T 1 Threats Catalogue Force Majeure

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.

Key positions in the IT area

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.

Loss of knowledge and secret information

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 central components

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. LAN server or data transmission facilities. Failure of components of the technical infrastructure, for example air conditioning or power supply facilities, can also help induce an IT system failure.

Technical failure / human error

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*, T *5.91 Sabotage*). Loss or damage can also occur as a result of 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 supply 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 loaded 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.
- A power failure in an internet service provider's storage system resulted in this being shut down. Although it was possible to fix the actual error quite quickly, the IT systems affected would not boot up correctly as there were inconsistencies in the file system. Several of the web servers operated by the ISP remained out of action for days until all the consequential problems had been resolved.

Failure of an archive component

- In electronic archives, it is possible for the date of first archiving to be misinterpreted as the document creation date if no other procedures for the introduction of evidence, such as time stamping services, are followed for certification purposes. This primarily affects business processes into which the electronic archiving of large quantities of document data is transparently integrated. In one case, failure of an archive component meant that archiving of some of the document data was delayed by a day. Because WORM media were used, the sequence in which the business documents were physically archived was documented and could therefore be proven, but the delay that occurred as a result of the failed archived component was not documented. As a result during a subsequent check it looked as if the documents had been tampered with after archiving.

T 1.3 Lightning

Release of electrical energy

The occurrence of lightning during a thunderstorm is a major threat to a building and the IT facilities accommodated there. With a voltage of several hundred thousand volts, lightning strikes can achieve currents of up to 200,000 amperes. This enormous electrical energy is released and dies away within a period of 50-100 microseconds. A lightning strike of this order of magnitude originating from a distance of about 2 km will still cause voltage peaks that are capable of destroying sensitive electronic devices in the power lines of the building. The closer the lightning strike is, the greater the indirect damage.

Damage to buildings

If a building is directly hit by lightning, damage will be caused by the dynamic energy of the lightning 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.

Examples:

- At a major German airport there was a lightning strike very close to the air traffic control tower. Despite the external lightning protection system (lightning conductor) that had been installed, the automatic fire extinguishing system in the IT area was triggered and as a result all airport operations were paralysed for two hours.
- As well as direct damage, lightning often has more far-reaching consequences. Reports such as that reporting a lightning strike on a high-voltage line in the vicinity of Darmstadt in April 1999 that resulted in a short-term power failure affecting around 80,000 persons are quite common.

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. For example, damage from water for fire fighting does not occur only 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, when combined 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. But even "normal" smoke given off by fire can have harmful effects on IT equipment.

Fires can be caused not only by careless handling of combustible material (e.g. Christmas candles, welding and soldering work etc.), but also by improper use of electric devices (e.g. unattended coffee machines, overloading of multiway socket outlets). Technical faults on electrical equipment can also cause fires.

Factors which help fires to spread include:

- wedging fire doors open
- improper storage of combustible materials
- failure to observe relevant standards and regulations
- absence of fire detection devices
- absence of hand fire extinguishers and automatic quenching systems
- deficient fire prevention (e.g. lack of fire insulation along cable routes).

Examples:

- In the early 90s, a mainframe computer centre in the Frankfurt region was hit by a disastrous fire, leading to total failure.
- It is an all too common occurrence that small electrical devices such as coffee machines or halogen lamps are not installed or operated in the proper manner, causing fires as a result.

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 installation
- defects in air conditioning systems connected to the water supply
- defects in sprinkler systems
- water used for fire-fighting
- water sabotage, e.g. deliberately turning on the taps and blocking drains.

Irrespective of how water enters buildings or rooms, there is a danger that it will damage supply facilities or IT components (e.g. short-circuit, mechanical damage, rust, etc.) or render them unserviceable. Where central supplies for the building (main power distributor, trunk distribution frame for telephone, data) are accommodated in basement rooms without automatic water removal, the ingress of water can cause considerable damage.

Examples

- Many commercial enterprises, even large companies, do not give sufficient thought to the danger of flooding. Thus, for example, one company has experienced "surprise" flooding of its computer centre on more than one occasion. The computer centre swam in the truest sense of the word a second time barely 14 months later. The resulting damage ran to several hundred thousand euros and was not covered by any insurance policy.
- A water pipe in a server room ran down from a ceiling that was covered with plasterboard. When one of the joints developed a leak, this went undetected for some time. The escaping water initially collected at the lowest point of the plasterboard, eventually escaping and causing a short-circuit in the power distributor underneath. The result was that until the repairs were completed, both the water and the power supply of the affected part of the building had to be switched off.

T 1.6 Burning cables

When a cable catches fire, either by spontaneous ignition or kindling, this can have a variety of consequences:

- The connection may go down.
- The formation of aggressive gases may occur. These could not only be corrosive and hence affect IT and communications equipment, but they could also be toxic, resulting in personal injury (e.g. poisoning).

"Aggressive" gases

- Cables with non fire-resistant or self-extinguishing insulation material may help the fire to spread. Even fire sealing cannot prevent this completely, but merely delay the spread of the fire.

Dispersion through cable shafts

- 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 breaks out into the open.

Example:

In an east German administrative building the existing electrical cables were not replaced for cost reasons but were unwisely overloaded. The necessary modification work was not carried out as the staff were expecting to be shortly relocated to a new administrative building.

The overloaded lines heated up and because they were laid so close together an accumulation of heat occurred. This eventually resulted in a smouldering fire. The fire was only discovered when the cables failed due to the huge amount of heat. It took two days to restore the workstations affected by the fire to a condition where they could be used again.

T 1.7 Inadmissible temperature and humidity

Every device has a defined temperature range within which its proper functioning is ensured. A rise or fall in the room temperature to a value outside that range could result in operational malfunctions or equipment failures.

IT systems as a source of heat

Thus, for example, equipment located in a server room converts electrical energy to heat, causing the temperature in the room to rise. If ventilation is insufficient, the operating temperature of the devices may exceed the permitted upper limit. In the case of solar radiation, it is quite feasible for the temperature in a room to exceed 50°C.

The windows in a server room are frequently opened for ventilation purposes. At times of temperature variation (in the spring or autumn), this can cause large temperature fluctuations, with humidity levels exceeding the permitted ceiling during subsequent drastic cooling down.

Defects in long-term storage media

Where long-term storage media are stored, it is possible for excessive fluctuations in temperature or excessive humidity to cause data errors and reduce the useful life of the media. Some manufacturers specify the optimal storage conditions for long-term storage media at temperatures of 20-22ºC and 40% humidity.

Example:

In a Bonn-based agency, the entire control and evaluation electronics system of a security facility was accommodated in a room in which there was only just enough space left to open the doors of the equipment cabinets. For security reasons, the doors to both the cabinets and the room were kept firmly locked.

After completion of the installation in the autumn, the equipment functioned smoothly, but the following summer, some unaccountable malfunctions occurred. These were followed soon afterwards by total system crashes, for which there was no obvious cause. Several days of troubleshooting, involving high technical and manpower effort and carried out with the doors open, yielded no results. It was only by accident that the cause of the problems, overheating of the facilities under external temperatures above 30°C, was finally identified, and was remedied with the installation of an air conditioning system.

T 1.8 Dust and dirt

Dust can damage electronics

Despite the pervasiveness of electronics in IT, this still relies on mechanical components. These include diskettes, hard disks, removable hard disks, disk drives, printers, scanners etc., plus fans for processors and power supply 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. Large amounts of dust and dirt can be generated, for example, in connection with

- work on walls, raised floors or other parts of the building,
- hardware upgrades,
- unpacking of equipment (e.g. escape of styrofoam packaging materials).

This can cause corresponding hardware failures.

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.

Examples:

- 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 supply 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 supply unit fan failed also, causing the power supply unit to overheat and short circuit. This in turn induced the total failure of the server.
- To hang a wall panel in an office, holes were drilled into the wall by the site technical service. The employee whose office it was had left his office for a short time. When he returned to his desk he found that his PC would not work any more. The reason for this was the dust generated by the drilling, which had penetrated into the PC power supply unit through the ventilation slits.

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 1.11 The effects of catastrophes in the environment

Problems in the vicinity of a public body or company can lead to a spectrum of problems ranging from operational difficulties through to non-productive time. These can run from technical accidents and collision damage through to political unrest, demonstrations or riots (see also T 1.12 *Problems caused by big public events*).

An organisation's property can be exposed to various dangers from the environment through traffic (roads, rail, air, water), business operations in the neighbourhood or residential areas. These could be caused, for example, by fire, explosions, dust, gases, blocking of access, radiation, emissions (chemical industry).

Preventive or rescue measures could directly affect the property. Due to the complexity of building technical services and IT facilities, however, there can also be indirect problems.

Example:

During a fire in a chemical operation in the immediate vicinity of a computer centre (approx. 1000 m away as the crow flies) a huge cloud of smoke developed. The computer centre had an air conditioning and ventilation system which did not have any external air monitoring sensors. It was only due to the thoughtfulness of a member of staff (the accident occurred during working hours) who followed the development and spread of the smoke that the outside air intake was manually switched off before it was too late.

T 1.12 Problems caused by big public events

Big events of all kinds can have a disruptive impact on normal business operations of an agency or company. These include street festivals, concerts, sporting events, industrial disputes and demonstrations. Rioting in the vicinity of such events can in addition have results such as intimidation of staff through to the use of violence against personnel or the building.

Examples:

- During the hot summer months a demonstration took place in the vicinity of a computer centre. The situation escalated and some violence occurred. In a side road one of the computer centre's windows was open, and a demonstrator took the opportunity to climb in and steal some IT hardware containing important data.
- During the setting up of a big fair by mistake an electrical transmission line was cut. In a computer centre that received its electrical supply from this transmission line this resulted in a failure, although it was possible to cushion it using the existing standby generator unit.

