the database, via which communications (issue of database queries, reading of data) with the database take place. The related ANSI-SQL-compliant SQL interface permits the creation of applications without having to take the different specific database products into account. For this reason, the application does not need to be re-configured on a change of database software; instead, it is sufficient to simply replace the ODBC driver. Developed originally for Microsoft products, ODBC has now established itself as a standard. ODBC drivers are available for all common databases supplied by diverse manufacturers.

ODBC drivers must be so installed that access control of the database system is not threatened by any security pitfalls.

Example:

In the case of MS Access databases, the employment of user IDs is optional. If access control is activated however, the user IDs are managed via *Systemdb*, a separate MS Access database which is also stored as an independent file.

During the installation of an ODBC driver for an MS Access database, *Systemdb* is not integrated automatically. The default installation settings do not take any existing *Systemdb* into account. Consequently, if *Systemdb* is not specified explicitly during the installation of the ODBC driver, *Systemdb* does not request any identification for database queries issued via ODBC. Access control is thus circumvented.

To avoid this, a regular check can be made as to whether *Systemdb* is integrated. However, as this mechanism can be undone or manipulated at any time, a safer solution is to encrypt MS Access databases. In this case, all attempts to access a database without *Systemdb* fail. For this purpose, the encryption mechanism integrated in MS Access needs to be activated (under *Extras / Access Rights / encrypt/decrypt Database*). Attempts to access the database via the ODBC interface then fail, as *Systemdb* is also required for the encryption mechanism.

Additional controls:

- Has an ODBC driver for the database been installed? If so, have the optional installation parameters and their effects been taken into consideration?

S 5.59 Protection against DNS spoofing

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

A threat from DNS spoofing can arise when authentication is performed using computer names. Host-based authentication, which means that permissions are granted on the basis of computer names or IP addresses, should be protected with one (or a combination) of the following measures:

1. IP addresses should be used, not host names.
2. If host names are used, they should all be resolved locally (entries in the file */etc/hosts*).
3. If host names are used and cannot be resolved locally, all names should be resolved directly by a name server which acts as primary or secondary name server, i.e. stores the names permanently instead of in a temporary cache.

The first configuration provides the highest security, the third provides the lowest security. The aim of these measures is to perform a mapping between IP addresses and computer names in a secure environment. If name resolution cannot be performed directly, i.e. if a temporary cache is made use of, then host-based access should never be allowed via a host name.

S 5.60 Selection of a suitable backbone technology

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section, Administrator

The selection of a network protocol for the backbone is a decisive factor for the security and availability of the local network because the protocol has major influence on the available bandwidth and performance. If the cabling is planned without commitment to special services (e.g. proprietary solutions) (see also T 2.45 conceptual weaknesses in the network), a change in backbone technology is principally feasible. Even though this requires a considerable organisational, personnel and financial effort.

A general recommendation with regards to IT security for a specific backbone technology cannot be given because many individual aspects have to be taken into account. The advantages and disadvantages of the most common network protocols are given in the following:

There are four base technologies Ethernet, Token-Ring, FDDI, and ATM which can be described as follows:

Ethernet

Ethernet technology is defined in the IEEE 802.3 standard and based on the CSMA/CD (Carrier Sense Multiple Access / Collision Detection) technique. With this technique, all stations are equally entitled to access the transmission medium, although it can only be used by one station at a time. When a station needs to transmit data, it first checks if the transmission medium is available for use (carrier sense). If it is, the station starts data transfer. If several stations start transmitting data simultaneously (multiple access), a collision occurs and is detected by the affected stations (collision detection), whereupon the medium is checked again and a renewed attempt is made at transmission.

As CSMA/CD is a stochastic technique, it does not guarantee the availability of any dedicated bandwidths. For this reason, it is not very suitable for multimedia applications which require a fixed bandwidth, for example. Consequently, Ethernet-based networks do not ensure any particular *Quality of Service* (QoS) in general. Gigabit Ethernet systems have a technique similar to QoS.

There are three types of Ethernet which basically differ from each other only in terms of the supported transmission rates:

- **Standard Ethernet**

  Standard Ethernet, a predecessor to the other two variants, has been in use for a long time. It provides a transmission rate of 10 Mbit/s, it is an unsuitable backbone technology for most local networks, as a rise in the network load is accompanied by a sharp increase in the number of collisions, causing the throughput to drop steadily.

- **Fast Ethernet**

  Due to the rising number of networked computers and the resulting increase in network loads, Standard Ethernet urgently needed to be

advanced in order to meet increasing technological demands. This led to the development of the Fast Ethernet with a transmission rate of 100 Mbit/s. Presently, this rate is sufficient for most networks in the backbone area, and is also advantageous in that the already established CSMA/CD technology can continue to be used. In this case however, the active network components generally need to be replaced or adapted; furthermore, the cabling needs to be checked for compatibility with Fast Ethernet.

- **Gigabit Ethernet**

  As Fast Ethernet proved extremely successful following its introduction, a demand for an even faster Ethernet-based backbone technology was voiced. This led to the founding of the Gigabit Ethernet Alliance (GEA) by several renowned manufacturers, who wanted to achieve a transmission rate of 1 Gbit/s. The standardisation phase is to be completed soon in cooperation with the IEEE. With the help of features such as a protocol extension (Resource Reservation Protocol, RSVP) for time-critical transmissions (e.g. in the multimedia sector), the new standard is intended to provide dedicated bandwidths in Gigabit Ethernet systems. The aim of this is to supply attributes similar to those applicable to ATM, such as *Quality of Service* (QoS). However, as the final standard has not been approved yet, this variant should not be selected, in order to avoid the use of an implementation which might still be incomplete.

Token-Ring

Token-Ring technology is defined in the IEEE 802.5 standard and is based on the token passing technique. With this technique, a special data packet (token) travelling on a circular path is used to determine which station may use the transmission medium. When a station receives the token, it occupies the medium and then forwards the token to the next station. This ensures that the medium is only occupied by one station at a time.

In contrast to Ethernet, this deterministic technique prevents stations from having to wait for indefinite periods of time on the occurrence of high network loads before being able to transmit data. Token-Ring makes it possible to firmly specify the maximum waiting period.

A Token-Ring network is usually configured as a physical double-ring, which considerably increases the availability of the network, because, in the event of a failure of a station or an interruption of one of the rings, the faulty point can be bridged by using the other ring.

Token-Ring allows a transmission rate of 4 or 16 Mbit/s, so that for most local networks, its use as a backbone technology is no longer recommended either. The available bandwidth is too narrow. In the middle of September 1997, a "High Speed Token Ring Alliance" (HSTR) was founded by several renowned manufacturers to achieve transmission rates of 100 Mbit/s and, at a later stage, 1 Gbit/s. For this purpose, the IEEE 802.5 standard is to be extended by the middle of 1998. As this variant is still being developed, its use is not recommended at present.

FDDI

The FDDI (Fiber Distributed Data Interface) standard was defined in 1989 by ANSI and is based - like Token-Ring - on the token passing technique. However, FDDI additionally makes use of early token release, which forwards the token to the next station immediately after the last data packet has been send. This reduces the idle times in the ring and helps achieve a higher bandwidth.

FDDI uses optical fibre cables as the transmission medium, and provides a transmission rate of 100 Mbit/s. Due to its high throughput, FDDI is ideal for use in the backbone areas. Additional advantages include the high fault tolerance resulting from the double-ring topology, and the electromagnetic stability arising from the use of optical fibre cables. As opposed to Ethernet, FDDI is also suitable for performance-dependent multimedia applications, because it ensures a maximum delay time.

If both rings are used for data transfer, a transmission rate of as much as 200 Mbit/s is achievable; the advantage of the high fault tolerance is eliminated in this case however, because if one of the rings malfunctions, it is no longer possible to switch over automatically to the other one.

FDDI components are more expensive than Ethernet components offering a similar functionality; for this reason, the benefits derived from the use of FDDI should always be compared with the costs it generates.

FDDI can also be operated on copper cables, in which case it is termed CDDI (Copper Distributed Data Interface).

ATM

ATM stands for Asynchronous Transfer Mode, and involves a transmission technique which is very suitable for use in the backbone area of a network, and which can also supply real-time services in this area.

In ATM, information of all types is transferred in packets of a fixed length, termed cells. The information can consist of any required data, including video and audio data. The standard length of the packets allows the ATM switches to process the cells almost entirely through the use of hardware components, thus achieving a higher throughput. This results in calculable delays during the transfer of any type of information, so that separate bandwidths can be guaranteed for individual applications. ATM is therefore a very suitable technology for multimedia applications, as it guarantees a computable real-time response and, thus, *Quality of Service* (QoS). This means that the required bandwidths can be allocated statically or dynamically to every connected device.

Transmission as such takes place on the basis of virtual links. No fixed channels are activated between communicating stations; instead, the cells are transferred through the network via routes determined shortly before the cells were generated. This achieves typical transmission rates of roughly 25 MBit/s, 155 MBit/s and 622 MBit/s.

ATM components are still very expensive though; so to safeguard investments, efforts should therefore be made to integrate ATM components with the other technologies already existing in the network. However, ATM

does not support broadcasts or MAC addresses, which is a prerequisite for the use of most protocol stacks such as TCP/IP and SPX/IPX. Three different solutions to this problem are available:

- **Classical IP-over-ATM (CIP)**

  RFC 1577 (Classical IP-over-ATM) was developed for the use of IP over ATM; this standard allows stations with a TCP/IP protocol stack to use ATM as a transfer medium.

- **LAN Emulation (LANE)**

  This standard emulates all relevant LAN technologies for clients on layer 2 of the OSI model. In this case, ATM is then represented as, for example, an Ethernet or Token-Ring network to the clients. This allows communications between conventional LANs and ATM.

- **Multiprotocol-over-ATM (MPOA)**

  MPOA is basically an advancement of the classical ATM and LANE. In contrast to LANE, MPOA operates on layer 3 of the OSI model and uses LANE for transmission on layer 2. Consequently, MPOA implements bridging (layer 2) as well as routing (layer 3), and can thus configure a fully routed ATM network. At the same time, it offers all the advantages of ATM technology, such as guaranteed bandwidths for individual applications.

Furthermore, it must be noted that no compatibility or interoperability is presently guaranteed between ATM components from different manufacturers. A corresponding check is therefore required in each case.

As mentioned at the start, a general recommendation concerning the selection of a suitable backbone technology cannot be made. In addition to security requirements, influential factors here include criteria concerning future orientation, economy, scalability and the integration of existing components.

Depending on the selected protocol, only certain types of cable can be used (e.g. optical fibre cables for FDDI); each cable type is restricted in length (also refer to S 5.2 *Selection of an appropriate network topography*).

Additional controls:

- Have requirements concerning the availability, bandwidth and performance of the backbone of the local network been formulated and documented?
- Have all the relevant backbone technologies been considered?

S 5.61 Suitable physical segmentation

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Physical segmentation involves separating the network with the help of active and passive network components on layer 1, 2 or 3. Suitable physical segmentation can increase availability, integrity and confidentiality. Various types of network components can be used to perform segmentation (refer to S 5.13 *Appropriate use of elements for network coupling*).

Availability

The performance and bandwidth offered by a network are also considered from the perspective of availability, which can be enhanced if the network is separated on layer 1, 2 or 3 of the OSI model. Separation on layer 1 achieves the smallest possible increase in the availability of the individual segments but the highest possible throughput between them, while separation in layer 3 achieves the largest possible increase in the availability of the individual segments but the lowest possible throughput between them.

Segmentation on layer 1 with the help of a repeater increases the availability of the network by preventing electrical errors in one segment from affecting the remaining segments.

Example: In a network consisting of two thinwire Ethernet segments linked together via a repeater, the absence of a terminator in one segment does not affect the functionality of the other segment.

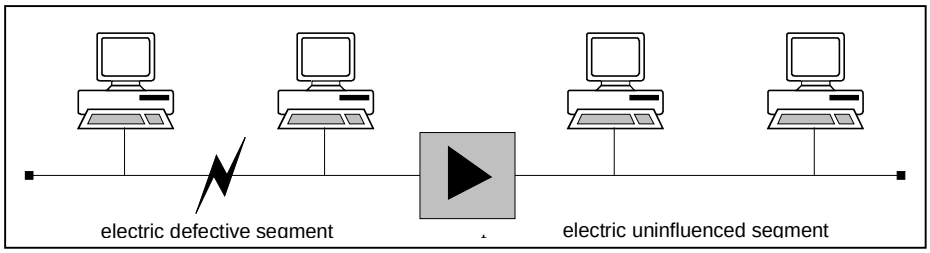


Figure 1: Electrical separation of segments with a repeater in order to increase availability

What applies to repeaters here also holds true for bridges and switches, as they cover layer 1 as well. In addition to this function, faulty data packets on layer 2 and collisions are isolated in one segment. The segments are also relieved, as data packets can be forwarded systematically between them. It must be ensured that the bridge or switch in use has a sufficiently high capacity (filter and transfer rates), to allow the data traffic between the segments to be processed without any major delays.

Generally, bridges and switches operate on layer 2 of the OSI model. To set up the connection matrix, these components evaluate the MAC addresses of the involved systems in the respective segments. Some manufacturers also offer switches which operate on layer 3, for example, using the IP address to set up the connection matrix. In both cases, setup is performed automatically, although certain models also allow manual intervention. Some manufacturers additionally offer the possibility of setting up the connection matrix manually

(via a central tool) on the port level, where the cables are actually routed (port or configuration switching).

Routers operating on layer 3 incorporate the characteristics of both repeaters and bridges as regards availability, and also allow an evaluation of protocols on layer 3. This results in a load separation on a higher level, thus permitting almost full control of network traffic. In particular, no broadcasts are forwarded between segments (subnets) separated by means of a router. Consequently, a broadcast storm occurring in one segment does not affect the other.

Based on the results of a traffic-flow analysis (refer to S 2.139 *Survey of the existing network environment)*, it might be necessary to perform physical segmentation in order to increase the bandwidth and performance to the required extent.

Example: Central server systems for file and printing services as well as applications are present or planned in a network. To achieve a high level of performance and availability, it might be advisable to connect these servers in a dedicated manner to a switch, from where the server systems are linked with the individual workstations (shared or switched mode). If possible, the connection between the server systems and the switch should at least comprise a Fast Ethernet link.

In general, a switched network provides higher performance than a shared network, as all subscribers connected to a shared network need to share the available bandwidth. In contrast, a switched network offers every subscriber the full bandwidth at least as far as the next active network component. However, it must be noted that such a network requires structured cabling (star configuration), and that a fully switched network generates relatively high costs.

Alternative solutions involve the coupling of individual segments in the backbone area or areas experiencing high network loads (e.g. workgroups) via a switch; these segments are configured as shared-media LANs (see Figure 2). Additionally, it is always possible to connect individual workstation systems with high performance requirements directly to a switch. Whereas a shared network or shared segment can be laid out in a bus or a star configuration, reasons of availability and investment safeguarding make it advisable to implement structured cabling (star configuration) in this case as well. (refer to S 5.2 *Selection of an appropriate network topography*).

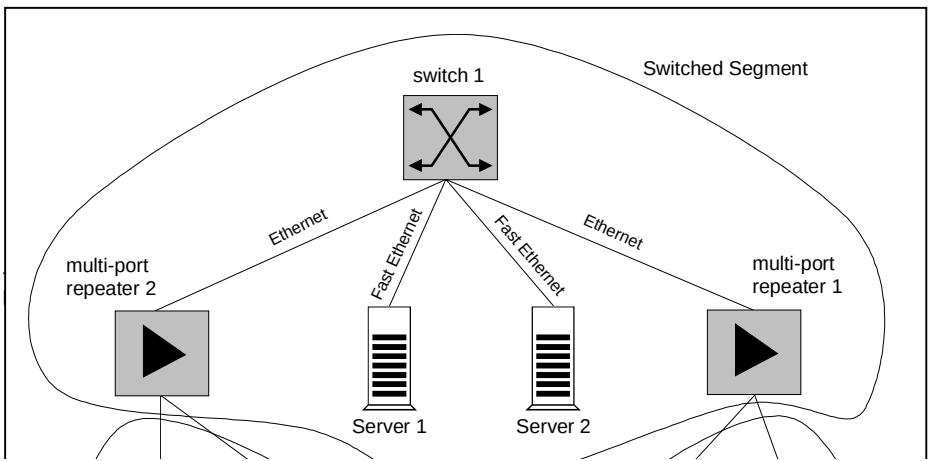


Figure 2: Example of a network consisting of switched and shared segments. The servers are linked via Fast Ethernet.

Confidentiality

All measures which prevent an exchange of data between two segments are suitable for increasing the confidentiality of the data. Consequently, a repeater alone is unsuitable for this purpose. Some manufacturers offer multi-port repeaters which can be configured so as to allow only certain network users to operate in the network via these repeaters. To a certain extent, this prevents unauthorised clients from establishing links with the network. Bridges / switches and routers increase confidentiality by preventing and checking data traffic on layers 2 and 3, and joining or separating segments on the port level in a dedicated manner. Certain manufacturers also offer bridges and switches which restrict access by network clients. Routers offer the most extensive possibilities of controlling the components dealt with here. Routers can not only be used to control access and routes for accessing other networks, but also to specify which clients may communicate with systems in another segment on which basis. By excluding certain layer-3 protocols the router can prevent the data related to these protocols from reaching the other segments. This is done by defining appropriate filter rules for the routers; these rules can be formulated on the protocol level. If a TCP/IP protocol stack is used, for example, individual TCP and UDP ports can be disabled or enabled selectively. Components operating on higher layers, such as application-level firewalls, are not considered here (refer to S 2.75 *Selection of a suitable application gateway*).

Example: Separating a network with the help of a router and appropriately configured filter rules prevents the transfer of FTP and TFTP data (ports 20 and 21 or 69 respectively) between the segments, so that this service cannot be intercepted on the other segment. This also prevents the transfer of broadcast

data between the subnets. In addition, the filters must be configured by default such that communications are initially restricted to the greatest possible extent and only enabled subsequently for individual services as the requirements for them arise. If necessary, IP-specific filtering should be considered here.

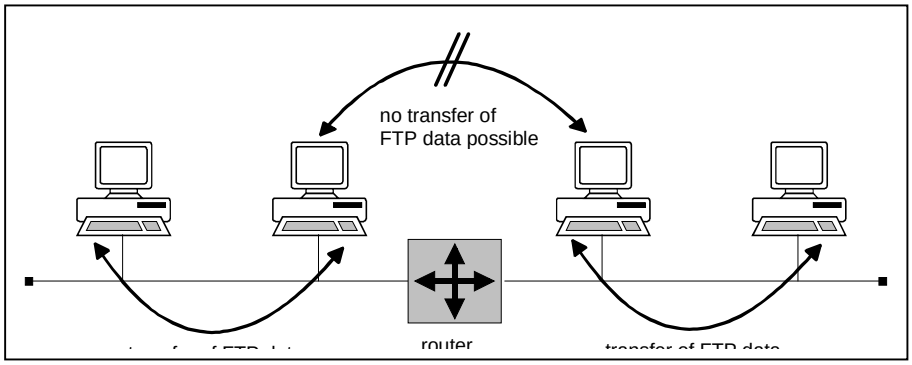


Figure 3: Example of segmentation into subnetworks on layer 3 by a router

Data and network integrity

As a rule, the integrity of data up to layer 3 is ensured by the network access protocol in use, whilst additional measures are required to ensure network integrity, i.e. concordance between the actual network environment and the planned physical, as well as logical, segmentation. These measures must prevent the establishment of unauthorised or incorrect communications links, as well as unauthorised system access which would impair the integrity of the network.

Consequently, network integrity is essentially ensured by

- Preventing, or at least detecting, direct modifications to network components (replacement of components or installation of new, unauthorised components). This is termed hardware-based security.
- Preventing, or at least detecting, changes to the configuration of network components (routing protocols, port-switching matrices or VLAN allocations). This is termed software-based security.

For this, it is necessary to restrict physical access to the network components to a sufficient extent (e.g. by implementing infrastructure-specific measures for the distributor room, cabling etc.) and conceive the network management system so as to prevent unauthorised access to the network components via the network.

The use of network components alone does not serve to enhance protection of the integrity of data on layer 3 (e.g. application data), although it does hinder selective attacks on data integrity. For this purpose, network components can be used which prevent data packets from being tapped and manipulated. Such components comprise, for example, bridges / switches and routers which can be used to separate a network into segments or subnetworks between which data communications are to be controlled, restricted or configured. A mapping of logical relationships to a physical configuration plays a key role,

particularly in the case of network components which can be configured automatically, such as bridges and switches. Only this ensures that the data packets of a logical group actually remain in the corresponding physical segment. In the case of bridges / switches which allow a configuration of the conceivable links on the port level (port switching), manual control of link establishment on layer 1 is also possible.

Example: Systems which allow the connection of terminals to a network (terminal servers) and systems to be accessed from the terminal servers need to be assigned to a segment separated from the rest of the network by means of a bridge. Only this prevents passwords transferred from the terminal server to the addressed system from being tapped and, possibly, modified from another segment.

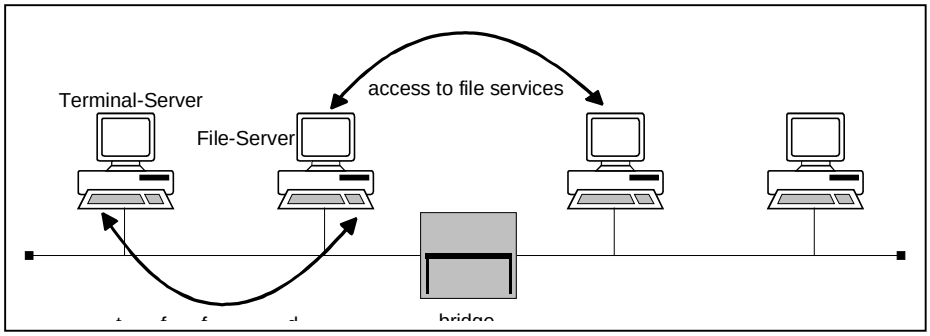


Figure 4: Separation into segments with a bridge in order to enhance integrity and confidentiality

Furthermore, network components should be selected and dimensioned appropriately in order to ensure that neither an overload nor a failure of these components will result in a loss or corruption of data packets.

Additional controls:

- Has physical segmentation been considered as part of the design of the local network?
- Have requirements concerning availability (particularly in terms of performance), confidentiality and integrity been ascertained and taken into account?

S 5.62 Suitable logical segmentation

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

With the help of appropriate network components, it is possible to segment a network logically even if a fixed physical segmentation is already in effect. This can be achieved using switches which operate on layers 2 and 3 of the OSI model. As these switches recognise the protocols used on layers 2 and 3, virtual LANs (VLANs) can be formed by controlling the data flow between the switch ports. This makes it possible to create network groups which are not mapped as such by the physical segmentation. In particular, this allows a quick and dynamic formation and rearrangement of groups without any modifications to the physical layout of the network. As in the case of physical segmentation on layers 2 and 3, criteria concerning confidentiality, availability and integrity are also to be applied here. Criteria for suitable logical segmentation can be applied similar to the criteria for physical segmentation.

The following illustration shows one possibility of forming a VLAN with the help of several layer-3 switches. The physical links between the stations and the switches are represented by the connecting lines. Logical segmentation is performed through grouping into VLANs using switches.

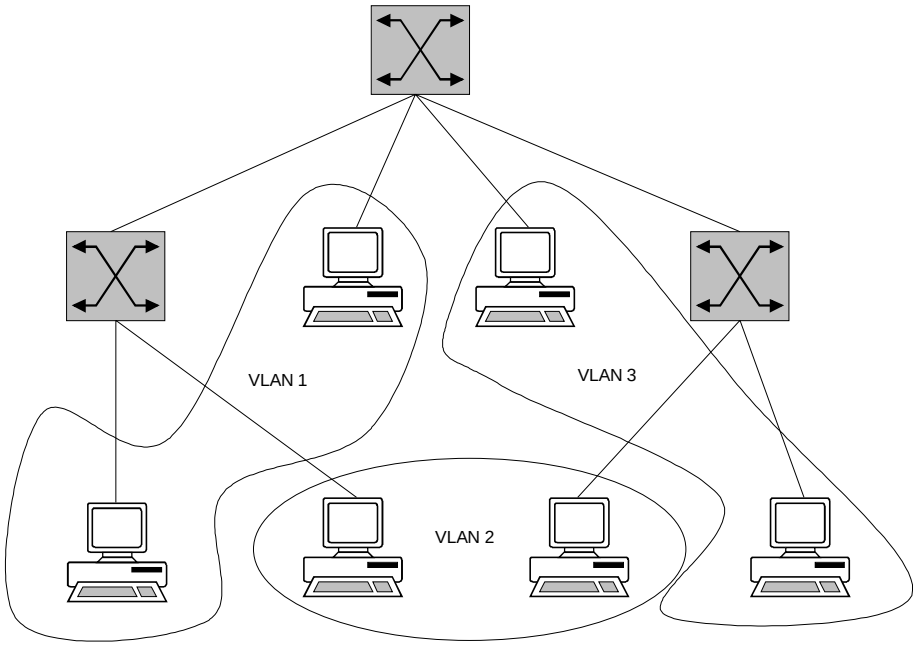


Figure 1: Formation of VLANs using several switches

If the VLAN structure shown in Figure 1 were to be achieved by means of a conventional physical segmentation, the layout shown in Figure 2 would be the result. The individual LANs can be mapped here by means of shared Ethernet segments, for example, and linked together with a bridge.

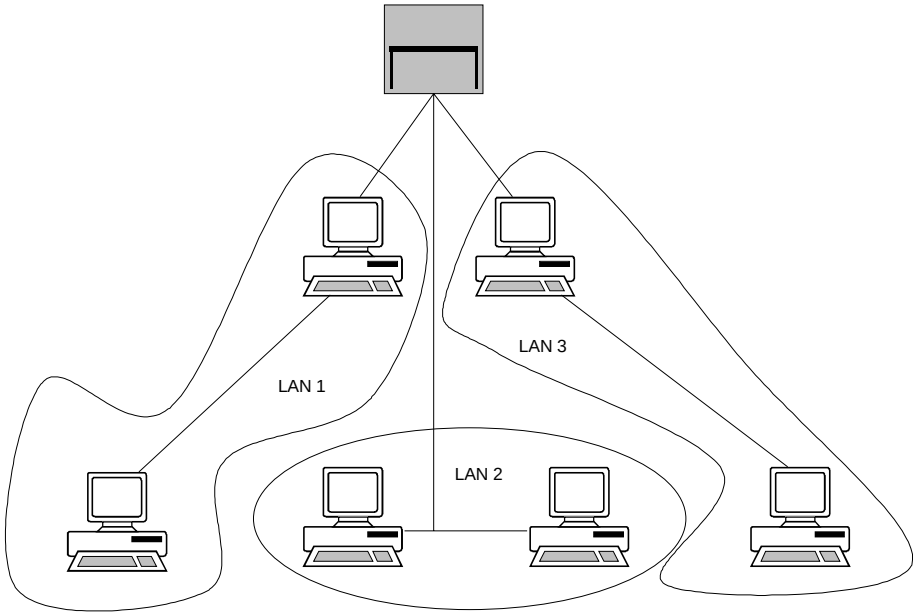


Figure 2:

Physical segmentation in compliance with Figure 1

On the basis of VLAN-compatible network components, virtual LANs can be formed without any physical restructuring. In accordance with the technologies used, these VLANs are created through segmentation on layers 2 and 3. Like LAN segmentation, this allows a network to be separated into areas where high demands are placed on the confidentiality of data, for example (refer to S 5.61 *Suitable physical segmentation*). Depending on the product in use, different functions are available for the formation of VLANs. Some products allow the formation of VLANs on layers 2 and 3, which can only be coupled by means of routers (and are thus termed secure VLANs). In this case, filter rules need to be defined for the router in order to ensure controlled transmissions between the individual VLANs. Other manufacturers even implement a routing function in layer-3 switches, which allows VLANS to be linked without the need for additional routers. In particular, the intended technologies and products must be checked to determine whether they fulfill requirements concerning the confidentiality and integrity of data.

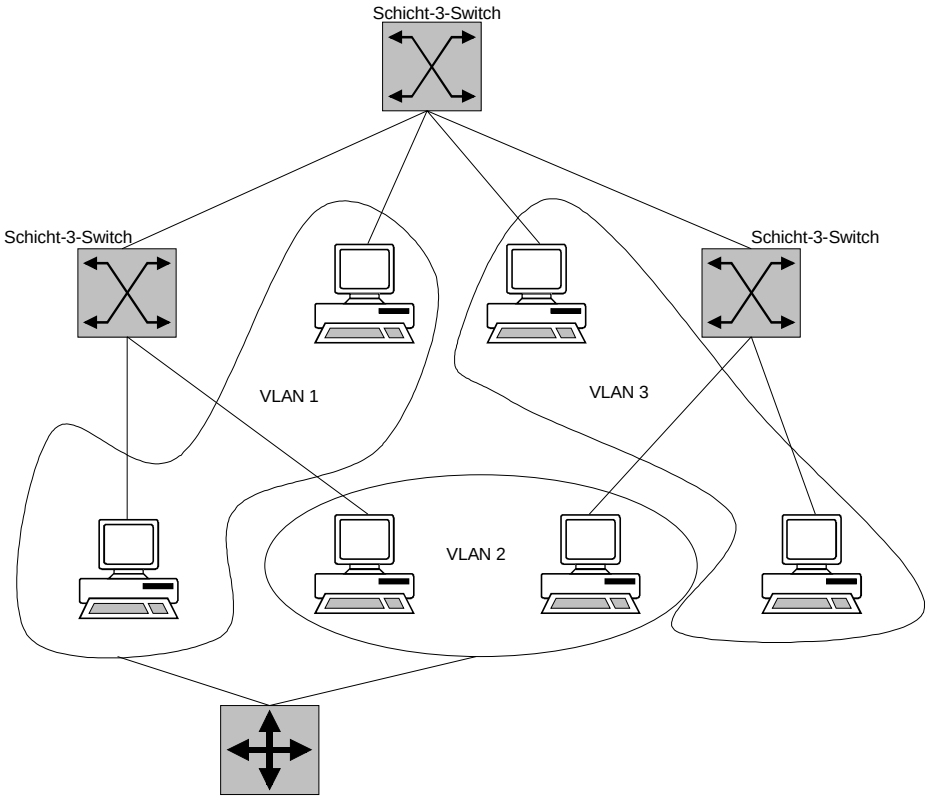


Figure 3: Formation of secure VLANs with layer-3 switches

In this case (Figure 3), layer-3 switches are used to configure secure VLANs on layer 3 of the OSI model. The switches illustrated here do not have a routing function. VLAN 1, VLAN 2 and VLAN 3 operate as though they have been segmented by means of a router, although no routing takes place between them. In other words, VLAN 3 is not linked with any of the other VLANs; only VLAN 1 and VLAN 2 can communicate with each other via a router. Communications can be controlled by configuring the router in the required manner. Other products which implement a routing functionality in the layer-3 switches eliminate the need for the displayed router, and allow routing with the help of the switches.

A general recommendation concerning logical segmentation cannot be made. During the installation of a new network however, a check must be made as to whether VLANs would help fulfill requirements concerning availability, confidentiality and integrity more easily than a more elaborate physical segmentation.

One advantage of logical segmentation is the easy and central configuration of new segments and reconfiguration of existing ones. Particularly in the case of products which support secure VLANs, this allows a quick and easy formation of workgroups in the network, which fulfill the high requirements concerning the confidentiality of each workgroup's data. On the other hand, secure remote access to the active network components also requires particular attention in this case, as segmentation here is only based on software configurations. During logical segmentation, a balance therefore needs to be struck between

the security requirements of the network (also as regards protection against unauthorised reconfiguration) and the need for flexible reconfiguration of the network.

Additional controls:

- Are the network components in use VLAN-capable?
- Has the network been segmented logically in a suitable manner?
- Are the network components in use interoperable in term of VLAN functionality?
- Are the active network components protected against remote access by unauthorised administrators?
- Have requirements concerning availability, confidentiality and integrity been ascertained and taken into account?

S 5.63 Use of PGP

Initiation responsibility: IT Security Management, Administrators

Implementation responsibility: IT users, Administrator

PGP (Pretty Good Privacy) is an encryption program that is in widespread use. PGP can be used to encrypt and decrypt messages and files, and to attach a digital signature (also referred to as an electronic signature) in order to be able to prove that unauthorised changes have been made to a message or file. Key-management tasks, such as adding and removing keys, can also be carried out with the aid of PGP.

Encryption and digital signatures

PGP makes use of symmetric and asymmetric cryptographic procedures. Symmetric procedures such as IDEA are used for data encryption, while asymmetric procedures such as Diffie-Hellmann are used for the exchange of keys and RSA or DSS for signature generation.

PGP creates and uses public and private keys in pairs of keys. For every private key, there is exactly one public key. It is practically impossible to determine the private key simply on the basis of the public one. A message that has been encrypted with a public key or signed with the private key can only be decrypted with the corresponding private key or verified with the originator's public key. The public key can be revealed to anyone. Its purpose is to encrypt messages to the owner of the private key.

In order to provide proof of unauthorised manipulation and therefore to protect messages against modifications, PGP uses the originator's private key to calculate a cryptographic checksum for the message - the digital signature. Using the public key belonging to the sender of a message, every communication partner can determine whether the cryptographic checksum at the end of the message is valid or whether the message has been modified without authorisation.

When using PGP it is advisable to use a combination of the two functionalities described above. The standard procedure should be for messages and files to be encrypted with the recipient's public key first and then to be signed with the sender's private key, in order to obtain the greatest possible protection.

Versions

PGP is available for a wide variety of computer platforms (Unix systems, DOS, Windows NT/9x etc.). The most commonly used versions are 2.6.3i, 5.x and 6.x. Versions 5.x and 6.x are equipped with a graphical user interface, but they are not downward-compatible with the preceding versions. Especially when these versions of PGP are used in conjunction with operating systems from the Windows family it should be borne in mind that it may be possible to circumvent the security mechanisms of PGP by exploiting security deficiencies in the operating system.

In view of the lack of downward compatibility, it is advisable to make inquiries as to which version of PGP will be used by the communication partners before exchanging encrypted messages. Version 2.6.3i is still in

widespread use. This version is command-line oriented, but it can also be integrated into graphical user interfaces and mail clients with add-on programs. PGP can be obtained from various sources; among others, there are public domain versions available from numerous WWW, FTP or mail servers.

The controversial Corporate Message Recovery (CMR) function was introduced with Version 5. CMR offers the option of making it possible for a third person to decrypt files or messages that have been encrypted by one person for a second. The use of a "third key" of this type can be made mandatory by the administrator in the configuration.

On account of the legal restrictions on the export of cryptographic products in force in the USA, it should be ensured with all versions of PGP that they are obtained from European suppliers or servers.

Secure installation and operation

Although PGP makes use of cryptographic procedures that are recognised as being secure, incorrect configuration or operator errors may result in lowering of the level of security. As with most relatively complex crypto products, the installation and configuration of PGP, including key generation, is not entirely easy. To prevent the possibility of operating errors creeping in, familiarisation with the product and with certain basic cryptographic terms is essential.

In every organisation, therefore, one member of staff should familiarise him- or herself with handling PGP and be available to the others as a PGP contact person. This person should then instruct the other users in the secure operation of PGP. In particular, users should have intensive practice in encryption, signatures and key management before they use PGP. It is also recommended that a uniform version of PGP should be used within a particular organisation in order to avoid any of the compatibility problems described above. There is extensive documentation accompanying PGP; this should be read before PGP is put to use. Experience shows, though, that not all users have the patience to read the documentation, so it is advisable to draw up written instructions that are adapted to the specifics of the organisation concerned.

If users have any questions about PGP which go beyond the scope of the supplied documentation, there are various means of obtaining answers:

- Firstly there is a collection of the most commonly posed questions about PGP and answers to these questions (Frequently Asked Questions - FAQ) on the Internet, as well as guides and explanations on the subject of PGP.
- It is possible to obtain answers to PGP problems very quickly via newsgroups such as *alt.security.pgp, de.comp.security* or *sci.crypt*.
- There are several books on PGP.

Key generation:

With PGP, all users generate their own "key pair" themselves. The following points should be borne in mind in this connection:

- When generating RSA keys it is possible to select between various key lengths. It should be remembered that resistance to deciphering increases with key length, but also that performance drops. The chosen key length should therefore be 768 bits or, preferably, 1024 bits.

- Pass phrase

  A pass phrase (also referred to as a "mantra") must be entered when generating a key; this protects the file with the private keys from unauthorised access. As with every password, this should also not be easy to guess.

  There are Trojan horses in circulation, for example, which selectively target the file with the private keys (SECRING.PGP) and send it to an external address by e-mail. If the chosen pass phrase is too simple, it will not offer sufficient resistance to brute force attacks (automated password guessing). The pass phrase should therefore consist of at least ten characters and include special characters.

- User ID

  The public PGP keys are associated with a user ID, which if possible should be unique and also contain the e-mail address, e.g. *userA@bsi.de*.

- To generate keys, PGP requires starting values that are as random as possible. The user is therefore asked to type in an arbitrary text. It is better in this case to enter "real" text; for example, it would be possible to type in this paragraph. Simply "typing away" on the keyboard usually produces worse results.

Safekeeping of keys

The private keys are stored in the file named SECRING.PGP. Although access to this file is protected by the pass phrase, it should not be stored on local networks, not even on insufficiently secure standalone systems. Key rings (collections of keys) should be stored on floppy disk, which the user must keep in a safe place. Preference is to be given to using chip cards for storing keys.

A backup copy of the SECRING.PGP file should also be created, and a note made of the pass phrase. The backup copy and the pass phrase should be stored securely, and best of all separately, to ensure that the private key will not be lost as a result of a hard disk crash or because of an operator error. Messages which have been encrypted with the public key can no longer be decrypted if this happens.

Writing down the pass phrase and placing it in safekeeping in a secure location should be seen as a critical process serving solely the purpose of contingency planning. A locked drawer in a desk or a similar "secure" location can **under no circumstances** be recommended as a storage location for the secret key or for the pass phrase.

Distribution of keys

For a recipient to be able to check the digital signature of the sender of a file or for the sender of a message to be able encrypt a message for a certain recipient, it is necessary to have the public key of the communication partner in each case. This can be obtained in various ways: for example as an attachment to an e-mail or from a WWW server. However, the user must satisfy himself that the key really belongs to the specified person. Certificates

are used to ensure the cryptographically secure assignment of a person to a public key. The certificates are allocated by a trustworthy third party.

With PGP, every user can authenticate the public keys of other people with certificates. However, a user should only certify a public key if he or she knows or has checked the identity of the owner of the key and the public key was handed over personally.

Alternatively, the authenticity of a public key can also be verified with the aid of what is known as the "fingerprint". This involves calculating a number sequence (hash value) from the public key and appending the value to the key. After a public key has been sent, the recipient can contact the sender to compare the number sequence, for example by telephone, in order to certify the public key after confirmation of the fingerprint.

Certification hierarchy - web of trust - Internet key server

Essentially, PGP can be used both in a certification hierarchy and in a "web of trust". In a web of trust, the certificates of other users are relied upon to be trustworthy, whereas in a certification hierarchy trustworthy third parties, known as certifying agencies, authenticate the keys of all of their users in a reliable and demonstrable way.

Within a company or an agency, a certification hierarchy should be established in the intranet. The PGP expert should certify all keys for his or her area of the organisation or for the organisation as a whole. The certified public keys should be accessible to all members of staff on a server in the intranet. Access to this area should be exclusively read-only, however. The web of trust method should only be used for the field of private communications.

In the Internet, public PGP keys can be made available on key servers. These must in no way be confused with certifying agencies, however. Key servers receive keys from anywhere, and distribute them on request. It should be made clear that keys which are obtained from a key server are not checked by the key server in any way.

In order to verify the authenticity of a public key that has been made available on a key server, the fingerprint technique mentioned above should be used.

The public key's own signature

Of the parts of a PGP public key, only the user ID is overwritten by the public key's own signature. The use of the public key's own signature makes it possible to detect a denial-of-service attack (see T 5.28 *Denial of services*), but it does not prevent such an attack. As the user ID of a public key is not encrypted, it can be corrupted. The consequence of this would be that, if a "corrupted" key is used, the encrypted e-mails would no longer reach the owner of the key because they would be redirected to a different e-mail address. The confidentiality of the encrypted message is not put at risk because of this, as the message can only be decrypted with the aid of the private key.

Key recovery

If the keys used for encryption are lost, this generally also means that the data protected by the keys is also lost. In the commercial versions, 5.0 or higher, PGP includes functions for retrieving data in such instances. These functions are also referred to as key recovery functions. The functionality they offer can prevent the loss of data by recovering stored, encrypted data in the event of a key or access password being lost.

If it is intended to use the recovery function, either one or two additional keys (ADKs, additional decryption keys) have to be generated. During key generation, these additional keys are attached to the newly created keys, and all data that is encrypted with the new keys additionally incorporates encryption of the session key with the ADKs. In this way it is possible in an emergency to decrypt the data using the ADKs, without using the original key. PGP is therefore able to offer a message recovery function without the need for central storage of retrieval information.

Use of key recovery can be enforced by making presettings to that effect on the clients, ensuring that this functionality cannot be circumvented by individual users. In that case, however, the security of the whole encryption system is dependent on the confidentiality of the ADKs. If the ADKs are revealed, they can be used to decrypt all of the data.

In order to prevent misuse of this highly sensitive function it is essential that the ADKs should be protected by a particularly carefully chosen, safely kept password. In addition, as of PGP Version 6.0, keys can also be divided into several parts, which means that several people have to take action jointly in order to use them. This form of the two-person control rule should always be used when ADKs are used. To give further protection, provision can be made for users to be warned every time that they encrypt data with a key to which ADKs are attached.

Before PGP is used with key recovery, the advantages and disadvantages should be weighed up against each other. On the one hand it protects against the loss of data as a result of losing a key, but on the other it creates a central weak point in the encryption system. This function should therefore only be used if PGP is used for encrypting stored data. If it is used solely for securing communications, in the event of the loss of a key is it also possible simply to request that the e-mail be sent again. It should also be examined whether as an alternative it would not be preferable to keep the password in a safe place in a sealed envelope and to create backup copies of the private key files.

Additional controls:

- Are users trained in the use of PGP?
- Are the data and keys stored separately?
- Are backup copies made of the private keys? Are these kept at a secure location?

S 5.64 Secure Shell

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators, users

Without special extensions, the *telnet* and *ftp* protocols offer only rudimentary mechanisms for authentication. As a rule, a simple request is issued for the user ID and password, which then – in exactly the same way as the user data – are sent as plain text. The confidentiality of the authentication data and user data can therefore not be ensured. The related protocols *rsh*, *rlogin* and *rcp*, which are often grouped under the term r-services, exhibit similar security deficiencies.

Secure Shell (*ssh*) can be used as a substitute for the r-services. It makes use of extensive functions designed to ensure secure authentication and to maintain confidentiality and integrity. This is achieved with a hybrid encryption technique, in other words a combination of asymmetric and symmetric encryption. The Secure Shell resides on layer 7 (application layer) of the ISO/OSI reference model; other protocols can also be transported via *ssh*, however, such as the *X11* protocol, which is used by the graphical user interface X-Windows.

Currently Secure Shell is based on three protocols, one built upon the other. An Internet draft has been drawn up for each one.

- The lowest protocol is the *transport layer protocol*. This protocol performs the majority of the security functions of *ssh*, namely authentication at the host level, encryption, and protection of data integrity. The cryptographic algorithms are negotiable between the communication partners.
- The middle protocol is the *user authentication protocol*. This allows authentication at the user level; in this case, too, the procedure can be negotiated. If a method of simple transmission of user IDs and passwords is used for the purpose of authentication, the confidentiality of the information with respect to the communication route is ensured by the underlying *transport layer protocol*. The recommended approach, however, is to use a public key procedure for authentication.
- The *connection protocol* is built on the two preceding protocols and allows several logical user information channels to be set up. The data on these user information channels is transmitted via a common single Secure Shell connection.

There are implementations of *ssh* clients and *ssh* servers for all commonly used Unix operating systems. There are also *ssh* clients for 32-bit Windows, OS/2 and Macintosh, among others, and as a Java applet.

Basically the use of Secure Shell is to be recommended if the functionalities of the r-services are used via communication channels which are not adequately protected against compromise and/or manipulation (for example via the Internet). A few notes on the secure use of *ssh* are given below.

One risk that is particularly significant is that of attacks known as *man-in-the-middle* attacks. These involve the attacker filtering all traffic between the

communication partners and forwarding forged public keys. If the communication partners are unable to check the public keys, the attacker can read and manipulate all of the traffic by decrypting the data himself, then reading it and modifying it before finally encrypting it with another key and forwarding it to its destination. This can be prevented with the aid of a suitable key/certificate management structure. When Secure Shell is in practical operation, however, a compromise solution is often used, which allows the use of *ssh* without any additional infrastructure. When a connection is set up to a host whose public key is not yet known, the public key is sent via the non-secure network and stored in a local database. For all subsequent connections with that host, the public key can then be checked using the local database. It must be clarified within the framework of the security concept whether this approach, which offers a lower level of security against man-in-the-middle attacks, is adequate for the application concerned.

The Internet drafts contain definitions of cryptographic procedures which have to be made available by the Secure Shell implementations. There is also the option, however, of implementing additional cryptographic algorithms. The procedures that are actually used are negotiated during the establishment of a connection. Suitable client and server programs must be chosen and an appropriate configuration put in place in order to ensure that the *ssh* client and *ssh* server agree on eligible cryptographic algorithms which satisfy the security requirements.

Whenever *ssh* is used, if possible all other protocols whose functionality is covered by Secure Shell, i.e. for example the r-services and *telnet*, should be entirely deactivated so that the safeguards cannot be circumvented. This assumes, however, that all communication partners have suitable implementations at their disposal.

There are known to have been program errors relevant to security in older implementations of *ssh*. A version should therefore be used in which any such deficiencies have been eliminated. Compatibility between implementations with widely differing program versions may be a problem in some circumstances. Mixed operation should therefore be avoided if possible.

It should be noted that when *ssh* is used across firewalls, it is no longer possible to have content-sensitive control of the data flow.

Additional controls:

- Are r-services or similar protocols used via non-secure communication channels?
- How is the verification of public host keys regulated when using Secure Shell (organisational measures, for example)?
- Have all of the known security deficiencies been corrected in the version of Secure Shell that is used?

S 5.65 Use of S-HTTP

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators, users

Secure HTTP (S-HTTP) provides for the securing of messages that are exchanged between an HTTP client and an HTTP server. S-HTTP makes the following mechanisms available as an extension of HTTP:

- Authentication of instances
- Negotiation of security services
- Protection of the confidentiality and integrity of HTML documents by means of cryptographic checksums and encryption.

S-HTTP protects submitted HTTP data at the sender's end by encrypting it or by attaching a cryptographically generated checksum, and transfers the protected data to the transport system. The protected data is then sent to the recipient. At the recipient's end, the encapsulated data is transferred from the transport system to the local S-HTTP. This decrypts the protected HTTP data and forwards it to the HTTP application.

The security services are based on the RSA, DES, RC2, MD2 and MD5 algorithms (in this connection see also S 3.23 *Introduction to basic cryptographic terms*). With S-HTTP, the security policy and the cryptographic algorithms that are to be used can be selected by means of an optional negotiation phase before every transmission.

In addition, various cryptographic security mechanisms can also be integrated into S-HTTP, for example PKCS-7 (cryptographic message syntax) and PEM. Interoperability between S-HTTP clients and servers which do not use S-HTTP is guaranteed by the optional negotiation phase.

The essential differences with respect to SSL (see S 5.66) are as follows:

- S-HTTP must be integrated into WWW clients and servers at the application level.
- S-HTTP offers its security services on the basis of the content of the HTML documents, whereas SSL protects the HTTP communication channel.

S-HTTP is used for protecting WWW applications. Nevertheless, malicious applets or MIME-encoded executable programs may get through to internal systems despite this protection or precisely because of it.

S 5.66 Use of SSL

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, users

The security protocol most commonly used on the WWW is SSL (Secure Socket Layer). SSL was developed by Netscape, and is supported by all the latest browsers. With SSL, connections can be protected

- by encryption of the connection content,
- by checking the completeness and integrity of the transmitted data,
- by checking the identity of the server,
- optionally, by checking the identity of the client.

With SSL, a connection is established between a user's browser and a provider's server, and first of all the certificates with the public keys are exchanged over this connection. Next a symmetric key is exchanged by secure means, protected by the RSA asymmetric encryption procedure. A symmetric procedure is then used to encrypt the actual data transmission, because this can encrypt large quantities of data more quickly. A different symmetric key is negotiated as the *session key* for each transaction. This is then used to encrypt the connection.

https

A user can tell if a given Web page allows SSL-protected data transmission, for example, from the fact that the initial part of the address contains an extra "s" (https://www...), in Netscape Navigator from the fact that the padlock at the bottom left of the screen is closed instead of open, or in Internet Explorer from the appearance of a closed padlock on the bottom right.

The use of SSL is not restricted to HTTP clients and servers. Applications such as Telnet or FTP can also use SSL for secure communications. This does require, however, that the clients and servers concerned have each been adapted to do this.

SSL consists of two layers. The SSL handshake protocol operates on the upper layer. This is used by the client and the server to identify and authenticate themselves to each other, and to negotiate a key and an encryption algorithm to be used for the subsequent data communication traffic. The lower layer, the SSL record protocol, which forms the interface to the TCP layer, encrypts and decrypts the actual data traffic. Because SSL resides on the socket interface for access to TCP and replaces this interface with an enhanced-security version, it can also be used for other services. As a result, SSL also runs transparently in the background of any Internet service. The only action required of users is selection of a certificate. This means that, in contrast to S-HTTP, they do not have the opportunity to configure the security functions and adapt them to their specific security requirements. On the other hand, users may find SSL more convenient as they do not have to stop to configure security functions every time there is a Web query.

Use Version 3 or higher

Only Version 3 or higher of SSL should be used, because the additional server authentication these versions provide means that man-in-the-middle attacks are no longer possible, as was the case with SSLv2.

Key length

Various cryptographic algorithms with different key lengths can be used with SSL, for example RC2 or RC4 with a 40-bit or 128-bit key length, DES with a 56-bit key length, triple-DES with a 112-bit key length, or IDEA with a 128-bit key length, as well as hash functions such as MD5 or SHA-1 (see also S 3.23 *Introduction to Basic Cryptographic Terms* in this connection). The client and server must agree on the procedures to be used in the session at the time when the connection is established.

Minimum key length 80 bits

Some browsers from US vendors the integrated encryption procedures have only extremely short key lengths (40-bit), on account of the US export restrictions. These cannot withstand a brute-force attack for long, i.e. an attack involving simply trying out all possible keys. If the protection requirements for the transmitted data are low, this short key length may be adequate, and it at least protects against opportunist offenders. Otherwise, browser versions which offer encryption procedures based on at least an 80-bit key length should be used. International versions of the commonly used browsers which support 128-bit key lengths are now available.

Alternatively, add-on products developed by German companies which likewise permit the use of longer keys inside standard browsers should be used. Public domain software such as SSLeay or OpenSSL can also be used for this purpose.

Certificates

One difficult problem with data communication across open networks is how to check the identity of communication partners, because one cannot rely on the stated name actually being correct. With SSL, the identity of communication partners is checked by means of certificates. Certificates contain their public keys together with confirmation provided from another authority of the correct assignment of the public key to its "owner", in this case therefore a server or client. The value of a certificate is therefore dependent not least on the trustworthiness of this verification entity (also known as a trust centre or certification body). The genuineness of the certificate can, in turn, be checked using the public key of the verification entity.

Three different types of certificates may be distinguished with SSL:

- user certificates, which are required for client authentication,
- certificates from certification bodies, although some certification bodies have several certificates, depending on their underlying security policy, and
- Certificates from software producers or from operators of Web pages

All browsers come supplied with SSL certificates from certain certification bodies when they are installed. These certification bodies have very different security guidelines and conditions under which they grant certificates. Initially, therefore, all certificates should be deactivated, and only reactivated when you are convinced that their security policy satisfies your own security needs.

When a new certificate is adopted, care should be taken to ensure that it is not activated until its fingerprint has been checked. The fingerprint is a hexadecimal number that is transmitted together with the certificate. It should also be transmitted via a different route and compared, to ensure that the certificate is correct.

Operators of WWW servers who intend exchanging security-relevant data with visitors to their websites should offer a channel protected by cryptographic techniques, e.g. SSL, for this purpose.

Note: If the users are protected against active content and computer viruses by a firewall, they must implement their own protective measures against these risks if they are using SSL, as described for example in S 4.33 *Use of a Virus Scanning Program on Exchange of Data Media and During Data Transfer* and S 5.69 *Protection Against Active Content*.

Additional controls:

- Is the use of SSL compatible with the existing security guidelines for the firewall or on the use of WWW services?
- Do the users know what needs to be taken into account when using SSL?

S 5.66 Use of SSL

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators, users

The most commonly used security protocol in relation to use of the WWW is SSL (Secure Socket Layer). SSL was developed by Netscape, and is supported by all relatively up-to-date browsers. Connections can be secured with SSL in various ways:

- By encryption of the connection content
- By checking the completeness and correctness of the transferred data
- By checking the identity of the servers
- Optionally by checking the identity of the client end

With SSL, a connection is set up between a user's browser and a provider's server, via which first of all the certificates with the public keys are exchanged. Next a symmetric key is exchanged by secure means, protected by the asymmetric encryption procedure RSA. A symmetric procedure is then used for the encryption of the actual data transmission, because these can encrypt large quantities of data faster. A different symmetric key is negotiated as the session key for each transaction; this is used to encrypt the connection. A hash procedure can also be used during data transmission for the purpose of data compression.

The ways that a user can recognise Web pages which allow SSL-secured data transmission include for example the fact that an "s" is added to the address (https://www...), that the key at the lower edge of the screen in Netscape Navigator, usually shown broken, is now joined together, or that in Internet Explorer the padlock is shown closed instead of open.

The use of SSL is not restricted to HTTP clients and servers. Applications such as Telnet or FTP can also use SSL for secure communications. This does require, however, that the clients and servers concerned have each been adapted to do this.

SSL consists of two layers. The SSL handshake protocol operates on the upper layer. This is used by the client and the server to identify and authenticate themselves to each other, and to negotiate a key and an encryption algorithm to be used for the subsequent data communication traffic. The lower layer, the SSL record protocol, which forms the interface to the TCP layer, encrypts and decrypts the actual data traffic. Because SSL sits on the socket interface for access to TCP and replaces this interface with an enhanced-security version, it can also be used for other services. As a result, SSL also runs transparently in the background of any Internet service. Users only need to have active involvement when selecting a certificate. In contrast with S-HTTP, therefore, they do not have the opportunity to configure the security functions and adapt them to their specific security requirements. On the other hand, SSL may appear to be more convenient to users who do not want to be held up by the configuration of security functions every time there is a Web query.

Only version 3 or higher of SSL should be used, because the additional server authentication these versions provide means that man-in-the-middle attacks are no longer possible, as was the case with SSLv2.

Key length

Various cryptographic algorithms with various key lengths can be used with SSL, for example RC2 or RC4 with a 40-bit or 128-bit key length, DES with a 56-bit key length, triple DES with a 112-bit key length, or IDEA with a 128-bit key length, and MD5 or SHA-1 for example as hash functions (see also S 3.23 *Introduction to basic cryptographic terms* in this connection). The client and server must agree on the procedures to be used in the session at the time when the connection is set up.

In browsers from US vendors the integrated encryption procedures have only extremely short key lengths (40-bit), on account of the US export restrictions. These do not stand up to brute-force attacks for long, i.e. attacks involving simply trying out all possible keys. If the protection requirements for the transmitted data are low, this short key length may be adequate, and it at least protects against opportunist offenders. Otherwise, to overcome this shortcoming use should be made of add-on products from local vendors, which also allow the use of longer keys even within standard browsers. Public domain software such as SSLeay or OpenSSL can also be used for this purpose.

Certificates

One difficult problem with data communications across open networks is how to check the identity of the communication partners, because it cannot be relied upon that specified names will be correct. With SSL, the identity of the communication partners is checked by means of certificates. Certificates contain their public keys together with verification from another entity of the correct assignment of the public key to its "owner", in this case therefore a server or client. The value of a certificate is therefore dependent not least on the trustworthiness of this verification entity (also known as a trust centre or certification body). The genuineness of the certificate can, in turn, be checked using the public key of the verification entity.

A distinction is drawn between three different types of certificates with SSL:

- User certificates, which are required for client authentication
- Certificates from certification bodies, although some certification bodies have several certificates, depending on their underlying security policy
- Certificates from software producers or from operators of Web pages

All browsers already contain SSL certificates from certain certification bodies when they are installed. These certification bodies have very different security guidelines and conditions under which they grant certificates. Initially, therefore, all certificates should be deactivated, and only reactivated when you are convinced that their security policy satisfies your own security needs.

When a new certificate is adopted, care should be taken that it is not activated until after its fingerprint has been checked. The fingerprint is a hexadecimal number that is transmitted together with the certificate. It should also be

transmitted via a different route and compared, to ensure that the certificate is correct.

Operators of WWW servers who intend exchanging security-related data with visitors to their WWW pages should offer a route protected by cryptographic techniques for this purpose, i.e. SSL, for example.

Note: If the users are protected against active content and computer viruses by a firewall, they must implement their own protective measures against these risks if they are using SSL, as described for example in S 4.33 *Use of a virus scanning program on exchange of data media and during data transfer* and S 5.69 *Protection against active content*.

Additional controls:

- Is the use of SSL compatible with the existing security guidelines for the firewall or on the use of WWW services?
- Do the users know what needs to be taken into account when using SSL?

S 5.67 Use of a time stamp service

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators, users

It is relatively easy to manipulate the time information entered in the header of an e-mail. If it is necessary to know the precise time when an e-mail has been sent or received, a time stamp service must be used. A time stamp is a time entry which is made by a neutral body, and which cannot be corrupted. It is applied either fully automatically by a time stamp server, i.e. transparently for the user, or on request by the sender.

A time stamp consists of a time stamp certificate in which the current date and the current time are documented together with the identity of the time stamp service itself, and of a digital signature via e-mail and certificate. In this way the time stamp provides evidence and confirmation of the existence of a certain message with certain contents at a certain time. The assurance of the authenticity of an e-mail by a time stamp presupposes that the sender has digitally signed the e-mail.

A time stamp service can be provided and used both in an internal network and on the Internet. It receives signed files, or even only the signatures from those files, as a server on the Internet or in the intranet, and provides them with a synchronised time stamp. In turn, all of this together is signed by the time stamp service, and either forwarded to the recipient or alternatively also sent back to the sender.

S 5.68 Use of encryption procedures for network communications

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Communication networks transport data between IT systems. The data is rarely transmitted via a dedicated communications line between the parties communicating with each other. Instead, the data is routed via a number of intermediate stations. Depending on the communication medium and the technology used, the data can be intercepted by the intermediate stations without authority, or also by third parties residing in the respective switching network (for example when using the Ethernet protocol without point-to-point networking). As the data being transmitted should not be tapped or modified by unauthorised third parties, nor used by them for subsequent reloading into the network (replay attacks), a suitable mechanism must be used to prevent this happening. Encryption of the data with – if necessary – mutual authentication of the communication partners can reduce this risk (depending on the strength of the chosen encryption procedure and the security of the keys used; see also Section 3.7 Crypto concept).

As a rule, applications communicate with each other in order to exchange application-related information. Encryption of the data can then be carried out at several levels:

- At the application level: the communicating applications each have to have the relevant encryption and decryption mechanisms available to them.
- At the operating system level: encryption is performed by the local operating system. All communication via the network is encrypted either automatically or on request.
- At the network switching element level: encryption takes place between the network switching elements (e.g. routers).

The individual mechanisms each have specific advantages and disadvantages. Encryption at the application level has the advantage that encryption is fully subject to the control of the respective application. One disadvantage is that the only partner applications that can be considered for encrypted communication are those that are equipped with the same encryption mechanism. It is also possible to use authentication mechanisms between the two partner applications.

In contrast with this, in the case of encryption at the operating system level encryption takes place transparently for every application. Each application can carry out encrypted communication with every other application, provided the operating system on which the partner application is running has the appropriate encryption mechanism. A drawback in this instance is that, with regard to authentication, only the computers can be authenticated to each other, not the respective partner applications.

Using encrypting network switching elements has the advantage that there do not have to be any encryption mechanisms on the application or computer side; in this case, too, encryption is transparent for the communication

partners. Communication on the link as far as the first encrypting network switching element, however, takes place without encryption, and therefore holds a residual risk. Authentication is only possible between the switching elements. The communication partners themselves are not authenticated with this method.

If sensitive data is transmitted via a network (even within an intranet), it is advisable to use encryption mechanisms. If the chosen applications do not have their own encryption mechanisms or if the available procedure is considered to be too weak, use should be made of the possibility of encryption on the operating system side. Procedures such as SSL suggest themselves here, which were designed for transparent encryption at the operating system level. Depending on the security policy it is also possible to use encrypting network switching elements, for example in order to implement a virtual private network (VPN) with a communication partner via the Internet (appropriate software mechanisms are generally also available in firewall systems (see Section 7.3 Firewall)).

Considerable planning within the framework of the security policy of a company or agency is necessary when using encrypted communication and mutual authentication. In the context of the communication encryption methods discussed here, particular attention should be paid to the following points:

- Which procedures are to be used or are offered for encryption (in routers, for example)?
- Do the encryption mechanisms that are employed support or use existing or planned standards (IPSec, IPv4, IPv6, IKE)?
- Have sufficiently strong procedures and correspondingly long keys been chosen, in accordance with the security policy?
- Are the keys held in secure storage?
- Are the keys generated in a secure environment, and do they have a secure route to the place where they are needed (computer, software component)?
- Are key recovery mechanisms required?

If certificates are used for the authentication of communication partners, similar questions have to be considered.

S 5.69 Protection against active content

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Administrators

Until recently, firewalls were considered to provide absolute protection against attacks on one's own network from the Internet. They ensured that no connection could be set up into the internal network from the Internet, and that internal users could access information on the Internet without difficulty. On account of the ever more widespread distribution of active content on WWW pages, however, this situation has changed. Information from the Internet is no longer simply viewed, but instead in some cases external program code is also executed during viewing. At present this means Java, ActiveX and JavaScript; others could be added to this list in future. There are also elements known as plug-ins which enable other programs to be started from the browser; in some cases this is even done automatically from an HTML page. Depending on the type of program involved, executing it may be associated with a certain security risk.

From today's standpoint there are several conceivable approaches to protecting an internal network against misuse by active content from the Internet. These are explained in the following using the examples of Java, ActiveX and JavaScript.

Prohibition of active content on the firewall

Even today it is still possible to have very good access to the Internet without really needing active content. This is the safest and therefore recommended method of accessing the Internet, because in that way the firewall can continue to exercise principal control. In order to prevent the acceptance of active content, it is necessary to have a proxy on the application gateway, which examines HTML pages for active content. If the proxy finds any such content, it must be filtered out of the page. There are a number of application gateways that offer this functionality (see S 2.75 *Selection of a suitable application gateway*).

It must be assumed, however, that this solution, although it is the safest, will be less and less acceptable in the future, because the number of pages where the active content contains the actual information is on the increase. If the active content is filtered out, the internal user will no longer be able to access the information.

Note: Active content may also be hidden in e-mails; these should therefore also be examined for such content. As encrypted communications cannot be checked for active content, SSL-based WWW access must not be allowed if there is central filtering.

Prohibition of active content in the WWW browser

In a network with centrally administered workstations, it is conceivable to restrict the rights of the individual users to the extent that they are no longer able to change the security settings of their WWW browsers. These can then be configured in such a way that active content will not be executed. It is thus also possible to dispense with the filtering of active content on the application

gateway, because in these circumstances active content can no longer cause any harm in the internal network.

Another solution is to allow only certain WWW browsers to be used for access to the Internet. Netscape Communicator and Internet Explorer are not the only browsers available; there are also other browsers that have no means of executing active content.

One option is to ensure that browsers of this type will be used by setting up the administration of the workstations to this effect. In this case, however, the operating systems of the workstation must provide reliable separation of roles between users and administrators, such that configurations set by the administrator cannot be revoked by a user. Additional security precautions are therefore necessary with operating systems such as Windows 3.1 and Windows 95.

Alternatively, the proxy on the firewall could be set up in such a way that only predefined browser software is allowed access to the Internet. It must be borne in mind in this case, however, that the security of this method is dependent on the ID of the WWW browser used. A skilled user with a hex editor should have no difficulty modifying a WWW browser of his choice in such a way that it has the desired ID.

Raising the awareness of users

It is also conceivable to place the responsibility entirely in the hands of the users. Active content should normally be deactivated in the WWW browser, but the users have permission to run active content in certain circumstances. This could be the case for example if they were no longer able to access the WWW information provided by a well-known manufacturer without running the active content.

ActiveX, in particular, has various security settings, which enable the execution of ActiveX to be restricted to certain WWW servers so that users are not forced to change their settings repeatedly.

There must be some doubt, however, whether users will really always change the security settings of their WWW browsers when they switch to another WWW page, for example where a link from the "well-known manufacturer" may have taken them. Besides, an individual Web page on a "secure" computer can also load other Web pages which are located on "non-secure" computers. As well as that, attacks can be made on the Internet which have the effect that users do not receive the WWW page that they requested (see T 5.48 *IP spoofing* and T 5.78 *DNS spoofing*, for example).

Filtering specific active content

Recently programs have been developed which work in a similar way to computer virus scanning programs by examining active content to determine whether it contains code that is a threat to security. This is a highly acceptable solution for users, because they can then access all harmless active content.

The question has to be asked, though, whether such programs really provide protection. A virus scanning program cannot provide protection against Trojan horses, for example, and these can of course cause considerable damage.

Running active content in a protected environment

Java and JavaScript are implemented in WWW browsers in such a way that they are executed in what is known as a sandbox. If the sandbox is correctly implemented, the active content cannot access data outside the sandbox. Although attacks on availability (denial-of-service (DOS) attacks) are still possible, the confidentiality and integrity or other data is not endangered. The sandbox technique cannot be further extended.

Two approaches suggest themselves here:

1. On an operating system with role separation, the WWW browser can run with minimal rights under the user's ID. Active content can therefore not cause any damage, provided the checking of rights operates correctly.

   On a Unix computer it is possible, for example, to launch a WWW browser in a *change-root* environment, in which the WWW browser only has access to a restricted file system. If active content does cause damage, it can only do so within this restricted environment. To enable a user to work from his workstation, the WWW browser must be displayed on it; this would be possible with X-Windows, for example. A similar setup is possible with Windows NT.

2. Recently proxies have been developed (see *www.digitivity.com* for example) which take over the running of Java applets instead of the workstation; this means that the Java applet is run on the proxy but displayed on the workstation. Compared with the first method, this approach makes much more careful use of the available network bandwidth.

Recommendation:

1. Active content in the form of ActiveX should only be executed (if at all) when it comes from a trustworthy source, i.e. when it has been signed, the signature has been verified and the signer is also trustworthy.
2. Java and JavaScript should only be allowed (if at all) when they come from a trustworthy source, or alternatively when the above safeguards have been verifiably implemented.
3. It is recommended not only to have active content encapsulated by the WWW browsers but also to ensure that it is additionally restricted by a suitable operating system.

S 5.70 Network address translation (NAT)

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

When existing networks are connected to the Internet, it is often not possible to use the current IP addresses because they have already been assigned to other computers in the Internet. So as not to have to reconfigure all of the computers, it may make sense to carry out an address translation from the internal addresses to the officially registered external addresses. The assignment of IP addresses in the local network also allows conclusions to be drawn about the network's structure. Knowledge of this could be exploited by a potential attacker. It is often also the case that more IP addresses are required in the local network than are officially registered.

Translation of the internal addresses into one or more officially registered IP addresses and vice versa can be performed via a proxy server or some other address translation component. This makes only the official address available on the external side, and forwards the packets to the respective internal computers. As only the external addresses are used externally and only the internal addresses internally, address translation has to take place at the gateway of the local network to the Internet.

Some routers and packet filters offer the option of address translation without the use of a proxy. In this case the headers of all IP packets are changed in the router or packet filter. This can be done either statically or dynamically. Static address translation is simple and fast. Every internal address is assigned to exactly one external address. For this it is of course necessary to have one external address for each internal address.

Today it is more common to use dynamic address translation. Especially when the number of internal IP addresses is larger than that of externally visible addresses, it is a requirement. An allocation table is maintained in the router or packet filter. In this table, the internal addresses with the associated port number of a packet are set against an external address with a new port number. Frequently only one IP address is made visible to the outside; this hides all internal IP addresses by means of the allocation of port numbers. One consequence of dynamic address translation is that it is normally not possible to set up a connection to an internal computer from the Internet.

If IP addresses that have already been assigned in the Internet are used internally, the Internet computer concerned can no longer be accessed from within the local network. As a way out, it is possible to fall back on various ranges of IP addresses that are not assigned in the Internet (known as private IP addresses). Certain services have to be given special treatment in relation to address translation (e.g. traceroute or ftp).

In order to ensure that no information about the structure of the organisation's own network is made known to the outside, address translation should be performed at the Internet gateway.

Additional controls:

- Are the internal addresses and internal network structure not made known to the outside?

S 5.71 Intrusion detection and intrusion response systems

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

One of the key tasks of a firewall administrator is to analyse the accruing logging data so as to be able to detect attacks soon after the event. In view of the wealth of data and the multitude and complexity of the various possible means of attack, this results in a considerable amount of work. Intrusion detection (ID) and intrusion response (IR) systems can help in this.

The aim of an ID system must be to provide assistance to an average administrator to the extent that he or she is able to detect an attack in a large number of logging files without the need for in-depth knowledge of the field of Internet security. IR systems, on the other hand, serve the purpose of initiating countermeasures automatically as soon as an attack has been detected.

In an ideal situation these programs will have as much information at their disposal as a good administrator, and will therefore be able not only to detect an attack in any logging data but also to provide indication of the severity of the threat and what countermeasures are necessary. Currently, however, this field is still the subject of intensive research, so significant improvements to existing programs are possible at any time.

Intrusion detection systems can essentially be divided into two classes: signature analysis and anomaly detection.

Signature analysis is based on the assumption that many attacks can be detected on the basis of a certain sequence of logging data. One example is the technique known as port scanning. In advance of an attack, the intruder first establishes which services on the attacked computer are addressable, i.e. to which TCP ports it is possible to set up a connection. This involves using a program to send a connection setup packet to all TCP ports one after the other. If a connection is established, a service is installed there and can be attacked. The corresponding signature, i.e. distinctive feature, of this attack is simple: connection setup packets which are successively sent to all TCP ports.

The problems with this type of intrusion detection also become immediately apparent, however: in what order do the ports have to be addressed and at what time intervals, if an attack is to be distinguished from normal operation? The latest port scanning programs operate in such a way that they do not scan port 1, port 2 through to port n, but do this in a random order. It is also possible for the packets not to be sent directly one after the other, but at random intervals (e.g. 1 s, 100 ms, 333 ms, 5 s ...). This makes it difficult to determine the signature.

A subtle variant of port scanning involves sending individual packets from different source addresses. Used in conjunction with the time-staggered initiation of the packets described above, the probability that an attack will remain undetected is currently very high.

In the case of anomaly detection, on the other hand, the assumption is that the normal behaviour of users or computers can be statistically recorded, and deviations from this are judged to be attacks. One example of this is the period of time within which a user is normally logged in at her computer. If she almost always works from Monday to Friday within the period from 8 a.m. to 5 p.m. with deviations of no more than 2 hours, any activity on Saturday or at midnight can be classified as an attack. The problem with anomaly detection is how to determine what is normal behaviour. Some conclusions can be drawn on the basis of threshold values or probability considerations. It appears questionable, however, whether it makes sense to immediately classify an activity by user A on Monday at 7.10 p.m. as an attack. Also, a user's normal behaviour usually changes, meaning that adaptations have to be made. Who tells the ID system, though, that this change in behaviour is OK and not an attack?

It also makes sense to subdivide ID systems according to the type of data acquisition involved. This can be done either with the aid of a dedicated sniffer somewhere in the network (network-based ID system), or it can be part of the normal logging functionality on one of the connected computers (host-based ID systems). There are advantages and disadvantages to both. It has to be said that it is easier for network-based systems to detect a wide-ranging attack that affects various computers at the same time. It is considerably more difficult, however, to detect complex attacks (e.g. via other intermediate stations) on one computer. Over and above this, network-based systems cannot analyse encrypted data. As for the host-based ID systems, extensive changes may have to be made to the logging functions for the computers before they can be used.

Because data privacy stipulations or staff agreements also have to be observed even when logging information is evaluated automatically, it may be necessary in some circumstances to store the data under a pseudonym.

The following aspects should be taken into account before coupling an ID system, IR system and firewall:

- Is it possible to deliberately initiate an attack on the firewall which is erroneously interpreted by the ID system as a genuine attack? If the IR system subsequently triggers the disabling of certain services across the firewall, this can have considerable consequences for availability.
- The interaction between the ID system, the IR system and the firewall should be sufficiently transparently documented. Otherwise it is not possible to assess at any one time who the firewall is administered by: by the IR system or by administration staff. If there is any doubt, decisions by the administration staff should take priority.

In order to rule out attacks against an ID system itself, it should be invisible from the network, as far as this is possible. The simplest provision is to assign an IP address that is not routed in the Internet. It is also recommended to deactivate the ARP protocol for the corresponding interface so that there will be no response to either ARP or IP packets.

S 5.72 Deactivation of unnecessary network services

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator

To disable any network services on a Unix system which are not actually required, the procedure described below should be adopted.

Under Unix there are two ways of starting network services, via the server service *inetd*, which is configured in file */etc/inetd.conf*, and via the start-up files, which are held in */etc/rc.d/init.d* or */etc/init.d*. To disable services which are not required in the */etc/inetd.conf* file, the relevant line should be commented out using a #. With a standard installation, generally more services are configured than are actually necessary. Among these, services will often be included which could constitute a risk. Therefore as few services as possible should be enabled, i.e. only those services which are really necessary on the system concerned (see also S 4.95 *Minimal operating system* and S 4.97 *One service per server*).

The services which are initiated by the start-up files are referenced via links from the subdirectories */etc/rc**X**.d* and */etc/rc.d/rc**X**.d*, where ***X*** stands for the Unix run level in which the start-up file is called. To deactivate the services which are not required, these can be moved to a subdirectory from where they can be reactivated if subsequently needed. This could be achieved, for example, as follows:

cd rc3.d; mkdir .s; mv S85sendmail .s/

The command *netstat –a* can be used to see which services are currently active.

Additional controls:

- Have the changes to the start-up files been documented?
- Who is allowed to add services on a Unix system?
- Is a check performed with *netstat –a* after every update of application programs and operating system components as to which services are available on the network connection?

S 5.73 Secure operation of a fax server

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, fax mail centre

Secure operation of a fax server requires that communication is secure both locally and also over the public switched network. The fax server accepts incoming fax transmissions from other fax servers or fax machines and if the automatic fax routing function has been activated, it then routes them to the connected users. Outgoing fax transmissions sent by the connected users are passed to the fax server and then sent on to recipients. The fax server must also ensure that local fax transmissions, i.e. fax transmissions from one workstation to another within the same organisation (or organisational unit) are sent on internally and not over the public network.

Test and documentation of configuration

If the fax server is to be operated securely, then, once purchased and installed, the configuration of its operating system and the fax server application must be tested thoroughly. If any error messages are generated, the configuration settings should be altered where this is possible. The test phase should be followed by a pilot run. Only once the fax server has been demonstrated to be running without errors in this phase also should it be cleared for actual operation. The configuration parameters should be documented meticulously, as should all changes to the configuration settings.

Deletion of fax data

Fax servers store all incoming and outgoing fax transmissions. The length of time for which these are stored depends on the facilities provided by the fax server application and the configuration. Thus, for example, it is possible that outgoing fax transmissions are only held temporarily until a given fax job has been completed and are then deleted. Again, it could be that incoming fax transmissions are only stored temporarily until they have been re-routed to recipients, following which they are deleted. However, another possibility is that all incoming and outgoing fax transmissions are held on the fax server until they are specifically deleted by the users concerned or by the fax mail centre or Administrator. On some fax servers it is also possible to have the data automatically deleted after a defined period of time. Thus, for example, all fax transmissions more than three months old are automatically deleted. Depending on the concept of use, procedures must be defined for the deletion of fax data on the fax server. At the same time, a procedure should be laid down as to where and to what extent archiving of fax data should be performed. As a general rule, fax data should not remain on the fax server any longer than is absolutely necessary.