T 1.13 Storms

The effects of a storm or hurricane on external facilities which are indirectly necessary for operation of computer centre are often underestimated. External installations can be damaged or uprooted as a result. Objects that are torn up and flung around by the storm can cause further consequential damage. Moreover technical components can have their functionality harmed as a result of storms.

Examples:

- Cooler pipes for the air conditioning system of a computer centre had been laid on the roof using flexible hard PVC hoses but over wide distances on the roof facing they were neither held down or fastened. They were grabbed during a hurricane and swept from the roof of the building, in the course of which they were uprooted from their fastenings. The cooling liquid escaped and the system had to be shut down for several hours. For the duration of the storm, due to the danger of being blown off the roof, it was not possible to undertake any repairs. The server park was down for almost 12 hours. It supplied approximately 12,000 users.

Loosely laid cooler pipes

- In another case a lamellar wall that was used to visually cover the recooling plant on the roof of the process computing centre of an industrial plant collapsed. The sharp metal edges cut through the electric cables of the recooling plant. There was a short-circuit with electric arc, as a result of which the roof facing that had been torn off by the storm caught fire. At the same time the overturned covering functioned to some extent as a windshield, but it allowed enough wind through to kindle the fire. The fire continued in the insulation between sheet with trapezoidal corrugations and liner sheets. It was only by good luck that total loss was avoided.

Protective covers torn off during storm

T 1.14 Loss of data due to strong light

CD-ROM, CD-RW, DVD-RAM, DVD-RW and MO are all typical data media that entail optical storage media. Information is added to them using read/write heads and lasers. Such data media are sensitive to strong light, especially in the ultraviolet spectrum, so that proximity to such light sources should be avoided.

The extent of data loss caused by this radiation depends on its intensity and duration. This is particularly critical for files which, due to their internal formatting, are rendered completely useless by just minor changes (e.g. Postscript files, databases or encrypted files).

Examples of strong light sources are:

- sunlight (especially on cloudless summer days or at altitude)
- halogen lamps
- special neon tubes

T 1.15 Degradation due to changing application environment

Mobile devices are used in a very wide range of environments and are subject to numerous hazards. These include, for example, damaging environmental conditions such as excessively high or excessively low temperatures, as well as dust or moisture. Other problems related to the portability of the devices include, for instance, transport damage.

Unknown environment - unknown risks

An important aspect of mobile devices is, however, also that they are used in areas of varying levels of security. In some environments the level of security is clearly known to the users, in other it is not. Along with portability, the ability to communicate with other IT systems is also a reason for the use of PDAs, laptops and other mobile devices. For this reason the problems that could be caused by interaction with other IT systems must also be taken into consideration. Within the own organisation, the integrity of IT systems can be estimated to a certain degree. However, this estimation is difficult in external environments. Communication with unknown IT systems and networks can always involve potential threats for the own mobile system and its applications and data. On making contact with other IT systems, for example, computer viruses or Trojan horses may also be transferred.

For this reason, on the return of mobile systems it always necessary to ask where the PDA has been used and to observe the related precautionary rules.

A further problem on the use of external infrastructures, such as on downloading information at trade shows, is the frequent insufficient transparency of the services offered. Many service providers collect customer data to be able to create profiles, on the one hand to be able to offer services that are better tailored to their customers, but also to be able to sell these data to other providers. For example, profiles could be created solely by evaluating the information on the physical locations and the communication behaviour of the user (which services, when, how often, with whom). It is also possible for applications run entirely on the own mobile terminal device to collect data (e. g. on frequency of use and type of use) and to forward the data as soon as the device goes online.

Mobile terminal devices are lost or stolen time and again. The smaller and more desirable such devices are, for example PDAs, the greater this risk. Along with the direct loss, in this case further damage can be caused by the loss and the disclosure of important data.

T 2 Threats Catalogue Organisational Shortcomings

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 Management
T 2.67	Inappropriate administration of access rights
T 2.68	Absence of or Inadequate Planning of Active Directory
T 2.69	Lack of, or inadequate, planning of the use of Novell eDirectory
T 2.70	Lack of, or inadequate, planning of partitioning and replication in Novell eDirectory
T 2.71	Lack of, or inadequate, planning of LDAP access to Novell eDirectory
T 2.72	Inadequate migration of archive systems
T 2.73	Inadequate audit trail of archive systems
T 2.74	Inadequate indexing keys for archives
T 2.75	Inadequate capacity of archival storage media
T 2.76	Inadequate documentation of archive accesses
T 2.77	Ineffectual transfer of paper data to electronic archives
T 2.78	Ineffectual regeneration of data stocks during archiving
T 2.79	Ineffectual regeneration of digital signatures during archiving
T 2.80	Ineffectual auditing of archiving procedures
T 2.81	Ineffectual destruction of data media during archiving
T 2.82	Poor planning of the archive system location
T 2.83	Flawed outsourcing strategy
T 2.84	Unsatisfactory contractual arrangements with an external service provider
T 2.85	Inadequate provisions for termination of the outsourcing project
T 2.86	Dependency on an outsourcing service provider
T 2.87	Insecure protocols in public networks

T 2.88	Negative impact of an outsourcing project on the organisational climate
T 2.89	Inadequate IT security during the outsourcing implementation phase
T 2.90	Weaknesses in the connections with an outsourcing service provider
T 2.91	Poor planning of the migration of Exchange 5.5 to Exchange 2000
T 2.92	Poor control of browser access to Exchange
T 2.93	Inadequate contingency planning concept with outsourcing
T 2.94	Inadequate planning of the use of IIS
T 2.95	Inadequate concept for linking other e-mail systems to Exchange/Outlook
T 2.96	Outdated or incorrect information on a website
T 2.97	Inadequate contingency planning with an Apache web server
T 2.98	Incorrect planning and design of the use of routers and switches
T 2.99	Inadequate or incorrect configuration of the zSeries system environment
T 2.100	Errors on applying for and managing Internet domain names
T 2.101	Inadequate contingency planning for a security gateway

T 2.1 Lack of, or insufficient, rules

The importance of organisational rules and requirements for IT security objectives increases with both the scope of information processing and the protection requirements of the information to be processed.

Starting from the assignment of responsibilities through to the distribution of control functions, the spectrum of rules can be very broad. The consequences of a lack of or insufficient rules are illustrated in T 2.2 ff.

Often existing rules are not modified after changes of a technical, organisational or personnel nature that have a significant impact on IT security. Out-of-date rules can impede smooth IT operations. Problems can also arise as a result of the fact that rules are written in a manner that is incomprehensible or without the contextual information needed, so that they are misunderstood.

The following **examples** illustrate the potentially harmful effects of shortcomings in this area:

- Poor resource management could seriously impair scheduled operations in a computer centre e.g. simply because an order for printer paper has been forgotten.
- Hand-held fire extinguishers once purchased need to be maintained systematically so that they are ready for operation in case of fire.

T 2.2 Insufficient knowledge of requirements documents

Drawing up rules and procedures does not of itself guarantee the smooth flow of IT operations. Each individual in the organisation must be aware of the rules and procedures that apply to him. The damage which can result from inadequate knowledge of existing rules and procedures cannot be excused by saying, "I didn't know I was responsible for that," or "I didn't know what to do."

Examples:

- If employees are not informed of the procedure for handling incoming floppy disks and e-mails, there is a danger that a computer virus could be spread throughout the company/agency.
- In one federal agency, differently coloured waste paper bins were introduced, with one colour intended for documents requiring disposal. Most employees were not aware of the significance of the waste paper bin colour.
- In a federal agency there were a number of rules regarding the carrying out of data backups which had been verbally agreed over a period of time between the IT Security Officer and the IT Department. On enquiry, it turned out that the IT users concerned knew nothing about the "agreements" and had no point of contact to discuss them with. The rules regarding data backups were not documented either. As a result many users unnecessarily took local backups.
- A new rule was introduced in a computer centre that in the event of problems with the intruder detection or fire alarm systems the porter's lodge would be manned by night as well. The security guard service, which organised its own rotas, was not informed of this new rule by the security officer. As a result, the computer centre was unprotected for several weeks.

T 2.3 Lack of compatible, or unsuitable, resources

Insufficient provision of resources or failure to make them available on time can disrupt IT operations considerably, interrupting service. Similarly, it can happen that unsuitable or even incompatible resources are procured, which consequently cannot be used.

Examples

- The change of millennium could have caused 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 connection is delayed.
- An example of an unsuitable resource is a graphical user interface that is installed on a computer with insufficient performance.
- An example of incompatible resources is connecting cables with different pin assignments that are intended to be used to connect 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 safeguards

Once measures aimed at achieving IT security (e.g. data backups, access control, rules regarding conduct during emergencies) have been introduced, they must also be consistently implemented. If monitoring of IT security safeguards is absent or only inadequate, it is not possible to ascertain whether they are being flouted or are proving effective. This makes it impossible to respond promptly and in a manner appropriate to the situation.

In addition, some security safeguards can only be effective if appropriate controls are implemented. These include, for example, logging functions whose security characteristics only become apparent when the log data is analysed.

Examples:

- The administration console for a computer system is connected to a console printer. All user inputs from the console are to be logged to the printer. It is only by analysing the printouts that any improper action by administrative staff can be detected. Unless such an analysis is carried out by an independent person, logging will be ineffective.
- As a prelude to committing a criminal offence, lock cylinders in external doors and gates are replaced. Access routes which are seldom used or are only envisaged as emergency accesses are frequently checked only to ensure that they permit free exit. The lock cylinder is not tried out.
- In a public agency some UNIX servers are used for external data communications. Due to the central importance of these IT systems the IT security policy specifies that UNIX servers are to be integrity checked on a weekly basis. It is only when investigating a security incident that it comes to light that the IT department has not been performing these integrity checks. The reason given was insufficient manpower resources in the department.
- The role of z/OS Security Auditor is unoccupied in a company. As a result, the RACF configuration settings gradually cease to be in line with the security requirements of the company. Only after a production failure is it noticed that some users have more substantial permissions than they require for their work. They have stopped an application that was important to production.

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 the 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 the 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 prevent a data medium from being 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. It is not possible to recover some data urgently needed for some time, as the tapes cannot be found immediately.
- By mistake, backup tapes with different contents are labelled identically. The archive keeper inadvertently releases the most recent tape for deletion. As a result only an outdated backup is available.
- Tape administration systems in the z/OS operating system use batch jobs to identify data backup tapes whose expiry dates have been reached so that they can be cleared for overwriting. If such a batch job crashes or does not even start, then it is possible that there might not be sufficient empty tapes ("scratch tapes") for the delta backups and this could result in bottlenecks in tape processing.

T 2.11 Insufficient route dimensioning

During planning of networks, server rooms or computer centres often the mistake is made of defining the functionality, capacity and/or technical security design from the present status. This approach fails to take account of the facts that

- the capacities of the network and computers will have to be extended in line with increases in data volumes or the use of new services;
- changes in technical standards may make architectural or technical security modifications necessary;
- the possibility that the network will need to be expanded can never be ruled out;

and

- new requirements imposed on a given network may make it necessary to lay other cables.

Examples:

- Expansion of networks is possible only to the extent permitted by the installed cables or by the availability of space for additional cables. Especially where cables are accommodated in closed routing (piping, plaster-covered underfloor channels, etc.), even where space is available, it is often not possible to insert additional cables without damaging new or old cables. The only alternative is to pull the existing cables out of the route and re-lay all the cables, old and new, at the same time. The resulting disruption of operations and costs can be considerable.

Not possible to replace individual cables

- In the early stages of planning a computer centre the only criteria considered were aesthetic considerations. Infrastructural and security technical requirements were given less priority and were only specified after the basic construction work was complete. The completion of the building had to be extensively delayed because routes that were required were not available and the size and positioning of individual rooms did not match the requirements. Changes during later operations were very difficult to implement.

Routes not planned in

- After ten years of operations a complete new network structure and IT cabling were planned in a company. On investigation it turned out that renewal of the private branch exchange and the PBX cabling, which up to now had followed the same routing as the IT cabling, was planned for the following year. Without co-ordinating these two measures, work on the routing would have had to be duplicated and possibly the routes planned would have been too small.

Poor co-ordination

T 2.12 Insufficient documentation on cabling

If, due to inadequate documentation the precise location of cables is not known, these cables could be damaged during construction work outside or within a building. This could 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 scope of the services to be provided did not include the preparation of documentation. Since no maintenance agreement was concluded with that firm after completion of the work, the required documentation was not available to the agency. This resulted in considerable delays when the agency subsequently tried to expand the network.

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, it 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

Where 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. In this case, anyone who gains possession of the disk could decrypt the information, provided that the encryption procedure used is known.
- Cryptographic keys are usually generated by random processes and may be post-worked. If the source of random numbers is unsuitable, insecure keys may be produced.

Bad source of random numbers

- It is vital for security that the cryptographic keys generated are not weak, particularly in the case of masterkeys. Weak keys may be those that are easily guessed or that are unsuitable for encryption (e.g. weak and semi-weak DES keys). If the weakness of keys is not checked when they are derived from masterkeys, weak keys may come into active use.

Poor choice of keys

- 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 by accidentally being deleted or 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 or incorrect supply of consumables

Many machines used every day in offices - such as fax machines, printers and data backup drives - require a sufficient supply of consumables to continue to work correctly. A lack of available consumables may cause critical interruptions to operations; in emergency situations, it may severely limit the capacity to respond, resulting in high consequential costs.

Examples:

- If paper or ink are used up, incoming fax transmissions can not be printed even if they were correctly received. Due to its limited capacity, the buffer memory can only delay the rejection or loss of fax transmissions; it can not prevent it altogether in the long-term.
- A newly purchased tape streamer is not compatible with the old tapes. No new, suitable tapes have been bought, meaning that no data backups can be performed for several days.
- An important print job is pending, but the spare ink cartridge that was bought is not suitable for the printer.

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 log data

Log data serves the purpose of allowing one to determine after the event whether any security breaches have taken place or have been attempted in the IT system. Log data can thus be used to identify the perpetrator in case of damage. Another important function of log data is deterrence. If log data is evaluated on a regular basis, wilful attacks on an IT system can be detected at an early stage. If the log data is not analysed or only inadequately and this becomes known, it losses its function as a deterrent.

Many IT systems or applications are lacking in adequate logging facilities. In some cases there is no provision for logging at all and in others it is often not possible to identify particular events in the log.

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. It is therefore impossible to determine whether any security breaches have occurred or have been attempted in the IT system.

T 2.23 Security flaws involved in integrating DOS PCs into a server-based network

The introduction of DOS PCs into a server-based network can create security flaws in an otherwise secure network.

If, for example, DOS PCs are integrated into a Unix network, the users will then be able to utilise Unix services such as *telnet*, *ftp*, NFS, RPCs and X-Windows. The security problems which arise as a result are basically no different from those in a pure Unix network.

Tapping of the network

However, when DOS PCs are integrated into a server-based network the opportunity may be created for additional uncontrolled access to the network. Every network connection can be misused to tap into the network. With appropriate sniffer software, this is also possible from a PC connected to the network. The result is that it is very easy to listen to, and to misuse, all kinds of information, i.e. all passwords and file contents, that are transmitted over the network.

Feigning a false identity

Moreover, it is normally possible for PC users to administer their PCs themselves. By configuring the PC so as to feign a false identity, they can avail themselves of all the services which that identity is authorised to access, e.g. NFS or RPC's, so as to gain access to directories and files of other users on the server. This information can then be read, copied, distorted or deleted unnoticed.

Uncontrolled import and export of information

DOS PCs which are integrated into a Windows NT network constitute a potential threat to the security of the network. Thus, for example, if files are copied from a server to the hard disk of a PC, information relevant to the security of the system can be stored in a physically unsatisfactory manner, or if files are copied to a local floppy disk drive, such information may be sent on to external destinations without this being logged by the server's auditing functions. Conversely, there is the danger of importing a computer virus from a floppy disk drive which is not adequately protected.

SAMBA

UNIX computers which make their file systems available to Windows computers via the SAMBA program can pose a high security risk if they have been inappropriately configured. Thus, for example, it is possible for a user who logs on to a Windows computer using the ID "root" to then log on again on the UNIX computer and obtain access to the "root" ID there as well, thus gaining Administrator privileges.

The use of a Primary Domain Controller (PDC) as password server for SAMBA will project any existing Windows NT security weaknesses onto the UNIX system, since if an NT server is compromised, it is possible for an unauthorised person to access the UNIX file system.

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, data belonging to 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 attacker has about potential targets of attack, the more opportunities he has to infiltrate. If an invader knows, for instance, any user names of an IT system, he can try to guess the associated passwords or find them through dictionary attacks (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

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 test and release procedures

If new hardware or software is inadequately tested or not tested at all and released without installation instructions, it is possible for errors in the hardware or software to go undetected or else for essential installation parameters not to be recognised or considered. These hardware, software or installation errors which result from non-existent or inadequate software testing and release procedures constitute a significant threat to IT operations.

Confidence that new hardware or software can be installed without any problems often results in overlooking of the possibility that damage quite out of proportion to the costs of implementing proper test and release procedures might occur. Programs or IT systems that have been inadequately tested and still contain bugs are integrated in the production environment. These errors then have a disruptive effect on operations which up to then had been functioning smoothly.

Examples of such damage are listed below:

Inadequate resources

- Programs or program updates cannot be used effectively because more resources (e.g. main memory or processor capacity) than expected are needed to achieve an acceptable processing speed. If this is not detected during test runs it can lead to significant sums of investment being wasted or to a requirement for significant additional investment. Decisions to save money rather than to make some additional investment not infrequently result in software products that have been ordered and paid for never being used.

Wrong choice of software creates obstacles to task performance

- Installation of new software impedes the execution of long-established work routines. The benefit expected to result from installation of the program is delayed until much later, as the staff expected to use it were not trained in advance or informed about the new program functions.
- Installation of a new release of DBMS standard software version that still contains bugs causes loss of availability of the database and can result in a loss of data.

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 relating to the IT components used is inadequate or lacking, this can have a significant impact both on the selection and decision-making processes regarding a product, and in terms of damage occurring during actual operation.

Damage repair difficult without documentation

If the documentation is inadequate, error diagnosis and rectification may be delayed considerably or rendered completely impractical following a damaging event such as a hardware failure or software malfunction.

The same applies as regards the documentation of cable paths and wiring within the building infrastructure. If, due to inadequate documentation the precise location of cables is not known, these cables could be damaged during construction work outside or within a building. This could entail prolonged downtime periods, resulting in an emergency situation or even life-threatening hazards, e.g. due to electric shock.

Examples:

Confidential information left out in the open by mistake

- 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 not properly protected and confidential information is 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 fixed more quickly.

Duty of documentation forgotten

- In a larger-sized agency, cabling for the IT facilities was carried out by an external firm. The scope of the services to be provided did not include the preparation of documentation. Since no maintenance agreement was concluded with that firm after completion of the work, the required documentation was not available to the agency. This resulted in considerable delays when the agency subsequently tried to expand the network.

  - In a z/OS installation automatic batch jobs were started up every evening to process application data. It was important to the processing that the batch jobs ran in the correct sequence. When the automation failed one evening, the jobs had to be started manually. Due to lack of documentation, the batch jobs were started in the wrong order. This caused the processing of the application data to break down, resulting in several hours delay in production.

T 2.28 Violation of copyright

The use of unlicensed software can be a violation of copyright and lead to both civil action and prosecution.