Secure siting of the fax server

Steps must be taken to ensure that unauthorised persons cannot access fax transmissions. As a first step, the fax server must be physically protected against unauthorised access. This can only be achieved if the server is located in a secure server room or server cabinet (see Section 4.3.2 *Server room* and Section 4.4 *Protective cabinets*).

Responsibility for administration

To ensure the fault-free operation of the fax server, it is also necessary to specify who is responsible for administration of the hardware components, the operating system and the fax server application. A fax mail centre should be set up (see also S 2.180 *Setting up a fax mail centre*). The administration personnel and the staff employed in the fax mail centre must be given training on the operating system and fax server application. To avoid disruption due to improper use, the users must also be trained in operation of the fax client application.

Granting of permissions on fax servers

Often the permissions which can be granted to users and user groups on fax servers for incoming fax transmissions include:

- Read rights,
- Forwarding rights
- Delete rights.

For outgoing fax transmissions, often the following rights can be granted:

- Send rights,
- Suspend rights,
- Delete rights,
- right to modify transmission options

Permissions should be granted in accordance with the provisions contained in the fax security guidelines (see also S 2.178 *Creation of security guidelines for the use of the fax server*).

Granting of access rights

Unless it is possible to ensure by technical means that fax transmissions are forwarded immediately, access rights should be granted in such a manner that only authorised users can access the relevant "mailboxes" on the server.

As a general rule, access to temporary areas in which the fax server application stores fax transmissions temporarily prior to their being sent out or distributed to recipients should only be granted to privileged users (e.g. administrators, fax mail centre).

The connections of the fax server to the private branch exchange or to the public switched telephone network should be checked at regular intervals to ensure that they are working properly. Where the fax server is linked to internal communications systems, such as, for example, an e-mail system or a workflow management system, the functioning of these connections should similarly be checked at regular intervals.

Checking of available hard disk space

Regular checks must also be performed to ensure that sufficient hard disk space is available for storage of fax transmissions (see also S 5.75 *Protecting against overloading the fax server*). If the hard disk space becomes exhausted, no further fax transmissions can be received or sent.

Analysis of log data

The fax server activities must be logged in accordance with the provisions of the fax security guidelines and the logs must be examined at regular intervals (see also S 2.64 *Checking the log files* and S 5.25 *Using transmission and reception logs*). When specifying the extent and content of logs, the need for

prompt involvement of the staff council or works council should be borne in mind.

Reservations regarding the use of a fax server are often due to the fact that an IT system which is integrated into the LAN can be accessed over the public telecommunications network.

Through careful selection and configuration of communications cards, operating system and fax server application and secure positioning of the server in the network topology, the danger of penetration of the network or the fax server can be reduced to a minimal residual risk.

Deactivation of unnecessary facilities

Where active ISDN cards are in use, features which are not necessary for receiving and sending faxes should be disabled (see S 4.59 *Deactivation of ISDN board functions which are not required*).

Where dedicated fax cards are used, once again it is important to find out at the outset exactly what facilities are provided, and, if possible, to disable any unnecessary features which are not required.

One service per server

The fax service should be the only service provided by the fax server. In particular, a fax server should not be used also as a data, printer, e-mail or Internet server or as a remote access computer. To reduce the probability of penetration over the telecommunications network, the operating system must be configured as "lean" as possible. This means that services and protocols which are not really necessary for operations are not installed. For example, if the Telnet service is not started up on a fax server, then it is not possible for an attack to occur from this source. When deciding which services and protocols are necessary, it should be borne in mind that dangers often arise from the combination of different services and protocols.

Position of the fax server in the network

How the server is securely positioned in the network topology depends partly on whether any firewall is in use in the organisation and, if so, which type.

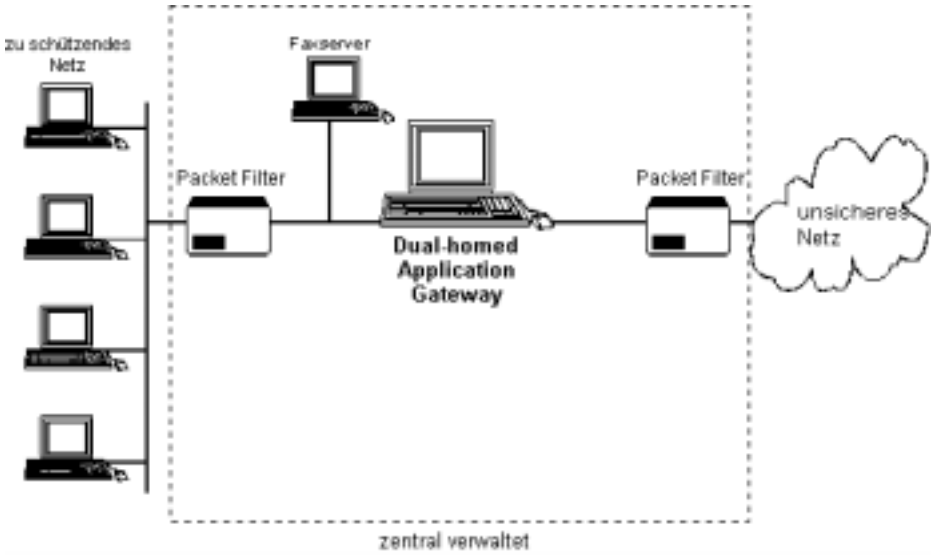
A fax server has a minimum of one interface to each of the telecommunications network and the LAN. The fax server should be placed in the network in such a way that in the event of a successful attack on the fax server it is not possible for the adversary to penetrate the entire network. On the other hand it must not be possible to attack the fax server successfully from within the network either. For example, it is conceivable that an attack could be launched by an adversary from the Internet. If such an attack succeeds, the perpetrator is then in a position to arrange for faxes to be sent out using the fax server of the attacked organisation. This not only results in telephone charges but, even more serious, could harm the company's reputation. If the attacker succeeds in getting through, he will also be able to view the fax transmissions stored either permanently or temporarily on the fax server, despite not being authorised to do so. Similarly, attacks by insiders over the LAN are also feasible.

As a fax server usually is not the only IT component which is connected to an external network, there will normally be a barrier to protect the internal network against external networks (see also Section 7.3 *Firewalls*).

Position of fax server where there is a firewall

If there is a screened subnet acting as Internet firewall (configuration 1 from S 2.73 *Selecting a suitable firewall*), the fax server should be positioned

between the inner packet filter and the Application Gateway (see Figure 1). The Application Gateway and the outer packet filter provide sufficient protection against attacks from the insecure network. The fax server is protected against attacks from the internal network by the inner packet filter.



Text zum Bild	
zu schützendes Netz	Network requiring protection
Packet Filter	Packet filter
Faxserver	Fax server
Dual-homed Application Gateway	Dual-homed Application Gateway
unsicheres Netz	Insecure network
zentral verwaltet	Centrally administered

Figure 1

Position of fax server without suitable firewall

Under all other firewall combinations, especially those in which there is only one packet filter, or when there is no firewall, the fax server should be linked straight into the secure network. If the protection requirement is such that the resulting residual risk is viewed as unacceptable, then either a separate packet filter should be provided or else the private branch exchange must be configured so that only outgoing connections are permitted. In the latter case, a conventional fax machine or a stand-alone system with an appropriate fax application must be used for incoming fax transmissions. In either case incoming fax transmissions must then be forwarded manually to recipients.

Additional controls:

- Is the configuration of the fax server documented?
- Is this documentation updated when changes are made to the configuration?
- Is fax data on the fax server deleted at regular intervals?
- Are the users aware of the rules applied to the deletion of fax data?
- Who is responsible for analysing the log data generated?

S 5.74 Maintenance of fax server address books and distribution lists

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, fax mail centre

Most fax servers provide facilities for both central and also individual address books. Central address books are available to all users of a fax server and should be maintained centrally by the fax mail centre. Individual address books can be created by any user but are generally available only to the author.

Protection against manipulation

It is especially important that central address books are protected against unauthorised changes. To achieve this, the user access rights for the fax server application should be granted in such a way that only the fax mail centre can alter the central address books, or, if this is not possible, then the resources of the operating system should be called on so as to achieve the same result.

Regular review of central address books

The fax mail centre should perform regular checks to ensure that all central address books are intact and up-to-date. Most fax servers allow several recipients to be grouped together in the address books as one group. If an adversary succeeds in manipulating such groups, he or other unauthorised persons can obtain access to confidential fax transmissions. The fax mail centre should therefore also regularly review the assignment of recipients to individual groups to ensure that these are up-to-date. Where faxes are exchanged between workstations within an organisation via the fax server, the fax mail centre must keep all internal address books up-to-date as well.

In addition, the users have an obligation to check the entries they use personally at regular intervals. This applies both to central address books and also to individual ones.

Regular review of distribution lists

Distribution lists are used by the fax server to route incoming fax transmissions to recipients. Incorrect entries in the distribution lists could result in unauthorised persons gaining access to fax transmissions containing confidential information. The fax mail centre should therefore check the distribution lists at regular intervals to ensure that they are up-to-date and intact.

To ensure that address books and distribution lists are kept up-to-date, the fax mail centre must be informed when any member of staff leaves the organisation.

To ensure that all administration work performed is traceable, all entries and alterations in central address books and distribution lists should be documented.

Additional controls:

- How often are address books and distribution lists checked to ensure they are intact and up-to-date?
- How does the fax mail centre find out when a member of staff leaves?

S 5.75 Protecting against overloading the fax server

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, fax mail centre

A fax server can become overloaded with either incoming or outgoing fax transmissions. If the fax server is overloaded, this could mean that no further fax transmissions can be received or sent for the time being. It is also possible that overloading of the fax server could cause the operating system or the fax server application to crash so that the fax server is temporarily completely unavailable.

The fax server can be said to be overloaded if all the channels available through the communications cards are blocked with incoming and outgoing fax transmissions. The result is that no more faxes can be received or sent until a channel becomes free again. If all the lines provided by the telecommunications company are busy with incoming and outgoing fax transmissions, this has the same result.

Procurement of suitable components

Before purchasing one or more fax servers the likely volume of faxes should be estimated. Components which are capable of handling this volume should then be purchased. Care should also be taken to ensure that sufficient telecommunications lines are available.

The fax server log files should be regularly examined so that if there are certain times when the server is overloaded or is functioning at the limits of its capacity, these can be identified.

Delayed transmission

Overloading of the fax server can occur if an attempt is made to send out a large number of faxes from within the organisation. Under unfavourable conditions, this could cause the fax server application or the operating system to crash. This could be triggered, for example, by an attempt to send out a large number of serial faxes. During the test or pilot phase, tests should therefore be run so as to determine the loading limits. To avoid exceeding these limits, a maximum size should be imposed on users for serial fax transmissions, e.g. through an appropriate standard operating procedure (SOP). Very large serial fax transmissions should then be split into several smaller transmissions. At times when the fax server is heavily loaded, steps should be taken to ensure that faxes are only sent in urgent cases. This can be achieved either using an appropriate SOP or by appropriate permission settings on the fax server. One possible solution is to stipulate that where possible faxes are only to be sent after working hours, which also has the advantage of lower telephone charges.

Agreement with the originator

If it is established that the fax server is always blocked at certain times by the same originating numbers sending large numbers of faxes, first of all the identity of the originators and the nature of the fax transmissions concerned should be established. If the organisation really needs these faxes, one possibility is to negotiate times with the originators at which they should send their faxes so that they can be received without any problems. If the faxes are not actually needed (e.g. unsolicited advertising material), an attempt can be made to block these originator numbers via the fax server application or else via the private branch exchange. However, this is only possible if the

originator identifier (CSID) is not disguised or, where ISDN is used, if the originator does not withhold his call number. If it is not possible to determine the originator's fax number, the only remaining option is to expand the existing capacity, as described above.

Ensure hard disk has sufficient space

Another potential problem with a fax server is hard disk capacity. The danger that an adversary will deliberately exhaust the hard disk capacity through an attack is slim. A single faxed DIN A4 page occupies around 70 KB. Given that most hard disks today hold several gigabytes, when one considers the telephone charges that would be incurred, an attack of this kind is improbable. Generally, all incoming and outgoing fax transmissions are stored either permanently or temporarily on the hard disk of the fax server. What happens then depends on the faxed server application and possibly on the configuration as well. One possibility is that all faxed transmissions are permanently stored or archived on the hard disk of the fax server. When this mode of operation is employed, depending on the volume of faxes, it is possible for the hard disk capacity to quickly become exhausted. In this case steps should be taken to ensure that outgoing fax transmissions and incoming faxes which have already been read are archived as soon as possible on external data media and deleted from the fax server. To achieve this result, the amount of memory placed at the disposal of users on the fax server should be limited. In addition, an SOP should be issued to the effect that fax transmissions which are no longer required are to be deleted. This applies especially to unsolicited advertising material received. Regular checks of the amount of free storage space on the fax server's hard disk should be performed by the fax mail centre.

Additional controls:

- At what times is the fax server heavily loaded?
- Are there any standard operating procedures in place restricting the sending of faxes at busy times to urgent cases?
- Is permanent archiving of faxes not performed on the fax server?

S 5.76 Use of suitable tunnel protocols for RAS communication

Initiation responsibility: Head of IT Section, IT Security Management Team

Implementation responsibility: Administrator

Protection of RAS communication

Remote access to a LAN is effected through a data link which is generally shared with external third parties. Thus, for example, direct dial-in entails use of the network of the telecommunications provider. If the connection is established over the Internet, then the data is forwarded over the networks of the Internet service providers involved (and possibly their partners). Since logging on of the RAS client to a LAN is effected over a RAS connection, the network path used for data transmission must be protected so that the security of the data (confidentiality, integrity, authenticity) is safeguarded. This protection is achieved through encryption and digital signing of the data packets exchanged after the communications partners have been authenticated (see also S 4.34 *Using encryption, checksums or digital signatures*). In the RAS environment, various procedures and mechanisms for protecting the communications link (e.g. tunnelling, see below) have been developed.

The choice of which procedure to use to protect a RAS connection depends on various factors such as:

- the security requirements regarding the strength of the procedure (for example, this determines the key lengths),
- the procedures which can be used at protocol level (see below),
- the procedures supported by the RAS hardware and software.

In general, the following applies:

- The RAS product normally offers a selection of standard procedures supported for the protection of communications. The aim here should be to have the widest possible range of procedures supported.
- The actual protocols used for data transport also offer security mechanisms. These can be used by the RAS product. Alternatively, the RAS product may offer a procedure of its own.

The security mechanisms are based on different cryptographic procedures. Safeguard S 3.23 contains a brief introduction to basic cryptographic concepts.

Encryption of protocol connections: tunnelling

If an encrypted data connection is established between two communications partners, then this connection constitutes a "secure channel". Any data can be securely transmitted over this channel with the underlying communications protocol (e.g. IP). If the data transmitted is in the form of data packets of a communications protocol, then the term "tunnel" is used also. The protocol which is used to encrypt the data, transmit it through the tunnel and manage the connection is also referred to as *tunnel protocol*. With tunnel protocols distinctions can be made as to

- which transport protocol is used and to which protocol layer (OSI layer) they must be assigned (see also S 4.90 *Use of cryptographic procedures on the various layers of the ISO/OSI reference model*);
- which protocols can be transmitted over the tunnel connection;
- which cryptographic procedures for implementing the tunnel are supported;
- whether the tunnel end points are authenticated;
- and whether it is possible to have several parallel tunnels on one instance of the transport protocol used.

The tunnel protocol is essentially responsible for

- management of the tunnel(s): establishment, maintenance and termination,
- negotiation of the cryptographic procedures to be used to implement the tunnel: key exchange procedures, encryption procedures and signature procedures,
- assembly and disassembly of the data packets of the protocols which can be transmitted through the tunnel, and
- encryption and decryption of the data packets.

In the RAS environment, the following tunnel protocols have been established:

- Layer 2 protocols:
  - Point to Point Tunnelling Protocol (PPTP) and
  - Layer 2 Tunnelling Protocol (L2TP): L2TP is a combination of PPTP and the Layer 2 Forwarding (L2F) protocol developed by Cisco which forwards Point to Point Protocol (PPP) packets from a PPP server over a WAN connection to an L2F-capable router which then disassembles them and feeds them into a network.
- The Layer 3 specification IPsec (Internet Protocol Security).

The protocols possess the characteristics summarised in the following table.

Tunnel protocol	Layer	Transported protocols	Required underlying protocol	Number of tunnels supported	Tunnel authentication
PPTP	2	IP, IPX, NetBEUI	IP	1	No
L2TP	2	IP, IPX, NetBEUI	IP, X.25, Frame Relay, ATM	Several	Yes
IPsec	3	IP	IP	1	Yes

All the protocols can establish secure connections to a LAN over an insecure switched network through the use of cryptographic procedures, thus protecting the confidentiality and integrity of the data. Depending on the particular protocol, it is possible to establish one or more tunnel connections.

Tunnelling at Layer 2: PPTP and L2TP

The Layer 2 tunnel protocols can tunnel both the most commonly used protocols, but differ as to over which underlying protocols tunnelling is possible: PPTP can only be transmitted over an IP-based network, whereas L2TP can also be transmitted over various WAN protocols and hence offers greater flexibility. The chart below shows how packets in an application are assembled by PPTP over a PPP connection. As can be seen from the table above, several independent tunnels (e.g. with different levels of quality assurance) can be generated with the more recent L2TP protocol. During user identification and encryption the security mechanisms of the underlining PPP connection make themselves felt under both protocols.

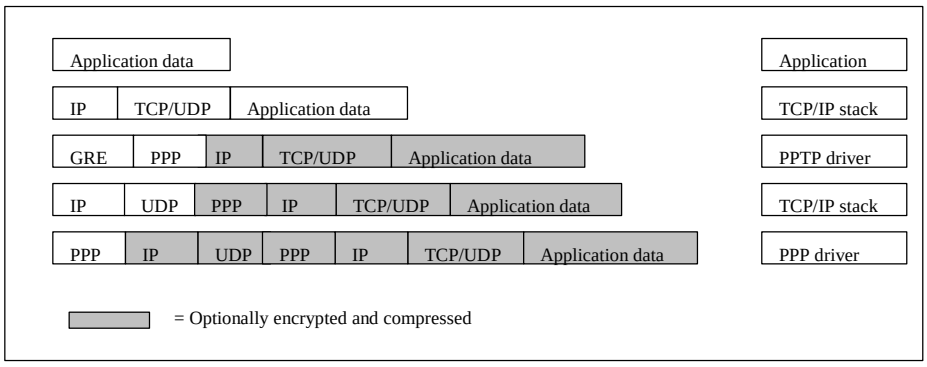


Figure: Assembly of packets of application data with the PPTP protocol

Security mechanisms of the PPP protocol

1. User authentication

   Most implementations of the PPP protocol support the following standard procedures for user authentication (see also S 5.50 *Authentication via PAP/CHAP*):

   - *Password Authentication Protocol (PAP).* The PPP-Server requests transmission of a user name and password by the PPP client. Both items are transmitted here in plaintext. This mechanism is insecure and cannot protect against "Replay" attacks, under which an unauthorised person can re-send the data intercepted at a later time. Use of the PAP authentication protocol is therefore not advised.
   - *Challenge-Handshake Authentication Protocol (CHAP).* The PPP sends a "challenge", consisting of a session ID and a random sequence of letters, the "challenge string", to the PPP client. The client sends back the user name in plaintext as the reply, together with the MD5 hash value made out of a combination of session ID, challenge string and user password. Here the password is not sent in plaintext. The use of the random sequence of letters ensures that the protocol protects against Replay attacks.

2. Data encryption and key management

   In the initialisation phase of the PPP protocol, the procedures to be used for data encryption (and compression) are negotiated between client and server. In general any procedure may be used here as long as client and

server have a corresponding implementation. With regard to negotiation of the procedure, care should be taken to ensure that client and server are both configured so that only the procedures specified in the IT security guidelines are accepted. Steps must also be taken to ensure that unencrypted communication is not chosen as callback variant if no compatible procedure could be negotiated between client and server. Explicit negotiation of the unencrypted communication must also be prohibited.

Tunnelling at Layer 3: IPsec

Whereas the Layer 2 protocols make use of the security mechanisms of the underlying PPP protocol, with the IPsec Layer 3 specification separate security procedures and mechanisms are specified. One limitation of IPsec is the fact that only IP-based communication is supported. However, in most cases this is not a serious disadvantage as today most operating systems and applications are able to utilise IP-based communication.

As regards security requirements, the situation regarding IPsec is as follows:

- User authentication

  Tunnel protocols at Layer 3 assume that authentication of the tunnel end points has been completed already before the tunnel is established and do not offer any separate mechanisms. The only exception here is the IPsec IKE procedure (formerly ISAKMP/Oakley), which allows mutual authentication of the tunnel end points at application level. However, authentication at user level is not possible with this. But since a Layer 3 protocol is actually transmitted over a Layer 2 protocol, in principle use can be made here of the security mechanisms of both protocol layers. When RAS is being used, the mechanisms for user authentication of the underlying Layer 2 protocol actually have to be used as otherwise an unauthorised third person could circumvent the security mechanism, for example, through a physical attack on the client.

- Data encryption

  The standard IPsec prescribes that IPsec-compliant implementations must as a minimum make available the DES and Triple-DES encryption procedures as well as the MD5 and SHA-1 hash functions. However there is no reason why another procedure should not be used here, although in this case the same procedure must also be available to the communication partner. In general, only generally recognised and established procedures should be used. The keys used for symmetric encryption procedures should be at least 80 bits long.

- Key management

  IPsec defines several methods for the generation, exchange and management of keys. With the "Manual IPsec" procedure, there is no automatic key management. In general keys are exchanged by the communication partners over a secure channel (e.g. courier, encrypted e-mail). The interval for the regular exchange of keys here is much larger than with the automatic procedures, such as the above-mentioned IKE

(ISAKMP/Oakley), or Sun Microsystems' SKIP. Both of these latter procedures administer the certificated keys automatically.

When choosing the RAS hardware and software to be used, care should be taken to ensure that as many different, established encryption procedures are supported as possible. This will increase the probability that a suitable procedure can be negotiated between client and server.

Examples

- To use MPPE data encryption under Windows NT, the option "Accept only Microsoft encrypted authentication" must be set in the "Security" tab of Dial-Up Networking properties and the option "Require data encryption" must be enabled. Use of the option "Use current username and password" is not recommended.
- Under Windows NT, the protocol VPN Adapter (RASPPTPM) must be installed on the RAS client for establishment of a PPTP connection over an Internet connection. This is performed by selecting *Control Panel, Network, Protocols.* A separate entry must be created in Dial-Up Networking for the VPN connection. Here, instead of a phone number, the IP address of the remote RAS server is entered. In the "Dial using" field, the VPN adapter must be selected. Once a connection has been successfully established with an ISP, thereafter the VPN connection is established over this existing Internet connection. This process can also be automated by defining a script for the ISP connection.
- Under Windows 2000, use of IPsec-based data encryption can be enabled in the properties for the TCP/IP protocol (under *Network Properties, Adapter Properties, Protocols*). To achieve this, on the "Options" tab, the properties of the "IP security" entry must be changed. The "Use IP security guidelines" option must be enabled and the desired security guidelines selected.

Additional controls:

- At which protocol level should tunnelling be enabled?
- Over which protocols must the tunnel protocol be processed?
- Which protocols must be transported through the tunnel?
- Is authentication of the tunnel end points necessary?

S 5.77 Establishment of Subnetworks

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section, Administrator

IT systems in agencies and companies are typically integrated into local networks (LANs) which in turn are linked to other networks. Simply for technical reasons it is generally necessary with medium-sized and larger networks to divide a LAN into several subnetworks, for example because there is a limit on the number of IT systems per subnetwork or on the overall length of the cabling.

However, the establishment of subnetworks is also recommended for reasons of IT security. Sensitive data can be restricted to certain areas within the LAN (confidentiality), while at the same time it is possible to prevent faults in or attacks on one subnetwork from impairing the operational capability of other subnetworks (integrity and availability).

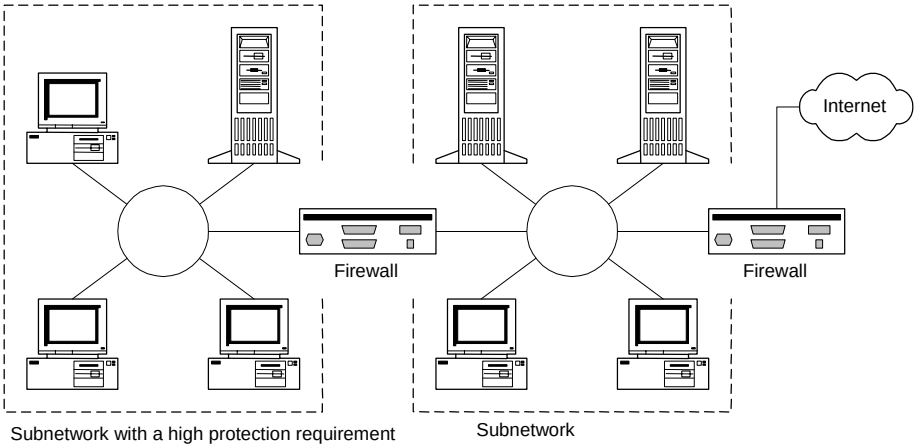
At the outset it is necessary to determine which IT systems should be operated in a common subnetwork. It is recommended here that reference is made to the results of the assessment of protection requirements and that the following procedure is adopted:

- All IT systems and communications links in a subnetwork should have the same protection requirements as regards the basic parameter of confidentiality. This will ensure that sensitive data is confined if possible to specially protected subnetworks. The protective measures required can then be concentrated on these subnetworks.
- IT systems and communications links with a high or very high protection requirement as regards availability or integrity should if possible be in a separate subnetwork. This will ensure that proper operation of these components is not impaired in the event of faults or problems on other subnetworks. Another advantage is that faults can be contained and rectified more quickly.

The second step entails the selection of suitable components for linking the subnetworks which have been established. Recommendations on this point will be found in safeguard S 5.13 *Appropriate Use of Equipment for Network Coupling*.

In particular, consideration should be given to the use of firewalls where subnetworks which contain components having a very high protection requirements are to be linked up. This will ensure that data flows to and from the subnetwork concerned in a selective and securely controlled manner.

The diagram below illustrates an example of a possible overall structure for a LAN after a subnetwork having a high protection requirement has been split off from the residual subnetwork using an additional firewall. For the sake of simplification, the two firewalls are shown as single symbols, but generally they consist of several components (packet filters, application gateway etc).



Recommendations for the technical implementation of segmentation in the LAN are contained in following safeguards:

- S 5.61 *Suitable Physical Segmentation* and
- S 5.62 *Suitable Logical Segmentation*

.Additional controls:

- Are there any IT systems or communications links which have different protection requirements?
- Has the local network being divided up into several subnetworks in accordance with the results of the assessment of protection requirements?
- Are suitable switching elements used for linking up the subnetworks?

S 5.78 Protection against mobile phone usage data being used to create movement profiles

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Users

When mobile phones are used, for technical reasons it is necessary for the mobile communication partners to be contactable. When one of these partners establishes a connection, information is given away about his location through the act of establishing the connection. This location information could be used by the network provider or service operator, or indeed by a third party, to create a person- or mobile phone-specific "movement profile".

If the creation of movement profiles due to use of a mobile phone is viewed as a threat, then if possible both the mobile phones and the SIM cards should be swapped around among staff more frequently. In this way it is at least more difficult to associate specific phones and cards with a particular user.

If it is desirable that the whereabouts of the user should be concealed at certain times, the only way to ensure this is by switching off the mobile phone. To be quite certain, the battery should be removed.

S 5.79 Protection against call number identification during use of mobile phones

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Users

In the GSM network the number from which a call is being made can be indicated to the recipient of a call. Whether this is in fact the case depends on the technical equipment and the configuration of the mobile phones and/or at the network provider's end.

It is possible to prevent one's own call number from being transmitted to the person telephoned by using the call number suppression function on the mobile phone (either for the next call or for all other calls). This option is often found in mobile phone menus under menu option names such as "Incognito" or "Anonymous".

Passing on of call number information can also be prevented on an ongoing basis through the network provider.

If mobile phones and SIM cards are swapped around between users, this can provide a certain protection against the association of call numbers with particular persons, as it prevents a permanent association between user and call number or between mobile phone and user from being deduced. However, the link, for example, to an agency or company, will remain.

Publication of phone numbers

A particular person's mobile phone number can be ascertained not only through transmission of the call number but also from public telephone directories, if the number is entered there. When concluding a mobile phone contract, the question of whether and in what form an entry should appear in public telephone directories should therefore be carefully considered. The same applies to the publication of call numbers in internal telephone directories and to the disclosure of these in various applications where entry of such data is requested (e.g. forms, prize draws etc.).

S 5.80 Protection against bugging of indoor conversations using mobile phones

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management

The only way to be sure that indoor conversations are not being bugged using mobile phones is to prohibit the taking of mobile phones into the rooms to be protected. If the IT security policy of an agency or company does not allow mobile phones to be brought into the building, clear notices to this effect must be placed on all the entrances. But without corresponding checks, a simple notice will generally be ineffectual.

Switching off the mobile phone does not ensure sufficient protection since in the case of manipulation there is no way of eliminating with certainty the possibility of the phone being switched on over the radio link. The only way to prevent this would be to remove the battery.

Mobile phone detectors

Mobile phone detectors are devices which detect whether one or more mobile phones is in transmission mode (i.e. a conversation is taking place) within a defined area.

Passive detectors

Passive warning devices are available on the market which report any mobile phones in transmission mode. The range of the devices can be adjusted so that it is confined to the area to be monitored. It is recommended that if this kind of protection is required, warning devices are installed and these are activated when conversations about sensitive or confidential matters are taking place.

However, these passive detectors cannot detect mobile phones which are currently in standby mode. Detection of such mobile phones is only possible if the detector has an active transmitter component. This transmitter component can then require the mobile phone to go into transmission mode. Once the mobile phone is in transmission mode, it can be picked up with a detector.

Active detectors

These active detectors are appropriate for conversations which involve sensitive material. They can detect all mobile phones that are switched on. Any mobile phone switched on subsequently has to register itself with the base station, and this action can be detected also. Another possibility is to use noise pulse generators to interfere with radio operations in a spatially defined area so that reception of mobile radio signals is not possible there.

At present only passive mobile phone detectors can be recommended. While active detectors could also be helpful, their use cannot be recommended in Germany as they are not approved for use in the Federal Republic of Germany. The same applies to transmitters which jam radio operations, which are also illegal in Germany.

S 5.81 Secure transmission of data over mobile phones

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, users

Mobile phones are normally used for voice transmissions, but data and faxes can also be transmitted using them. Some of these services require additional accessories.

Short messages

With the Short Message Service (SMS) it is possible to send out up to 160 characters of text from one mobile phone to another or to an e-mail address. Short messages are always transmitted via the SMS message centre, which forwards the messages to the appropriate recipient.

Storage space is limited

Short messages are stored in the mobile phone as long as there is sufficient free memory available. If all the available memory has been used up, no further short messages can be received. If there are further messages to be delivered, the network provider will reattempt to transmit them, but only for a limited period of time. If the required storage space does not become free within that time, the short messages will be deleted by the network provider.

It is sometimes also possible to alter the period for which short messages will be temporarily stored at the network provider's from the mobile phone. The default setting is normally between 24 and 48 hours. However, unless the contract with the network provider allows for this, the storage period cannot be extended by changing such a setting. It should also not be reduced.

In order to be able to send SMS messages, the call number of the SMS message centre (SMS Gateway) must be pre-configured on the mobile phone via the appropriate menu. Usually this is already preconfigured on the SIM card by the network provider.

SMS spam

A variety of services offered on the Internet allow SMS messages to be sent at minimal cost. It is possible in this way to send a large number of short messages to a mobile phone quite cheaply. The effects of SMS spam are similar to those of e-mail spam (see also T 5.75 *Overload due to incoming e-mails*). The spam messages use up the available space in the mailbox or in the memory of the mobile phone so that serious requests cannot get through. Receiving these spam messages also costs the user money (and could in fact be quite expensive). The only remedy is to limit distribution of one's own call number, e.g. to forego entry in telephone directories or in case of damage to do without SMS for an extended period.

Identification of the originator is unreliable with SMS

It is not always possible to reliably identify the originator of an SMS message. At the most, identification will be based on the call number of the originator and, depending on the network provider and/or the configuration of the mobile phone, this is not always transmitted with the message. When short messages are sent over the Internet, generally there is no unique identification. This should be clear to all users so that they can correctly assess the genuineness of a message. Messages such as the following should not be taken seriously: "Due to reorganisation, we need your ec-PIN. Please send this to the specified

call number. Your bank." Depending on the content of a short message received, it may be appropriate to make subsequent enquiries as to whether the originator really did send this message.

It is quite common for short messages to end up with the wrong recipient as an incorrect call number has been entered or the wrong entry has been selected from the telephone directory as the recipient. Even if mobile phone displays are small, the recipient details should still be checked prior to sending a message.

Faxes

It is also possible to send faxes to the landline network via SMS. Again, faxes can be received as long as they satisfy the restrictions of SMS transmissions, especially as regards containing only a short text. Faxes can also be sent and received using an IT system linked to the mobile phone (e.g. a notebook).

When using the fax capability, the points to be noted are similar to those which apply to conventional fax machines (see Section 8.2 *Fax machines*), namely:

- The memory of the mobile phone can become overloaded by incoming faxes.
- Depending on the importance of the faxes, it may be necessary to make copies of them, something which can be difficult with a mobile phone.
- It may be appropriate to block the call numbers of certain fax recipients and originators.
- It may be appropriate to enquire after sending a fax whether it arrived in legible fashion.
- It may be appropriate after receiving a fax to check whether it was really sent by the originator indicated.
- It may be appropriate to review the destination addresses programmed from time to time.

E-mail

Again, it is possible to receive and send e-mails over mobile phones as well as short messages. The permitted length of an e-mail is usually only 160 characters, as for short messages. When this service is configured by the network provider, the mobile phone is given its own e-mail address.

With some network providers, e-mail services can be combined with other services. Thus, for example, incoming e-mails can be read by voice output software, forwarded to a fax machine or to a different e-mail address. Outgoing e-mails can be spoken into the mobile phone and sent as an audio file (WAV file).

Like short messages and faxes, e-mails too can quickly exhaust the available memory space. Moreover, the contract with the network provider may specify that only a limited number of e-mails can be sent or received per month.

Potential security problems and safeguards to be adopted in connection with the use of e-mail are described in Section 7.4 *E-mail*. It should be noted here

that the e-mail functionality offered on mobile phones is severely restricted compared with other e-mail applications. Like SMS, e-mail should be viewed here as primarily a means of transmitting short messages with a short life. It is not possible to implement security measures such as encryption or digital signatures (unless additional modules or special devices are used).

The boundaries between the various types of message such as SMS, fax and e-mail are relatively fluid. What distinguishes them as far as the user is concerned is generally not the type of data input but the transmission format. Here the network provider may also offer other formats such as X.400 or paging.

Data transmission

If the mobile phone is linked to another IT system (e.g. a notebook or organiser), it is also possible to transmit larger quantities of data. Coupling of the devices may be effected in a number of ways, depending on the technologies supported by the two devices.

Plug-in card. A plug-in card (PC card or PCMCIA) is the conventional solution for connecting mobile phone and notebook. However, most plug-in cards can only be connected to mobile phones of a particular manufacturer.

Soft modem. Under this solution, special software is installed on the notebook instead of a plug-in card. The mobile phone is then simply connected to the notebook over the serial interface. This solution is cheaper than a plug-in card.

Infra-red. With an infra-red interface, data can be transmitted from the mobile phone to an IT system (e.g. a laptop or organiser) without any cables. This requires that both the mobile phone and also the IT system support Infrared Data Association (IrDA). IrDA is a world-wide standard for data transmission by infra-red.

Bluetooth. Bluetooth is a more recent standard which enables devices to exchange data with each other over short distances by radio. The Bluetooth technology uses the freely available Industrial Scientific Medical (ISM) radio network, which operates in the 2.45 GHz band.

Encrypt data transmissions

Where data is to be transmitted e.g. from a laptop over GSM, it should be encrypted on the terminal device prior to transmission. A number of programs are available for achieving this relatively simply. Encryption of the information prior to transmission protects it over the entire route between originator and recipient. This goes beyond protection of the radio interface between mobile phone and base station, as is standard with GSM. Moreover, the messages can then also be digitally signed. Section 3.7 *Crypto concept* describes how to select cryptographic procedures and systems that are suitable.

Downloading data

There are a number of sites on the Internet from where additional ring tones, display icons or similar can be downloaded for the various mobile phones. It should, however, be noted that loading such data can sometimes render a mobile phone inoperable.

Control of data transmission

Data transmission should be properly controlled in all organisations. All data transmission facilities should be approved and their use should be subject to clear rules (see also S 2.n2 Prevention of insecure network access).

In order that no security loopholes are created through data transmission over GSM interfaces, these should be subject to restrictions. For example, no mobile phone cards should be permitted on IT systems on which sensitive data is handled. This applies also to all IT systems which are connected to a computer network, to ensure that it is not possible for the firewall protection to be undermined.

S 5.82 Secure Use of SAMBA

Initiation responsibility: Head of IT Section, Administrator

Implementation responsibility: Administrator

SAMBA is a freeware software package for UNIX operating systems which, amongst other things, provides file, print and authentication services over the Server Message Block (SMB) and Common Internet File System (CIFS) protocols. The most important examples of SMB/CIFS clients are definitely the operating systems in the Microsoft Windows family. With SAMBA it is possible, for example, for Windows 9x or Windows NT computers to access shared files on a UNIX server directly. This obviates the need to take a detour over the FTP or NFS protocols or to install additional software on the client. In the current version, SAMBA simulates a whole range of Windows NT server functions so that in many cases it is possible to use a UNIX system with SAMBA in lieu of such a server.

If SAMBA is in use within the agency/company, the recommendations set out below should be considered.

Programming errors which sometimes can induce security loopholes have been discovered in older versions of SAMBA. An up-to-date version should be used, in which as far as possible all known security-relevant errors have been eliminated.