Agencies and companies in which pirate copies are used may be held liable for damages by the copyright owner under corporate liability, irrespective of the type of offence (intent or gross negligence).

Example:

A large number of graphical user interfaces in an organisation were used without the necessary licences. The costs of retrospectively licensing them plus 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 and eventually the availability 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-So lines for data communication. After the installation of a GUI based Intranet, the data communication nearly broke down. Finally, only a switch to S2M 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 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 in the environment of non-standard or only partly standard communication procedures, such as ATM or Tag switching. To enable use of the communication procedures concerned, the manufacturers are forced to employ proprietary implementations to offset the missing, or only partially available standards.

Incompatibility problems 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 communication procedure are running parallel within the same network, this may impair the availability of the entire network, individual segments, or certain services within the network. Depending on the type of incompatibility, two different cases can be distinguished:

- Different implementations of a communication procedure that are not interoperable can make communication between the related components impossible.

  Example: ATM components might use different signalling protocols which are not interoperable, e.g. in compliance with UNI (User Network Interface) Version 3.0 and UNI Version 3.1.

- Even if active network components are interoperable in principle, certain specific services could 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 over these components 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 together without the use of the relevant 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 cannot 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 residual data.

During electronic data communication or transmission of data media, it not infrequently happens that information that should not leave the organisation is passed on. The following are some examples of possible reasons why information might be unintentionally disclosed:

- A file contains passages of text that are formatted in a hidden or non-visible mode. Such passages of text can include remarks that are not addressed to the recipient.
- Files created with standard software, including word processors or spreadsheet programs, can contain a lot of extraneous information, such as the directory structure of directories, version numbers, author(s), comments, time spent editing it, last date of printing, document name and document descriptions. In this connection, functions that allow several persons to work on a document simultaneously require special emphasis. When one person deletes or overwrites passages of text in a document, thanks to these functions the passages are not really taken out of the document, but are merely flagged as deleted, so that later on another person can reverse the changes either wholly or partially. Virtually all office software (Microsoft Office, StarOffice, OpenOffice) offer this facility. If the data contained in these changes is not removed before the document is passed on, the recipient could receive not just the actual document but a wealth of additional information as well.
- Virtually all the office packages around today provide facilities for "fast saving" documents, under which only the modifications that have been made to a document are saved. This is quicker than a full save operation, in which the entire updated file is saved. However, a full save requires less storage space on the hard disk than a fast save. The critical disadvantage, however, is the fact that a file that has been fast saved can contain fragments of text which the author had not intended to pass on.
- Another way that information not intended for outsiders can be passed on is functions which, for example, allow a table from a spreadsheet document to be embedded in a text document or presentation in such a way that the spreadsheet can be edited directly in the text document. If such a text document is passed on, it is possible that a lot more information contained in the spreadsheet document than is actually visible in the text document will also be passed on.
- When a file is copied to a floppy disk, the physical memory block needed is entirely filled. If the original file does not require a complete memory block, the unused section of the block (after the end-of-file indicator) is filled up with any old residual IT system data.

z/OS systems

- In z/OS systems, deleted members are not immediately overwritten in the library (PDS - *Partitioned Dataset*). Only the entry for the member in the PDS directory is deleted. Only when free space is required in the PDS does the information relating to the old member get overwritten. Data not yet overwritten can be read using a utility.

- When a file on a hard disk is deleted in a z/OS system, the file in the *Volume Table of Content (VTOC)* is flagged as deleted, but the file itself is not deleted on the hard disk. The file is not overwritten until new data needs to be saved on the hard disk and there is no free space available. If someone can succeed in reading the storage location of the file from the VTOC, then he would be able to edit and restore the file using special software. The same applies to tapes that may be flagged as empty tapes but have not yet been overwritten.

Residual information on data media

In most file systems, files that are deleted by the user entering a delete command are not really deleted in the sense that the information no longer exists after the command has been executed. Normally only the references to the file from the administration information of the file system (from the *file allocation table* in a FAT file system) are deleted and the blocks that belong to the file are marked as "free". The actual content of the blocks on the data medium is retained, however, and can be reconstructed with appropriate tools.

If data media are passed on to third parties, for example,

- when a computer is withdrawn from service and sold,
- when a faulty machine is sent to be repaired or is replaced under the terms of guarantee, or
- when a data medium is handed to a business partner in the course of an exchange of data media,

sensitive information can reach the outside world.

Examples:

- Between 2000 and 2002 the researchers Simson Garfinkel and Abhi Shelat of MIT purchased a large number of second-hand hard disks from various dealers through the online auction house eBay and examined these to see what residual information they contained, if any. They found an alarming quantity of data, for example,
  - internal company memos relating to personnel
  - a large number of credit card numbers
  - medical information
  - e-mails

  and much more besides. The published their results in an IEEE Journal.
- While using a different editor, a user accidentally discovered several URLs, along with a user name and a password for a web server in a file he was about to send out. The address of a web document is called a URL (Uniform Request Locator). Access to a web page can be password-protected.
- Presentation slides created with Microsoft PowerPoint were handed over as files to a third party by a public agency. Later it transpired that as well as the presentations, the files had also contained information about the users computer environment, such as the names of the newsgroups to which he

was subscribed and which news items he had already read. Among other things the PowerPoint file contained the following entries:

de.alt.drugs! s21718 0

de.alt.sex s125 0

- Two salesmen from competing companies exchanged presentations after attending a business event. One of the PowerPoint documents contained a small table with end customer prices for products from that company. On opening the presentations, the recipient discovered that this small table was part of an extensive spreadsheet document that had been embedded in the presentation and contained all the price calculations of its competitor.

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

since version November 2004 omitted

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 person related 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 protection 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 a poorly-protected area for temporary 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 is the result of "organisational shortcomings" of the 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 can then no longer be kept 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.

  Installations which do 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

- If legal privacy protection requirements are not observed when transferring person related data between the components of a RAS system, breaches of the law may occur. For example, when setting up automated retrieval processes, participants must make sure that the reliability of the retrieval

  Lacking observation of legal privacy protection requirements

process can be verified (see Section 10, Para. 2 of the German data protection act).

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 2.67 Inappropriate administration of access rights

If the assignment of access rights is not properly controlled, this can quickly result in serious security loopholes, e.g. due to proliferation in the granting of rights.

High work effort

In many organisations the administration of access rights is an extremely labour-intensive task because it is poorly controlled or the wrong tools are used to do it. As a result, a lot of manual labour may be required, and this in turn is prone to errors. Moreover, often many different roles and groups of persons are involved in this process so that it is easy to lose sight of the tasks performed.

Difficult to maintain an overview

Organisations also exist in which there is no systematic record of all the users configured on the various IT systems and their access rights profiles. Typically this results in accounts being maintained for users who left the agency or company some time ago or who due to changes in job content have accumulated too many rights.

If the tools for the administration of access rights are poorly selected, they will often not be flexible enough to permit modification in response to changes in the organisational structure or to the replacement of IT systems.

Incorrect division of roles

Mistakes may be made in the division of user roles so that security loopholes arise, for example due to incorrect allocation of users groups or over-generous granting of rights. Users can be assigned to roles which do not match their tasks (too many or too few rights) or which the tasks they perform do not warrant (role conflicts).

T 2.68 Absence of or Inadequate Planning of Active Directory

The global structure of Active Directory, i.e. its breakdown into domains, has far-reaching effects on the security of a Windows 2000 installation. In particular, problems can arise when different domains have different security requirements or domains belong to different organisational areas.

For example, if planning is omitted or inadequate, the following cross-domain threats can apply:

- All the domains in an Active Directory must use the same schema. If a software package that will require a change to the schema is to be installed in only one domain, all the other domains must register this change as well. Incompatible schema changes resulting from different software products can have the effect that software cannot be installed or does not run correctly. **incompatible change of the scheme**
- Certain user data from the Active Directory (Global Catalog) is available in every domain. This can be a problem from the point of view of data protection. **Data Protection**
- Administrators of the forest root domain have extensive privileges in other domains as well. **delayed account lockout**
- If a domain is distributed over several locations that are not adequately networked with each other it can take a long time before an account lockout takes effect in all the locations. This means that a user whose account has been locked may be able to log on to the system unauthorised in other locations.

Within a domain, the structure of the Active Directory must be carefully planned as otherwise the following threats can apply:

- If computer and user accounts are arranged in the default containers *Computers* and *Users* below the domain, it will not be possible to configure any group policy corresponding to different types of user account or different computer types.
- If organisational units (OUs) are deeply nested, the structure of the domain could become unwieldy so that the Active Directory is susceptible to configuration mistakes. Moreover, the performance of the Active Directory Service declines as depth of nesting increases, especially if OUs are nested over more than four levels.

T 2.69 Lack of, or inadequate, planning of the use of Novell eDirectory

As a tool for resource management in networks, eDirectory is designed for use in a heterogeneous IT environment, with a number of operating systems supported. The security of the overall system by its nature depends on the security of each of the subsystems. The security of the operating system and especially the security of the file system provide the basis on which the security of eDirectory relies.

As both eDirectory and also the possible client software can be installed and operated on a number of operating systems, there is a requirement for a large number of security settings to be made for the operating systems used. This increases the planning requirements and presupposes knowledge of all the operating systems involved. There is therefore a risk that use of eDirectory will not be planned in sufficient detail or to sufficient depth if the overall solution is very heterogeneous.

Unsatisfactory operation of the directory service

Where eDirectory is to be used on the intranet, planning of the tree structure and mapping of the corporate infrastructure are extremely important. If planning is defective, there is a risk of inconsistencies and excessive complexity in the design of the directory service. This can result in configuration errors and incorrect or inadequate operation of the system.

Inconsistency of security guidelines between individual tree hierarchies

The global tree structure of the eDirectory directory service has far-reaching effects on the security of an eDirectory installation. In particular, problems can arise when different subtrees have different security requirements or belong to different organisational areas. The implicit inheritance mechanisms and the complexity of the rules for working out the actual effective rights of individual objects place high requirements on planning of the system.

The Certificate Authority (CA) implicitly used is an essential element of the security of eDirectory. Once again, defective planning can impair the security of the directory service.

Uncertainty as regards the actual effective rights used

Planning of the options for accessing eDirectory service is a core subject for system security. This applies both to use on the intranet and also especially to the use of eDirectory as an LDAP server on the internet.

Possible unwanted access posibilites to the directory service

Planning of the administration of the directory service is also an important subject. eDirectory supports role-based administration and also the delegation of administrative tasks. This is especially important in relation to security administration. Planning of administration requires extreme care and circumspection; otherwise there is a risk that unauthorised users of the system could obtain unintended access.

In addition, the eDirectory software offers the *iMonitor* tool, which permits web-based monitoring access to the eDirectory servers and the directory system. Defective planning of the use of this functionality may allow unauthorised users to access the internal structure of the eDirectory installation.

Partitioning of the directory service and its replication are important issues in the operation of eDirectory. Inadequate planning in this area can result in poor performance, inconsistencies in data storage through to loss of data.

Inconsistency of security guidelines between eDirectory and the relevant operating system environments

The eDirectory directory service allows role-based administration of the directory database and also delegation of individual administrative tasks. Planning of administrative roles and delegation options must be co-ordinated with the security guidelines to be specified (see S 2.238 *Specification of Security Guidelines for Novell eDirectory*). In the event of lack of or defective planning of administrative tasks, there is a danger that the system could be administered in an insecure or inadequate manner.

Inadequate administration of the directory system

eDirectory allows directory data to be synchronised with other directory services via DirXML. DirXML consists of an engine and specialised drivers (e.g. for Windows 2000 Active Directory, Lotus Notes, SAP R/3, Netscape, etc.) for the exchange of directory information in XML format. The external directory services can communicate changes to eDirectory via a *publisher channel*. With the corresponding rights, which depend on the target system under consideration, these changes then become active in eDirectory too. At the same time, the external directories can be registered in eDirectory so that they can learn of changes to the eDirectory information status over this channel (*subscriber channel*) and align their directory accordingly. This synchronisation requires detailed planning, as otherwise sensitive data could be automatically duplicated to the outside world unintentionally. Conversely, existing data could be unintentionally overwritten by this means. SSL can be used to protect the data during transportation. Mistakes in planning here can result in loss of the integrity and confidentiality of directory data.

Last but not least, the use of login scripts for users and user groups must be planned. If planning is incomplete or inadequate, inconsistencies with the defined security guidelines can occur.

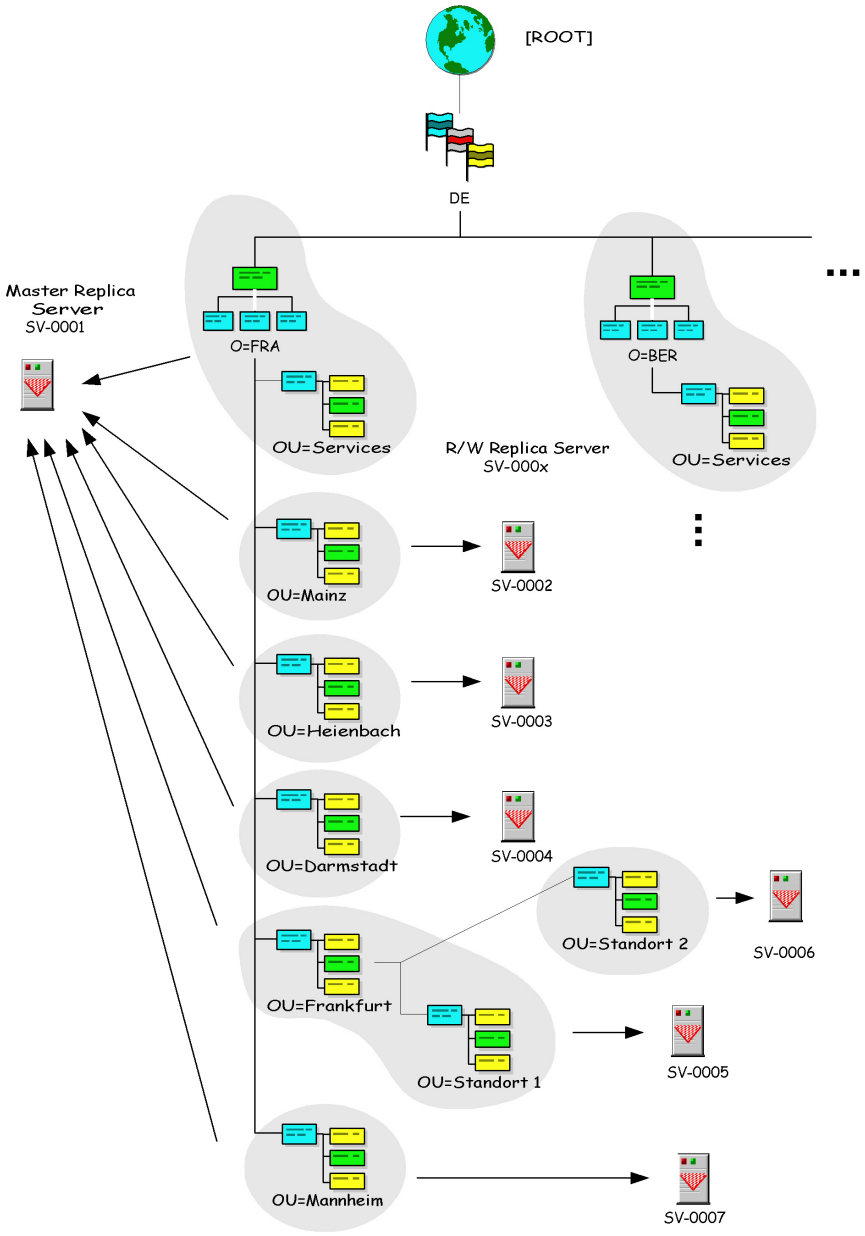
In addition, lack of or inadequate planning can also produce the following problems:

- Administrative access to the system might not be adequately protected.
- Operation of the public key infrastructure may be unsatisfactory.
- System performance may be too low.
- Losses of data may occur if replication and backup are not considered properly.

T 2.70 Lack of, or inadequate, planning of partitioning and replication in Novell eDirectory

Partitioning and replication of the eDirectory directory service are important aspects of planning the use of eDirectory.

Partitioning entails dividing the directory data contained in eDirectory into individual sub-areas or partitions. This division cannot be carried out any old way, but must comply with certain rules which derive from the logic of the hierarchical tree structure. The aim of partitioning is firstly to distribute the load of the directory system into several parts and secondly to achieve physical separation between the locations in which directory data is stored, for example, corresponding to the various locations within an organisation. Partitions can also represent administrative units of the directory system.



Replication of eDirectory partitions serves primarily to increase availability and load distribution of the directory system. This redundancy in data storage increases operational reliability.

Planning is therefore also of critical importance as subsequent changes to the partition and replication settings, while possible in theory, may in practice cause inconsistencies.

Time window with inconsistencies

Where changes are made to eDirectory, by their nature a certain amount of time is required for the new settings to be propagated all over the system. Consequently there can be a time window within which eDirectory is inconsistent. Such inconsistencies can constitute a problem especially with regard to the definition of authentication data or rights of access to eDirectory objects.

Partitioning of the eDirectory directory has direct consequences on the inheritance of access rights (Access Control Lists, ACL). To receive the inheritance rules in an existing eDirectory tree, during a partitioning the superordinate ACL is notified to the root object of the new partition as an *inherited ACL* of the system.

administrative overhead

The definition of partitions for the eDirectory directory service has a direct impact on the replication activities of the entire system. In order to be able to search for objects over the entire tree (*tree walking*), eDirectory automatically creates *subordinate reference replicas* which essentially contain jump addresses. If planning is inadequate (e.g. the tree structure is too shallow) very extensive replication rings are created here. If a replication ring becomes very big, there is a certain probability that at least one eDirectory server in the ring will be momentarily inaccessible. In such a case, error and status messages are generated on each of the other eDirectory servers in the replication ring. This can result in increased administrative overhead, which can extend over extensive parts of the directory tree.

Other problem areas are described in T 2.42 *Complexity of the NDS*.

Moreover, defective or inadequate planning of partitioning and replication of the directory service can also lead to loss of data as well as to inconsistencies in the data store, unsatisfactory availability of the directory service and poor system performance overall through to system failures.

T 2.71 Lack of, or inadequate, planning of LDAP access to Novell eDirectory

The possibility of accessing the eDirectory directory service with LDAP is an important feature of the software product. User access is effected using LDAP protocol Version 3, a widely used internet standard. Operators who use eDirectory as an e-business platform usually provide their users with special clients. However, simple web browsers or e-mail clients can also act as LDAP clients.

The LDAP interface also has the advantage that network applications and their services can access the directory service via it. This access requires thorough planning, especially also in relation to the eDirectory rights that are necessary to sensibly use the applications.

different types of connection

Planning of LDAP access thus depends significantly on the eDirectory operational scenario. In principle, from the point of view of eDirectory there are three different types of connection for an LDAP client:

- As [Public] object (*anonymous bind*): in this case no authentication information is requested and the [Public] object always possesses as standard the unrestricted right to browse the directory tree.
- As Proxy User (*proxy user anonymous bind*): this configuration option can be chosen instead of anonymous login. The Proxy User needs to be configured on eDirectory.
- As NDS user (*NDS user bind*): here the user logs on to the directory service with his eDirectory rights. The corresponding user object must be created in eDirectory.