Using the file *smb.conf*, it is possible to configure the SAMBA server in an extremely flexible and detailed manner. However, this also makes the system somewhat complex. Before using SAMBA, it is therefore important to read the documentation thoroughly. The configuration should be carefully planned, documented and implemented through appropriate parameter settings in file *smb.conf*. For example, a long description of the various parameters can be viewed by entering the command *man smb.conf*. In the event that configuration settings are altered, checks should be performed using the documentation and appropriate tests to ensure that the change in configuration does not result in unwanted side-effects.

The following parameters are particularly problematic in terms of the possible security risks associated with them. They should therefore only be used after checking thoroughly all the possible effects on the IT security of the server.

[...] command postexec
add user script preexec / exec
delete user script root postexec
fake oplocks root preexec
ldap [...] smbrun
panic action unix password sync
passwd program

With the *testparm* program it is possible to check whether the settings in file *smb.conf* are permitted. Of course it is **not** possible using that program to draw any conclusions as to whether the settings do have the desired effect or security-relevant effects. Creation and maintenance of the *smb.conf* file can also be supported by graphical user interfaces, for example using the Samba

Web Administration Tool (SWAT) which is supplied as standard with the SAMBA package.

SAMBA currently offers four different means of achieving client authentication. With the setting *security = user*, the SAMBA server checks whether the client is transmitting a valid combination of user ID and password. With *security = server* or *security = domain* it leaves this check to one or more other SMB/CIFS servers which it trusts and are specified via the parameter *password server*. On the other hand, if *security = share* is set, only a simple password check is performed and the client does not have to transmit any user ID. This procedure is considerably weaker than authentication via user ID and password and should only be used if the data on the SAMBA server does not have to be protected. An example here might be a server with write-protected data medium and data that can be accessed by the public. In this case it is appropriate not to have any authentication, and the easiest way of implementing this is via the setting *security = share.*

Either plaintext passwords or encrypted passwords can be used for client authentication. As plaintext passwords can easily be intercepted during their transportation over the network using freely accessible tools, in principle only encrypted passwords should be used. On the client side, encrypted passwords are supported e.g. by Windows 95 (with installed SMB update), Windows 98, Windows NT 4.0 and Windows 2000. In file *smb.conf* on the SAMBA server, encrypted passwords are activated by the parameter *encrypt passwords = yes*. Unlike plaintext passwords, a SAMBA server cannot check encrypted passwords with the authentication mechanisms of the underlying UNIX operating system (which, for example, references */etc/passwd* or */etc/shadow*). It is therefore necessary to have an additional password file, which is specified via the parameter *smb passwd file*. This file contains the encrypted passwords and must be carefully protected from unauthorised access.

The rights of a user to access directories and files via SAMBA are derived partly from the settings in file *smb.conf* and partly from the access rights of the file system on which the shared data is held. Here too careful configuration is necessary to ensure that access rights are granted in a consistent manner. Unlike on Windows NT servers with NTFS drives, when SAMBA is used it is not always appropriate to grant access rights exclusively through the file system. The reason for this is that commonly used UNIX file systems implement a different security model, based on permissions and ownership, than NTFS. Depending on the specific application, it is therefore necessary to check whether certain superordinate access restrictions can be better configured through file *smb.conf*. Reference is made here to the parameters *(in)valid users* and *read/write list*.

The following parameters can potentially allow access restrictions to be circumvented:

admin users
force group / group
force user
guest account
hosts equiv
username / users / user

username map

If any of these parameters are used, the possible security implications should therefore be carefully examined.

Symbolic links in shared directories can have the result of giving clients unauthorised access to files *outside* of the shared area. It is recommended that this is prevented by setting the parameter *wide links = no*. However, it should be noted that this parameter can slow down throughput as the extra checks required use up some of the processor capacity. If this could result in operations being hampered, one could try setting the parameter *getwd cache = yes*. As an alternative to checking symbolic links, consideration should be given to using the parameter *root directory = <path>*. This setting prevents access to directories and files outside of *<path>*. However, all the files needed to run SAMBA, including the password files, must then be copied to subdirectories of *<path>*, including the password files.

Amongst other things, logon scripts for clients can be provided on the server via the share *[netlogon]*. Under no circumstances should users be able to modify files in this share. It is recommended that *writeable = no* and *guest ok = no* or that equivalent parameters are set for this share.

The following parameters are preconfigured and should not be altered as this might impair proper and secure operation of IT systems.

kernel oplocks = <automatic>
locking = yes
magic [...] = <disabled>
map to guest = Never
passwd chat debug = no
password level = 0
share modes = yes
use rhosts = no

If the services of a SAMBA server are used over larger networks which are not completely under the organisation's own control, consideration should be given to protecting the communications links through the use of cryptographic procedures. This is especially recommended if there are compelling reasons as to why plaintext passwords have to be used. Protection can be provided through appropriate hardware or software components. SAMBA provides special support for the use of SSL. To avail oneself of this possibility, an SSL software package, normally the freeware SSLeay software, must be installed on the SAMBA server. On the client side, a SSL proxy software package is needed; this is available free of charge for Windows NT and UNIX clients. Windows 9x clients can use the SSL proxy of a Windows NT or UNIX client in their subnetwork. The first steps of configuration involve defining a Certification Authority (CA) and generating key pairs and certificates for the server and clients (assuming this has not already been done). The corresponding procedures are explained in the documentation for SSLeay. To activate SSL on the SAMBA server, as a minimum the parameters *ssl = yes* and *ssl server cert = <path>* should be set in file *smb.conf*. If the private key of the server is not stored in the same file as the server certificate, the parameter *ssl server key = <path>* is necessary as well. It is recommended enabling checking of server and client certificates. This requires the parameter

settings *ssl require clientcert = yes* and *ssl require servercert = yes*, also *ssl CA certDir = <path>* or *ssl CA certFile = <path>*. For every client on which an SSL proxy is used, the key pair and the certificate for that client must be copied to a protected directory. The paths of these files and the name of the SAMBA server are sent to the SSL proxy on start-up as parameters. The clients can now call up the desired SMB/CIFS services from the relevant SSL proxy. The proxy forwards the requests - protected through the SSL protocol - to the actual SAMBA server. As a result, as far as the clients are concerned, the services appear to be provided by the SSL proxy rather than by the SAMBA server.

If there are compelling reasons why plaintext passwords have to be used, this can be enforced on clients which run under the operating systems Windows 9x, Windows NT 4.0 and Windows 2000 through particular Registry entries. For example, this is necessary under Windows NT 4.0 with Service Pack 3 or higher, as unless the Registry entries are modified this version of the operating system also refuses to transmit plaintext passwords even if the server does not support encrypted passwords. Otherwise the client may be unable to log on successfully to the server. However, it should be noted that where plaintext passwords are used, additional protective measures (e.g. VPN or SSL) are needed for the communications links in every case.

Even once the Registry has been modified, it may be difficult for a Windows NT 4.0 client to log on to the server using a plaintext password, as in this case the user is asked to enter his password every time he wishes to establish a connection, and where different resources are used on the server this can be very annoying. This is another reason why, if possible, the use of plaintext passwords should be avoided completely.

Further recommendations regarding the secure configuration of clients will be found in safeguard S 5.38 *Secure Integration of DOS PC's into a UNIX Network* and in the modules 5.5 "PC under Windows NT" and 5.6 "PC with Windows 95".

Additional controls:

- Are changes in the SAMBA configuration documented and tested in actual operation prior to use?
- Are encrypted passwords used?
- Are write accesses to the share *[netlogon]* prohibited?

S 5.83 Secure Connection of an External Network with Linux FreeS/WAN

Initiation responsibility: Head of IT Section, Administrator

Implementation responsibility: Administrator

In many organisations there is a requirement to link up the various local networks which are installed at individual locations. In most cases this is achieved using leased lines or public networks which are outside the control of the organisation. In such cases there is a danger that the transmitted data could be intercepted or tampered with or that an adversary could pass himself off as an authorised communication partner (a masquerade attack). These threats can be countered through use of a *Virtual Private Network* (VPN). With the aid of cryptographic procedures, it is then possible to protect the integrity and confidentiality of the data and to reliably authenticate communication partners. *Linux FreeS/WAN* is a freeware software package for the Linux operating system, with whose assistance a VPN that complies with the IPSEC standard can be established.

Planning

As the first step in the planning phase, the requirements which the product that will be used to protect the communications link must satisfy should be established. These include, for example, whether it needs to work alongside existing components or whether other protocols apart from TCP/IP have to be transported. The documentation for FreeS/WAN should then be worked through and used to determine whether this software package is suitable for the task in hand. If it is suitable, then the next step is to identify and document which functions of FreeS/WAN are to be used for what purpose and how it should be incorporated into the existing network structure.

Installation

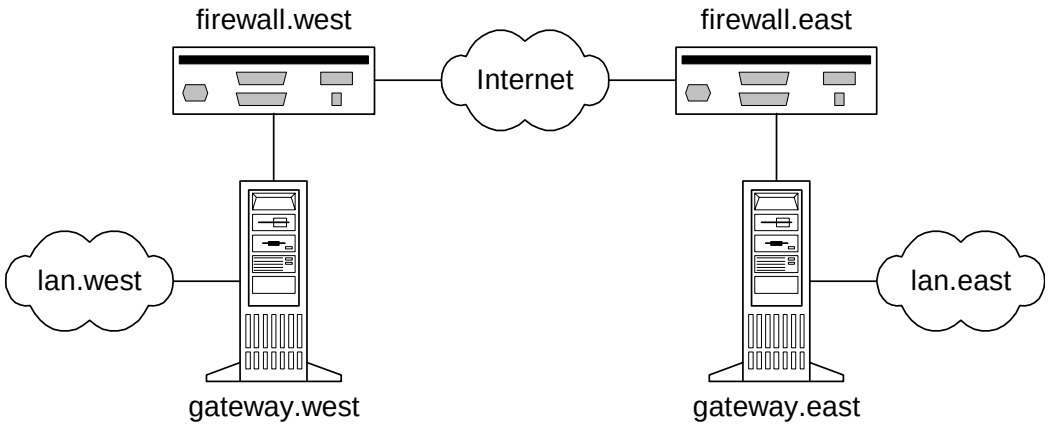
FreeS/WAN runs on the freeware operating system Linux and meshes with the IP protocol stack of the kernel.

It is recommended that FreeS/WAN is only run on PCs that are configured for this purpose and that no other services - apart from any routing functions which may be required - are activated on these PCs (see also S 4.97 *One Service per Server*). In particular, they should not execute any firewall functions but should be independent of the firewall system. To install the operating system it is recommended using a Linux package which already contains FreeS/WAN. This facilitates installation considerably, as otherwise it is usually necessary to recompile the Linux kernel. Reference should be made here to the FreeS/WAN documentation. Moreover, only those software modules within the Linux package which are absolutely necessary should be installed.

Configuration

FreeS/WAN implements a whole range of different functions which are defined in IPSEC. Through appropriate configuration settings it is therefore possible to use this software package in many different environments, and for quite different application areas. The example provided below illustrates how

FreeS/WAN can be used to protect communications between two local networks over the Internet. The configuration of the components in the two networks is as follows:



The two locations *west* and *east* of an organisation both have a connection to the Internet. They both use a **multi-level firewall system** which, however, for the sake of simplification is represented in the diagram by a single symbol. *gateway.west* and *gateway.east* are IT systems which run under the Linux operating system and are to serve as gateways for the local networks *lan.west* and *lan.east* with the aid of FreeS/WAN. Each of the gateways has two network cards connecting it to the firewall systems and the local networks. The aim is to ensure that all the IT systems in *lan.west* and *lan.east* can communicate securely with each other. Protection of communications is to be transparent for these IT systems.

It is important that a suitable key management procedure is chosen. It is recommended that automatic exchange of keys over a public key procedure (RSA) is used. Compared with the other procedures supported by the FreeS/WAN, this offers the highest security level. The first step in the configuration process therefore entails the generation of RSA key pairs for the two gateways. This can be achieved, for example, using the command *ipsec rsasigkey*. The keys should be at least 768 bits long. As noted in the documentation, the keys thus generated may only be used for signatures and **not** for encryption. The FreeS/WAN software package ensures that this is the case. The command *ipsec rsasigkey* produces in each case the public and private RSA keys. It is critical to the security of the VPN that the private key **cannot** be compromised **under any circumstances** (see also S 2.46 *Appropriate Key Management*). The private key is stored in file */etc/ipsec.secrets* on the gateway. Ownership and permissions should be set as follows:

-rw------- root root /etc/ipsec.secrets

By contrast, the public key is entered in file */etc/ipsec.conf* (see below). This file is where all the other settings for FreeS/WAN are made. The format is designed in such a way that it may be possible to use the same file on both gateways. Configuration entails making settings in the form *parameter = value* in several sections. All the parameters which have to be set differently for the two gateways have the prefix *left* or *right*. The relevant FreeS/WAN

entity can tell independently from the IP address which of the two parameters applies to it. Generally, the only difference between the versions of file */etc/ipsec.conf* which are stored on the two gateways is therefore confined to the parameter *interfaces*, for example because on one side an ethernet is used and on the other side a token ring. In the present example recommendations as to how to configure file */etc/ipsec.conf* are provided below.

config setup section

This section contains general settings which are not specific to any particular connection.

interfaces = ipsec0=eth0

First of all, the parameter *interfaces* is used to specify over which network interfaces secure connections should be established. No encrypted packets are sent over any other interfaces. In the example presented above, the connection to the firewall is in each case established by the *eth0* interface of the gateway.

forwardcontrol = yes

If the parameter *forwardcontrol* is set to the value *yes*, FreeS/WAN will independently enable or disable the forwarding of IP packets when IPSEC is activated or inactivated. This is recommended as this setting will prevent packets from being transmitted unencrypted when the VPN is not available. On starting up the Linux system, steps should be taken to ensure that forwarding of IP packets is disabled until the network interfaces have been activated. How this setting is implemented will depend on the version of Linux that is being used.

dumpdir =

The *dumpdir* parameter should be set to a blank value in order to prevent the FreeS/WAN components from generating core dumps in the event of a program error. Otherwise there is a danger that unauthorised persons could extract secret keys, for example, from these core dumps.

plutoload = %search
plutostart = %search

The *pluto* daemon is part of the FreeS/WAN package and is used for automatic key management. The parameters *plutoload* and *plutostart* determine which connections are automatically loaded into the *pluto* database and activated. It is advisable to set these parameters in each case to the special value *%search*. This will ensure that the connections which have been specified via the *auto* parameter are loaded and activated.

conn west-east section

This section contains settings which apply specifically to a particular connection, for example *west-east*.

type = tunnel

The operating mode for this connection is specified with the *type* parameter. Since in the present case the network traffic is to be protected between two local networks using gateways, it is imperative that the *tunnel* mode is used.

The *transport* mode is only permitted for host-to-host communication, *passthrough* only for manual key management.

auto = start

If the parameters *plutoload* and *plutostart* are set to the special value *%search*, then the parameter *auto* determines whether the present connection is automatically loaded into the *pluto* database and activated. In our example the connection is to be directly activated, so the parameter *auto* is therefore set to *start*.

auth = esp

The parameter *auth* determines which of the two IPSEC functions, *Encapsulating Security Payload* (ESP) or *Authentication Header* (AH) is used during authentication. In the present case both encryption and authentication with ESP are possible. This is the standard setting.

authby = rsasig

It is recommended that authentication is performed using digital signatures with the RSA algorithm (*rsasig* setting). This provides a higher level of security than the "shared secrets" procedure (*secret* setting) as well as simplifying administration.

pfs = yes

pfs stands for *Perfect Forward Secrecy* and means that messages which have been exchanged in the past are not compromised even if the private keys of the two gateways become known. (However, the security of future connections can no longer be assured.) The recommended setting for this parameter is the default value *yes*.

keyingtries = 0

Parameter *keyingtries* specifies the maximum permitted number of attempts at establishing or updating the corresponding connection. It is recommended that the special value *0* is entered, i.e. so that there is no limit on the number of attempts. The preconfigured value *3* for the parameter *keyingtries* is inadequate for most applications.

left = <IP address of gateway.west>
right = <IP address of gateway.east>

The IP addresses of the two gateways are set through parameters *left* and *right*. It is recommended that the IP addresses are entered numerically rather than using the special value *%defaultroute*. By performing a comparison with the IP addresses which have been assigned to the corresponding network interfaces of the IT system, FreeS/WAN can detect which of the two roles (*left* or *right*) this IT system is assuming.

leftnexthop = <IP address of firewall.west>
rightnexthop = <IP address of firewall.east>

For parameters *leftnexthop* and *rightnexthop*, in each case the IP address of the component which forwards the packets over the insecure network should be entered. In the present example this component is part of the firewall system. However, depending on the segmentation and layout of the active network

components in the local network, in many cases the next router downstream on the route to the Internet firewall should be entered.

leftsubnet = <subnetwork/mask of lan.west>
rightsubnet = <subnetwork/mask of lan.east>

These two parameters determine which two subnetworks should communicate securely with each other. In the present example these are the local networks *lan.west* and *lan.east*. The values are entered in the format *subnetwork/mask*, for example *10.10.0.0/16*.

leftid = @gateway.west
rightid = @gateway.east

The parameters *leftid* and *rightid* are used to assign names which are necessary for authentication to the two gateways. It is recommended that the names are specified in the form of DNS names with the prefix "@". This will prevent FreeS/WAN from resolving the DNS names to IP addresses before they can be used to query the DNS server.

leftrsasigkey = <public RSA key of gateway.west>
rightrsasigkey = <public RSA key of gateway.east>

These two parameters are used to specify the public keys for the gateways. By contrast, the matching secret keys must be entered in file */etc/ipsec.secrets* on the relevant gateway.

Routing

FreeS/WAN uses the routing tables of the underlying Linux operating system when forwarding IP packets. It is therefore necessary to generate rules on both gateways using the *route* command so that packets for the local and remote networks are forwarded via the appropriate network card.

Remote administration of a gateway

In the default configuration, *gateway.west* and *gateway.east* cannot communicate over the VPN. The secure tunnel only transports data between *lan.west* and *lan.east*. This is desirable for security reasons unless one of the two gateways is to be administered from the respective other side. In that case another connection must be defined in the *ipsec.conf* file. This additional connection differs from the *west-east* connection in that the parameter *leftsubnet* is missing (if *gateway.west* is to be remotely administered from *lan.east*) or else that the parameter *rightsubnet* is missing (if *gateway.east* is to be remotely administered from *lan.west*).

Firewall settings

firewall.west and *firewall.east* should be configured so that the encrypted user packets and the necessary management packets can be exchanged between the two gateways. In the present example, the following rules are necessary to achieve this:

- IP packets with protocol number 50 from *gateway.west* to *gateway.east* and vice versa are allowed.
- UDP packets, port 500 from *gateway.west* to *gateway.east* and vice versa are allowed.

If, contrary to the example, the value *ah* was set for the parameter *auth*, IP packets with protocol number 51 must be allowed through. Any other communication with the gateway or the local network must be prevented by the relevant firewall system.

As the firewall system and the gateway are implemented so that they are separate from each other, the parameters *leftfirewall* and *rightfirewall*, plus *leftupdown* and *rightupdown* are not used.

Where *Network Address Translation* (NAT) is used, it should be noted that address translation must be performed either on a component between the gateway and the local network or on the gateway itself. Generally the addresses cannot be translated within the firewall system. The reason for this is that parts of the IP packets are modified when NAT is used, so that IPSEC integrity checking generally will not work. NAT may therefore only be performed "behind" the IPSEC gateway. If address translation is to be performed on the same IT system on which FreeS/WAN is also operated, it should be noted that this will make processing of the IP packets on that IT system very complex. Information on this point will be found in the FreeS/WAN documentation. It is therefore simpler and administration is also easier if NAT is carried out on a separate component between the gateway and the local network.

VPN functional test

Before the VPN is used in actual operations, it is necessary to check that it is functioning as desired. During the test phase, instead of the two local networks only test computers should be connected to the gateways. Otherwise the possibility that "real" data will be sent unprotected over the Internet if the VPN does not function correctly straightaway cannot be excluded.

It is necessary to check that the packets are really encrypted. As described in the documentation, the simplest way of doing this is using the tools *ping* and *tcpdump*. The *ping* tool enables IP packets which are easy to detect to be generated, while *tcpdump* can be used to monitor the network traffic generated by FreeS/WAN. It should be noted that the *ping* command must be run on the test computer and not on the gateway. In the present configuration example, the VPN only protects the traffic between the local networks (which are replaced during the test phase by one or more test computers) and not the traffic from or to the gateways. (See also "Remote administration of a gateway" above on this point.) The command *tcpdump* for monitoring the network traffic generated can be run on any IT system between the two gateways.

If the VPN is not functioning as desired, for example no communication is possible or the network traffic is not encrypted, FreeS/WAN provides a number of diagnostic tools. For example, information on the status of the software program can be obtained from examining the contents of the pseudo-file */proc/net/ipsec_tncfg* and by running the command *ipsec look*. Further information on this subject is contained in the FreeS/WAN documentation.

Additional controls:

- Is FreeS/WAN run on stand-alone IT systems on which the minimum Linux operating system functionality has been installed?
- Have steps being taken to ensure that private RSA keys never leave the gateways?
- Has the VPN been tested for correct operation prior to operation for real?

S 6 Safeguard Catalogue: Contingency Planning

S 6.1 Development of a survey of availability requirements

S 6.2 Definition of "emergency", person-in-charge in an "emergency"

S 6.3 Development of an Emergency Procedure Manual

S 6.4 Documentation on the capacity requirements of IT applications

S 6.5 Definition of "restricted IT operation"

S 6.6 Study of internally and externally available alternatives

S 6.7 Responsibilities in an emergency

S 6.8 Alert plan

S 6.9 Contingency plans for selected incidents

S 6.10 Contingency plans for breakdown of data transmission

S 6.11 Development of a post-incident recovery plan

S 6.12 Emergency preparedness exercises

S 6.13 Development of a data backup plan

S 6.14 Replacement procurement plan

S 6.15 Agreements with suppliers

S 6.16 Taking out insurance

S 6.17 Alert plan and fire drills

S 6.18 Provision of redundant lines

S 6.19 Data backup on PCs

S 6.20 Appropriate storage of backup data media

S 6.21 Backup copy of the software used

S 6.22 Sporadic checks of the restorability of backups

S 6.23 Procedures in the event of computer virus infection

S 6.24 PC emergency floppy disk

S 6.25 Regular backup of the server hard disk

S 6.26 Regular backup of PBX configuration data

S 6.27 Backup of the CMOS RAM

S 6.28 Agreement on the delivery deadlines for "vital" PBX units

S 6.29 PBX base line for emergency calls

S 6.30 Emergency circuit

S 6.31 Procedural patterns following a loss of system integrity

S 6.32 Regular data backup

S 6.33 Development of a data backup policy

S 6.34 Determining the factors influencing data backup

S 6.35 Stipulating data backup procedures

S 6.36 Stipulating a minimal data backup policy

S 6.37 Documenting data backup procedures

S 6.38 Back-up copies of transferred data

S 6.39 Listing dealerships for re-procurement of fax products

S 6.40 Regular battery checks/replacements

S 6.41 Training data reconstruction

S 6.42 Creating start-up disks for Windows NT

S 6.43 Use of redundant Windows NT servers

S 6.44 Data back-up under Windows NT

S 6.45 Data backup under Windows 95

S 6.46 Creating a start-up disk for Windows 95

S 6.47 Storage of backup copies as part of telecommuting

S 6.48 Procedures in case of a loss of database integrity

S 6.49 Data backup in a database

S 6.50 Archiving database

S 6.51 Restoring a database

S 6.52 Regular backup of configuration data of active network components

S 6.53 Redundant arrangement of network components

S 6.54 Procedures in case of a loss of network integrity

S 6.55 Reduction of restart times for Novell Netware servers

S 6.56 Data backup when using cryptographic procedures

S 6.57 Creation of an emergency plan for the failure of the management system

S 6.58 Establishment of a management system for handling security incidents

S 6.59 Specification of responsibilities for dealing with security incidents

S 6.60 Procedural rules and reporting channels for security incidents

S 6.61 Escalation strategy for security incidents

S 6.62 Specifying priorities for handling security incidents

S 6.63 Investigation and assessment of a security incident

S 6.64 Remedial action in connection with security incidents

S 6.65 Notification of parties affected

S 6.66 Evaluation of security incidents

S 6.67 Use of detection measures for security incidents

S 6.68 Testing the effectiveness of the management system for the handling of security incidents

S 6.69 Contingency planning and operational reliability of fax servers

S 6.70 Creation of a contingency plan for failure of the RAS system

S 6.71 Data backup for a mobile IT system

S 6.72 Precautions relating to mobile phone failures

S 6.1 Development of a survey of availability requirements

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Staff responsible for the individual IT applications

The availability requirements are to be identified for the IT applications run on an IT system and for their data. Since an IT application does not necessarily require each element of the IT system, the availability requirements of IT applications are to be mapped onto the essential components of the given IT system. The result of this activity can be represented in the form of a survey covering the following:

IT-System	**IT component**	**IT procedure**	**tolerable down-time**
central system	host	travel allowance	5 man-days
		accounting	**3 hours**
	data transmission	E-Mail	3 man-days
		accounting	**1 man-day**
	printer	travel allowance	10 man-days
		accounting	2 man-days
		applications planning	**1 man-day**
LAN	Servers	data acquisition	1 man-day
		control station	**4 hours**
	PC	data acquisition	10 man-days
	PC	control station	**4 hours**

(Reading: The IT component "*host*" in the IT system "*central system*" has a maximum tolerable down-time of "*3 hours*" due to the "*accounting*".)

A practicable approach is to ask the procedures officer about the tolerable down-times of the used IT components with regard to the various IT applications, in order to list the results by IT system and component in the table.

Such a survey makes it easier to extract those components of the IT system which are particularly time-critical and for which contingency planning is indispensable. In addition, this survey provides information about the affected IT applications and their availability requirements in case of the failure of any one of the components.

The users and/or customer departments/specialised divisions must provide the rationale for such availability requirements. This must be done at this stage

unless it has already been done elsewhere. The availability requirements must be confirmed by the agency/company management.

In case of failure of a component of the IT system, this survey makes it possible to establish quickly from when an emergency exists. The fact than an emergency need not necessarily occur even in the case of the failure of a particularly time-critical component, can be established on the basis of the *replacement procurement plan* (S 6.14 *Replacement procurement plan*) and of the *study of internally and externally available alternatives* (S 6.6 *Study of internally and externally available alternatives*).

Additional controls:

- Do availability requirements, provided with a rationale, exist for each IT application?
- Do these availability requirements tally with the actual status regarding procedures? When was the last up-dating of the table?

S 6.2 Definition of "emergency", person-in-charge in an "emergency"

Initiation responsibility: Agency/company management; IT Security Management

Implementation responsibility: Agency/company management; IT Security Management

However, not every partial or complete failure of the system constitutes an emergency. Often, failures of the IT system can be remedied by planned measures, e.g. replacement procurement, even within a short time. An emergency will arise only when a state has been reached where restoration of availability could not be achieved within the required time (see S 6.1 *Development of a survey of availability requirements*) and this would result in very significant damage. As soon as an incident occurs which could give rise to an emergency, the necessary steps, leading to a reduction in damage, should be taken.

A person-in-charge should be appointed to provide authorised and timely instructions to introduce contingency measures . The agency/company management must authorise the person-in-charge to both take the decision as to whether an emergency situation has occurred. and to initiate the necessary contingency measures.

Additional controls:

- Who is authorised to determine the existence of an emergency?

S 6.3 Development of an Emergency Procedure Manual

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section; staff responsible for the individual IT applications

A *Contingency Manual* should contain all measures to be taken after an emergency situation arises and all other relevant information. This Manual must be organised in such a way that an expert third person will be in a position to carry out the respective contingency measures.

By way of example, a comprehensive table of contents of a Contingency Manual is provided in the following for orientation. Which parts of this proposal are taken over depends on the existing system and application documentation and can thus only be decided on an individual basis.

TABLE OF CONTENTS - CONTINGENCY MANUAL

Part A: Immediate Measures

1 Warning in an Emergency

1.1 Alert plan and reporting channels
1.2 Lists of the addresses of the staff members concerned
1.3 Determination of specific tasks for individual persons/functions in an emergency
1.4 Emergency Call Numbers
(e.g. fire department, police, doctor, water and power utility, alternate computer centre, external data-media archive, external telecommunications supplier)

2 Instructions on Actions to be taken as regards Special Incidents

2.1 Fire
2.2 Ingress of water
2.3 Power failure
2.4 Failure of the air-conditioning system
2.5 Explosion
2.6 Sabotage
2.7 Failure of data transmission facilities
2.8 Unauthorised entry into a building
2.9 Vandalism
2.10 Bomb threat
2.11 Strikes/Demonstrations
2.12 .....

Part B: Contigency Provisions

3 General Regulations for an Actual Emergency

3.1 Staff responsible for emergency preparedness(contingency planning)

3.2 Designation of the organisational units involved in the implementation of contingency plans; division of responsibilities

3.3 Organisational guidelines; rules of conduct

4 Table of Availability Requirements

Part C: Post-Incident Recovery Plans for Critical Components

5 Recovery Plans

5.1 Post-incident recovery plan for Component 1 (e.g. host)

5.1.1 Replacement options

5.1.2 Internally/externally available alternatives

5.1.3 Data transmission provision

5.1.4 Restricted IT operation

5.1.5 Post-incident recovery procedure

5.2 Post-incident recovery plan for Component 2 (e.g. printer)

...

Part D: Documentation

6 Description of the IT Systems

6.1 Description of the IT system A (outline)

6.1.1 Description of hardware components

6.1.2 Description of software components

6.1.2.1 Inventory of system software

6.1.2.2 Inventory of the system data belonging to the IT system

6.1.3 Description of the network connections of the IT system

6.1.4 Description of the IT applications

6.1.4.1 Inventory of the application software

6.1.4.2 Inventory of the system data belonging to the IT application

6.1.4.3 Capacity requirements of individual IT applications in normal situations

6.1.4.4 Minimum capacity requirements of IT applications for an emergency

6.1.4.5 Restart procedures of the IT applications

6.1.5 Data backup policy

6.1.6 Description of required infrastructure

6.1.7 Other documentation (manuals, etc.)

6.2 Description of the IT system B

...

7 Important Information

7.1 Replacement procurement plan

7.2 List of manufacturers and suppliers

7.3 List of service companies in the area of "redevelopment"

Date of last change _____

The Contingency Manual is to be enforced by the agency/company management and must be up-dated when required. Availability of the Emergency Procedure Manual is of critical importance. Therefore, a copy of the most recent edition must be deposited and held externally. A copy must also be submitted to every person and organisational unit mentioned in the Manual.

(The detailed contents of important items can be inferred from the following description of measures.)

Additional controls:

- Is the contingency manual up-to-date?
- Is consideration given to all possible emergencies?

S 6.4 Documentation on the capacity requirements of IT applications

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section; staff responsible for the individual IT applications

As regards internally and externally available alternatives to IT applications, the relevant capacity requirements are to be documented. These include:

- CPU power;
- disk capacities;
- data transmission speed; and
- speed of other hardware components (printer, document reader, etc.)

The capacity requirements of an IT application are to be reviewed to see whether they might be reduced for the duration of an emergency so as to allow restricted IT operations (e.g. reduction of the number of connected terminals). These restricted capacity requirements for an emergency must also be documented and up-dated.

Additional controls:

- Have capacity requirements been established for every IT application?
- Do these capacity requirements tally with the actual status regarding procedures?
- Have the IT applications been reviewed as regards reducing the capacity requirements?

S 6.5 Definition of "restricted IT operation"

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section; staff responsible for the individual IT applications

To provide against possible failure of parts of the IT system, it should be examined whether restricted IT operations are required or feasible. In order to allow as many IT applications as possible in case of restricted IT operations, the capacity requirements of each IT application must be confined to the necessary level (cf. S 6.4 *Documentation on the capacity requirements of IT applications*).

For restricted IT operations, it must be determined which IT application will be operated with what priority. This is to be laid down in writing.

Manual substitute techniques can be a suitable means of reducing the availability requirements of an IT procedure. However, the resources required for the use of a manual alternative technique (forms, paper lists, microfiches) must be kept on hand for this purpose.

Additional controls:

- Have provisions been laid down as to which IT application, with which priority, will have to be carried out during restricted IT operations?
- Have the qualitative and quantitative predefined conditions for restricted IT operations been agreed upon with the respective specialised units?

S 6.6 Study of internally and externally available alternatives

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Staff responsible for the individual IT applications

In order to avoid capacity shortfalls during restricted IT operations, internally and externally available alternatives must be explored.

When studying such alternatives, particular consideration must be given to the technical specifications of the alternative IT system. The compatibility and sufficient capacity (cf. S 6.4 *Documentation on the capacity requirements of IT applications*) of the alternative IT system are the basic prerequisites for its use.

The primary objective is the internal transfer of IT applications from one IT system to another (e.g. recourse to the development computer in case of failure of the production computer). External alternatives will have to be relied on when it is no longer possible to meet the availability requirements in an economically feasible way.

Alternatives for non IT-specific components should also be considered. In the infrastructure domain, for instance, consideration is to be given to alternatives regarding IT rooms.

Additional controls:

- Have internally and externally available alternatives been checked for their effectiveness?
- Are the configuration, capacity and compatibility of internal and external alternatives being adapted to the current status of procedures?
- Are the integrity and confidentiality of IT application and data moved to external resources ensured in the case of recourse to external alternatives?

S 6.7 Responsibilities in an emergency

Initiation responsibility: Agency/company management

Implementation responsibility: Head of IT Section; Head of Organisational Section; IT Security Management; staff responsible for the individual IT applications

An **emergency organisation** of limited duration may be required for the period following the occurrence of a damaging incident up to the full restoration of availability.

It is necessary to designate individuals who are authorised to determine the existence of an emergency and who can initiate the appropriate measures in the Contingency Manual (cf. S 6.2 *Definition of emergency, person-in-charge in an emergency*). The organisational units involved in the implementation of contingency preparedness measures must be authorised to carry out the tasks entrusted to them under their own responsibility. The regulations required to this end must be laid down in writing. Such an "emergency organigram" (organisational chart) must be approved by the agency/company management.

Additional controls:

- Is a description of the emergency organisation available?
- Are all persons and organisational units stated in the Manual aware of the emergency organisation?
- When was its last up-dating?
- Who co-ordinates which measures?

S 6.8 Alert plan

Initiation responsibility: Agency/company management

Implementation responsibility: Head of IT Section; Head of Organisational Section; IT Security Management; staff responsible for the individual IT applications

An alert plan contains a description of the reporting channel through which the units/individuals concerned are to be notified when an emergency has occurred. The alert can be given, for instance, over the telephone, by fax, by paging systems, or by courier. It must be laid down who notifies whom, who is alternatively to be notified and what action should be taken if this person/unit cannot be contacted. For this purpose, address and telephone lists might have to be kept.

The alert plan must be available to all persons responsible for emergency procedures and, in addition, a redundant copy must be held centrally (e.g. entrance control staff, guards). The individuals listed in the alert plan must be familiar with the part concerning them. All staff members must know the contact persons to whom the occurrence of an incident, which might lead to an emergency, can be reported.

Different alert plans may have been established for different damaging incidents (fire, water, breakdown of data transmission). In that case, care must be taken to cover all types of incidents.

In addition to the compilation of an alert plan, the establishment of an on-duty service should be considered.

Additional controls:

- Is the alert reporting channel being tested sporadically?
- When was the alert plan last reviewed?
- Are all individuals listed in the alert plan still employed in the agency/company?

S 6.9 Contingency plans for selected incidents

Initiation responsibility: Head of IT Section; Head of Organisational Section; IT Security Management; staff responsible for the individual IT applications

Implementation responsibility: Staff responsible for emergency preparedness(contingency planning)

Contingency plans contain instructions on action to be taken and rules of conduct in case of specific damaging incidents. These are incidents jeopardising parts of the IT system which are of vital importance. A contingency plan is aimed at ensuring restoration of availability as quickly as possible.

A contingency plan must also take account of the interaction of a damaging incident and of the respective contingency measure taken. For instance, a fire can be controlled by means of a sprinkler. However, the use of water can, in its turn, give rise to new threats, e.g. to power supply, to data media archives, etc.

Depending on the factors in the operational environment, contingency plans will have to be established to provide against the following incidents:

- fire
- water ingress
- power failure
- failure of the air-conditioning system
- explosion
- breakdown of data transmission (cf. S 6.10)
- sabotage.

The effectiveness of contingency plans is to be verified by means of emergency preparedness exercises (cf. S 6.12).

Additional controls:

- Do contingency plans exist?
- Has the effectiveness of contingency plans been verified?

S 6.10 Contingency plans for breakdown of data transmission

Initiation responsibility: Head of IT Section, IT Security Management,

Staff responsible for the individual IT applications

Implementation responsibility: Staff responsible for emergency preparedness (contingency planning); administrator

The contingency plan for a breakdown of data transmission covers the instructions on actions to be taken in case of any failure of data transmission facilities. In particular, it must be known what internal and external alternatives are available before a definitive decision is made on how to compensate for a system failure.

Possible alternatives are, for instance:

- replacing data transmission by courier-carried exchanges of data media or printed material (cf. Chapter 7.1);
- data transfer viaother data transmission facilities; or
- use of mobile communications facilities (e.g. PAMR, mobile telephony, satellite communication).

Additional controls:

- Has the data transmission capacity required for the use of alternative resources been adequately dimensioned?

S 6.11 Development of a post-incident recovery plan

Initiation responsibility: Head of IT Section; IT Security Management; staff responsible for the individual IT applications

Implementation responsibility: Head of IT Section; staff responsible for emergency preparedness (contingency planning); administrator

In order to ensure correct restart after failure of an IT system, the following information should be documented (see example in S 6.3 *Development of an Emergency Procedure Manual, Part C*).

- Repurchase opportunities, e.g. the use of a test computer for interactive communication or replacement procurement (c.f. S 6.14 *Replacement procurement plan),*
- internal/external alternatives for IT applications should be listed (c.f. S 6.6 *Study of internally and externally available alternatives)*;
- data transmission supply (c.f. S 6.10 *Contingency plans for breakdown of data transmission)* for emergency operation in order to guarantee the minimum data transmission required,
- IT applications in reduced IT operations (c.f. S 6.5 Definition of "restricted IT operation"),
- system start-up of the IT components and inclusion into the IT system,
- In order to meet the availability requirements (cf. S 6.1 *Development of a survey of availability requirements*) of the various IT applications, a sequence for restart of the IT applications must be laid down.

The steps required for restarting an IT application should be shown in the Contingency Manual (c.f. example in S 6.3 *Development of an Emerngency Procedure Manual*, Part D). Such steps include, for example:

- set-up and installation of the required hardware components;
- Loading of the system software
- installation of the application software;
- provision of the necessary data, including configuration files;
- Restarting

Auditable logging of the restart must be ensured.

The feasibility of the post-incident recovery plan is to be checked by emergency preparedness exercises (for both internally and externally available alternatives). When carrying out such tests, particular attention must be given to the exclusive use of the software and data held in internal or external backup archives.

Depending on the size of the used IT applications, restart can be very time-consuming. The times required by the restarting steps can be ascertained with

the help of such emergency routines, and must be taken into account when reviewing the restart plan.

Additional controls:

- Does the post-incident recovery plan meet the requirements of the current IT procedures?
- Has the restart plan been tested?
- Have the time targets for restart been agreed upon with the specialised units?

S 6.12 Emergency preparedness exercises

Initiation responsibility: Agency/company management; IT Security Management

Implementation responsibility: Head of IT Section; staff responsible for emergency preparedness (contingency planning); Administrators

Emergency preparedness exercises serve to check the effectiveness of measures in the field of contingency planning. On the one hand, the effective and smooth execution of a contingency plan will be tested in an emergency preparedness exercise, and on the other hand, previously undiscovered shortcomings will be detected. Typical exercises are:

- alerting exercise;
- conducting fire drills (c.f. S 6.17 *Alert plan and fire drills*);
- functional testing of generators;
- restart after failure of a selected IT component; and
- restoring of data backups.

The results of an emergency preparedness exercise must be documented.

Emergency preparedness exercises are to be held at regular intervals. Since such exercises can have a disruptive effect on normal operations, their frequency should be geared to the threat scenario; however, the pertinent exercises should, as a minimum, be held once a year. Staff training activities (first-aid, fire-fighting, etc.) must be carried out to a necessary extent.

Before an emergency preparedness exercise is held, prior approval must be obtained from the agency/company management.

Additional controls:

- Are emergency preparedness exercises held at regular intervals?
- Do detected shortcomings give rise to a revision of contingency plans?

S 6.13 Development of a data backup plan

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator; staff responsible for the individual IT applications

The data backup plan must enable an expert third person to obtain within reasonable time, and to install, the entire software required for the restart of an IT procedure (operating system software, application software) and the associated data.

A data backup policy must provide information on:

- the storage location of the data during normal operation (disk-memory space allocation table);
- stock of backup data (inventory);
- the time of data saving;
- nature and extent of data backup (logical/physical; partial/full);
- the procedure used for data saving and for reconstruction of backup data;
- the location where the media are kept (indication of any access means required).

The systematic compilation of a data-backup policy as the basis for a data-backup plan is described in Chapter 3.4.

Additional controls:

- Are data backup measures carried out in accordance with the data backup policy?
- Has the possibility to obtain, without delay, the required data media from external data backup stocks been ascertained during emergency preparedness exercises?
- How up-to-date is the existing data backup policy?

S 6.14 Replacement procurement plan

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator; staff responsible for the individual IT applications

In case of the failure of parts of the IT system, in addition to repair, replacement procurement will initially be the most purposive measure to achieve restoration of availability.

In order to expedite the replacement process, it is useful to establish a replacement procurement plan. For each major IT component, this plan must provide information on:

- designation of the IT component (name, device number, date of procurement);
- manufacturer;
- supplier;
- period of delivery; and
- time required for re-installation.

If several manufacturers or suppliers can be named for a given IT component, they are to be listed as alternatives. It may also be possible to include references to other products. In the replacement procurement process, such information is needed for economical resource management.

In addition to restoring the availability of the IT system, advances in information technology must also be taken account of in the context of replacement measures. If used parts of the IT system no longer come up to the best available technology, a replacement procurement activity must not be aimed exclusively at restoring the *status ante quo*. For this purpose, the replacement procurement plan must be regularly revised. Attention must be paid to the interrelations with resources control (cf. S 2.2 *Resources control*).

Additional controls:

- At what intervals are revisions made of the replacement procurement plan?
- In case of changes made to the IT system, will the replacement procurement plan be revised?

S 6.15 Agreements with suppliers

Initiation responsibility: Head of IT Section; Head of Procurement Section

Implementation responsibility: Head of Procurement Section

When purchasing IT products, the IT operator is faced with the need to plan replacement procurement measures. Particularly important points to be considered in the purchasing process are; a guarantee for the supply of replacement goods provided by the manufacturer or supplier; delivery of spare parts, guaranteed periods of delivery, the warranty period in case of any emerging defects, and the support offered.

Contracts of hire, or leasing contracts, must cover provisions for damage-preventing repairs and the requirements regarding the elimination of malfunctions or damage.

As opposed to the purchase of IT products, hiring or leasing of such products already covers provisions by the lessor against a variety of risks. As a rule, a lessor will take out a fire insurance for the rented IT products, which will be partly paid for by the hirer/lessee under the contract of hire. Thus, when renting or leasing IT products, attention must be paid to those items for which no insurance coverage is provided under the contract.

Additional controls:

- Have agreements with suppliers been concluded for central IT components?

S 6.16 Taking out insurance

Initiation responsibility: Agency/company management

Implementation responsibility: Agency/company management

For federal authorities, it is not a common practice to effect insurance.

The remaining risks - which cannot be precluded even in case of sufficient contingency preparedness – can, in part, be covered by insurance policies. The types of insurance can be categorised as follows:

- Property insurance
  - fire insurance
  - pipe water damage insurance
  - burglary insurance
  - installation/disassembly insurance
  - transport insurance
  - data media insurance
  - electronics insurance
- Follow-up costs insurance
  - service interruption (fire) insurance
  - service interruption (machinery) insurance
  - extra costs insurance
  - service interruption (electronics) insurance
- Personal insurance
  - commercial fidelity insurance
  - computer abuse insurance
  - data privacy insurance

S 6.17 Alert plan and fire drills

Initiation responsibility: Agency/company management; site fire protection officer

Implementation responsibility: Site fire protection officer

It is necessary to prepare plans for the measures to be taken in case of fire. Such a plan must lay down, for instance,

- what measures are to be taken against what incidents;
- whether, and how, parts of buildings might have to be evacuated (persons and equipment);
- who must be informed;
- which emergency services must be notified.

The alert plan may be complemented by rules of conduct in case of fire, of which all staff members must be informed. For details, cf. Chapter 3.3 *Contingency Planning*.

However, the best conceivable alert plan will be of little use unless it has been ensured that the listed measures are appropriate and practicable. Thus, the alert plan must be reviewed and up-dated on a continuing basis. One of such review measures is to organise fire drills.

Example:

A fire drill carried out in a 21-storey office building in Bonn in the autumn of 1993 showed that many staff members did not know where to find a fire extinguisher or where the staircase was located. In the actual event, such ignorance can lead to disaster. The fire drill was disregarded by some who, out of indolence, chose not to leave their rooms.

Special importance should be attached, in particular, to fire drills which can protect both IT assets and human lives. Scheduling of such exercises must be co-ordinated in advance with the agency/ company management.

Additional controls:

- What were the results of the last fire drill?

S 6.18 Provision of redundant lines

Initiation responsibility: Head of IT Section; staff responsible for the individual IT applications

Implementation responsibility: Head of Site/Bldg Technical Service; administrator

Redundant wiring means that, apart from the lines used for normal operation, additional lines are provided between appropriate points in the network. Such lines should be run over an alternate route. This will make it possible to switch to a redundant line in case of malfunction. Such switching can be effected automatically or manually. Automatic switching must be indicated to a unit which will arrange for fault clearing on the normal line.

The working order of redundant lines must be tested by their actual use at reasonable intervals. Dimensioning, test intervals and the basic need for redundant lines depend directly on the availability requirements of the network. Similarly, account must be taken of the relation between the activation time of the redundant line and the recovery time of the normal line. When answering such questions, it is crucial to know whether the lines are operated by the public sector (*TELEKOM*) or by the private sector.

- As regards public-sector lines, the user has no influence on their protection. The public network generally provides a sufficient number of redundant lines. In most instances it will suffice, in case of failure of a line (either a fixed connection or a switched line), to restore the connection by setting up a switched line. Provision of redundant fixed connections is usually too expensive and, in most cases, is not absolutely required.
- In a private network, the operator can significantly influence the security of lines. In most cases, cost considerations result in no redundant lines being provided. In private networks, however, redundant lines entail no current expenditure in addition to the cost of production.

S 6.19 Data backup on PCs

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-users

The requirements of S 6.32 *Regular data backup* should generally be observed. The following example demonstrates effective data backup on a PC.

Under the *three-generations principle* (three different data backups are made before the first is overwritten), all application data and the configuration data of the used software is saved at weekly intervals on externally storable or externally held data media (floppy disks, removable hard disks, streamer tapes, server). If the data stock to be saved is too voluminous, data backup can be confined to files whose content has changed since the last data backup (incremental backup). However, it is still necessary to back up the entire data stock (full backup) every third data backup.

Data backup must be documented; as a minimum, the designation of the data medium and the date of the backup should be recorded. the name of the data medium and the date of the backup is to be recorded, for instance: "*BP940518*" = **b**acku**p** of **18.05.94**. In addition, the parameters selected for data backup must be documented (for documentation, cf. S 2.24 *Introduction of a PC Checklist Booklet*).

Data backup must comply with any established data backup policy (cf. S 6.13 *Development of a data backup policy*).

If no products are available for easy data backup, system applications such as the DOS command *BACKUP* can be used. If the program used allows the data backup to be password-protected, use should be made of this option. In this case, the password must then be deposited safely (cf. S 2.22 *Depositing of passwords*).

Additional controls:

- Is all computer data backed up?
- Are completed data backups documented?
- Does the data backup procedure comply with existing data backup policy?

Note: this safeguard is no longer used by any of the components covered in the IT Baseline Protection Manual. The contents of this safeguard have already been added to the text for S 6.32 *Regular data backups.*

S 6.20 Appropriate storage of backup data media

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

Special requirements apply as regards storage of backup data media:

- Only authorised persons may have access to these data media so as to prevent purloining.
- Sufficient speed of access must be ensured in case of need.
- As a safeguard in case of disaster, data backup media must be physically separated from the computer and, where possible, be held in a different fire lobby.

Attention must also be paid to the requirements entailed by S 2.3 *Data media control*.

Additional controls:

- Where are the data media of the data backups for each computer held?

S 6.21 Backup copy of the software used

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

Backup copies of the original data media of standard (purchased) software and/or of the original versions of individual software must be made from which the respective software can be replayed in case of need. The original data media and the backup copies must be kept in different places. It must be ensured that the physical write-protect feature of the data media will prevent unintentional deletion or overwriting of the data.

In case the software is provided on CD-ROM, a backup copy should alternatively be made of the software after installation as the data contained on the CD ROM is generally too comprehensive.

Any unauthorised access, e.g. for the purpose of pirating, must be ruled out.

Additional controls:

- Have backup copies been made of the software used?
- Is storage of the data media sufficiently secure?

S 6.22 Sporadic checks of the restorability of backups

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

For reconstruction of a data stock, the feasibility of achieving this objective by means of the existing backup copies of such data must be established. On account of technical defects, wrong parameterisation, inadequate data media management or non-compliance with the regulations prescribed under a data backup policy, it can happen that reconstruction of a data stock will not be possible. Therefore, sporadic checks are required to see whether the produced data backups can be used for the restoration of lost data.

Additional controls:

- When was a check last made to ascertain whether backed-up data can be reconstructed?

S 6.23 Procedures in the event of computer virus infection

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

If there is reason to assume that a computer has been infected by viruses (e.g. longer program files, inexplicable system behaviour, untraceable files, modified file contents, continuous reduction of storage space although no data has been saved), the following steps are to be taken for virus detection and subsequent eradication:

1. Keep calm.
2. If possible, call upon an expert attending to PCs for help.
3. Close the current programs and switch the computer off.
4. Insert a flawless, write-protected system floppy disk (the emergency floppy disk, see S 6.24 *PC emergency floppy disk*) in drive A.
5. Boot the computer from this diskette (if required, first change the booting sequence in the CMOS setup, cf. S 4.84 *Use of BIOS security mechanisms*).
6. Check the computer with a current virus scanning program to establish whether the computer has been affected by a virus and if so, which computer virus it is.
7. Eliminate the virus depending on the virus type involved (if any problems are encountered, you can use the BSI *virus hotline*, tel. ++49+0228/9582-444).
8. Check the hard disk again with the virus detection program.
9. Check all other data media (floppy disks, removable hard disks) for virus infections and clean them if required.
10. Try to establish the source of the virus. If the source can be traced to original data media, the manufacturer should be informed. If the source is a files or e-mail, the person who created the file should be informed.
11. Warn all other IT users who have exchanged data with the infected computer.
12. Send a virus report to BSI (report form is contained in the appendix)

Should the virus have deleted or modified any of your data, try to reconstruct those data from the data backups (cf. S 6.32 *Regular data backup*) and the programs from their backup copies (cf. S 6.21 *Backup copy of the software used*). Then Step 8 should be repeated once more.

Additional controls:

- Are all affected staff members informed of these rules of conduct?
- Are there expert persons who, in case of need, are able to carry out the aforementioned steps?

S 6.24 PC emergency floppy disk

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

At the time of the initial installation of an IT system, an emergency floppy disk (or other suitable type of data medium) should be produced which, in case of failure of a hard disk, can be used for starting the system or, in case of virus infection, for generating a controlled system state.

An emergency diskette for a DOS PC should be formatted as a system floppy disk (DOS command FORMAT A: /S). Subsequently, if sufficient storage space is available, the following programs should be saved on it: the German keyboard driver KEYB.COM as well as KEYBOARD.SYS, COUNTRY.SYS, HIMEM.SYS and the programs FORMAT.EXE, SYS.COM, FDISK.EXE, CHKDSK.EXE, MEM.EXE and DEBUG.EXE.

Appropriate AUTOEXEC.BAT and CONFIG.SYS files should be generated on the floppy disk. These files should provide the usual keyboard layout and DOS prompt. It should be ensured that all path names refer to the floppy disk. Programs must not be loaded from the hard disk (the path names must not contain C:)

The floppy disk should also contain a text editor. The availability of the used backup program must also be ensured. If the storage capacity is exceeded, a second floppy disk can be used. If the hard disk is compressed, an appropriate driver must be found on the emergency floppy disk in order to be able to access the hard disk.

In addition to the operating system files, the emergency floppy disk can also contain auxiliary programs for determining errors and repairing possible defects. It is also an advantage if the files of the system configuration are available. These should be recorded in writing, for example in a PC Checklist Booklet as described in S 2.24 *Introduction of a PC Checklist booklet*, or be available on data media. For this purpose, there are various programs which read the main configuration data of a PC. Then, if data is interfered with, it can easily be compared to the data saved earlier and corrected if necessary.

The completed emergency floppy disk should be checked for computer viruses using an up-to-data virus scanning program then write protected.

Whenever an operating system is changed (e.g. to a more recent version), a new emergency floppy disk must be created immediately. So that the hard disk can be accessed without problems, the version of the operating system must correspond to the version of the computer concerned. Depending on the operating system, system-specific aspects must also be taken into account (see, for example, S 6.46 *Creating an emergency floppy disk for Windows 95* or S 6.42 *Creating start-up floppy disks for Windows NT*).

If the emergency floppy disk is available to the expert attending to the PCs, this will facilitate his work, especially as regards eradication of computer viruses.

Additional controls:

- Has an emergency floppy disk been produced for every employed computer type and/or every employed operating system?
- Has immediate access to this floppy disk been ensured?

S 6.25 Regular backup of the server hard disk

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

High standards must be set as regards the availability of the data stored on the hard disk of the server since, as a rule, these data are accessed by many users. Regular data backups must provide for reconstruction of all data on the server hard disk which, for instance, are not older than one day (cf. also S 6.32 *Regular data backup*).

A possible data backup policy is to backup data daily on an incremental basis (i.e. all modified data) and to make a complete backup once a week or once a month. As a minimum, the *three-generations principle* should be applied (three subsequent data backups are made before overwriting the first).

Documentation must be provided on all backups. As a minimum, the designation (as telling as possible) of the storage medium, the date and the type of data backup (incremental, complete) must be recorded.

Additional controls:

- Have the latest possible backups been made of all data on the hard disk of the server?
- Are generated data backups being documented?
- Is the backup process in conformity with the data backup policy, where established (cf. S 6.13 *Development of a data backup policy*)?

S 6.26 Regular backup of PBX configuration data

Initiation responsibility: PBX officer

Implementation responsibility: Administrators

Regular backups must be made of the data stored in the PBX (telecommunications facility). This can be done by means of an internal or external tape drive. The backup cycle decisively depends on the number of the executed administration processes. As an example of a reasonable frequency, data backup after approx. 50 administration activities can be assumed. On the basis of the very common rate of one change per subscriber and year, a resultant backup cycle of one month can be established for 600 subscribers. In addition to these regular backups, data should also be saved after any fundamental changes have been made.

Additional controls:

- Are regular data backups made?
- Can the PBX (telecommunications facility) be started-up correctly by using the existing data backups?
- Have appropriate tests already been carried out?
- Are the backup tapes held in safe storage?

S 6.27 Backup of the CMOS RAM

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: Administrator, IT users

Normally, users of AT bus disks must manually enter the number of heads, sectors and cylinders of their hard disk in the set-up. Manuals very seldom contain such information; therefore it should, in any case, be recorded in writing after every change (e.g. in the PC Checklist Booklet, S 2.24 *Introduction of a PC Checklist Booklet*) or saved on diskette by means of an appropriate program.

Additional controls:

- Have entries in the CMOS RAM of a computer been recorded in writing?

S 6.28 Agreement on the delivery deadlines for "vital" PBX units

Initiation responsibility: PBX officer

Implementation responsibility: PBX officer

Vital elements, such as CPUs, digital switching networks, etc. should, even where redundancy has been provided, be available for delivery within a sufficiently short period of time or should be kept in store. From time to time. redundant modules should be exchanged for the active ones.

Additional controls:

- Which of your units are "vital"?
- Has redundancy been provided?
- Are regular checks made of the working order of the reserve units?
- What are the delivery lead-times for vital units?

S 6.29 PBX base line for emergency calls

Initiation responsibility: PBX officer

Implementation responsibility: Administrators

In case of a complete or partial breakdown of the PBX, it may happen that communication is no longer possible over the direct-exchange lines connected to that PBX. In order to be able to obtain help nevertheless, it is useful to set up an entirely separate base line or a similar subscriber line.

Additional controls:

- How can emergency calls be passed on in case of PBX failure?

S 6.30 Emergency circuit

Initiation responsibility: Agency/company management; staff responsible for emergency preparedness (contingency planning); PBX officer

Implementation responsibility: Administrators

In order to have lines available for the initiation of measures in emergencies, a feature offered by some PBXs (telecommunications facilities) is to allocate, by means of a so-called emergency circuit, the existing incoming and outgoing lines to predetermined terminals. This ensures that essential institutions will, in case of emergency, retain their capacity to act. Use should be made of this option wherever it is available.

Additional controls:

- Is the allocation of lines for emergency circuit updated?
- Is activation of the emergency circuit defined in the Contingency Manual?
- Has the use of lines been designated in the Contingency Manual?

S 6.31 Procedural patterns following a loss of system integrity

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: Administrator, IT users

Misuse

If a UNIX system starts behaving in an unexpected manner (e.g. undefined system behaviour, data gone missing, modified file contents, steady reduction of storage space although no data has been saved), a loss of integrity may have occurred. This can result from misuse of the system, for example, as a result of changes to the system settings, import of a Trojan horse or a computer virus.

Users should observe the following procedure in this case:

Do not panic!

- Keep calm.
- Notify the Administrator.
- Exit the current programs.

The Administrator must take the following steps:

- Shut down the system.
- Start up the system so that it can only be accessed from the console (e.g. single-user mode).

Complete data backup

- Take a complete backup (this can be helpful if data or tracks are destroyed in the subsequent investigation).

Check executable files

- Check the executable files for visible modifications, e.g. creation date and file size (as an aggressor could reset these to their original values, the integrity of the files should be checked with checksum procedures, such as *tripwire*).

Reload original files

- Deletion of the executable files and play-back of the original files from write-protected data media (cf. S 6.21 *Backup copy of the software used*). (Programs from data backups must not be replayed).
- Check and, if necessary, reload the system directories and files and their attributes (e.g. */etc/inetd.conf*, */etc/hosts.equiv*, *cron*- and *at*-jobs, etc.),

Check attributes

- Check the attributes of all user directories and files, e.g. using checksum procedures like *tripwire*, and if necessary reset to minimal settings (i.e. rights confined to file owner, no *root* files in user domains, *rhost* and *.forward* files, also blocked accounts).
- Change all the passwords.
- Ask users to check their domains for irregularities.

Generate new passwords using randomisation

Once all the passwords have been changed, they must be notified to the users concerned. **No** password or password derivation scheme which is known to all the users should be used here. It is better to generate the passwords randomly and notify the users by a reliable route, e.g. in sealed envelopes. These passwords should be changed immediately after logging on for the first time.

Implement alarm plan

If there are signs of a deliberate attack on a UNIX system, it is essential to act immediately in order to minimise the damage and prevent further damage from occurring. This requires that there is an alarm plan which lists the steps to be implemented and specifies who should be informed of the incident (see also S 6.60 *Procedural rules and reporting channels for security incidents*). The alarm plan should also specify whether and how the Data Privacy Officer and the legal department should be involved.

In case of problems, you can use the BSI hotline, tel. +49 228/-9582-444 or e-mail *cert@bsi.de*.

Any data which has been deleted or undergone undesired modification can be restored from the data backups.

Additional controls:

- Are the users regularly advised of the requirement to inform the Administrator at once in case of irregularities?
- Are these procedures actually followed?
- Do the Administrators have the required expertise?
- Has a procedure for the rapid assignment of passwords been established and tested?

S 6.32 Regular data backup

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: Administrator, IT users

Develop data backup policy

To avoid irretrievable losses of data, regular backups must be made. In most computer systems this can be largely automated. Procedures must be defined as to what data is saved by whom at what intervals. Development of a data backup policy is recommended.

Depending on the volume and importance of the data generated and with due regard to the possible damage in case of loss of such data, the following must be specified:

- Intervals

  Examples daily, weekly, monthly (depending on the data quantities).

- Time

  Examples at night, on Friday evening.

- Number of generations to be kept

  Example: in case of daily full backup, the last seven backups will be kept, as well as the Friday evening backups of the past two months.

- Extent of data to be saved

  The simplest approach is to define partitions or directories to be covered by regular data backup; appropriate differentiation can make it easier to obtain an overview and help to save effort and cost.

  Example: self-made files and individual configuration files.

- Data media

  Examples tapes, cartridges, floppy disks, mirroring on 2nd hard disk.

- Prior wiping of data media prior to reuse (tapes, cassettes).

- Implementation responsibility (Administrator, user).

- Responsibility for monitoring the backup activities, especially in the case of automatic backup (error messages, remaining storage capacity of data media).

- Documentation on backups (date, type of backup procedure / selected parameters; labelling of data media).

Incremental backups

In view of the large amount of time and effort involved, it is generally possible only to make one full backup per day, at the most. It is not possible to restore the data generated after the last backup. For this reason and to reduce costs, incremental backups, whereby only the data newly generated since the last full backup is saved, should be made at regular intervals between full backups. (If several incremental backups are made between two full backups, it is also possible to back up only the data generated after the last incremental backup.)

Incremental backups can be made more frequently, e.g. immediately after the set-up of important files or several times per day. Compatibility with current operations must be ensured.

As regards the software used, it will, as a rule, suffice to keep the original data media and their backup copies. It will then not be necessary to include such software in regular backup arrangements.

Inform users

All users should be informed of the data backup procedures so that they are able to point out any deficiencies (e.g. intervals too short for their requirements) or to take supplementary measures on an individual basis (e.g. interim mirroring of essential data on their own disks). It is also important to inform users as to the length of time for which data is kept and is therefore available should it need to be restored. If, for example, only two generations are retained in a system where a full backup is taken once a week, then, depending on the point of time at which the loss occurs, it will only be possible to restore lost data which is a maximum of two to three weeks old.

If, in the case of networked computers, backups are made only of the server disks, steps must be taken to ensure that the data to be saved is regularly transferred to those disks either by the users or else automatically.

Encryption of confidential data

Confidential data should if possible be encrypted prior to backup. Care should be taken here to ensure that decryption of the data will still be possible after an extended period (see S 6.56 *Data backup when using cryptographic procedures*).

Hard copy printouts of data are not considered an appropriate means of data backup.

Additional controls:

- Is all computer data backed up?
- Are completed data backups documented?
- Does the data backup procedure comply with existing data backup policy?

S 6.33 Development of a data backup policy

Initiation responsibility: IT Security Management

Implementation responsibility: Head of IT Section; IT Security Management; staff responsible for the individual IT applications

The procedure of data backup is determined by a large number of factors, including the IT system, volume of data, frequency of modification of the data, and requirements concerning availability. The data backup policy attempts to find a solution which takes these factors, as well as profitability, into account.

There are numerous technical possibilities of data backup. However, their selection is always determined by the aforementioned factors. For this reason, the decisive parameters of the IT system and their related applications need to be determined first and documented clearly. Subsequently, a suitable procedure must be developed and documented. Finally, the procedure must be implemented by the agency/company management.

In order to ensure that the data-backup system functions correctly, the data backup policy must involve the restorability of data by means of practical exercises (c.f. S 6.41 *Training data reconstruction*)

The results should be listed as part of the data backup policy, and updated according to requirement. An example of a data backup policy is shown in the following table of contents:

Table of contents - Data Backup Policy

1. Definitions

- Application data, system data, software, protocol data
- Full backup, incremental backup

2. Threat scenario as motivational background

- Dependence of the institution on the data stock
- Typical threats like usage by untrained personnel, joint usage of data stocks, computer viruses, hackers, power failure, hard disk errors.
- Causes of damage specific to individual institutions
- In-house cases of damage

3. Influential factors of an IT system

- Specifying the data to be backed up
- Data availability requirements of the IT applications
- Effort required for data reconstruction without data backup
- Data volumes
- Modification volumes
- Modification times

- Deadlines
- Confidentiality requirements
- Integrity requirements
- Knowledge and data-processing competence of IT users

4. Data backup plan for an IT system

4.1 Specifications for each type of data

- Type of data backup
- Frequency and times of data backup
- Number of generations
- Data backup medium
- Responsibility for data backup
- Storage location for backup copies
- Requirements concerning the data backup archive
- Transport modes
- Reconstruction times for the existing data backup system

4.2 Determining procedures of data restoration

4.3 Basic requirements for the data backup archive

- Contractual terms (for external archives)
- Refresh cycles for data backup
- Inventory listing
- Erasing data backups
- Destroying useless data media

4.4 Store of operational reading devices

5. Minimal data backup policy

6. Employees' commitment to data backup

7. Periodic restoration exercises

Individual items of this data backup policy are described more closely in the S 6.34 *Determining the factors influencing data backup*, S 6.35 *Stipulating data backup procedures*, S 6.37 *Documenting generated data backups*, S 6.41 *Training data reconstruction*, S 2.41 *Employees' commitment to data backup*, so that the processing of these measures results in the realisation of the essential aspects of a user-oriented data backup policy for individual IT systems.

Additional controls:

- Is a data backup policy for the institute documented and updated?
- Are all relevant IT systems included in this policy?
- How are staff members informed about the sections of the concept which are applicable to them?
- Is adherence to the concept monitored?
- How are changes in the influencing factors taken into account?

S 6.34 Determining the factors influencing data backup

Initiation responsibility: IT Security Management

Implementation responsibility: Administrator; staff responsible for the individual IT applications

The following influential factors must be determined for each IT system, possibly even for each individual IT application of particular significance. The system administrators and persons-in-charge of the various IT applications can be interviewed for this purpose. The results are to be comprehensibly documented.

The following theoretical example is to demonstrate how the influential factors can be determined in practice. This example involves a server-based LAN with 10 PC's connected as workstations. The IT system is used for processing orders with the help of a database. The application data are stored centrally on the network server.

The following individual items need to be established:

Specifying the data to be backed up

The data stock of the IT system (IT application) required to perform the specialised task must be determined. This includes the application and operational software, system data (e.g. initialisation files, macro definitions, configuration data, text blocks, password files, access-right files), the application data as such and the protocol data (log-ins, security violations, data transmissions).

Sample result 1: Specifying the data to be backed up

IT system: Server-based LAN with 10 connected PC's

Data to be backed-up:

- Software: Network operating system, PC operating systems, word processing software, database software etc. in the form of standard software
- System data:

  On the network server: System-internal settings (e.g. authorisation structure, passwords)

  On the PC's: Initialisation data of the word processing and database software, macro definitions and text blocks
- Application data on the network server: Files of written correspondence, customer database
- Protocol data on the network server: Logs of network activities

Data availability requirements of the IT applications

The availability requirements for the data stated in the first step must now be stipulated. A proven standard here is the maximum permissible downtime (MPD). It specifies the time period during which the specialised task can be performed without the availability of these data and without the need for resorting to backup copies. Consideration must also be given as to whether paper usage would allow short- term continuation of operations without IT support.

Sample result 2: Availability requirements

- Software: MPD 1 day
- System data:

  On the network server: MPD 1 day

  On PC's: MPD 1 week (a PC can be dispensed with for up to one week)
- Application data:

  Files of written correspondence: MPD 1 week

  Customer database: MPD 1 day
- Protocol data: MPD 3 days

Effort required for data reconstruction without data backup

To develop an economically efficient data backup policy, it is necessary to know whether, and how easily, destroyed databases could be reconstructed if backup data were not available. The sources from which the data could be reconstructed should be examined. Examples include documented files, printouts, microfiche, interviews and surveys.

The financial or operational effort required by a data registration crew should be calculated in terms of working days (WD).

Sample result 3: Reconstruction requirement

Software:

Retrieval through purchase and subsequent installation within 24 hours (provided original software is no longer available)

System data:

On the network server: manual reconstruction: 1 WD

On PC's: 1 WD

Application data:

Files of written correspondence: Selective registration on paper: 10 WD; (complete registration of written correspondence is not necessary)

Customer database: Complete registration on paper: 10 WD

Protocol data: Cannot be reconstructed, as no printout on paper is possible

Data volumes

A decisive factor in determining selection of the storage medium is the volume of data to be backed up. The required specification is based purely on the data to be backed up and is stated in megabytes (MB).

Sample result 4: Data volumes

Software: 100 MB

System data:

On the network server: 2 MB

On PC's: 0.3 MB

Application data:

Files of written correspondence: 100 MB

Customer database: 10 MB

Protocol data: 10 MB (weekly check in addition to erasure)

Modification volumes

To establish the frequency of data backup and an adequate backup procedure, the volume of data which is modified over a certain time period must be known. MB/week can conceivably be used as units here. Statements are also necessary as to whether the contents of existing files change or whether new files are generated .

Sample result 5: Modification volumes

Software: An average of 50 MB on version replacement, once a year at most

System data:

On the network server: 0,1 MB/week

On PC's: 0,1 MB/week

Application data:

Files of written correspondence: 1 MB/week generated by new files

Customer database: *10 MB/week generated by changes in the database (the data base can only be saved in its entirety).*

Protocol data: 10 MB/week

Modification times

In some IT applications, data modifications take place only at certain times, e.g. bookkeeping at the end of the month. In such cases, data backup is only useful immediately after these points in time. For this reason, it should be specified as to whether the data to be backed up is modified daily, weekly or at other intervals.

Sample result 6: Modification times

Software: Modification only on a change of version

System data: Frequent modifications

Application data:

Files of written correspondence: Daily modifications

Customer database: Daily modifications

Protocol data: Continuous modifications

Deadlines

It should be clarified as to whether certain deadlines must be observed for the data. This can involve storage or deletion deadlines relating to person-related data. These deadlines must be considered when laying down the data backup policy.

Sample result 7: Deadlines

Software: Storage not necessary

System data: Storage not necessary

Application data:

Files of written correspondence: storage period for accounting documents is six years (§257 HGB), an annual data backup should be stored for this period

Customer database: Storage not necessary; deletion deadlines are to be observed in accordance with Federal Data Privacy Laws (§ 20 and § 35)

Protocol data:

After weekly evaluation of the protocol data, 2 MB must be stored regularly for one year or until checks are conducted by the Data Privacy Officer.

Confidentiality requirements

The confidentiality requirement of a file also applies to any backup copy. When adding backup copies with the same confidentiality requirement on to one data medium, this can result in an increased confidentiality requirement of the data stored. Consequently, specifications must be made as to the confidentiality requirements of the individual data blocks needing backup, as well as the data combinations which have a higher degree of confidentiality than the original data.

Sample result 8: Confidentiality requirements

Software:

Low confidentiality requirement as these are publicly available data, only copyright regulations must be observed

System data:

On the network server: medium-level confidentiality (passwords are stored in the encrypted form)

On PC's: Not confidential

Application data:

Files of written correspondence: Individual files are of medium-level confidentiality; all the data together are of high-level confidentiality

Customer database: High-level confidentiality

Protocol data:

High-level confidentiality (data disclosing personality profiles)

Integrity requirements

Data backups must ensure that data are stored integrally and not modified during the period of storage. The importance of this increases with the integrity requirements of the data in question. The integrity requirements of the data to be backed up must therefore be stated.

Sample result 9: Integrity requirements

Software: The software must meet high integrity requirements

System data:

On the network server: High-level integrity requirements (due to rights administration)

On PC's: High-level integrity requirements

Application data:

Files of written correspondence: Individual files have medium-level integrity requirements

Customer database: High-level integrity requirements

Protocol data:

Before evaluation, these data have high-level integrity requirements; following evaluation, the data still requiring storage have medium-level integrity requirements

Knowledge and data-processing competence of IT users

To determine whether IT users, specially appointed employees or the system administrators are to carry out data backups, the knowledge and data processing capabilities of IT users as well as the tools available to them must be given primary consideration. If the time required by IT users for carrying out data backups is too long, this should be stated.

Sample result 10: Knowledge

Network administrators possess sufficient knowledge to carry out data backups on network servers. IT users of PC's possess sufficient knowledge and competence to independently perform backups of the PC system data.

Additional controls:

- Are system administrators as well as IT users considered during the determination of influential factors?
- How are these stipulations updated?
- Are new requirements incorporated promptly in the updating of the data backup policy?

S 6.35 Stipulating data backup procedures

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management, IT Procedures Officer

The process governing how data backups are to be made is determined by the influential factors set forth in S 6.34 *Determining the factors influencing data backup*. Data backup procedures must be stipulated for every IT system and type of data. If necessary, even individual applications of the IT system should be distinguished should they require different data backup strategies; this is particularly applicable to mainframe computers.

The following methods of making data backups should be considered when determining a backup system:

- Type of data backup
- Frequency and time of the data backup
- Number of generations
- Procedure and storage medium
- Responsibility for data backup
- Storage site
- Requirements concerning the data backup archive
- Transport modes
- Storage modes

The dependency between data backup modes and influential factors is shown in the following table:

	Type of data backup	Frequency and time of data back-up	Number of generations	Procedure and storage medium	Respon-sibility for data back-up	Storage site	Require-ments for backup archive	Transport modes	Storage modes
Availability requirements	X	(X)	X	X	X	X	X	X	
Effort for reconstruction without backup		(X)	X						
Data volumes	X		X	X		X	X	X	
Modification volumes	X	X	X	X					
Modification times	(X)	X						(X)	
Deadlines				X			X		X
Confidentiality requirements				(X)	X		X	X	X
Integrity requirements			(X)	(X)	X		X	X	X
Knowledge of IT users	X			X	X				

X implies direct influence, (X) implies indirect influence

Remarks:

Type of data backup

The following types of data backup are evident:

- **Data mirroring**: With this procedure, copies of data are stored redundantly on several different media. These data media are usually fast, so that duplication of the data media and the required control software result in high costs. The major advantage of data mirroring is that a failure of one of these data media can be counteracted quickly.
- **Full data backup**: With this procedure, all data requiring backup are stored on an additional data medium without consideration as to whether the files have been changed since the last backup. For this reason, full data backup requires a high storage capacity. Its advantage is the simple and quick restoration of data due to the fact that only the relevant files need to be extracted from the last full data backup. If full data backups are carried out infrequently, extensive changes to a file can result in major updating requirements.
- **Incremental data backup**: In contrast to full data backup, this procedure simply stores the files which have been changed since the last (incremental or full) backup. This saves storage capacity and shortens the time required for the data backup. The restoration time for data is generally high, as the relevant files must be extracted from backups made at different stages.

Incremental data backups are always based on full data backups and should be interspersed periodically by full data backups. During restoration, the last full backup is taken as a basis which is then extended with the updates from subsequent, incremental backups.

- **Differential data backup**: This procedure stores only the files that have been changed since the last full data backup. A differential backup requires more memory space than an incremental backup but the files can be restored quicker and easier. For restoration of data, the last full data backup will suffice as will the most recent differential backup. This is not the case with an incremental backup, since under some circumstances many data backups must be read one after the other.

A special form of the above-mentioned data backup strategies is image backup. This procedure backs up the physical sectors of the hard disk instead of the individual files on it. This is a full backup which allows very quick restoration on hard disks of the same type.

Another form of backup is Hierarchic Storage Management (HSM). This primarily involves the profitable utilisation of expensive data media. Depending on the frequency at which they are accessed, files are stored on fast on-line media (hard disks), near-line media (automatic data- media changing systems) or off-line media (magnetic tape). Generally, these HSM systems also allow a combination of incremental and full data backup.

Redundant data storage is allowed by RAID (Redundant Array of Inexpensive Disks) systems. The RAID concept represents the linkage of several hard disks under the command of an array controller. There are various RAID levels, RAID level 1 involving data mirroring.

RAID systems are no replacement for data backups! The do not offer assistance in case of theft or fire. The data stores on RAID systems therefore has to be stored on additional media which have to be sited in different fire lobbies.

To select a suitable and economically efficient data backup strategy, the following factors should be taken into account:

Availability requirements:

If availability requirements are extremely high, data mirroring should be considered. If availability requirements are high, full data backup is preferable to incremental data backup.