Which data may be transmitted in plaintext?

During planning it is necessary to consider whether and which data should be allowed to be transmitted in plaintext under the security guidelines internal to the organisation. This applies to use on the intranet and also, in particular, to connection to the internet.

For example, at issue here is whether user passwords should be allowed to be transmitted in plaintext and how systematic use of SSL encryption should be. In accordance with the LDAP standard, Version 3, eDirectory supports two types of connection:

- *anonymous bind*: without user name or password,
- *clear-text password bind*: user name and plaintext password used for authentication.

LDAP/SSL is also supported. It must be configured in eDirectory whether the first two types of connection are to be supported or not.

SSL itself is supported in two modes, single-sided and mutual authentication. In mutual authentication, the necessary credentials, including the root certificate of the Certificate Authority, must be generally accessible.

Configuration errors

Because of the diversity of configuration options for LDAP access to the eDirectory directory service, as described above, it is easy for errors to creep into the configuration settings. Such configuration errors can result in:

- incorrect assignment of access rights

- unauthorised access to the eDirectory directory service
- transmission of user password in plaintext
- interception of unencrypted information
- errors in LDAP access, especially for network-based applications
- poor productivity of the overall system

T 2.72 Inadequate migration of archive systems

Archived data typically has to be kept in storage for a very long time. During this period the underlying technical system components, storage media and data formats may age physically or technologically and as a result become unusable. Moreover, in the course of time problems regarding the compatibility of the data formats used can occur.

Ageing of components

If appropriate steps are not taken to counteract the ageing of the existing system, then it can be expected that in the long-term

- archived raw data may cease to be physically readable from the archival media;
- archived data may be corrupted due to physical defects in the archive system and media;
- spare parts for hardware components may no longer be available;
- updates for software components may no longer be available;
- data formats used may no longer comply with the integrity requirements;
- digital signatures may become unusable;
- it may be possible for unauthorised persons to read encrypted data.

Ageing of cryptographic methods

Even if system components are replaced in good time or the data is copied, problems may still occur through the use of cryptographic procedures. For example, vulnerabilities in integrity-protecting procedures may occur since, as computing power increases over time, encryption and signature algorithms may cease to provide adequate protection (see also T 2.79 *Ineffectual regeneration of digital signatures during archiving*).

Examples:

- Data media can be damaged by physical long-term factors, such as wear on materials, distortion, scratching of media surfaces or softening. Depending on the intended purpose of the data media concerned as system or archival media, the archive system may cease to function properly or data stored on the archival media may be lost.
- The manufacturer of an archive system had provided a debug field in the context data for documents. During the pilot phase of the archive system documents from normal business operations were archived for test purposes, in the course of which the test status was recorded in the debug information. During the subsequent transition to the operational phrase, the test documents were not deleted as they had been archived on WORM data media, but the documents marked with the relevant debug information concerned were no longer displayed. The successor system was supplied by another manufacturer who presented debug information in a different way. During subsequent migration of the archive data to the new archive system, however, by mistake the old debug field was not evaluated. After the data had been migrated, the old test documents were still in the archive and suddenly surfaced during a later search as supposedly authentic documents.

- Digital signature procedures could be compromised by someone trying to guess the signature key or using mathematical algorithms. If this occurs within the archiving period, digital signatures could also be retroactively counterfeited.

T 2.73 Inadequate audit trail of archive systems

Auditing of an archiving procedure must take into account both organisational and also technical criteria. Checking of archive systems must therefore include not only expert evaluation of the system configuration but also checking of the assignment and use of access rights.

If the selected archive system does not supply the necessary technical support, e.g. in the form of special user accounts for auditing purposes, monitoring tools, integrity-protected log files (see T 2.76 *Inadequate documentation of archive accesses*), than the checking procedure can be very labour-intensive. Moreover, as a result there is a danger that checking will not be complete and that important items will be overlooked. This in turn can endanger the whole process of auditing the archiving process.

Legal or financial problems could follow, for example, due to loss of evidential strength of archived documents.

T 2.74 Inadequate indexing keys for archives

Electronic archives can contain huge quantities of data. Indexing keys are used to facilitate the filing and retrieval of individual data records. A distinction must be made here between index data used in the document management system (DMS) and those of the archive system.

Document Management System

DMS indexing keys are used to administer context and content information along with each document. An unsuitable choice of context criteria would have the effect of making it time-consuming or even impossible to retrieve archived documents or would mean that the semantics of archived documents could not be properly determined. On the other hand, the more context criteria are used, the more administrative effort is required and the worse the performance of the document management system as the number of archived documents grows.

Archive system

By contrast, the indexing keys used in the archive system are more of a technical nature. They are used to identify individual items of raw data and to organise the filing of raw data on storage media. Their selection is generally determined not by the DMS but by the configuration of the archive server and the underlying storage architecture. It is essential that documents are uniquely identified. Failure to do so, i.e. so that two documents have the same document identifier, can result, depending on the search procedure used, in the wrong document being returned to the DMS during retrieval and then being assigned a new document context. In such a case, the document that was not found would physically exist, but would no longer be uniquely assigned to a process in the DMS.

Unique identification

If the archiving process is to ensure a complete audit trail, it is essential that all documents administered are uniquely identified and that the link between documents and context information is verifiable.

T 2.75 Inadequate capacity of archival storage media

Incorrect assessment of the amount of data to be archived can result in the use of archival media whose capacity is too small, so that archiving is incomplete or delayed.

Document amendment frequency

When assessing the necessary data volume, often only the expected maximum size of the documents to be stored is considered. In fact, however, the storage requirement in archive systems can be many times that amount, as the type of data storage and also the frequency with which documents are amended can have a significant impact.

For example, where WORM media (Write Once Read Multiple) are used for archiving, several versions of the same document need to be stored, i.e. after each change a new document is saved. This can mean that even small documents can generate a high data volume if changes are made frequently. It is not possible to delete old versions of documents from the archival medium. As well as capacity bottlenecks, this can also lead to data protection or confidentiality problems, as data marked as ¿to be deleted¿ is not actually deleted.

T 2.76 Inadequate documentation of archive accesses

Like other IT systems, archive systems too are vulnerable to manipulation if they are poorly protected. Users could try to add forged documents to the archive and, through specification of appropriate context information, assign these documents to existing administrative procedures or even forge completely new procedures. System administrators could tamper with files bypassing the archive system and conceal such manipulations by altering the log files.

Log files are often neglected

It is normally the case that log files are viewed as less important than the documents to be archived themselves. This frequently results in lower retention periods for log files and less careful handling of log files.

If archived documents are to be reused in later administrative procedures, it is essential to be able to verify their authenticity, i.e. to distinguish between proper and manipulated documents and, in the case of disputed documents, to be able to prove the document history. This can be endangered if

- archive accesses, and especially write accesses, are not adequately logged;
- logged data is inadequately protected against tampering by users and system administrators;
- logged data is lost;
- logged data is retained only for short retention periods.

If the documents to be archived are classified by sensitivity level, it must always be possible to trace who examined which document when. This cannot be guaranteed if read accesses and search requests are not documented.

Examples:

- In the context of an archive search, a document is found which casts a poor light on a person in a particular way in an ongoing administrative procedure. The authenticity of the document is verified using the context information stored with it. However, the document was actually created by an unauthorised person who had deliberately specified false context information (including the author of the document and the date it was written) in order to later be able to show the person in question in a poor light. As the files logging archive accesses have meanwhile been deleted, this can no longer be proven. The employee concerned is falsely incriminated as a result.
- A user with administrative privileges tampers with files in the cache area of the archive system before these are stored on permanent media. It is not possible to trace the manipulation as the user has tampered with both the data itself and also the log files.

T 2.77 Ineffectual transfer of paper data to electronic archives

In many electronic archives documents are regularly stored which originally were available only in paper form and therefore have to be transferred to an electronic format. During this process selected features of the original document are preserved. Depending on the intended use of the document, there may be different requirements. These could include matching the external appearance of the copy with the original, for example, using an image file. Agreement of text excerpts, e.g. using a text file, or matching of other features, e.g. biometric data or context data, may also be required.

Storage as a text or image file alone is not always sufficient to prove the faithfulness of the document to the original, as both tampering and errors could occur:

- Existing documents can be tampered with using text and image processing programs. **Tampering**
- Errors in scanning can result in corruption of the semantics of the recorded data, which could subsequently cause misinterpretations and miscalculations. For example, important parts of the document could be left out during scanning. **Errors during scanning**

Some archiving scenarios entail destroying all paper copies of a document after it has been scanned in, in order to save space. It must be assumed here that once the original document has been destroyed, it will no longer be possible to prove directly at a later date that the copy is a faithful reproduction of the original.

This means that all features of the original document that are necessary for the purposes of subsequent verification must be captured during the phase of conversion to electronic form and must be stored along with the electronic copy in a traceable way. If during this process any features are ignored or forgotten (e.g. the number of pages of an original document), this can significantly limit the evidential strength of a document, as often it will no longer be possible to gather information subsequently about features of the original document.

An ineffectual procedure for the transfer of documents endangers the effectiveness and traceability of subsequent processing of documents and ultimately the properness of the archived documents.

Examples:

- The incoming correspondence received by a public agency is scanned in for subsequent electronic processing and stored in the archive. However, occasionally the reverse side of a letter is overlooked during scanning. As the incoming letter is destroyed after scanning, it is no longer possible to prove the original state of the letter. **Originals are destroyed**
- When text is scanned in and automatically captured, passages that have not been correctly recognised by the optical character recognition (OCR) program are left out or corrupted. For example, this can affect printed text when the print is faint or the writing unclear, also where handwritten notes **Text is incorrectly recognised**

have been added in documents or a printed image has been smudged by an inkjet printer. Incorrectly recognised invoiced amounts (decimal points not recognised etc.) are likewise a possible source of errors which could cause misunderstandings later on.