Data and modification volumes:

If the modification volume is similar to the data volume (e.g. in the use of a database), the storage capacity saved by incremental data backup is so negligible that full backup should be considered. However, if the modification volume is much smaller than the data volume, the storage capacity saved by incremental data backup is considerable and reduces costs to a large extent.

Data modification times:

Data modification times can have a minor influence on the data backup strategy. If an application requires backup of the entire database at certain

intervals (e.g. daily, weekly, monthly or annual bookkeeping statements), only full backups are recommended for this purpose.

Knowledge of IT users:

Implementing data mirroring requires appropriate knowledge of the system administrator but no previous knowledge of the IT user. A full data backup can be carried out by an IT user with little system knowledge. Compared with full data backup, incremental data backups require much greater familiarity with the system being used.

Frequency and times of data backup

If data is lost (e.g. due to a head crash on the hard disk), all data changes since the last backup must be restored. The shorter the backup intervals, the less the restoration effort in general. At the same time, it must be noted that in addition to regular data backup intervals (daily, weekly, every workday...), event-dependent backup intervals (e.g. after certain transactions or following the execution of certain programs after system modifications) might also be required.

The following factors must be considered during the determination of the frequency and times of data backup:

Availability requirements, reconstruction effort without data backup, modification volumes:

The interval between data backups should be selected so that the restoration time (the restoration time required for modified data which has not been backed up) for the data changed within this period (modification volume) is shorter than the maximum permissible downtime.

Data modification times:

If data are changed to a large extent (e.g. program sequence for salary payments or different software version) or the entire database needs to be made available at certain points in time, it is advisable to carry out a full data backup immediately afterwards. Regular as well as event-dependent intervals need to be stipulated here.

Number of generations

On the one hand, data backups are repeated in short intervals in order to have up-to-date data available, on the other hand, the data backup must guarantee that saved data are stored for as long as possible. If a full data backup is considered as a generation, the number of generations should be determined, as should the time intervals which must be observed between the generations. These requirements are illustrated using the following examples:

- If a file is deleted intentionally or unintentionally, it will no longer be available in later data backups. If it turns out that the deleted file is still required, it can only be restored by using a backup version made before the time of deletion. If such a generation no longer exists, the file must be created again.
- A loss of integrity in a file (e.g. due to a technical failure, inadvertent modification or computer virus) will probably be noticed at a later stage

instead of immediately. The integrity of such files can only be restored using a generation dated earlier than the occurrence of the loss.

- It is always possible for data backups to be carried out incompletely or incorrectly. In such cases, an additional generation often proves to be useful.

For the generation principle to remain useful, a basic condition must be fulfilled, i.e. the time interval between generations must not fall short of a minimum value. Example: an automatic data backup process is disrupted repeatedly; as a result, all existing generations are overwritten successively. This is prevented by overwriting generations only after ensuring that their minimum age has been maintained.

The generation principle is characterised by two values: the minimum age of the oldest generation and the number of available generations. The following applies here:

- The higher the minimum age of the oldest generation, the greater the probability of the existence of a previous version of a file in which a loss of integrity has occurred (including deleted files which would have proved useful later).
- The greater the number of available generations, the higher the degree of updating of the previous version.

However, the number of available generations is directly related to the costs of data backup, as a sufficient number of data media must be available, too. This is because every generation needs separate data media. For reasons of economy, the number of generations must be restricted to an appropriate value.

The parameters of the generation principle are selected in accordance with the following standards:

Data availability and integrity requirements:

The higher the data availability or integrity requirements, the greater the number of generations required to minimise the time needed to recover from a loss of integrity. If file loss or integrity infringement can not be detected until very late, additional quarterly or annual data backups are recommended.

Reconstruction effort without data backup:

If the database is extensive but can be reconstructed without backups, it can be considered as an additional "pseudo generation".

Data volumes:

The higher the volume of data, the higher the costs of maintaining a generation, due to the increased storage requirement. High volumes of data can therefore restrict the number of generations for reasons of economy.

Modification volume:

The higher the modification volume, the shorter the intervals between the generations should be in order to achieve close updating of files and minimum restoration effort.

Procedure and storage medium

Having determined the type of data backup, the frequency and the generation principle, it is now necessary to select the procedure, including appropriate and economically feasible data media. Examples of standard data backup procedures are described in the following:

Example 1: Manual, decentralised data backup on PC's

On non-networked PC's, backups of application data are usually performed manually by IT users as a full backup. Floppy diskettes are used as data media.

Example 2: Manual, central data backup in UNIX systems

For UNIX systems with connected terminals or PC's with terminal emulation, central data backup is advisable due to the central data stock. In such cases, data backup often consists of a combination of weekly full backups, and daily incremental backups, performed manually by the UNIX administrator using streamer tapes.

Example 3: Manual, central data backup in LAN's

In LAN's (Local Area Networks) with connected PC's, data backup is often carried out in that the PC user backs up his application data on a central network server, after which the network administrator backs up these data centrally; this involves weekly full backup and daily incremental backup.

Example 4: Automatic, central data backup on mainframe computers

Similar to example 2, central data backups on mainframe computers consist of a combination of weekly full backups and daily incremental backups. Often, this is done automatically using HSM (Hierarchic Storage Management) tools. For individual IT applications, additional event-dependent full backups are often performed.

Example 5: Automatic, central data backup in distributed systems

Another alternative consists of a combination of examples 3 and 4. The local data of distributed systems are transmitted to a central, mainframe computer or server, where a combination of full and incremental data backups is performed.

Example 6: Fully automatic centralised backup of decentralised data in distributed systems

As opposed to the above example, the transfer from the decentralised to the centralised system is automatic. Tools are now available which allow access from a central data backup server to decentralised data. Data backup can thus be performed centrally for decentralised users.

To minimise the volume of data on the storage medium, data compression algorithms can also be used. They allow the volume of data to be reduced by

up to 80%. When compression is employed for backup, the selected parameters and algorithms must be documented and observed later during data restoration (decompression).

Two parameters must be specified for the backup procedure: the degree of automation and the centralisation (storage location).

There are two degrees of automation: manual and automatic.

- Manual data backup implies manual triggering of the backup procedure. Its advantage is that the operator can individually select the interval of data backup in accordance with the work schedule. Its disadvantage is that the efficiency of data backup depends on the discipline and motivation of the operator. Data backups may not be made due to illness or other reasons for absence.
- Automatic data backups are triggered by a program at certain intervals. Their advantage is that discipline and reliability are not required of the operator if the backup schedule is complete and accurate. Their disadvantage is that the backup program generates costs and the backup schedule must be updated on changes in the work schedule otherwise important changes might not be backed up in time.

There are two degrees of centralisation: central and decentralised data backup.

- Central data backups are characterised by the fact that the storage location and the performance of the data backup are carried out on a central IT system by one operator. This procedure is advantageous in that only the operator requires thorough training and the remaining IT users are relieved of this responsibility. Furthermore, increased centralisation of the database allows more economical usage of data media. The disadvantage is that confidential data might be transferred and disclosed to non-authorised persons.
- Decentralised data backups are performed by IT users without being transferred to a central IT system. Their advantage is that IT users are able to control the information flow and data media, particularly if confidential data are backed up. Their disadvantage is that the consistency of data backup depends on the reliability of the IT user; furthermore, decentralised procedures are more time-consuming for IT users.

Following selection of manual or automatic, central or decentralised data backup, a suitable storage medium must be found for the backup copies. The following parameters can be considered for this:

- **Acquisition time for data media:** The time required for priming data restoration depends on the time required for identifying the data media necessary for backup and making them available to the system. Cassettes in a robot-system can be made available for restoration within a matter of minutes; it may be necessary for stored tapes to first be transported in an elaborate procedure and then cued.
- **Access time, transfer rate:** The time required for actually restoring the data depends on the average time needed to access the data on the storage medium and the rate of data transfer. Hard disks allow access to certain files in a few milliseconds, whereas magnetic tapes must first be wound to

the correct position. When selecting the data medium, it should be noted that the transfer channels must not be overloaded in the case of high transfer rates.

- **Practicability/storage capacity:** The more elaborate a data backup procedure, the greater the risk of it being performed incorrectly or even ignored. Data media with a low storage capacity prevent effective data backup, as their repeated interchange is time-consuming and susceptible to errors.
- **Costs:** The effort of data backup, i.e. the costs of procuring read/write devices and data media as well as the times required for computations and operations, must be commensurate with the importance of the backup. The life and reliability of the data media should also be taken into consideration. On no account must the running cost of data backup exceed the total cost of restoration without backup including the consequential damage.

The following table (1995 version) contains key figures on acquisition costs, access times, transfer times etc. providing a basis for selecting the correct procedure and storage medium.

Storage medium	Capacity (MB)	Cost (DM)	Cost per MB	Average access time in sec.	Data transfer in KB/sec.
A 4 paper	0,002	0,03	15,00	-	-
IDE hard disk HDD 1 GB	1000	400,00	0,400	0,01	3000
SCSI hard disk 4 GB	4000	2000,00	0,500	0,08	6000
3.5" HD floppy	1,44	1,00	0,700	0,10	60
WORM 5.25"	800	700,00	0,870	0,02	6000
Microfilm	0,6	0,50	0,830	10,00	40
MO/ROD 3.5" 5,25"	230 1300	40,00 120,00	0,170 0,090	0,03	read: 3000 write: 1000
CD-WORM	680	15,00	0,022	0,15	300-600
CD-ROM	680	2,00	0,003	0,15	600-1200
Data cartridge QIC DAT	2500 4000	60,00 30,00	0,020 0,008	10,00	200 ... 800
Magnetic removable hard disk	270	100,00	0,370	0,015	2000

Due to the steady drop in the price of data media and continuing technological advances, the above figures can only be used for rough orientation. Currently applicable prices are to be established during the actual selection of the data media.

The following factors are of significance here:

Availability requirements:

The higher the availability requirements, the faster the required access to data media for backup purposes, and the shorter the required time for re-importing the relevant data from the data media.
For reasons of availability, it must be ensured that the data media are still usable for restoration even if a reading device fails. A compatible and fully operational replacement for this reading device must be obtainable at short notice.

Data and modification volumes:

With an increasing data volume, use is generally made of economical, tape-data media like magnetic tapes or cassettes (data cartridges).

Deadlines:

If erasure deadlines are to be maintained (e.g. in the case of person-related data), the selected storage medium must allow this erasure. Data media for which erasure is impossible or difficult (e.g. WORM) should be avoided here.

Data confidentiality and integrity requirements:

If the confidentiality and integrity requirements of the original data are high, the same is applicable to the data media used for backing up this data. If encrypted data backup is not possible, consideration should be given to selecting data media whose design and transport characteristics would allow their storage in appropriate cabinets or safes.

Knowledge of IT users:

The knowledge and data processing capabilities of IT users are instrumental in determining whether the selected procedure should allow IT users to personally and manually perform data backups, whether different, qualified persons should perform decentralised backup, or whether automatic data backup would be more practical.

Responsibility for data backup

One of three groups can be assigned the responsibility to carry out data backups: IT users (usually chosen for decentralised and non-networked systems), system managers or administrators intended specially for data backup. Parties responsible for data backups not performed by IT users must be committed to keeping these data confidential and encryption should be considered.

Persons responsible for organising data restoration must also be appointed, in addition to persons authorised to access backup data media, particularly if

these are archived. Only these authorised persons must be allowed to access these archives. Furthermore, persons authorised to carry out restorations of complete data stocks or selected, individual files must be appointed.

When determining these responsibilities, particular regard must be given to data confidentiality and integrity requirements, as well as the reliability of the employees in question. It must be ensured that the person-in-charge is available at all times and a substitute should be appointed and trained.

The following factor is influential in this context:

Knowledge possessed by IT users:

The knowledge and data processing capabilities of each IT user determine whether these individuals can be charged with the responsibility of carrying out data backups. If the IT user in question does not possess sufficient knowledge, responsibility must be transferred to the system administrator or a qualified person.

Storage site

Data backup media and original data media must always be stored in different fire sections. In the event that data backup media are stored in a different building or off the premises, the probability of backup copies being damaged in a crisis situation is lowered. However, the greater the distance between the data media and the IT periphery required for restoration (e.g. tape station), the longer the potential transport routes and times, and the longer the resulting restoration periods. The following factor is influential in this context:

Availability requirements:

The higher the availability requirements, the more quickly the data media need to be obtained for data backup. If data media with high availability requirements are stored externally for safety reasons, consideration should be given to storing additional backup copies in the immediate vicinity of the IT system.

Data confidentiality and integrity requirements:

The higher these requirements are, the more important it is to prevent data media from being manipulated. The necessary access control can generally be achieved by appropriate infrastructural and organisational measures, see Chapter 4.3.3. *Data Media Archive*

Data volume:

With increasing data volumes, the security of the storage site increases in importance.

Requirements concerning the data backup archive

Due to the concentration of data on backup data media, the degree of confidentiality and integrity of the backed up data is at least as high as that of the original data. Consequently, appropriate IT security measures, e.g. access control, are required for data media stored in a central archive.

In addition, organisational and personnel-related measures should be implemented (data media management) to allow quick and accurate access to

required data media. For this, the measures in S 2.3 *Data media control* and Chapter 4.3.3 *Data media archive* must be observed**.**

The following factors are influential in this context:

Availability requirements:

The higher the availability requirements, the faster the required access to relevant data media. If manual inventory-keeping does not fulfil the availability requirements, automatic access systems (e.g. robotic cassette archives) can be used.

Data volumes:

The data volume decisively determines the number of data media to be stored. Large data volumes require correspondingly large storage capacities of the data archive.

Deadlines:

If erasures deadlines need to be maintained, the data backup archive must be organised appropriately and equipped with the required erasure devices. Erasures are to be executed and documented in the data backup archive by the specified deadlines. In the event that erasure is not technically possible, organisational measures can prevent reuse of files to be erased.

Data confidentiality and integrity requirements:

The higher these requirements are, the more important it is to prevent data media from being manipulated. In general, the access control necessary for this can only be achieved by the infrastructure and organisation-related measures described in Chapter 4.3.3 *Data Media Archive.*

Transport modes

Data are transferred during any backup process. The following must be observed in such situations, irrespective of whether data are being transferred through a network or line, or whether data media are being dispatched to an archive.

Availability requirements:

The higher the availability requirements, the more quickly data need to be obtained for restoration. This is to be considered during the selection of the transmission medium or transport mode.

Data volumes:

If data required for restoration are to be transferred through a network, the selection of the network's transmission capacity must also be based on the data volumes. It must be ensured that the data volumes can be transmitted within the required time periods (availability requirement).

Data modification times:

If data backups are performed through a network (particularly at specified intervals), the data volumes involved can result in congestions during transmission. A sufficient transmission capacity must, therefore, be ensured at the time of data backup.

Data confidentiality and integrity requirements:

The higher these requirements are, the more important it is to prevent data from being intercepted, copied or manipulated by unauthorised persons during transport. Encryption or cryptographic measures against manipulation must be considered for such data transmissions. Secure containers and routes must be selected for physical transport, and the degree and usefulness of encryption procedures should also be evaluated here.

Storage modes

As part of the data backup policy, it must also be established whether storage or erasure deadlines need to be maintained for certain data.

Deadlines:

If storage deadlines need to be maintained, this can be achieved by archiving a data backup generation. In the case of extended storage deadlines, additional consideration must be given to the required inventory of reading devices and the fact that a refresh (renewed import of magnetically stored data) might become necessary, as such media are demagnetised over long periods of time, so that their data content is eventually lost.

If erasure deadlines are to be maintained, appropriate organisation is necessary; availability of the required erasure devices must also be ensured. Erasure is to be initiated and executed at the specified intervals.

Additional controls:

- Are data backup procedures updated in accordance with changes to the IT system?
- Are data restoration exercises carried out periodically?
- Is adherence to the conditions stipulated in the data backup policy being checked?
- Are the persons responsible for data backup sufficiently trained?

S 6.36 Stipulating a minimal data backup policy

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

The minimum requirements which a company/agency needs to fulfil as regards data backup must be determined. This allows universal handling of many cases which would otherwise require extremely detailed investigations and complex data backup policies. It also provides a basis generally applicable to all IT systems, including new ones for which data backup policy have not been prepared yet.

This is demonstrated by the following example:

Minimal data backup policy

Software:

All software, whether purchased or created personally, is to be protected once by means of a full backup.

System data:

System data are to be backed up with at least one generation per month.

Application data:

All application data are to be protected by means of a full backup at least once a month using the three-generation principle.

Protocol data:

All protocol data are to be protected by means of a full backup at least once a month using the three-generation principle.

Additional controls:

- Are all employees, including new ones, instructed on, and committed to, the data backup or minimal data backup policy?
- Is the minimal data backup policy updated?
- Are the operative resources required for minimal data backup available?

S 6.37 Documenting data backup procedures

Initiation responsibility: IT Security Management

Implementation responsibility: Person-in-charge of data backup

A data backup policy must determine how the generated data backups should be documented. Documentation is necessary for orderly and efficient data backup. The following items are to be documented for each generated data backup:

- Date of data backup
- Extent of data backup (files/directories)
- Data media on which the operational data are stored
- Data media on which the backup data are stored
- Data backup hardware and software (with version number)
- Data backup parameters (type of data backup etc.)

The procedure required for data restoration must also be documented. The necessary hardware and software must be described, as must the required parameters and the procedure to be followed for data reconstruction.

Additional controls:

- Are data backups documented to the required degree?
- Can data restoration be performed with the help of the documentation even by a person other than the one who backed up the data?

S 6.38 Back-up copies of transferred data

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

If the data intended for transfer have only been compiled for this purpose, without having been stored on another data medium, a backup copy of this data is required. If the data medium is lost or damaged, the data can be dispatched again easily.

Additional controls:

- Are backup copies required for data intended for exchange?

S 6.39 Listing dealerships for re-procurement of fax products

Initiation responsibility: IT Security Management

Implementation responsibility: Fax Person-In-Charge, Purchase Department

The contingency plan should include a list of specialised dealerships from which new fax machines can be acquired immediately if there is no time for repair work in an emergency situation.

Additional controls:

- Does the contingency plan include a list of dealerships specialising in fax machines?

S 6.40 Regular battery checks/replacements

Initiation responsibility: IT Security Management

Implementation responsibility: IT-user

Batteries and accumulators are discharged in the course of time. Consequently, these sources of energy in the standby power-supply units of answering machines which digitally store incoming or outgoing messages should be replaced regularly. As a rule, such replacements should be performed once a year.

S 6.41 Training data reconstruction

Initiation responsibility: IT Security Management

Implementation responsibility: Person-in-charge of data backup

The restoration of data using data backups must be tested at irregular intervals, at least after every modification to the data backup procedure. It must at least once be proven that complete data restoration is possible (e.g. all data contained in a server). This ensures reliable testing as to whether

- data restoration is possible
- the data backup procedure is practicable
- there is sufficient documentation of the data backup, thus allowing a substitute to carry out the data restoration if necessary
- the time required for the data restoration meets the availability requirements (c.f. S 6.1 *Development of a survey of availability requirements*)

When training for data restoration, the following should also be taken into consideration:

- the data must be installed on an alternative IT system
- different writing/reading equipment is used for the data backup and data restoration

Additional controls:

- Can a specialist carry out the data restoration using the existing documentation?

S 6.42 Creating start-up disks for Windows NT

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: Administrators

For every system operated under Windows NT with a floppy disk drive, a set of repair floppy disks should be kept at hand. For computers with Intel processors, this is contained in the three set-up floppy disks supplied with Windows NT as well as an emergency floppy disk with which the primary set-up status can be reproduced if files are damaged. An emergency floppy disk must be created for every computer as these floppy disks cannot be exchanged between different computers.

During the Windows NT set-up, the user will be asked if he wishes to create an emergency floppy disk. To create an emergency floppy disk, an empty 3½" floppy disk must be placed in drive A: as required. The information necessary to repair the system will be saved on this floppy disk.

Given that no emergency floppy disk was created during installation, this can be carried out afterwards with the service program RDISK (in the Windows System directory *%SystemRoot%\SYSTEM32*, for example *\WINNT\SYSTEM32*). The program must be started with the parameter /s, if the user accounts and access rights should also be stored. However, the selection of this parameter can mean that the backup no longer fits on one floppy disk, if a large number of user profiles are defined on the system concerned. Therefore, the option "*Actualise Emergency Information*" should be selected at first, in order to save the present system state. The actual emergency floppy disk should then be generated with the option "*Create an Emergency diskette*".

Note: This process should be repeated after every change to the system configuration so that the emergency floppy disk always reflects the present system state. Only in this way can it be ensured that new entries in the configuration, drive letter assignment, Stripe Sets, data-media sets and mirroring are observed in the repair information. Otherwise access to certain drives can be impossible after system failures. Creation of the emergency floppy disk should thus be carried out after the next successful system boot-up to ensure that a properly running system is being backed-up.

If no start-up floppy disks are available, they can be created with the Windows NT set-up program (*WINNT* for MS-DOS or Windows 95 set-up and *WINNT32* for Windows NT set-up) found on the Windows NT installation CD by executing the program with the parameter */ox*. The program requires three empty 3½" disks. They must be placed in drive A: and the files necessary to start-up Windows NT will then be copied onto the floppy disks.

If system files, boot variables or the boot sector is damaged and the previous start configuration cannot be reproduced with the method of using the most recently known functional configuration, the repair procedure in the Windows NT set-up must be used to reproduce the previous system state.

For the repair procedure, the Windows NT set-up program requires either the emergency floppy disk or the configuration information which is saved in the

sub-directory REPAIR under the Windows directory *%SystemRoot%*, e.g. under *\WINNT\REPAIR*.

To reproduce a damaged Windows NT installation, the first of the three set-up floppy disks must be placed in drive A: and the computer booted from this drive. In the text window of the set-up program, it will be asked whether Windows NT should be installed or if files should be repaired. The parameter **r** must be entered. The set-up program then requires the emergency floppy disk. If no emergency disk is available, the set-up program shows a list of available Windows NT installations that have been found on the computer and asks which installation should be repaired. Once the final message has been shown, the emergency floppy disk must be removed from drive A: and the computer re-booted.

The repair procedure in the set-up program allows various elements to be selected for repair:

- **System files** - The set-up program checks that the directory tree of Windows NT corresponds with the log file on the emergency floppy disk to ensure that all system files are present and intact. If files are missing or damaged files are found, these will be reproduced from the relevant Windows NT set-up source (e.g. CD-ROM). The set-up program also checks Windows NT files on the system partition to ensure that all boot files are available and intact.
- **Standard system configuration** - The set-up program offers the opportunity to reproduce damaged registry files from those that were initially installed with Windows NT. It must be borne in mind that user accounts and permissions that have been set up since the first installation, or since the last renewal of the emergency floppy disk, are lost.
- **Boot variables** - By choosing this option, the set-up program reproduces the boot variables from the emergency floppy disk for the special installation of Windows NT onto the hard disk
- **Boot sector** (only for computers with x86 processors) - By choosing this option the set-up program creates a new boot sector in the system partition.

If other files are missing or damaged, the set-up program reproduces these files from the appropriate Windows NT set-up floppy disks or from the CD-ROM. If the system partition on a computer with an x86 processor has been mistakenly formatted or changed in such a way that Windows NT no longer starts, the repair program reproduces the original boot configuration.

Note: If the system files are repaired, the set-up program will remove the security settings from these files if they are found on an NTFS partition. This is wise, in order to be able to reverse falsely granted permissions for system files which would otherwise prevent Windows NT from accessing the system files necessary for system start-up. For this reason, it is absolutely necessary to keep the emergency floppy disk and the set-up floppy disks safe in such a way that they are protected against any kind of misuse.

Additional controls:

- Is the information on the emergency floppy disk up-to-date?
- Are repair floppy disks kept under lock and key to avoid possible misuse?
- Has an emergency floppy disk been created for every Windows NT system?

S 6.43 Use of redundant Windows NT servers

Initiation responsibility: Head of IT Section, IT Security management

Implementation responsibility: Administrators

Depending upon the availability requirements of data and applications, a redundancy can be created with an acceptable amount of effort which prevents a total loss of data. According to these requirements, parts of the stored data or the complete data stock can be copied parallel onto several hard disks. If one hard disk then fails, the data is not lost and users can continue working without having to wait for re-installation of a backup.

According to the defined availability requirements, the systems can be laid out in such a way that if a server fails, tasks can be taken over by one or more other servers. However, care must be taken that the common stored data remains consistent; this must also be ensured when single machines fail. In this context considerable differences exist as regards the performance of various redundancy concepts:

- A direct physical redundancy can be attained with RAID disk systems (RAID: Redundant Array of Independent Disks). When choosing this procedure, it must be borne in mind that the physical distance between the single disks of a RAID system is subject to considerable restrictions, so that in case of fire or similar damage, all parallel copies will be damaged to the same extent. RAID systems are, therefore, no substitute for data backup.
- By installing Windows NT clusters, parallel copies of stored data can exist on different disks and under the control of different computers. By using high-performance clusters with up to four servers, the number of server systems can be reduced which in turn leads to a reduction of administrative effort and thus an improvement in security.
- Replication of single directories allows data to be similarly distributed. But there are no synchronisation mechanisms which allow data currently being edited to be consistently copied in parallel. In this case, a failure of the primary disk more or less always leads to considerable loss of data. Implementation of replication services under Windows NT should, therefore, remain restricted to those circumstances in which changes are only made in one place. In any case, this should never be considered as a substitute for a regular data backup.

To prevent failure of server computers, these must be laid out redundantly as required. Many possibilities are available here from which the appropriate alternative must be selected, depending upon the tolerable down time (MTD):

- If the tolerable duration of a failure amounts to half an hour, a separate computer must be made available which takes over the tasks of the failed server. To obtain access to the data of the failed server, its hard disk must be switched over to the substitute computer.
- If failure is only tolerable for a few minutes, a cluster-system should be installed which has access to all hard disks on all computers. The system

must be configured in such a way that, when failure of a server occurs, it automatically switches over to a substitute computer within the system.

- In the extreme case where failures are only tolerable for a number of seconds, installation of a completely redundant fail-safe system is necessary, with multiple CPUs working in parallel. In this case, failure of a CPU or main memory module will not be noticed by the user. This option offers the highest form of security against failure but also requires more effort and greater financial expenditure. Therefore this option will only be selected for extreme availability requirements. At present Windows NT cannot satisfy such requirements. In this case, special systems should be installed that run under other operating systems.

The concrete availability requirements must, in any case, be determined via careful analysis. Within the framework of detailed planning of system and network architecture, an appropriate combination of redundant computers and/or hard disks must be found which fulfil these requirements.

Additional controls:

- Are the current availability requirements of applications and their inter-dependencies known?

S 6.44 Data back-up under Windows NT

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

Under Windows NT, data backup can be carried out with the service program *NTBACKUP.EXE* which is integrated into the system. It must be borne in mind that this program only supports backups onto tape and is not capable of encrypting the backup tapes these must, therefore, be securely stored in a safe place.

When carrying out data backup, the following points must be taken into account:

- Access rights to the Windows System directory *%SysRoot%\SYSTEM32* (usually *\WINNT\SYSTEM32*) are necessary for data backup since NTBACKUP stores temporary and log files there.
- Back-up software is able to back up the registry of the local computer. This should be carried out at regular intervals and after significant changes to the configuration.
- Quarter-inch tapes used for data backup should be wound up properly at regular intervals (after being used approximately 20 times) via the option "*Wind Tape*" to avoid loose sections and possible damage due to abrasion. This safeguard is not necessary for 4 mm (DAT) and 8 mm (Video 8) tapes; the appropriate operation is not available for these tapes.
- When entering the option "*Delete Tape*", "*Secure Deletion*" should be selected if the tape contained valuable data as this will ensure that the old data is overwritten. If this option is not selected, a large portion of the data originally stored on the tape remains available and can be reconstructed without a great deal of effort.
- When carrying out a backup operation the opportunity to create a log-file absolutely must be used. Once the operation is completed, the log-file can be used to check whether all the relevant data was really backed up or if any faults occurred during the backup. The option "*Log all entries*" is recommended, since it can thus also be determined if all relevant data was backed up and whether the directories to be backed up were, in fact, included in the backup.
- When reproducing backed up files, their access protection will also be reproduced, given that the directory into which they are reproduced does not assert any explicit access controls on the files saved therein. If, however, such control is specified in the directory, this then applies to the files and the original access control information is ignored.
- The choice of files and directories to be backed up cannot be saved under the graphic user interface. To regularly back up the same directories, Scripts can be created; these are, however, not designed for file selection.

Due to the restrictions existing in the service program *NTBACKUP.EXE*, additional data backup software should be installed to ensure extensive installation or for high availability requirements. When selecting backup

software of this type, it should be taken into account that the following requirements are satisfied:

- The installed file systems, i.e. FAT, NTFS and, if applicable, HPFS should be supported during backup and restoration.
- It should be possible to allow backup to be executed automatically at pre-determined times, i.e. at pre-set intervals, without the necessity of manual intervention (except possibly for the provision of backup data media).
- It should be possible to inform one or several selected users, via E-Mail or a similar mechanism, of the result of the backup and of any faults.
- The backup software should support securing of the backup medium via a password or, better still, via encryption. Furthermore, it should be able to save the backed up data in compressed form.
- By entering appropriate Include and Exclude lists when selecting files and directories, it should be possible to specify exactly which data ought (and ought not) to be backed up. It should be possible to create backup profiles where the lists can be summarised, saved and re-used for later backups.
- It should be possible to select data to be backed up independent of the date it was created and the last modification.
- The backup software should support the creation of logical and physical full copies as well as incremental copies (backup of changes).
- Back-up should also be possible onto hard disks and network drives.
- The backup software should be able to carry out an automatic comparison after backup between the backed up data and the original. After restoring data, it should be able to carry out a respective comparison between the restored data and the content of the backup data medium.
- When restoring files it should be possible to select whether the files are to be restored into their original location or onto another disk or directory. In the same way it should be possible to control how the software reacts if a file with the same name already exists at the target location. It should be possible to select whether the existing file is to be always, never or only overwritten if it is older than the restored file, or that in this situation an explicit request appears.

Further to the carrying out of normal data backup, it is recommended to back up the current system configuration with the service program *RDISK* after every significant change in the save directory *%SystemRoot%\REPAIR* (e.g. *\WINNT\REPAIR*) as well as on an emergency disk, in order to be able to reproduce this configuration if possible inconsistencies show up (see also S 6.42 *Creating start-up floppy disks for Windows NT*). It must be taken into account that the current security entries in the registry (in the area *SECURITY* and *SAM*) will only be backed up if RDISK is executed with the parameter/**s**. However, the selection of this parameter can mean that the backup no longer fits on one floppy disk, if a large number of user profiles are defined on the system concerned.

A backup of the registry is also possible with the service program *REGBACK.EXE* in the Windows NT Resource Kit; in this case restoration

takes place with the service program *REGREST.EXE* in the Windows NT Resource Kit.

Additional controls:

- Are all computer data backed up?
- Are generated data backups being documented?
- Does the data backup procedure conform to an available data backup policy?

S 6.45 Data backup under Windows 95

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT-user

The requirements of S 6.32 *Regular data backup* should generally be observed. In the following, particular aspects of data backup which must be taken into account under Windows 95 are listed:

When possible under Windows 95, the only backup programs that should be used are those that support long file names (e.g. the Windows 95 program *BACKUP.EXE*). To convert long file names to the conventional 8.3, the supplied program LFNBK.EXE is available. Particular care must be taken when using this program. Possible file names or even single files cannot be reconstructed if, after the backup, changes have been made to the directory structure of the PC from which the backup is being made.

Additional controls:

- Are backup programs being used that cannot process long file names?

S 6.46 Creating a start-up disk for Windows 95

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

An emergency floppy disk should be created for every Windows 95 computer. If system problems then arise, it is possible to restart the computer and restore user-specific profiles where applicable.

For this purpose, on the one hand a system floppy disk is required that can be used to restart all computers; on the other hand a user/computer-specific floppy disk containing the individual settings for the user and for the respective computer.

Creating a system start-up floppy disk

With the register card *START-UP DISK* under the control panel option *SOFTWARE*, a system start-up floppy disk can be created which can be used for all computers. However, a Windows 95 CD is also required. Alternatively, an experienced user can manually copy all the relevant files onto a floppy disk. These include, for example, *COMMAND.COM*, *IO.SYS*, *DRVSPACE.BIN* and *MSDOS.SYS*. In this case the german keyboard driver *KEYB.COM* and *KEYBOARD.SYS*, *COUNTRY.SYS* should also be copied and, if applicable, further system files (e.g. CD-ROM driver). The german keyboard can be set with the command *KEYB GR, KEYBOARD.SYS*. If applicable, an additional floppy disk can be used for other necessary files, e.g. an editor, a program for hard disk compression or backup programs.

Creating user/computer-specific floppy disks

For this purpose a previously formatted floppy disk and the program *EMERGENCY RECOVERY UTILITY (ERU)* will be required, which are supplied with the system. The program is not installed as standard but can be found on the Windows 95 CD-ROM. With the help of this program, the relevant and up-to-date system files can easily be copied onto a floppy disk; in particular the file containing the user settings *USER.DAT* and the file containing the system settings *SYSTEM.DAT*. The files *USER.DAT* and *SYSTEM.DAT* contain respective information which is saved in the *ini*-files under Windows 3.x. This disk should be brought up-to-date if extensive or important changes have been made to the computer configuration or the user settings.

Once a start-up floppy disk and an emergency floppy disk have been created, they should be checked for computer viruses and write-protection should be enabled thereafter.

Using a start-up floppy disk

To boot up with the system floppy disk, it must first be placed in the floppy disk drive, the start sequence in the BIOS prioritised for the floppy disk drive, and the computer restarted. The computer then boots up in line mode.

Using a computer/user-specific floppy disk

If the computer boots up correctly (with or without a start-up floppy disk), but the computer/user-specific files are however damaged, these can be played back with the program *ERD.EXE* which can be found on the computer/user-specific floppy disk. The corresponding data on the hard disk will have been moved into the directory *C:\WINDOWS\ERUNDO* and can, if applicable, be reconstructed with the command *ERD/UNDO*.

Note: It is necessary to start the computer in line mode in order to use the program *ERD.EXE*. This can be attained, for example by booting from the start floppy disk, by selecting *RESTART COMPUTER IN MS-DOS MODE* when quitting Windows 95 or by pressing the F8 key when the computer is booting up when the message "Windows 95 starting up" appears and then selecting option "5. Manual entry only". The latter is only possible if the line **BootKeys=1** is contained in the *MSDOS.SYS* file.

Additional controls:

- Has a start-up floppy disk been created for Windows 95 computers?
- Has a computer/user-specific emergency disk been created for **every** Windows 95 computer?

S 6.47 Storage of backup copies as part of telecommuting

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Telecommuter

Backup media have to be stored under lock and key in the home area. It has to be ensured that only the telecommuter and his substitute have access to the media.

One generation of backup media should be kept in the institution to enable the substitute to access the backups in case of an emergency.

Additional controls:

- Where are the data media of the data backups for the telecommuting computer held?

S 6.48 Procedures in case of a loss of database integrity

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

Misuse

In the event that the database system behaves in a manner for which there is no obvious explanation (e.g. undefined system behaviour, tables or data records going missing, modified table contents, inexplicably long response times), a loss of database integrity may have occurred. This can result from misuse of the system, for example, as a result of changes to the system settings or exceedance of the maximum number of permitted connects.

Users should observe the following procedure in this case:

Do not panic!

- Keep calm.
- Inform the Database Administrator.
- Do not use the database any longer.

The Database Administrator should take the following steps:

- Inform all affected users.
- Shut down the database system.
- Start up the database system in the exclusive mode (if this is supported by the database system).

Back up log files

- Back up all files which could provide information on the nature and cause of the problem (for example, whether an intrusion has taken place, and if so, how penetration was effected), i.e. it is especially important to back up all the relevant log files.
- Check and, if necessary, reset the access rights for system tables.

Check software for modifications

- Check the database software for any visible changes, for example, to the date of creation and size of the corresponding files. As these attributes can be reset to their original values by an intruder, the integrity of the files should be tested using checksum procedures.

Reload original files

- If necessary, delete the executable files and reinstall the original files from write-protected data media (cf. S 6.21 *Backup copy of the software used*). Programs should not be restored from data backups as these could already contain the error.
- Check the log files for irregularities (in co-operation with the Auditor).
- Change all the passwords.
- Ask users to check their domains for irregularities.

Generate new passwords using randomisation

Once all the passwords have been changed, they must be notified to the users concerned. **No** password or password derivation scheme which is known to all the users should be used here. It is better to generate the passwords randomly and notify the users by a reliable route, e.g. in sealed envelopes. These passwords should be changed immediately after logging on for the first time.

If data was deleted or modified in an unwanted manner, it can be restored from the data backups (refer to S 6.51 *Restoring a database*).

Implement alarm plan

If there are signs of a deliberate attack on the database, it is essential to act immediately in order to minimise the damage and prevent further damage from occurring. This requires that there is an alarm plan which lists the steps to be implemented and specifies who should be informed of the incident (see also S 6.60 *Procedural rules and reporting channels for security incidents*). The alarm plan should also specify whether and how the Data Privacy Officer and the legal department should be involved.

Additional controls:

- Are the users regularly advised of the requirement to inform the Database Administrator at once in case of irregularities?
- Are these procedures actually followed?
- Do the Database Administrators have the required expertise?
- Has a procedure for the rapid assignment of passwords been established and tested?

S 6.49 Data backup in a database

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

As a rule, database systems cannot be backed up fully using backup programs on the operating system level. In most cases, these programs simply act as a link for writing the data on backup media. As far as most products are concerned, backup of the database management system and information in the database additionally requires the use of the database utility programs integrated in the database management system.

The easiest and most reliable way of backing up a database is to perform a full backup with the database shut down. In this process, all files belonging to the database are saved on the storage medium. Usually however, this technique is not feasible due to requirements of database availability or the volume of data to be backed up.

One alternative to the full backup described above is online database backup. In this case, the database is backed up while remaining in operation, i.e. it does not need to be shut down. The disadvantages of this type of backup are that inconsistencies cannot be ruled out explicitly, and that a full, offline backup must nevertheless be available in the event of damage to the database, to serve as a secure foundation for re-loading the online backups. For this reason, online backups should only be performed if the database needs to remain available on a continuous basis. Full, offline backups should nevertheless be performed at reasonably regular intervals.