- Manual signatures on documents are scanned in as images. In the event of a subsequent legal dispute about the authenticity of document and signature, it is no longer possible for a handwriting expert to determine authenticity conclusively, as the image file could have been tampered with using an image processing program or another document could have been copied. Features of the original document, such as the physical properties and composition of the paper used or the pressure exerted in the process of signing it manually can no longer be determined.

Manual signature cannot be checked

T 2.78 Ineffectual regeneration of data stocks during archiving

Data media can age both physically and technologically. Similarly, data formats are occasionally extended to include new syntactic or structural features. Both of these factors can have the effect of rendering archived data no longer readable (see also T 2.72 *Inadequate migration of archive systems*).

Every few years electronically archived documents should therefore be copied onto new data media or transferred to new, more up-to-date data formats. There is a risk here that during the transfer to new data media data is taken out of its document context or that during recopying to a different data format semantic changes are introduced by mistake.

There is also the possibility that tampering could occur during transfer of the data to a new storage medium. Even data stored on WORM media can be ¿modified¿ during such an operation.

It may be necessary to destroy the old data media once the data stocks have been migrated. In this context the reader is referred to threat T 2.81 *Ineffectual destruction of data media during archiving*.

Examples:

- During the process of migrating data stocks, to save space previous versions of versioned stored documents are deleted although these are still needed for verification purposes.
- Files which originally were stored on WORM media so that they were protected against alteration (having a complete audit trail) are transferred to new data media. In this process files are exchanged during the copying process, i.e. individual files are not transferred to the new medium but instead forged files are inserted.

T 2.79 Ineffectual regeneration of digital signatures during archiving

The algorithms and key lengths that are used with digital signatures have to be updated at regular intervals in accordance with advances in technology if the protection they provide is to remain effective (see T 4.47 *Obsolescence of cryptomethods*). This means that the cryptographic keys used and the associated certificates are only reliably valid for a limited time. Compared with the archive life that is aimed for, this may be a relatively short period. If the evidential value of digital signatures is to be retained, then the electronic signature on every individual document must be regenerated in good time.

The following security problems can occur in connection with regular re-signing of archived documents:

- If documents that have previously had an invalid or no digital signature are mistakenly given a valid new signature, these documents could henceforth be wrongly viewed as authentic.

  ¿Inadvertent¿ new signature

- It could happen that documents are overlooked during the re-signing process, i.e. they are not given a new, valid signature although they had previously had a valid signature. As a result from this point onwards it may no longer be possible to verify the authenticity or integrity of the document concerned unless alternative evidence using other features can be found.

  Documents are forgotten

- The underlying cryptographic procedure could already be compromised at the time of re-signing or the original signature key could be known (e.g. calculated using a massive amount of computing power). As a result, unauthorised persons could create documents and give them a technically valid signature, if necessary with a timestamp as well. If these documents are successfully introduced into the process of re-signing, they could wrongly be viewed as authentic.

  Compromised cryptographic procedures

T 2.80 Ineffectual auditing of archiving procedures

Electronic archiving imposes very high requirements on the process of transforming paper documents to electronic documents. The activities that have to be carried out in connection with archiving should be laid down in detail in a procedural document and should be made traceable through an audit trail that includes logging which user carried out what activities in the archive when.

If the operating procedures followed during archiving or the recorded logged data are not checked frequently or carefully enough, the legitimacy of the archiving process and hence the properness of the archived documents themselves is thrown into doubt.

T 2.81 Ineffectual destruction of data media during archiving

Archive systems and their storage media do not generally provide any protection against access to the stored data of themselves. Instead, this function is carried out by the superordinate document management system (DMS). If archival storage media are accessible outside the archiving environment (archive system and DMS), it must be assumed that anyone who can read the medium can access the information stored there.

Misuse of old archival media

Especially when archived data is recopied to new data media, there is a significant risk that old archival media no longer needed which have not been properly and entirely destroyed could be abused to gain information.

One-off encryption does not protect forever

Even where archived data is encrypted, improper destruction of data media can still cause problems, as the security of cryptoalgorithms can always be guaranteed only for a limited period of time (see also T 4.47 *Obsolescence of cryptomethods*). One-off encryption therefore does not provide permanent protection against data misuse.

T 2.82 Poor planning of the archive system location

Due to the sensitivity of the stored data and the very long retention period, archive systems must satisfy high requirements with regard to the quality of data storage. The choice of location for the archive system is a major influence here.

The following potential security problems can arise in this context:

- Unsatisfactory climatic conditions
- Too high or too low a temperature or excessive humidity can cause technical components to malfunction and damage archival media. These effects are aggravated by frequent fluctuations in the climatic conditions. Similar climatic pollution can be caused by secondary damage. An example here would be the fumes given off by walls following a fire in an adjacent room.
- Inadequate physical protection of the archive system
- Inadequate protection of the archive system against unauthorised access can encourage wilful actions such as theft, tampering or sabotage.
- Inadequate protection against other environmental influences
- Other environmental influences (for example, vibration or exposure to a lot of dust) could cause damage to technical components of the archive system and/or storage media. This is especially irritating when the damaging influences could have been foreseen, for example in the case of building work.

Example:

In the course of setting up a central IT area close to production facilities, occasional vibration occurs. As a result the technical components of the archive system, which is also maintained in the IT area, keeps malfunctioning.

T 2.83 Flawed outsourcing strategy

The decision to carry out an outsourcing project has far reaching consequences. As a result, an enterprise or agency enters into a close relationship of dependency on the outsourcing service provider. Therefore any mistakes in this area can have long-term and serious consequences. These can be of an organisational or technical nature and/or have extremely serious financial repercussions.

Security and safety problems (e.g. with inadequate availability) at the outsourcing service provider can be not only expensive but also place the survival of the organisation in jeopardy. However, errors of judgement by the outsourcing organisation can also have serious consequences. If, for example, the effort entailed (e.g. to prepare documentation, perform tests, protect systems) is underestimated, slippage can occur. To make up for lost time and save money, experience suggests that cuts are frequently made in the amount of test work carried out, and this in turn can result in cuts in security.

T 2.84 Unsatisfactory contractual arrangements with an external service provider

If situations occur that are not clearly covered by the terms of the contract, they can cause problems for the customer (e.g. within the context of an outsourcing project).

Thus, for example, an outsourcing customer can be held responsible for shortcomings in security which are under the control of the outsourcing service provider but are not the subject of clear contractual stipulations.

One of the main causes of problems between the contractual partners is over-optimistic cost estimates. If it turns out that the outsourcing service provider cannot provide the service at the cost it has estimated and tendered or there is a disagreement as to what is "obvious", this can lead directly to security problems. Experience suggests that shortcuts will be made in the area of IT security if there is cost pressure in other areas which can be countered without the consequences being directly visible. The contractual arrangements between customer and contractor can therefore have momentous consequences. Only provisions which are fixed in the contract from the start will also be implemented later on!

Other examples of the consequences of unsatisfactory contractual arrangements with external service providers are as follows:

- If the service provider does not allow entry to its premises or access to the necessary documentation, the customer may be unable to comply with its duty to provide information to the regulatory agencies or to its auditors.
- The customer will be forced to take responsibility for breaches of statutory requirements if the service provider has not been placed under an obligation to comply with this legislation.
- Responsibilities, performance parameters and manpower effort are poorly or ambiguously stated in the contract so that security safeguards are not implemented due to ignorance or lack of resources.
- The customer cannot comply with new requirements (e.g. technical, legal requirements, availability, technical development) if change management and system modifications have not been adequately specified in the terms of the contract.
- In the case of outsourcing projects, management of the customer organisation may carry the full responsibility for the outsourced business areas, but due to lack of control possibilities it may be unable to fulfil this responsibility.
- Outsourced data or systems are inadequately protected because the outsourcing service provider is not aware of their protection requirement.
- The quality of service is poor, and there is no possibility of intervening because no sanctions have been stipulated in the contract.
- The service provider takes qualified personnel off the project or substitutes of the permanent staff are not adequately prepared, resulting in security problems.

Special problems often occur when service agreements are terminated (see also T 2.85 *Inadequate provisions for termination of the outsourcing project*) and this situation has not been properly covered in the terms of the contract.

T 2.85 Inadequate provisions for termination of the outsourcing project

Outsourcing projects normally result in the loss of expertise within the customer organisation and in dependence on the part of the customer on the outsourcing service provider. For this reason inadequate contractual provisions covering the possibility of termination of the contractual relationship can have serious consequences for the customer. Experience suggests that this is a particular problem when unforeseen circumstances which are critical as far as the customer is concerned occur, for example the insolvency or sale of the outsourcing service provider.

Examples

- The outsourcing service provider is purchased by a competitor of the customer.
- A national law enforcement agency has outsourced processes to a computer centre that is later purchased by a foreign company.
- There are legal disputes between customer and outsourcing service provider over poor quality of service or serious security shortcomings, as a result of which one of the parties to the contract wishes to terminate it.

Without adequate internal precautions and precise contractual stipulations, there is always a danger that it will be extremely difficult for the customer to free itself from the contract with the outsourcing service provider. In this case it could be difficult or impossible, for example, to transfer the outsourced area to another service provider or to restore it to the control of the customer, should this appear necessary.

The following is a list of some of the other problems which can occur in this situation:

- Due to inflexible provisions regarding the right of termination, the contract cannot be terminated in a manner that satisfies the customer's requirements.
- If the notice periods are insufficiently long, termination by the service provider may mean that there is not enough time to arrange a proper handover.
- Inadequate provisions regarding the rights of ownership in the hardware and software used (interface programs, tools, batch processes, macros, licences, backups) can impede a controlled transition, for example, to a new outsourcing service provider.
- Inadequate stipulation regarding the handing over of documentation can make it impossible to continue to operate the IT systems in an ordered fashion.
- Inadequate provisions regarding the deletion of data at the outsourcing service provider can result in confidential data falling into the hands of third parties.
- The customer may no longer be able to perform its functions, as availability can no longer be guaranteed.