Partial database backups constitute another alternative. They should be made use of whenever the data volume requiring backup is too large to allow a full backup. This can result from situations in which the capacity of the backup media has been exhausted or insufficient time is available for performing a full backup.

If possible, all transactions between two full, offline backups should be archived. In Oracle databases, for instance, the ARCHIVE mode can be activated for this purpose. In Oracle, transactions are recorded in several log files. These log files are written consecutively. Once all the files are full, the first file is overwritten again. The ARCHIVE mode prepares backup copies of the files before they are overwritten. This permits all transactions to be reconstructed fully in the event of damage to the database. However, the existence of a full database backup is also a prerequisite in this case. The duration of such a recovery increases with the number of archived log files which need to be restored.

A database backup policy needs to be prepared for backing up a database system. Influencing factors in this policy are:

- **Requirements of database availability**

  If a database needs to remain available round the clock on weekdays, for example, full backups can only be performed on weekends, as the database generally needs to be shut down for this purpose.

- **Data volumes**

  The total volume of data requiring backup must be compared with the available storage capacity of the backup media. Here it is necessary to determine whether the backup storage capacity (for example, one DAT tape per backup session) is sufficiently large for the volume of data held in the database.

  If the backup storage capacity is insufficient, a concept for partial backup of the database must be prepared. This might involve, for example, backing up the data of individual applications or individual sectors of the database in rotation, or only backing up modified data. The possibilities of partial backup depend on the database software in use.

- **Maximum permissible data loss**

  Here, it is necessary to specify whether a loss of data accumulated in the course of one day is permissible in the event of damage to a database, or whether the database should be restorable right up to the last transaction. The latter option is generally chosen in cases where high demands are placed on the availability and integrity of the data.

- **Restart time**

  The maximum permissible time taken to restore a database after a crash must also be specified in order to meet the applicable availability requirements.

- **Possibilities of backing up provided by the database software**

  Standard database software does not generally support all conceivable possibilities of data backup, such as partial database backup. In individual cases, a check is therefore required as to whether the prepared database backup policy can be implemented with the available mechanisms.

This information can be used as a basis for defining a database backup policy which must include a specification of the following items (also refer to Chapter 3.4 *Data backup policy*)

- Persons responsible for the orderly carrying out of data backups
- The intervals at which database backups are to be performed
- The database backup techniques
- The times at which database backups are to be performed
- The data volume which is to be backed up in each session
- Documentation on performed data backups
- Storage locations for the database backup media

Example:

Backup from Monday to Saturday:

- Starting time: 3.00 am.

- A backup of all relevant data is performed using the online database backup feature of the database management system, i.e. the database is not shut down.

Backup on Sunday

- Starting time: 3.00 am.
- The database is shut down and a full offline backup is performed.

Additional controls:

- Is there any documentation describing how the database is to be restored in the event of a crash?
- Has a current database backup policy been documented for the institution in question?
- How are staff members informed about the sections of the concept which are applicable to them?
- Is adherence to the concept monitored?
- How are changes in the influencing factors taken into account?

S 6.50 Archiving database

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

If the information in a database system needs to be archived, an appropriate concept needs to be prepared for making the data available when it is required at a later stage. The following items must be considered here:

Archiving

- The available possibilities of archiving must be identified.
- The data model underlying the data to be archived must be documented.
- The times of archiving must be documented.
- The archive must be specified in terms of design, methodology and configuration criteria.
- A maximum life span must be specified for all archiving media on the basis of the related manufacturers' specifications and empirical values. The times of refreshing the archived data must be determined accordingly.
- The availability of the archived data is to be tested and adapted on actual requirements, if necessary. For example, there might be a requirement to make data archived over the last six months available at short notice, whereas information dated earlier is only to be restored on request at longer notice. This criterion influences, among other things, the selection of the archiving medium and archiving method. If high demands are placed on availability, a redundant archive might need to be maintained.
- It must be ensured that all existing storage deadlines are observed.

Restoring

- The current data stock must not be influenced by the archived data stock.
- Sufficient storage space must be available for restoring archived data.
- The archived data must remain restorable, even if the data model changes in the meantime. In this case, the data model applicable at the time of archiving must be known in order to allow restoration of the previous version.
- If the restored data needs to be processed by an application, the version of the application supporting the previous data model must also be available.
- Sporadic checks are required as to whether archived data can be restored.

During the archiving of person related data, it is necessary to take into account the fact that these persons have the right to correct, lock and delete the stored data concerning them. Appropriate technical and organisational procedures must be developed to allow this. In particular, previously performed corrections, locks and deletions must be retained even after old data have been restored.

Additional controls:

- Is there documentation in existence which describes the procedures for restoring archived data?
- Has a current archiving strategy for the institution been documented?
- How are changes in the influencing factors taken into account?

S 6.51 Restoring a database

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

It is necessary to prepare a concept describing how database backups are to be restored. This concept must be structured in accordance with

- The data backup policy (refer to S 6.49 *Data backup in a database*) and
- Potential error situations creating a need for the restoration of data backups.

These two aspects should be used as a basis for determining which database backups are to be restored using which techniques.

The restoration of a database is a complex task which must be performed carefully by experienced personnel. In spite of this, errors and hitches must always be reckoned with during a restoration. For this reason, a damaged database should not be overwritten simply by restoring the database backup.

In many cases, a seemingly corrupt database can be fixed again. In order to minimise the restart time however, trouble shooting should be accompanied by an attempt to restore the database in a separate storage area. Even if damaged data can no longer be repaired, it should be retained so that it can be analysed and the cause of the error can be determined.

During restoration, the database backup should therefore first be loaded on a separate storage medium. Here, it must be noted that the backup requires the same amount of disk space as the defective database.

This disk space must be reserved for emergencies, in order to prevent a loss of database integrity and meet availability requirements. If this is not possible, it is necessary to determine a technique whereby the required disk space can be made available at short notice. Naturally, this should not result in an additional loss of data, for example if areas of the hard disk holding other data need to be overwritten in order to release the resources necessary for loading the database backup. If data nevertheless needs to be deleted due to a lack of disk space, it must first be backed up carefully to ensure that it can be made fully available again after restoration has been completed.

If only individual data records need to be restored instead of the entire database, the backup data should always be loaded separately from the original data. Corresponding disk space must be available in this case, too. Here, it is more advisable to configure a separate database so as to ensure that the original database remains unaffected at all events. This applies even if it is possible to read the backup data individually into the original database.

Additional controls:

- Has a concept for the restoring of database backups been prepared?
- When was the restoring of database backups last rehearsed?
- Has enough disk space been reserved for emergencies?

S 6.52 Regular backup of configuration data of active network components

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Central active network components need to remain highly available because a large number of users are generally dependent upon the smooth operation of a local network. To allow operations to be resumed as quickly as possible following the occurrence of a malfunction, all the configuration data of the active network components should be backed up electronically (also refer to S 6.32 *Regular data backups*). In principle, such backups can be performed locally on the individual components, or via the network using a network management tool, for example. Once the data have been backed up electronically, the corresponding configurations can be restored more quickly and reliably, thus eliminating the need for time-consuming manual entries. The data can be restored automatically, for example, by means of a central network management tool, or manually by an administrator.

When backing up configuration data via the network though, it must be noted that, in contrast to a local backup, it might be possible for potential intruders to monitor the transferred data and thus obtain security-critical information on the configuration of the active network components, such as passwords, and consequently even acquire details on the overall network configuration. The *Trivial File Transfer Protocol* (TFTP) or *Remote Copy Protocol* (RCP) is generally used here; wherever possible, use should be made of RCP with authentication (refer to S 5.20 *Use of the security mechanisms of rlogin, rsh and rcp*). In contrast, TFTP does not offer any mechanisms for protection against unauthorised access to configuration data (also refer to S 5.21 *Secure use of telnet, ftp, tftp and rexec*), so that its use is not recommended.

For all backup techniques, a test is required to ascertain whether the backup was performed successfully and whether the configuration data can be restored properly. This particularly applies to backups performed via the network, because the occurrence of an error here may give rise to a situation in which restoration is no longer possible via the network.

Additional controls:

- Have the configuration data of all active network components been backed up?
- Are generated data backups being documented?
- Is the backup process in conformity with the data backup policy, where established (cf. S 6.13 *Development of a data backup policy*)?

S 6.53 Redundant arrangement of network components

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, Purchase Department

Central active network components need to remain highly available because a large number of users are generally dependent upon the smooth operation of a local network. To allow operations to be resumed as quickly as possible following the occurrence of a malfunction, a redundancy must be created for each area in accordance with the applicable availability requirements, so that a partial or complete failure of the related network components can be tolerated, whilst keeping the resources required for prevention within acceptable limits.

There are two different ways of achieving redundancy:

- The redundant network components can be stored in a warehouse, in order to allow quick replacement in an emergency. If this is not done, long-drawn procurement routines will often be required before errors can be remedied. Alternatively, maintenance or delivery contracts can be concluded with the related manufacturers in order to guarantee a quick replacement of defective components (also refer to S 6.14 *Replacement procurement plan*). After that, the configuration backup data can be reloaded in order to minimise the downtime for the affected network segments (refer to S 6.52 *Regular backup of configuration data of active network components*).
- Even during planning of the network, it is advisable to allow for a redundancy of network components. For example, all central switches and - depending on the protocols in use - all routers should be mirrored at least once in the network in order to achieve redundant server connections and redundant links between the individual network components (refer to Figure 1). Correct operation is to be guaranteed by means of a suitable, logical network configuration.

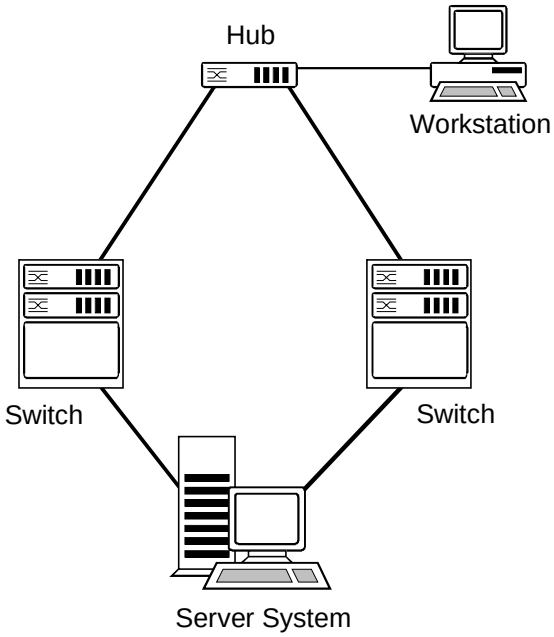


Figure 1: Redundant links between network components

If availability requirements also entail a redundancy of links to terminal devices, each terminal device should be equipped with two network adapters (refer to Figure 2).

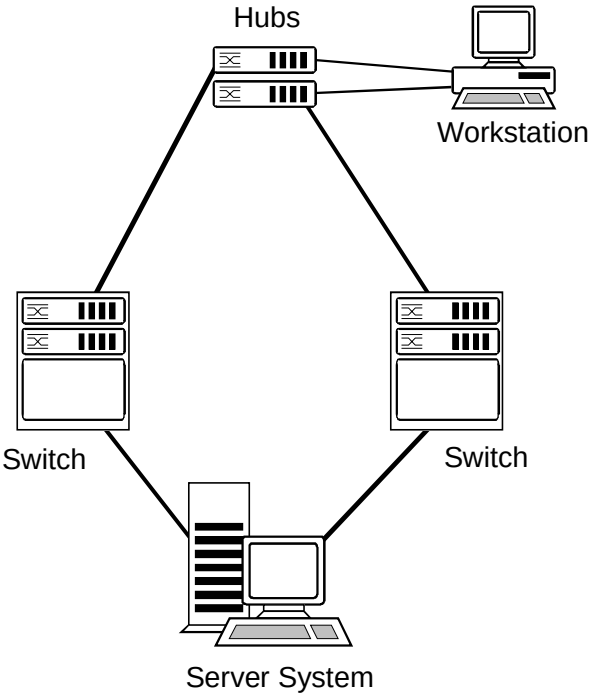


Figure 2: Redundancy of terminal-device links

In each case, a check is required as to whether this technology is supported by the active network components and operating systems in use.

The power supply units of active network components constitute a frequent source of errors, as these units have to rely on a stable mains voltage. For this reason, many components can be retrofitted with redundant power supply units, or are already equipped with them before delivery. This lowers the failure susceptibility of individual network components without requiring their duplication. However, this measure does not increase the operational reliability of the network components as such.

In each case, a careful analysis is required to determine the actual availability requirements. As part of a detailed planning of the system and network architecture, a suitable redundancy concept must be developed to fulfil these requirements. In this context, also refer to S 6.18 *Provision of redundant lines*.

Additional controls:

- Have network availability requirements been ascertained and documented?
- Are all important network components replicated in a warehouse, or have delivery contracts been concluded in this context?
- Has the redundancy of components been taken into account during planning of the network?

S 6.54 Procedures in case of a loss of network integrity

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, IT users

Misuse

If the network acts unexpectedly (for example, servers are not available, access to network resources is not possible, or network performance is consistently poor), a loss of network integrity could have occurred. This could be due to misuse of the network, e.g. due to changes in the configuration of the active network components or damage to them.

Users should observe the following procedure in this case:

- Working documents should be saved and any programs still running should be closed down.
- **Notify Administrator**
  The Administrator must be informed via an appropriate escalation stage (e.g. User Help Desk). The reporting procedure should not be allowed to significantly hinder the Administrator's activities.

The Network Administrator should observe the following procedure:

- Narrow the faulty response down to a network segment or network component.
- Check the configuration of the active network components present there (this also includes password checks).
- **Back up log files**
  Back up all files which could provide information on the nature and cause of the problem (for example, whether an intrusion has taken place, and if so, how penetration was effected), i.e. it is especially important to back up all the relevant log files.
- If necessary, restore the original configuration data (refer to S 6.52 *Regular backup of configuration data of active network components*).
- If necessary, check the hardware in use (cabling, plug connectors, active network components etc.) for faults.
- Request all users to check their working domains for irregularities.

Implement alarm plan

If there are signs of a deliberate attack on the network, it is essential to act immediately in order to minimise the damage and prevent further damage from occurring. This requires that there is an alarm plan which lists the steps to be implemented and specifies who should be informed of the incident (see also S 6.60 *Procedural rules and reporting channels for security incidents*). The alarm plan should also specify whether and how the Data Privacy Officer and the legal department should be involved.

Additional controls:

- What steps have been taken to ensure to ensure that the Administrator is properly informed?
- Are these procedures actually followed?

- Has a procedure for the rapid assignment of passwords been established and tested?

Intentional blank page

S 6.55 Reduction of restart times for Novell Netware servers

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

To reduce the time required for restarting a Novell Netware server after a failure, the necessary software and start drivers (for hard disks, network adapter cards etc.) should be saved separately on external data media in case a new installation is required at any stage. It is advisable to stow these data media together with the remaining data backup media. The required configuration parameters are provided by the server documentation (refer to S 2.153 *Documentation of Novell Netware 4.x networks*).

Furthermore, a procedure for restarting the Netware server should be developed in co-operation with the responsible staff members. This procedure should be simulated regularly as part of emergency routines so that it can be verified and tested in terms of functionality. In particular, such routines should test whether the exclusive use of software and data stored in internal or external backup archives is sufficient for performing a full reconstruction.

The steps required for restarting a Novell Netware server must be described in an emergency manual (refer to S 6.3 *Development of an contingency manual*, Part D). Such steps include, for example:

- Configuration and installation of any required hardware components
- Loading of the system software
- Loading of the start drivers
- Supply of the required data, including configuration files
- Restarting

Depending on the scope and complexity of the NDS, restarting can take a great deal of time. The times required by the restarting steps can be ascertained with the help of such emergency routines, and must be taken into account when reviewing the restart plan.

Additional controls:

- Has the restart plan been tested?
- When was a check last made to ascertain whether backed-up data can be reconstructed?

S 6.56 Data backup when using cryptographic procedures

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Officer

When a company or agency is using cryptographic procedures, it is important not to neglect the subject of data backup. Apart from the question of how a backup of the encrypted data should best be performed, it is also necessary to consider whether the cryptographic keys should be backed up, and if so, how. It also makes sense to back up the configuration data relating to the crypto products that are used.

Backing up the keys

Very careful thought must be given to the question of whether and how to back up the cryptographic keys, because every copy of a key is a potential weak point.

Nevertheless, there may be various reasons why it is necessary to store cryptographic keys. A variety of methods can be used for storing keys:

- Storage on a transportable data medium, such as a floppy disk or chip card (mainly used for distributing or exchanging keys, see S 2.46 *Appropriate key management*), for transport purposes
- Storage in IT components which have to have permanent access to cryptographic keys, for example for communication encryption
- The safekeeping of keys as a precaution against key loss, or as part of arrangements for substitution

The following points always have to be observed in this connection:

- Cryptographic keys should be stored or kept in safekeeping in such a way that unauthorised users cannot read them out without this being noticed. For example, keys could be stored in special security hardware which automatically deletes the keys in the event of an attack. If they are stored in software, they should always be protected by a second encryption. It should be borne in mind that most standard applications which involve storing keys or passwords in the application generally do this using techniques that are easy to break. Another possible variant is to use the two person rule in the storage of keys, in other words dividing a key into two halves or different parts for storage purposes.
- No copies should be made of communication keys or other short-lived keys. To rule out the possibility of unauthorised use, there should generally not be any copies made of private signature keys either. If it is decided to opt for a key storage solution in software only, i.e. without using a chip card or similar device, the risk of key loss is increased, for example as a result of bit errors or a hard disk defect. In this case it may be less costly to provide a sufficiently secure means of key storage than to inform every communications partner every time that a key is lost.

- Backup copies should always be made of long-lived keys, for example keys that are used for the archiving of data or for generating session keys.

Backing up encrypted data

Particular care needs to be taken when backing up encrypted data or when using encryption during a backup procedure. If errors occur at such times, it usually means that all of the data will be unusable, not just a few records.

The long-term storage of encrypted or signed data is associated with many additional problems. It is not only necessary to see to it that the data media are regularly refreshed and that the technical components for processing these media are available at all times, it must also be ensured that the cryptographic algorithms and the key lengths still represent the state of the art. As far as the long-term archiving of data is concerned, it may therefore make more sense to store the data unencrypted and instead store it in an appropriately secure location, for example in a safe.

As a precaution, the crypto modules should always be archived because experience shows that even after a number of years data may crop up which has not been stored in the archive.

Backing up the configuration data of the products used

When using relatively complex crypto products, it is important not to forget to back up their configuration data (see also S 4.78 *Careful modifications of configurations*). Once chosen, the configuration should be documented so that it can be set up again quickly after a system failure of if reinstallation becomes necessary.

Additional controls:

- Are there any stipulations within the company or agency regarding the safekeeping of copies of keys?
- How is it ensured that data stored in encrypted form can still be accessed even after a long period of time?

S 6.57 Creation of an emergency plan for the failure of the management system

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrators

Even management systems are liable to fail, for a variety of reasons - for example as a result of a computer crash due to a software error or hardware fault, or after a power failure or an act of sabotage. Because management systems are used above all in relatively large installations, there should be both a contingency planning concept (as described in Section 3.3) and a data backup concept (see Section 3.4) in place for these systems.

The scope of any such contingency planning concept must then also include the specification and documentation of arrangements for the failure of the management system. In particular, arrangements must be made covering rules of behaviour in the event of failure of the various management system components (manager, management server, management console).

Furthermore, it is absolutely imperative to draw up a post-incident recovery plan for the management system as a whole or its individual components. Ideally, restarting of the management system should proceed automatically. As part of the backup policy, backup copies of the management system software should be available for the eventuality of total data loss (disk crash). The storage location must be noted in the emergency procedure manual. The details required to gain access to the storage location must also be noted in the manual, for example the names and telephone numbers of the members of staff who know the necessary safe combinations or passwords (see also S 2.22 *Depositing of Passwords*).

S 6.58 Establishment of a management system for handling security incidents

Initiation responsibility: Agency/Company management

Implementation responsibility: IT Security Management

As IT is increasingly integrated into every area of an agency's or company's operations, its correct functioning is becoming ever more critical. A major function of IT Security Management is therefore to take sufficient proactive measures to deal with security incidents of all kinds. Security incidents can be triggered by many different events and, for example, result in loss of availability, integrity and/or the confidentiality of data, individual IT systems or the entire network.

The security incidents which require special handling by IT Security Management are those which have the potential to cause significant damage. Security problems which cause or can cause only minor damage which is locally confined should be resolved locally so as to avoid overloading IT Security Management.

Objectives in the handling of security incidents

Handling of security incidents is ultimately the responsibility of IT Security Management and should be aimed at ensuring the following:

- the ability to respond so that security incidents and security problems are detected and reported to the appropriate responsible person(s) promptly;
- the ability to decide whether it is a local security problem or constitutes a security incident;
- the ability to take action so that in the event of a security incident the necessary measures can be taken and implemented at short notice;
- minimisation of damage - this is achieved through prompt notification of any other parts of the organisation which could be affected, and
- effectiveness - this is achieved by practising and monitoring the capability to handle security incidents.

Involvement of Management

To achieve these objectives, a management system must be established for dealing with security incidents. It is essential here that Management is involved and ultimately puts the management system into effect so as to ensure that the necessary awareness of IT security issues is generated, decision-making responsibilities are assigned and the security objectives are supported.

The steps described below provide a suggested approach as to how to establish a management system handling security incidents.

Step 1: Inclusion in the security guidelines

The handling of security incidents is one aspect of IT security management and, as such, should be spelt out in the security guidelines and/or IT security policy of the agency or company. These documents must specify that security incidents and security problems are to be reported by users and those affected to the responsible security officer. In addition, the decision-making process must be described and staff must be motivated as to the necessity of following

the stipulated procedures. At the same time, inclusion in the security guidelines is a way of demonstrating Management's support for IT security.

Step 2: Specification of responsibilities

This step entails specifying who has what responsibility in the event of security incidents occurring. For example, the following groups might have these responsibilities:

- IT users: report security problems and security incidents.
- IT Administrators: receive reports, take initial steps enabling decision as to whether the occurrence is a security problem or a security incident, initiate escalation.
- Person responsible for IT application: participate in decision process and selection of measures in the light of own assessment of the degree of protection required by the IT application.
- IT Security Officer or IT Security Management: receive reports, decide whether it is a case of a security problem or a security incident, set escalation in motion, implement necessary measures.
- Security Incident Team: a team composed of IT administrators, IT users, IT Security Officers concerned, together with Public Relations staff and possibly Management, for handling a security incident.
- Public Relations staff or Press Office: prepare information policy regarding the security incident as required.
- IT Security Auditor: review management system and evaluate security incident.
- Management: make final decisions

The responsibilities must be defined and put into effect. For further information, see safeguard S 6.59 *Specification of responsibilities for dealing with security incidents*.

Step 3: Procedural rules and reporting channel for handling security incidents

To deal with security incidents effectively, it is essential that those affected behave in a correct and level-headed manner and report the incident immediately. The necessary procedural rules (keep calm, reporting obligation, duty to provide information on attendant circumstances etc.) must be defined and IT users trained accordingly. In particular, the person to whom IT security problems or incidents should be reported must be determined.

Consider typical security incidents in advance

Instructions on actions to be taken in the event of security incidents which may typically be expected (e.g. appearance of a computer virus, manipulation of data by insiders, hacking attempts by outsiders etc.) can be drawn up in advance. If an emergency occurs, people will then be able to respond more quickly so that the damage can be reduced. Since the effort required to prepare these action options is not inconsiderable, it should be restricted to the relevant areas in which it is possible to make plans.

This topic is covered in detailed in safeguard S 6.60 *Procedural rules and reporting channels in the event of security incidents*.

Step 4: Escalation strategy for security incidents

The more critical a security incident is, the greater the authority that is required as a rule to deal with the security incident. In the extreme this can mean that Management has to be informed and involved early in order that necessary measures such as a ban on divulging any information, calling in the police, taking costly alternative measures can be implemented. However, this requires that an escalation strategy specifying who should be consulted in what cases is drawn up in advance. Further information on this is provided in safeguard S 6.61 *Escalation strategy for security incidents*.

Step 5: Setting priorities

Because security incidents are generally the culmination of a chain of different causes and affect different IT application areas, the measures to be adopted should be implemented with the aid of a priority list. This setting of priorities depends on the protection requirement, the range of IT applications and the individual dependencies of the agency/company. Just as is necessary when determining the protection requirements, a list of priorities must be drawn up in advance for the purpose of specifying the order in which damage resulting from a security incident should be tackled (see S 6.62 *Specifying priorities for handling security incidents*).

Step 6: Methodology for investigating and assessing security incidents

Once a security-relevant irregularity has been reported, a decision must be made initially as to whether it can be regarded as a local security problem or constitutes a potentially more damaging security incident. A number of factors have to be ascertained and assessed before this decision can be made (the extent of the potential damage and consequential damage, the cause, which IT systems are affected, what immediate measures are required). If necessary, the next levels of management should be consulted, as specified in an escalation strategy. Further details will be found in safeguard S 6.63 *Investigation and assessment of a security incident.*

Step 7: Implementation of measures for taking remedial action in connection with security incidents

When implementing the measures necessary to remedy security incidents, it should be borne in mind that these measures will generally have to be implemented under time pressure. Therefore it is not inconceivable that the measures taken could themselves create new problems. Consequently it is important to document implementation of the measures adequately. Furthermore, assuming that the incident is the result of wilful action, the question of how the "perpetrator" should be dealt with should also be thought about. In some circumstances there may be personnel implications. For further information, see S 6.64 *Remedial action in connection with security incidents.*

Step 8: Notification of the parties affected

If it transpires that the impact of a security incident is not confined to the agency/company or individual organisational unit(s) concerned, to contain the

damage all the other internal departments and external agencies affected must be notified. To accelerate notification, the communication channels should be ascertained and a dependency analysis should be carried out in advance (see S 6.65 *Notification of the parties affected*).

Step 9: Evaluation of a security incident

To ensure that the appropriate lessons are learnt from a security incident which has occurred, the procedure to be adopted for evaluating the handling of security incidents should be specified. Often this will result in improvements in dealing with security incidents or permit conclusions to be drawn as to the effectiveness of the IT security concept. The aspects to be considered here include the following:

- Time taken to react
- Extent of awareness of the reporting channel
- Effectiveness of the escalation strategy
- Effectiveness of the investigation
- Means for notifying affected parties

This subject is addressed in detailed in safeguard S 6.66 *Evaluation of security incidents*.

Step 10: Use of detection measures for security incidents

The sooner a security incident is detected and reported, the more effectively can countermeasures be taken. Any automated detection measures available should be used so as to reduce any delays induced by reliance on human actions. Examples of such measures are anti-virus programs, analysis of logged data and intrusion detection systems. Identification and activation of these measures and the related communication channels are described in safeguard S 6.67 *Use of detection measures for security incidents*.

Step 11: Effectiveness testing

In order to be able to measure the effectiveness of a management system for the handling of security incidents and promote the necessary practice at these management tasks, exercises and gaming should be performed. As these may require considerable personnel resources and can interfere with normal operations, they should be confined to important areas. Further suggestions will be found in safeguard S 6.68 *Testing the effectiveness of the management system for the handling of security incidents*.

The results of these steps should be documented appropriately in a "Concept for handling security incidents" paper. This concept should be updated at regular intervals and be notified to those affected in a suitable way.

Develop concepts and update regularly

Additional controls:

- Are there clearly defined procedures and rules covering the different types of security incident?
- Are the procedural rules and reporting channels to be used in the event of security incidents specified in writing?
- Are these known to all employees?

S 6.59 Specification of responsibilities for dealing with security incidents

Initiation responsibility: Agency/company Management, IT Security Management

Implementation responsibility: IT Security Management

Define tasks and responsibilities

When specifying the responsibilities for handling security incidents, it is worthwhile considering the sequence of events in a hypothetical security incident. The tasks and responsibilities of the person groups involved must be determined and an appropriate method of obligating and instructing them must be devised. To give an idea how this might be done, examples are set out below for some of the groups typically affected.

IT-users

Task:

As soon as IT-users become aware of a security-relevant irregularity, they must observe the appropriate procedural rules and report the irregularity.

Responsibility:

IT users must decide what the appropriate reporting channel is in the present case (see S 6.60 *Investigation and assessment of a security incident*).

Duty / information:

Every IT user should have a duty under the in-house security guidelines to report any security-relevant irregularities. Furthermore, all users should be given written instructions informing them of the actions they should take and to whom which incidents should be reported.

IT Administrator

Task:

The IT Administrator's task here is to receive reports regarding security-relevant irregularities relating to IT systems for which he is responsible. He must then decide whether to take corrective action himself or whether he should report the incident to the next higher escalation level.

Responsibility:

An administrator must be able to decide whether there is a security problem, whether he can deal with it himself, whether he should consult other persons immediately (in accordance with the escalation plan) and whom he should inform.

Duty / information:

This should be specified in the job description and in the "Policy for handling security incidents".

IT Security Officer / IT Security Management

Task:

The IT Security Officer receives reports on security incidents. He investigates and assesses the incident. He selects appropriate measures and arranges for them to be implemented where this does not lie outside his area of responsibility. If necessary, he assembles a Security Incident Team or informs line management for the purpose of escalation.

Responsibility:

He is authorised to undertake an assessment of a security incident and to escalate an incident up the management chain. In addition he has been granted the financial and personnel resources (e.g. DM 100,000 and 2 man-months) which he may use to handle incidents independently.

Duty / information:

IT Security Management develops the "Policy for handling security incidents". Therefore all IT Security Officers should be informed of their tasks and responsibilities in the handling of security incidents.

IT Security Auditor

Task:

The IT Security Auditor can be assigned the task of checking the effectiveness of the management system for security incidents at regular intervals. He can also be required to participate in the evaluation of security incidents.

Responsibility:

In agreement with line management, predefined checks can be initiated and performed.

Duty / information:

This should be specified in the job description and in the "Policy for handling security incidents".

Public Relations / Press Office

Task:

Where a serious security incident has occurred, no information should be divulged to the public except through the Press Office. The aim here is not to gloss over or play down the incident, but to present it in an objective manner so as to avoid any loss of image as a consequence of conflicting information.

Responsibility:

The Press Office must prepare information regarding the security incident together with the technical experts and agree this with line management prior to distribution.

Duty / information:

This should be specified in the job description and in the "Policy for handling security incidents".

Agency/company management

Task:

In cases of serious security incidents, management should be informed and if necessary should be required to make decisions.

Responsibility:

In its capacity as having overall responsibility, it can delegate responsibility to the above-mentioned groups. In addition it can call in the police and criminal prosecution authorities where criminal activity is suspected.

Duty / information:

Management must approve the "Policy for handling security incidents" and the escalation plans which are based thereon. As part of this, line management is also informed of its role in the handling of security incidents.

Security Incident Team

In addition to the above groups, where a difficult or serious security incident has occurred it may be necessary to invoke a Security Incident Team for a limited period to handle the incident. This is normally initiated by the IT Security Officer, who may involve line management in advance.

Appoint members and determine tasks

Even if the Security Incident Team only meets for a specific security incident, to ensure as fast a response as possible to the security incident, its members must be appointed and fully briefed of their assigned tasks in advance. The members of the Security Incident Team should be authorised to perform their assigned tasks on their own authority. The procedures necessary for this must be specified in writing and authorised by management. In particular, the person who heads the team must be specified.

Depending on the type of security incident, the members of a Security Incident Team can include the following, for example:

- Agency/company management
- IT Security Management / IT Security Officer
- Head of IT section
- Press office
- Data privacy officer
- Legal adviser
- Staff council / works council

If necessary, additional parties/departments must be called in, e.g.

- the specialist departments concerned (head of department, IT Procedures Officer),
- IT Administrators,

- the purchasing, site technical service, general service section, organisation, human resources departments and
- the fire protection officer.

Procedures regarding overtime

It should be clarified in advance how the additional work caused by the occurrence of a security incident is to be performed, i.e. whether the provisions relating to working hours at the authority/company need to be expanded to include exceptional procedures to cover overtime, weekend working etc. in the event of a security incident. Steps must also be taken to ensure that this team can use the office premises outside of regular working hours should this be required.

Additional controls:

- Has a Security Incident Team been appointed?
- Have the members of the team been briefed as to their assigned tasks?
- Who co-ordinates which measures?
- When was the composition of the Catastrophe Management Team last updated?

S 6.60 Procedural rules and reporting channels for security incidents

Initiation responsibility: Agency/company Management, IT Security Management

Implementation responsibility: IT Security Management

Many security incidents only turn into serious problems because inappropriate action was taken in response to them as a result of hasty decisions, for example, resulting in the spontaneous deletion of data which was needed to understand the event.

A distinction should be made here between generally applicable procedural rules which apply to all imaginable security incidents and IT-specific procedural rules. The following general procedural rules can be specified for all types of security-relevant irregularities:

- All those involved should remain calm and desist from taking hasty measures. **Do not panic!**
- Irregularities should be reported immediately in accordance with a reporting plan. **Proceed in an orderly manner!**
- Countermeasures must not be taken until or unless they have been requested by authorised persons.
- All the attendant circumstances must be explained frankly and transparently and without any glossing over, so that the damage can be minimised. **No covering up!**
- Based on personal experience, an initial assessment of the potential extent of the damage, the consequential damage, the parties both within and without the organisation who are potentially affected and the possible consequences should be performed. **Damage assessment**
- Information regarding the security incident should not be passed to third parties without authorisation.

All staff in the agency/company who are potentially affected must be notified of these general procedural rules in a suitable fashion.

In addition, specific procedural rules can be provided to those affected, especially those in positions which are notified in cases of security incidents and are expected to take the first decisions and/or initiate the first measures. This includes IT Administrators, those responsible for IT applications and IT Security Management. These procedural rules should cover the measures described in **Make procedural rules known**

- S 6.23 *Procedure in the event of computer virus infection*
- S 6.31 *Procedural patterns following a loss of system integrity*
- S 6.48 *Procedures in case of a loss of database integrity*
- S 6.54 *Procedures in case of a loss of network integrity*

Once the procedural rules have been specified, the reporting channels must also be defined. We recommend proceeding on the following lines:

- In cases of force majeure such as fire, water, power failure, break-in and theft, the relevant local services should be informed (fire department, site technical service, entrance control staff, security guards etc.).
- In cases of hardware problems or irregularities in the operation of IT systems, the responsible IT Administrator should be informed.
- In cases of suspected wilful action and events which cannot be explained by any other means (e.g. manipulation of data, unauthorised exercise of permissions, suspected espionage or sabotage), the IT Security Officer and/or IT Security Management must be informed.

Make reporting channels known

It is especially important here that all employees know whom to contact and the reporting channels which apply to all types of security incident. For example, a list of names, telephone numbers and e-mail addresses of the relevant points of contact could be included in the internal telephone directory or on the Intranet. However, it must not be difficult to report one's suspicions, nor must this entail any longwinded procedure. Fast and secure communication connections must be available for this purpose. The authenticity of the communication partner must be assured and the information reported concerning the suspicious occurrences must be treated as confidential.

All staff should also be informed that information regarding the security incident may only be divulged to third parties via IT Security Management (see S 6.65 *Notification of the parties affected*).

Perform practice runs

Exercises or practice runs should be held sporadically to check whether the procedural rules for security incidents are appropriate and can be implemented and whether all staff are aware of them (see also S 6.68 *Testing the effectiveness of the management system for the handling of security incidents*).

Experience of security incidents shows how important a good operating environment and a healthy communications culture are for the prompt and frank reporting of security incidents (see also S 3.8 *Avoidance of factors impairing the organisation climate*).

Leaflet containing reporting plan and the most important procedural rules

One possible way of informing all employees affected of the procedural rules and reporting plan is to issue an information sheet signed by the Management, on which the most important information is summarised. This can be held at the workplace and **additionally** on the Intranet. An example of such an information sheet can be found in the help available on the IT Baseline Protection Manual CD-ROM (directory ...\HILFSMI\15VERHAL.DOC). To ensure that the information is actually available when the real thing happens, we do not advise distributing this information sheet only in electronic form as the electronic version itself could then be affected by the security incident.

All information sheets on potential security incidents must be immediately updated whenever a relevant change takes place in the organisation, in order that the procedural rules described in them remain applicable and the reporting channels are correct.

Additional controls:

- Are there clearly defined procedural rules covering the different types of security incident?
- Are these known to all employees?
- When was this information last updated?

S 6.61 Escalation strategy for security incidents

Initiation responsibility: Agency/company Management, IT Security Management

Implementation responsibility: IT Security Management

Once the responsibilities for security incidents have been determined (see S 6.59 *Specification of responsibilities for dealing with security incidents*) and the procedural rules and reporting channels are familiar to all those concerned (see S 6.60 *Procedural rules and reporting channels in case of security incidents*), the next step is to determine how to proceed once reports have been received.

As a first step, the person receiving a report regarding a security incident must investigate and assess it (see also S 6.63). If it turns out to indeed be a case of a security incident, additional measures must be taken. The following questions arise:

- Where escalation is required, i.e. the action chain is extended, who should be informed?
- What cases require immediate escalation?
- Under what other circumstances is escalation appropriate?
- When should escalation occur (immediately, the next day, the next working day)?
- What media should be used to pass on the report?

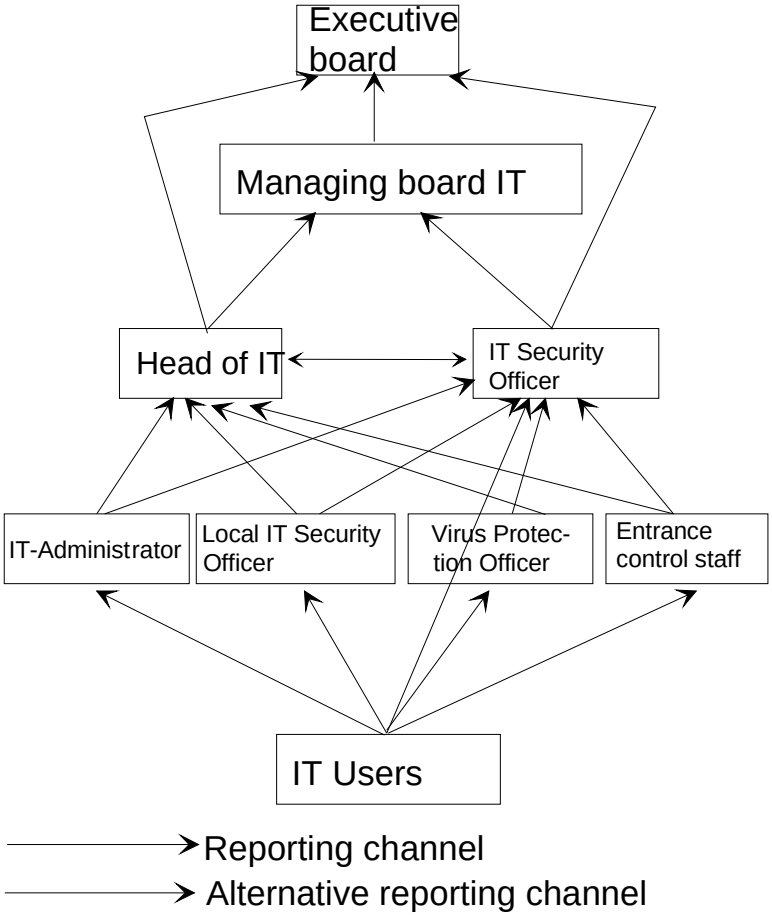
The answers to these questions must be specified in an escalation strategy and made known. The escalation strategy can be created in three stages, as follows:

Stage 1: Specification of escalation channels

Who informs whom?

Who is responsible for handling security incidents is specified in safeguard S 6.59 *Specification of responsibilities for dealing with security incidents*. Specification of the escalation channel should include defining who should send a report to whom. This is easy to see when the relevant hierarchy is presented in diagrammatic form. Both the regular escalation channels and also the channels to be used during staff absences should be considered.

Example



Stage 2: Decision aid for escalation

Who needs to be informed quickly?

This stage entails firstly establishing in which cases escalation should be immediate before any further investigation or assessment is performed. An example of a tabular representation is shown below.

Event	**To be informed immediately**
Infection with a computer virus	Virus Protection Officer, Administrator
Fire	Entrance control staff, fire department
Wilful acts and suspected criminal acts	IT Security Officer
Suspected industrial espionage	IT Security Officer, executive board
Necessity to call in the police and criminal prosecution authority	Executive board
Existence-threatening damage	Executive board

Under what other circumstances escalation is required should then be specified. Possible grounds for escalation are as follows:

- The expected level of damage exceeds the area of responsibility of the person who received the report.
- The costs and resources required to control the damage exceed his area of competence.
- The complexity of the security incident exceeds his competence or area of responsibility.

Stage 3: Manner of escalation

How should the alerting be done?

It is now necessary to specify how the next level up in the escalation chain should be informed. The options are:

- in person
- written report
- E mail
- telephone, mobile phone
- messenger with sealed envelope

The timescale within which notification should occur must also be specified. Examples are:

- events which require immediate escalation: within one hour;
- events which require immediate measures: within one hour;
- events which may be under control but still require that the next escalation level is notified: the next working day.

This escalation strategy should be notified to all possible recipients of reports of security incidents so as to ensure a prompt response.

Procedures regarding overtime

To contain a security incident, it is usually necessary to take action promptly. It may be necessary to recall staff from other projects or to call them in out of working hours. Procedures must therefore be defined as to how the necessary additional work is to be handled and how to ensure that staff are on call (see also S6.59 *Specification of responsibilities for dealing with security incidents*).

Additional controls:

- When was the escalation strategy last updated?
- Have the escalation channels been tried out in exercises/practice runs?

S 6.62 Specifying priorities for handling security incidents

Initiation responsibility: Agency/company Management, IT Security Management

Implementation responsibility: IT Security Management

Experience suggests that security incidents are the result of a conjunction of different causes. As a consequence it is generally the case that the resulting potential damage involves several categories of damage (for example, impairment of physical integrity of a person, negative effects on external relationships, financial consequences, see also Section 2.2, *Determination of protection requirements*). It is therefore important to establish as far in advance as possible exactly where priorities lie with regard to dealing with problems. This priority assignment determines among other things the sequence in which problems should be tackled.

Security incidents compete with other problems

The assignment of priorities depends heavily on an organisation's particular circumstances. To assign priorities, the following questions should be considered:

- What categories of damage are relevant to the organisation?
- In what order should damage in the individual damage categories be rectified?

In answering these questions, it can be helpful to work through a procedure for determining protection requirements from the IT baseline protection point of view (see Section 2.2). This procedure for determining protection requirements defines the damage categories which are relevant to the organisation.

Examples of relevant damage categories are as follows:

How serious is the damage?

- Violation of laws, regulations or contracts
- Impairment of the right to informational self-determination
- Impairment of the physical integrity of a person
- Impaired performance of duties
- Negative effects on external relationships
- Financial consequences

As part of the exercise of specifying the protection requirements, the extent of the damage is defined for each damage category.

Example: damage category "financial consequences"

Damage category: financial consequences	
Damage / loss = medium	Damage or loss is less than DM 25,000
Damage / loss = high	Damage or loss is between DM 25,000 and DM 5 million

Damage / loss = very high	Damage or loss is greater than DM 5 million

Prioritisation either in 3 stages or using ranking

Using the above categories and damage or loss brackets, priorities can be assigned as described below. The damage categories are listed in the first column of a table. The next three columns have as headings the three levels of damage/loss, medium, high and very high. A priority is then assigned to each permutation of damage category and damage/loss. One approach to the assignment of priorities is to use a priority classification system with categories such as

1 = especially important,
2 = important,
3 = relatively unimportant

Alternatively, each damage category can be assigned a ranking.

Example

In this example the organisation concerned is a municipal authority which also offers services to the public over the Internet. The public can send requests to the municipal authority by E mail and see how their cases are progressing over the Internet. As an information service, this municipal authority provides the use of an Internet server.

An example of how the results of prioritisation might appear in this case is provided in the next table.

Damage category	**Damage / loss = medium**	**Damage / loss = high**	**Damage / loss = very high**
Violation of laws, regulations or contracts	2	2	2
Impairment of the right to informational self-determination	2	2	1
Impairment of the physical integrity of a person	2	1	1
Impaired performance of duties	3	3	2
Negative effects on external relationships	3	2	1
Financial consequences	3	3	2

Example of how the results of prioritisation might appear where ranking is used:

Damage category	**Damage / loss = medium**	**Damage / loss = high**	**Damage / loss = very high**
Violation of laws, regulations or contracts	13	12	11
Impairment of the right to informational self-determination	8	6	3
Impairment of the physical integrity of a person	5	2	1
Impaired performance of duties	15	14	7
Negative effects on external relationships	17	9	4
Financial consequences	18	16	10

Approval by Management

This priority assignment must be approved by Management and put into effect. The approved priority assignment must be notified to all persons who would need to make decisions in connection with handling security incidents.

In the event that a security incident occurs, the priority assignment is used as follows. Once the security incident has been investigated and assessed, an estimate can be made of the expected damage. The resulting damage figures are then assigned to the known damage categories, following which they are allocated to the classes "medium", "high" and "very high". The priority assignment table indicates the order in which each type of damage should be addressed. However, the prior assignment of priorities should be viewed only as an initial guide. It may need to be adapted in individual cases.

Example

Suppose that in the above example, a hacker has succeeded in manipulating the information on the Internet information server so that the municipal authority appears in a bad light. This is spotted promptly, IT Security Management is called in and the above damage assessment is carried out. The results of the assessment might appear as follows:

Damage category	Damage / loss = medium	Damage / loss = high	Damage / loss = very high
Violation of laws, regulations or contracts	D1		
Impairment of the right to informational self-determination			
Impairment of the physical integrity of a person			
Impaired performance of duties	D2		
Negative effects on external relationships			D3
Financial consequences	D4		

Damage cases D1 to D4 are assigned the following priorities on the basis of the previous priority assignment:

Priority classification method: D1 = 2, D2 = 3, D3 = 1, D4 = 3

Priority rating method: D1 = 13, D2 = 15, D3 = 4, D4 = 18

In both cases it would be clear that damage limitation effort should initially be concentrated on damage case D3 (negative effects on external relationships) before any attempt is made to tackle the other types of damage. In the example, to limit the negative effects on external relationships, the Internet server which has been tampered with would be taken off the network as the prelude to other measures. If the damage resulting from negative effects on external relationships had been assigned a lower priority and greater importance had been attached to impairment of the municipal authority's ability to accomplish its work, disconnecting the Internet server might not be viewed as a measure which should be implemented immediately.

Additional controls:

- Has the priority assignment been agreed with Management?
- Has the priority assignment been notified to all the decision makers in the management system for the handling of security incidents?
- When was the priority assignment last updated?

S 6.63 Investigation and assessment of a security incident

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management, IT Administrator, IT Application Manager, Security Incident Team

Not every security incident is recognised as such immediately. Especially where targeted and wilful attacks are aimed at IT systems, many security incidents only come to light days or weeks after the event. False alarms are also a common occurrence, e.g. because hardware or software problems have been wrongly interpreted as cases of infection with computer viruses.

However, in order to be able to investigate and assess a security-relevant irregularity, it is necessary that certain preliminary assessments have already been carried out. These include:

- ascertaining the existing IT structure and IT network,
- ascertaining the point of contacts and users of the IT systems,
- ascertaining the IT applications on the IT systems concerned, and
- defining the protection requirements of the IT systems.

These investigations are carried out as the first stage of using the IT Baseline Protection Manual (see Section 2.2) and the results should therefore be available to IT Security Management.

How much is affected?

Following receipt of an incoming report, the above information can be used to decide quickly which IT system is affected, and what IT applications and protection requirements are involved. At the same time, since the point of contact is known, this person can be called in quickly to assist with making the appropriate decisions.

Should it transpire that an IT system or an IT application with a high-level protection requirement is affected, then the matter should be regarded as a security incident and the predefined steps required to handle it must be implemented. On the other hand, if only IT applications and IT systems having a low protection requirement are affected, an attempt can be made to resolve the security problem locally.

Mobilising the Security Incident Team

If it appears that the security incident could have serious consequences and is sufficiently complex, it may be appropriate to call in the Security Incident Team without delay (see S 6.59 *Specification of responsibilities for dealing with security incidents*).

The following factors should be ascertained as a first step to investigating and assessing the security incident:

- What additional IT systems and IT applications could be affected by the security incident?
- Could any consequential damage also occur through networking of the IT systems?

- Which IT systems and IT applications will definitely not suffer any damage or consequential damage?
- How high could any direct damage or consequential damage caused by the security incident be? Particular attention should be paid here to the dependence of the various IT systems and IT applications.
- What was the trigger for the security incident (e.g. carelessness, an adversary or failure of the infrastructure)?
- When and in which location did the security incident occur? This could actually be some time prior to when the security incident was first detected. Well maintained log files can be extremely useful here, but only if one can be sure that they have not been tampered with.

Consult log data

- Are only internal IT users affected by the security incident, or are external third parties affected also?
- How much information regarding the security incident has already leaked out to the public?

If it transpires that the security incident could have serious consequences then it should be escalated to at least the next level.

Determine actions

Once these factors have been clarified, the options available must be specified. These will consist of both immediate measures and supplementary measures. The previously determined assignment of priorities should be considered here (see S 6.62 *Specifying priorities for handling security incidents*). The time that will be required to implement these measures and the cost and resources which will be necessary to resolve the problem and restore normal operating conditions must also be estimated.

If the level of the damage, the time required to repair the situation and the cost of this exceed predefined limits, then the next higher escalation and decision levels must be called in before any decisions are made as to which measures should be selected. The outcome of a structured investigation and assessment of a security incident on the lines outlined above will be the various options available.

Additional controls:

- Is the necessary information generated from the definition of protection requirements available to the persons receiving reports of security incidents and the next escalation levels?
- Are any technical means available to support the evaluation of security incidents, for example, tools for analysing logged data?

S 6.64 Remedial action in connection with security incidents

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: IT Security Management, Head of IT Section, Administrator

As soon as the cause of a security incident has been identified, the measures needed to deal with it should be selected and implemented. This requires first of all containing and removing the problem, and then restoring the "normal" state of affairs.

Supplying the necessary expert knowledge

List of addresses of experts

To investigate and deal with a security weakness, it is essential to have the relevant technical knowledge. Therefore either staff must have the appropriate training or else experts will have to be called in. For this purpose, a list containing the contact addresses of appropriate internal and external experts from the various subject areas must be prepared so that they can be called upon for advice without delay. External experts include

- Computer Emergency Response Teams (CERTs) (see also S 2.35 *Obtaining information on security weaknesses of the system*),
- vendors and distributors of the IT systems concerned (see also S 4.107 *Use of vendor resources*),
- vendors and distributors of security systems used such as anti-virus programs, firewalls, access control etc.,
- external consultants with specialist security expertise.

Restoring secure operations

Investigation of the affected IT systems

To eliminate any security weaknesses, the IT systems concerned must be taken off the network and all the files which could provide any information about the nature and cause of the problem which has occurred must be backed up. This includes especially all relevant log files. As the entire IT system should be viewed as insecure or as having been tampered with, the operating system and all the applications must be examined for changes. In addition to programs, configuration files and user files must also be examined for possible manipulation. It is appropriate here to use checksum procedures. However, this presupposes that the checksums associated with the "secure" condition have been ascertained in advance and transferred to write-protected data media (see also S 4.93 *Regular integrity checking*).

Be cautious about importing data backups

To be certain that any Trojan horses left behind by an adversary have really been removed, the original files should be reimported from write-protected data media. Care should be taken here that all security-relevant configurations and patches are also imported as well. Where files are reimported from data backups, steps must be taken to ensure that these have not been affected by the security incident, i.e. they have not already been infected with the computer virus. On the other hand, examination of the data backups may be helpful in order to establish when the attack began or when infection with a computer virus occurred.

Before restoring operations after an attack, all passwords on the IT systems concerned should be changed. This also includes IT systems which were not directly affected by manipulation, but from which the attacker may already have obtained information about users and/or passwords.

Change passwords

It should be assumed that once the "secure" condition has been restored, the adversary will attempt a further attack. For this reason the IT systems, especially the network connections, should be monitored using the appropriate monitoring tools (see also S 5.71 *Intrusion detection and intrusion response systems*).

Monitoring of the affected IT systems

Documentation

All actions performed while dealing with a security problem should be documented in as much detail as possible so as to

- retain the details of what happened,
- make it possible to retrace the problems which occurred,
- be able to rectify any problems/faults which could result from hasty implementation of countermeasures,
- be able to resolve problems already known more quickly should they occur again,
- be able to eliminate the security weaknesses and draw up preventive measures and
- collect evidence if a prosecution is to be brought.

Such documentation includes not only a description of the actions carried out including the times at which they were taken, but also the log files of the affected IT systems.

Reaction to deliberate action

Where a security incident was triggered by an adversary, a decision must be made as to whether to stand back and watch the attack or whether countermeasures should be implemented as soon as possible. Naturally an attempt can be made to catch the adversary "red-handed" but this runs the risk that in the meantime he will destroy, tamper with or read data.

Regrettably, investigation of security problems indicates that these are often caused by staff from within the organisation. This can be the result of an oversight, inappropriate working procedures or technical problems, but it could also be a case of failure to observe security measures or even deliberate action.

Dealing with insiders

Wherever security problems are caused internally, the trigger must be investigated. Often the problems turn out to stem from inappropriate or incomprehensible procedures. It is then necessary to amend the procedures accordingly or else to supplement them with additional measures, e.g. of a technical nature.

If the security problems are the result of deliberate action or negligence, appropriate disciplinary measures should be taken.

Additional controls:

- When was the list of security experts last updated?
- Have any deliberate attacks perpetrated by insiders been observed before?

S 6.65 Notification of the parties affected

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management, Head of IT Section, Administrator, Press Office

When a security incident has occurred, all the internal and external parties affected by it must be informed. This is especially important for departments or agencies which could sustain damage as a direct result of the security incident and need to take countermeasures or for any parties which process information about security incidents and can assist in preventing or resolving them. If necessary, the public should also be informed, especially if information has already leaked out.

Who informs whom?

A clear concept of who should inform whom, in what sequence and in how much detail must be developed for the particular security incident concerned. In this connection steps must be taken to ensure that information regarding the security incident is only given out by appointed responsible persons, such as, for example IT Security Management or the Press Office.

No glossing over!

Who receives information and in how much detail naturally will depend primarily on the technical background. No incorrect or embellished information should be passed on, as this could lead to confusion, false assessments and loss of image.

An example is presented below of which departments/agencies should typically be informed of what information.

Internal departments

If it is still unclear as to whether a security incident has occurred or how serious it is, the internal staff potentially affected should be asked to examine their areas of work for possible irregularities.

If the countermeasures required to deal with a security incident are known, the internal departments concerned should be informed promptly as to what they must do in order to minimise the effects of a security incident or to restore secure operations.

The parties who should be considered include the following:

- Head of IT Section
- heads of specialist departments concerned,
- IT users,
- IT Administrators,
- IT user service,
- site technical service
- surveillance staff,
- internal security staff and
- entrance control staff.

External parties

If the impact of the security incident is not confined simply to the organisation, all external parties which are also affected or could also be

affected should be informed of the security problem which has occurred, what countermeasures are necessary and how the effects can be contained.

If this information is not passed on but the incident subsequently becomes known, an existing co-operative relationship based on trust between the organisation and the external party could be permanently impaired.

The following groups should be considered here:

- customers,
- suppliers,
- freelance staff,
- subcontractors,
- IT service providers,
- parties to which there are communication links,
- companies developing software and
- network operators.

Depending on the type of incident, it may also be necessary to call in the police and/or take legal advice.

The public

Only issue statements through the Press Office

Where major or complex security incidents have occurred it may be necessary to inform the public. Press statements should only be issued through the Press Officer. Care must be taken here to ensure that the Press Officer is adequately briefed on the security incident, the extent of the damage, any necessary countermeasures and the parties which have been informed.

However, the information provided to the public should be kept non-specific so as to avoid encouraging copycat attacks.

It is important to check the identity of anyone seeking information about security incidents so that perpetrators are not kept up-to-date about the success of their attacks.

IT security community

Pass on warning about security weakness

If the security incident is due to a security weakness which is not already familiar, this fact should not be kept secret but should be forwarded to other parties so that they can be warned about the security weakness and countermeasures can be developed. Typically the following parties should be informed:

- vendors of anti-virus programs where infection by a new computer virus is suspected but this was not detected by the virus scanner;
- vendor of any operating system or application software within which the security weakness was resident;
- Computer Emergency Response Teams (CERTs) (see also S 2.35 *Obtaining information on security weaknesses of the system*), where the security incident is attributable to system- or application-specific security weaknesses;
- the IT specialist press or
- public agencies concerned with IT security, such as the BSI.

Example

It is noticed that data is sporadically tempered with on PCs or goes missing. After this was reported and subsequently investigated it transpired that the problems were caused by a previously unknown macro-virus. This virus is spread via E mail attachments. In this case, the following departments and parties should be notified immediately:

- Head of IT Section,
- IT users,
- IT Administrators,
- IT user service,
- all parties with whom data has been exchanged since the computer virus first appeared,
- vendor of the anti-virus program which failed to detect the virus,
- a Computer Emergency Response Team.

Additional controls:

- Who passes information about security incidents to third parties?
- What steps are taken to ensure that no unauthorised persons are passing on any information about the security incident?

S 6.66 Evaluation of security incidents

Initiation responsibility: Agency/company Management, IT Security Management

Implementation responsibility: IT Security Management, IT Security Auditor

Something can be learned from every security incident. To obtain the maximum training benefit from a security incident, evaluation should not be neglected. Often this will result in improvements in dealing with security incidents or permit conclusions to be drawn as to the effectiveness of IT Security Management or the existing IT security measures. The aspects to be considered here include the following:

Time taken to react

Information should be sought on how quickly the security incident was detected. It is necessary here to check whether the technical measures in place for the detection of such incidents require improvement.

The question of how long it took for the report of the incident to travel through the relevant reporting channel should also be examined. Additional aspects which should be considered include how soon decisions were made as to what measures were required, how long they took to implement and when the internal and external parties affected by the incident were informed.

Did the information flow work?

When tracing back the reporting channels used, consideration should be given to whether the reporting channel was known to everyone or whether additional measures are necessary to create the necessary awareness and provide additional information.

Effectiveness of the escalation strategy

The particular security incident should be used to examine whether the defined escalation strategy was adhered to, what additional information is necessary and whether the escalation strategy requires modification.

Effectiveness of the assessment

When looking back on the incident, consideration should be given to whether the extent of the damage caused was correctly assessed, whether the priorities considered were appropriate and whether a Security Incident Team suitable for the investigation was used.

Notification of parties affected

It is necessary here to consider whether all the parties affected were actually notified and whether such notification occurred soon enough. It may be necessary for faster notification channels to be found.

Feedback to the person who reported the incident

Once the problem has been resolved, the parties who discovered the security incident and reported it to the responsible experts should also be informed of the damage which occurred and the measures which were taken. This will demonstrate that such reports are taken seriously and encourage reporting of similar cases in the future. It might also be appropriate to praise or reward

correct reporting in order to bring home to staff just how important it is to report security incidents.

Motivation of perpetrator

If it turns out that the security incident was due to deliberate action, the perpetrator's motivation should be investigated. The motivation is especially important when an insider is involved. If it transpires that the cause lies in the organisation environment, this should be notified to Management as it can then be expected that mistakes and/or deliberate action will occur again.

Depending on the relevance of the evaluation results, Management should be informed so that it can arrange for improvements. It can therefore be sensible to have this evaluation performed by an organisational unit which is not part of the reporting plan.

Development of instructions on actions to be taken

As part of the evaluation of a security incident it is useful to use the results to prepare instructions on actions to be taken or to review the procedures to be followed in the event that a similar security incident occurs again. Once practical experience of the problems is available, instructions on actions to be taken can be developed more efficiently than when the authors are working purely on a theoretical basis. The security incident which occurred also shows that there is a specific need for instructions on the actions to be taken for this type of security incident. Instructions so prepared should be notified to the relevant groups of persons in an appropriate manner.

Additional controls:

- Were the most recent security incidents evaluated?
- Is Management informed once a year about the security incidents?
- How are the specific instructions on actions to be taken updated and communicated?

S 6.67 Use of detection measures for security incidents

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management

Uncovering security incidents

It is very important to detect when security incidents occur as well as trying to prevent them. There are a number of security-relevant irregularities whose detection can be automated using appropriate technical measures, enabling them to be detected early. These detection measures generally increase the reliability of detection and significantly reduce the time between the occurrence of an irregularity and its detection. However, the gain in the ability to react early comes at the effort that is required to implement and monitor such measures. This effort should be estimated in advance. If the potential damage is very large or even entails personal injury, then there is virtually no choice but to adopt such detection measures.

Examples of this kind of detection measures include:

- alarm annunciation devices (see S 1.18 *Intruder and fire detection devices*)
- remote indication of malfunctions (see S 1.31 *Remote indication of malfunctions*)
- virus scanning programs (see S 2.157 *Selection of a suitable computer virus scanning program*)
- intrusion detection and intrusion response systems (see S 5.71 *Intrusion detection and intrusion response systems*)
- cryptographic checksums (see S 4.34 *Using encryption, checksums or digital signatures*)

Combination of technical and organisational measures

Not all security incidents can be detected promptly using only technical measures. Often organisational measures must be used as well. The reliability of automatic detection measures generally depends on how up-to-date these are and how well suited they are to the actual circumstances. The effectiveness of organisational detection measures depends heavily on the reliability of the persons tasked with implementing them and also on how easily the measures lend themselves to being implemented in actual ongoing operations.

Typical examples of detection measures which are wholly or partially of an organisational nature are:

- obtaining information on security weaknesses of the system (see S 2.35 *Obtaining information on security weaknesses of the system*)
- regular security checks of selected IT systems (e.g. see S 2.92 *Performing security checks in the Windows NT client-server network*, S 4.93 *Regular integrity checking* and S 5.8 *Monthly security checks of the network*)
- regular analysis of log files (e.g. see S 2.64 *Checking the log files*, S 4.5 *Logging of PBX administration jobs*, S 4.25 *Use of logging in UNIX systems*, S 4.47 *Logging of firewall activities*, S 4.54 *Logging under Windows NT*, S 5.9 *Logging at the server*)

Additional controls:

- What detection measures are in use?
- Are steps taken to ensure that anything unusual in the log files gets reported?

S 6.68 Testing the effectiveness of the management system for the handling of security incidents

Initiation responsibility: IT Security Management

Implementation responsibility: IT Security Management, IT Security Auditor

The management system for handling security incidents must be checked at regular intervals to ensure that it is up-to-date and effective. In addition, the measures incorporated within it should be regularly tested to see whether

- they are known to the staff concerned,
- it is feasible to implement them under stress, i.e. in the event of a security incident which prevents operations from running in the proper manner, and
- they can be integrated into operating procedures.

Review of the management system

To test the effectiveness of the management system, damaging events should be simulated in order to review whether defined procedures are being adhered to or whether it is actually feasible to implement them. If they are not actually implementable, appropriate changes must be made.

To test this, both announced and unannounced exercises/practice runs can be held.

Practice runs must not result in any damage

When exercises/practice runs are carried out unannounced, under no circumstances must any actions be triggered which could result in any damage to IT systems, data or otherwise, either of a permanent nature or which can only be rectified with difficulty.

Before beginning any exercise/practice run, careful consideration should be given as to who should receive advance notice of it. It is essential to ensure that the exercise/practice run is authorised by Management. It can sometimes be useful not to inform certain person groups, e.g. entrance control staff or administrators. However, steps should be taken to ensure that this does not prevent the situation from remaining under control. Alarming the police or fire department or cutting back the network connections of the authority/company should thus be avoided.

Examples:

Simulated damaging events

- Phone the switchboard of your company/authority and pretend to be a hacker who has broken into the internal network. Alternatively, you could pretend to be a journalist who claims to have heard that a hacker has broken into the internal network and copied sensitive data. The staff who would typically be called in in such cases, such as the Press Officer or the Head of the IT Section, could also be phoned. The aim of such a phonecall should be to find out whether internal panic breaks out or whether actions which would be adequate for such a case are implemented in a purposeful fashion.
- All the actions and reporting channels which are supposed to be employed in a case of infection with a computer virus could be tested in one day. Those involved should not necessarily all be informed in advance, but at the latest at the point where they are integrated into the action chain.

Additional controls:

- What exercises/practice runs were last carried out?
- Are exercises/practice runs agreed with Management in advance?

S 6.69 Contingency planning and operational reliability of fax servers

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Administrator, fax mail centre

Measures for contingency planning and operational reliability of fax servers depend on the volume of material processed over the fax server(s) and the required availability of this service.

Document configuration parameters

As a first step all configuration parameters for the communications cards, operating system and fax server application used must be documented. Whenever the configuration is changed, the documentation must be updated accordingly. Only in this way will it be possible to reinstall a fax server in the shortest possible time in an emergency.

Regular data backup

Moreover, data backups should be performed at regular intervals, as stipulated in the data backup policy and the security policy. Backups should not be confined to the data partitions but also cover the partitions on which the operating system and the fax server applications are located.

The fax transmissions stored on the fax server must be backed up at regular intervals. Where permanent archiving of fax data is desirable, this should be performed not on the fax server but on external data media.

Hold conventional fax machines in reserve

One or more conventional fax machines should be held in reserve so that in the event of failure of the fax server or the network it is still possible to send and receive faxes. The number of machines required depends on the volume of incoming and outgoing fax transmissions in emergencies. It is sensible to keep the fax machines which were used prior to installation of the fax server as an emergency fallback.

All other available measures aimed at increasing operational reliability are expensive and should therefore only be considered where availability is very important. Such measures should be considered on a case-by-case basis.

Use of RAID systems

As a first step, the IT system on which the fax server is installed can be equipped with a RAID system. This entails merging several hard disks into a single pool and distributing the data contained on them in such a way as to ensure data redundancy. With RAID level 5, this means that if one hard disk fails no loss of data occurs. However, when RAID technology is used, it has the effect of reducing the overall capacity of the hard disks due to the creation of redundancy. It should also be remembered that this solution is no substitute for external data backups, nor does it protect against total failure of the system.

Use of several fax servers

Operational reliability can also be achieved through the use of several fax servers. If one server fails, the load can be distributed over the other servers. Another advantage of this solution is that the load is split so that the danger of overloading one individual fax server is reduced. On the other hand, any incoming fax transmissions which are located on the failed server will not be available at least for the duration of the failure.

Use of redundant fax servers

If the availability requirements are such that failures on fax servers can only be tolerated for a matter of minutes, then the use of redundant servers is recommended. For each fax server which is integrated into such a redundancy concept, a second server is then available on which the relevant data is replicated. This solution, if necessary combined with RAID systems, provides the maximum operational reliability; however it is very expensive.

Additional controls:

- Is documentation of the configuration up-to-date?
- Who is responsible for performing backups?
- Are any conventional fax machines available in case of emergency?

S 6.70 Creation of a contingency plan for failure of the RAS system

Initiation responsibility: Head of IT Section, IT Security Management Team

Implementation responsibility: Administrator

Depending on the availability requirements, failure or non-availability of RAS connections could be extremely serious. However, there are a large number of potential sources of failure so that it is often difficult to establish the exact cause. As well as failure of the connection infrastructure (see on this point also T 1.10 *Failure of a wide area network*), RAS clients and the RAS server, plus the network switching elements used for the connection (see also T 4.31 *Failure or malfunction of a network component*), are naturally additional potential points of failure in a RAS system.

If a component of the RAS system (client, server, network switching elements) fails, the result could be that important data and information cannot be exchanged and that work routines are interrupted until the connection is re-established or alternative solutions have been found.

If the RAS system fails, the linking of external computers (e.g. individual telecommuting workstations or entire LANs of branch offices) can no longer be assured so that, for example, it is possible that data can no longer be exchanged. Depending on the operational scenario, this can lead to significant impairment of IT operations. Contingency planning and the creation of a contingency plan for the partial (e.g. failure of the authentication server) or total failure of the RAS system are therefore extremely important.

In the context of contingency planning for the RAS system, the general safeguards contained in module 3.3 *Contingency planning concept* are relevant. The following safeguards should also be considered:

- S 6.18 *Provision of redundant lines*
- S 6.31 *Procedural rules following a loss of system integrity*
- S 6.37 *Documenting data backup procedures*
- S 6.54 *Procedures in case of a loss of network integrity*

These safeguards should be made more specific to the components and data which reside in the RAS system environment and implemented.

In particular, the contingency plan should cover the following aspects:

- What specific faults, damage and consequential damage will occur upon failure of a RAS connection?
- For which RAS connections must high availability be guaranteed?
- How quickly can the failure of a RAS system be determined?
- Can faults in the telecommunications networks used for connections (e.g. connection problems, problems with the transmission of call numbers, problems with the connection of closed user groups) be detected quickly as such or are they communicated to the responsible administrator?

- How quickly can a RAS connection be restored (by replacement of equipment, restarting the system)?
- Which component failures require that the RAS system is shut down even though technically RAS connections can still be established (e.g. failure of logging, encryption of communications or of the authentication server)?

Setting up emergency call numbers

For remote users, an emergency call number should be available so that they can notify the responsible persons promptly of any RAS problems. Moreover, the RAS system should be permanently monitored at critical periods (e.g. office hours, periods in which data is primarily exchanged by RAS).

Create contingency documentation

Suitable procedures should be developed for individual damage scenarios in the form of contingency documentation. All the data that is necessary to resolve an emergency should be included in this documentation and presented in such a way that deputising staff can also work with it. The contingency documentation should also contain information on alternative connection paths, e.g. alternative telecommunications providers or alternative transmission media.

Prepare recovery plan

Depending on the availability requirements for the RAS system, it may be necessary to hold replacement equipment in reserve so that faulty items can be replaced immediately. To ensure that the RAS system can be started up again after equipment replacement or a system crash, the contingency documentation must contain a recovery plan. If necessary, it may even be necessary for it to be possible to replace certain components while the system is running. Such a hot swap must be supported by the components used.

Check data integrity after failures

Depending on the RAS system, the consistency of data being transmitted by RAS during a system crash cannot be assured. After every failure the integrity of this data should therefore be checked and a problem analysis should be carried out in order to avoid repetitions as far as possible.

Secure emergency configuration

In certain situations it can be necessary to operate the RAS system with limited functionality or performance. In this case a corresponding fallback configuration must be activated (see also S 4.111 *Secure configuration of the RAS system*). This enables the security of the RAS system (access security, communication security) to be maintained even during restricted operation.

S 6.71 Data backup for a mobile IT system

Initiation responsibility: IT Security Management Team, Head of IT Section

Implementation responsibility: Administrator, IT users

Mobile IT systems (laptops, notebooks) are generally not permanently integrated into a network. Data exchange with other IT systems is normally effected over data media or temporary network connections and can, for example, be implemented through remote access or direct connection to a LAN on returning to the workplace. Unlike with stationary clients, it is therefore generally unavoidable with mobile IT systems that data at least temporarily has to be stored locally instead of on a central server. Appropriate data backup measures must be taken to prevent loss of this data.

Generally the following data backup procedures are available:

1. **Data backup on external data media**

   The advantage of this method is that the data can be backed up in virtually any location and at any time. The disadvantage is that a suitable drive and sufficient data media must be carried and that proper handling of the data media entails additional effort on the part of the user. The data media should possess sufficient storage capacity so that the user does not have to insert several media into the drive every time a backup is performed. Where the data is kept in unencrypted form, there is also the danger that data media could get lost and that as a result sensitive data could be compromised. The data media and the mobile IT system should as far as possible be kept separate from each other so that in the event of loss or theft of the IT system the data media are not lost as well.

   Storage on external data media for data backup purposes is especially recommended where data is also exchanged with other IT systems using external data media, as it may be possible to combine the two processes. On returning to the workplace, the data backups on the data media must be incorporated into the backup system or the operational system or into the central databank of the organisation.

2. **Data backup over temporary network connections**

   If it is possible to connect the IT system to a network regularly, for example using remote access, the local data can also be backed up over the network connection. The advantage of this is that the user does not have to bother with any data media, nor does he have to take the appropriate drive along with him. Moreover, the procedure can be largely automated, for example, with remote access data backup can be automatically initiated following every dial-in.

   When backing up data over a temporary network connection it is essential that the bandwidth of the connection is adequate for the volume of data to be backed up. Transmission of the data must not take too long or lead to excessive delays if the user has to access remote resources at the same time. With current access technologies (e.g. ISDN, modem, mobile phone) this means that only low volumes of data can be transported on each

backup process. Some data backup programs therefore offer the possibility of only transmitting information about changes in the data set which have occurred since the last backup over the network connection. In many cases, this can significantly reduce the volume of data to be transported.

An important requirement for the software used for data backup is that unexpected termination of a connection should be detected and handled in a proper manner. Termination of a connection must not result in impairment of the consistency of the data backed up.

Under both data backup methods it is desirable to minimise the volume of data to be backed up. As well as using loss-free compression techniques, which are integrated into many data backup programs, incremental or differential backup procedures can also be used (see also S 6.35 *Stipulating data backup procedures*). However, use of such procedures means that restoration of a data backup takes longer.

Data backup should be automated as far as possible so that users themselves are required to perform as few actions as possible. If users must be involved, they should be placed under an obligation to perform regular backups (see S 2.41 *Employees' commitment to data backup*). Finally, sporadic checks should be carried out to verify that data backups created can be restored (see S 6.22 *Sporadic checks of the restorability of backups*).

Additional controls:

- Is all the data which is stored locally on mobile IT Systems backed up regularly?
- Is the chosen backup method suitable for the volume of data?
- Is the number of actions required of the user during data backup kept to a minimum?

S 6.72 Precautions relating to mobile phone failures

Initiation responsibility: Head of IT Section, IT Security Management

Implementation responsibility: Head of IT Section, users

There are a number of reasons why a mobile phone could fail or its operational capability could be impaired. This is of course particularly annoying when the mobile phone is needed urgently or the result of its being unoperational is that important data is lost. Therefore appropriate precautions should be taken in advance to avert the possibility of failure or at least minimise any problems which this will entail.

Power supply

The state of charge and functional condition of the mobile phone battery should be checked at regular intervals (see also S 4.115 *Safeguarding the power supply of mobile phones*).

Regular data backups

All data stored on the mobile phone such as telephone directory entries, messages etc should be saved to a different medium at regular intervals so that in case of doubt they can be reconstructed. A number of possibilities are available here:

- The most important settings, PINs and the configuration of security mechanisms should be documented in writing and stored securely to reflect the relevant protection requirements.
- All data which is stored on the SIM card, e.g. telephone directories, can be read into a PC with a SIM card reader and appropriate software and managed there. This has the further advantage that address data is easier to maintain and synchronise with other address databases on a PC than on a mobile phone. In particular, where several mobile phones are used (see also S 2.190 *Setting up a mobile phone pool*) it is appropriate to use such means to make sure that all telephone directories are consistent with each other. If only the data on the SIM card is backed up, all the users must be informed that they should always save call numbers and similar there.
- The mobile phone can also be coupled with another IT system, e.g. a notebook or organiser, which in turn is then used to exchange the data to be backed up (see also S 5.81 *Secure transmission of data over mobile phones*). Here, the data held both on the SIM card and also in the phone itself can be backed up.

Keep a spare phone handy

If it is important that a mobile phone is available at all times, a spare mobile phone, or at least a spare battery, should be carried too.

Where mobile phones play a critical role in the generation of alarms, e.g. if an intruder detection device sends alarm messages over GSM or emergency personnel are to be informed by mobile phone, a contingency option must always be available.

Repairs

When a mobile phone develops a fault, it could be that the entire device fails or only individual components. Repairs should only be undertaken by trusted specialist businesses. For this reason, a list of appropriate specialist businesses should be available.

Many dealers also provide replacement equipment for the duration of the repairs. With devices like mobile phones, where the technology is changing all the time, it is often not worth performing a repair so that sometimes a replacement device is offered. Since it is particularly important with a mobile phone that the device is available at all times, when selecting the mobile phone or dealer care should be taken to ensure that such services are offered.

Before taking the mobile phone to be repaired, all personal data, e.g. the call memory, any e-mails saved and the telephone directory held on the phone should be deleted (see also S 2.4 *Maintenance/repair regulations*). It goes without saying that these should be backed up first. The SIM card should also be removed.

Additional controls:

- Does the contingency plan include a list of dealers who specialise in mobile phones?
- Is data stored on mobile phones backed up at regular intervals?