- In the final phase of the termination process, data and systems may no longer be properly protected as these are viewed as "old systems".

T 2.86 Dependency on an outsourcing service provider

An outsourcing project always has the effect of making the customer dependent on the outsourcing service provider. This can result in the following typical dangers:

Loss of expertise

- Outsourcing of business processes means that the relevant expertise is lost in-house.
- Employees of the customer leave the company or are transferred and take their expertise with them.

Loss of control

- IT systems and resources are handed over to the outsourcing service provider so that there is no longer full control over them.
- Customer and contractor assess the protection requirement of the outsourced information differently, for example, due to misunderstandings in communications or a different security culture. This can cause the security measures previously in place to be inadequately or incorrectly applied at the service provider's.

Moreover, excessive dependence can have the following consequences, which need to be borne in mind:

Problems with change of service provider

- Insourcing is generally expensive and even impossible in extreme cases.
- Generally it is difficult to change service provider and the attempt to do so can lead to extremely serious situations as regards availability or costs.
- It may not be possible to respond appropriately to changes in the framework conditions (e.g. a change of ownership of the outsourcing service provider, change of legal situation, doubts regarding the reliability of the outsourcing service provider).

If the outsourcing service provider realises that the customer is overly dependent on it, the following additional problems can arise:

- The service provider raises its prices dramatically.
- The quality of service deteriorates.
- The threat of discontinuing the service immediately is used as a means of applying pressure, e.g. in case of termination of the contract or in the event of a dispute.

T 2.87 Insecure protocols in public networks

Where communication occurs over public networks, especially the internet, there are a number of threats that arise from the use of insecure protocols.

Loss of confidentiality of data transmitted using plaintext protocols

One serious threat is the possibility that confidential information could fall into the hands of outsiders. Protocols under which information is transmitted in plaintext must be viewed as particularly insecure. As it is not possible to predict the route by which data packets will pass through the internet, the information transmitted could be read at many different points. This is particularly critical where the data transmitted is

- authentication data, such as user names and passwords
- authorisation data, for example, transaction numbers in electronic banking or electronic brokerage
- other confidential information, for example, contained in documents that are sent by e-mail

Telnet, HTTP, FTP, SMTP etc.

Protocols under which all information is transferred in plaintext include:

- the *Hypertext Transfer Protocol* (HTTP), which is used in communication between web browsers and web servers
- the *Telnet* protocol, which is still used in some places for remote logins
- the *File Transfer Protocol* (FTP), which is still frequently used to access servers which provide files for download
- the *Simple Mail Transfer Protocol* (SMTP), which is used to transmit e-mail
- the protocols rsh (*Remote Shell*), rlogin (*Remote Login*) and other similar protocols.

With such protocols, it is possible for all the information transmitted to be read and possibly also altered on every computer which has the appropriate connection. The transmission of credit card numbers and passwords over HTTP connections on the web is particularly critical.

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.

Man-in-the-middle attacks and session hijacking

With the protocols mentioned (especially HTTP and Telnet), there is a danger of man-in-the-middle attacks or session hijacking (see *T 5.89 Hijacking of network connections*). Under this type of attack, an attacker is not only able to read information but he can also actively inflict damage by altering transactions that are in progress. For example, prices or order quantities of e-tailers could be altered over the internet so that the ordering party only sees the article or delivery address and confirms his entries, whereas the attacker has sent a significantly higher quantity and a different delivery address to the seller.

As well as the protocols mentioned, under which all information is transmitted in plaintext, there are also other protocols under which at least the

authentication data is encrypted during transmission. However, there remains a threat that the other useful information transmitted could be read by unauthorised persons.

T 2.88 Negative impact of an outsourcing project on the organisational climate

Depending on their nature and scope, outsourcing projects can not only affect the business processes but also the personnel within the customer organisation. As well as the positive effects expected by the customer, outsourcing may also have a negative side as far as its employees are concerned. Examples include:

- Jobs may be lost in the area that is outsourced and, associated with this, staff may be relocated or made redundant.
- Outsourcing of business transactions alters established work processes.
- Workload can be high before, during or after the introduction of an outsourcing project.
- The need to co-operate with employees of an outsourcing service provider or external consultants may mean that individual employees have to relinquish their status as repositories of expertise and their responsibilities. It is equally possible that employees will have to assume new responsibilities and that they may feel overloaded as a consequence.
- Reorganisations in conjunction with an outsourcing project may result in a change of employer on the part of employees (e.g. where the work is transferred to a subsidiary or taken over by the outsourcing service provider). Under such circumstances, employees may be forced to accept worse conditions or at least they may regard them as such.

This and similar changes may have the effect of permanently souring the organisational climate. Possible dangers include:

- Employees or former employees could exact revenge. **Wilful acts**
- The workforce is unmotivated and either unintentionally or wilfully neglects its duties, especially security measures. **Breach of duty**
- Persons who have specialist expertise (for example IT managers and administrators) could leave the company during the implementation phase. This could cause the outsourcing project to fail to be implemented as needed or indeed at all, which could have extremely serious consequences for the organisation. Often the outsourcing service provider even relies on the staff with the all-important expertise to join its workforce. **Loss of expertise**

T 2.89 Inadequate IT security during the outsourcing implementation phase

An outsourcing project is generally implemented in several stages. Usually the implementation phase involves drastic internal changes on the part of the customer. In addition, an outsourcing project will be accompanied by stringent constraints with regard to deadlines and financial constraints. Often there is no time left for regular security checks and audits. Frequently the quality of work suffers and security concepts are neglected in the interests of adhering to deadlines and budgets during the implementation phase. However, this has a serious impact on IT security. Other possible dangers to IT security include:

Nothing persists longer than temporary solutions!

- Temporary solutions with low security standards are adopted. Often the rationale is, "The main thing is that it is working!" but for a number of reasons such temporary solutions then remain in operation for years.
- Time and resource constraints mean that "old systems" are ignored while people work on the new systems.

As a result of high workload and time pressure, problems are increasingly caused by conscious or unconscious neglect or errors. Possible reasons are:

- During the implementation phase it is necessary to maintain parallel operation of the systems affected by the outsourcing.
- The transition over to the outsourcing service provider may create many new organisational and technical interfaces.
- Employees will have to familiarise themselves with new tasks, resulting in the additional commitment of resources.
- An outsourcing project normally implies the use of new software and hardware. Incorrect testing or the failure to carry out testing, lack of experience with new security mechanisms, installation and administration errors and/or software errors may expose operations to risks.

However, shortcomings in IT security can also result from organisational weaknesses during the implementation phase. The reasons could include the following, for example:

Initial communication difficulties

- Co-operation between the customer’s staff and those of the outsourcing service provider or external consultants may not function properly. The causes could be communication problems of a technical or personal nature. Since initially the contact persons on the opposite side will not yet been known, social engineering attacks are particularly easy to bring off during this phase.
- Decision hierarchies do not yet function or contact persons and responsibilities have not yet been clarified or else change frequently. As a result, decisions are not made or are made only hesitantly or late. This could have the effect that security instructions are not adhered to, are circumvented or not monitored.

For example, a scenario like this created problems for a well-known financial institution, in that while people were preoccupied with setting up a new web server, the "old system" was no longer adequately maintained and was the

target of an attack during which customer data was compromised. Millions of people learned about the incident due to reports in the media.

T 2.90 Weaknesses in the connections with an outsourcing service provider

Outsourcing projects generally require the service provider to have access to internal resources belonging to the customer. Often this is implemented through the reciprocal connection of parts of the relevant IT infrastructure. Special information channels (e.g. dedicated leased lines, VPN connections, access for remote maintenance) may be set up to accelerate the exchange of information between customer and contractor.

If this connection is not protected or if weaknesses appear in the protection, a number of threats inevitably arise:

- The confidentiality of communications can be endangered.
- The integrity of the data transmitted is no longer guaranteed.
- The receipt of information and messages transmitted can be disputed.
- The service provider may gain a greater insight into the internal operations of the customer than it actually needs.
- External parties may gain the means of accessing the intranet of the organisation, and thus potentially placing it at risk.
- Where IT access is opened or poorly protected, tampering may be possible.
- Confidential information and intellectual property could be divulged to external parties.
- External system accesses may not be adequately monitored.

The IT connection between outsourcing organisation and outsourcing service provider could also break down completely. As a result, data that was in the process of being transmitted at the time of the failure could be destroyed or be rendered inconsistent. Depending on the duration and type of failure, the consequences could be extremely serious. This danger is even more pronounced if there is no contingency planning concept (see also T 2.93 *Inadequate contingency planning concept with outsourcing*).

T 2.91 Poor planning of the migration of Exchange 5.5 to Exchange 2000

In practice, instead of installing an Exchange 2000 e-mail system from scratch, it is more common to migrate an existing Exchange 5.5 installation to Exchange 2000. In many cases, this upgrade is combined with a change of operating system from Windows NT to Windows 2000. This change of operating system is actually a precondition to the operation of an Exchange 2000 server.

This upgrade entails moving from the NT domain concept to the Windows 2000 Active Directory directory service. This is a planning and organisational challenge which, specifically from a security viewpoint, requires careful familiarisation and thorough replanning (see S 2.233 *Planning the Migration from Windows NT to Windows 2000*).

The following security problems can occur when the migration is inadequately planned:

- An NT domain could be incorrectly configured or inconsistently mapped into the *Active Directory* of Windows 2000, as this necessitates a complete redesign of the previous infrastructure. Furthermore, incorrect integration into the Active Directory could have the result of rendering the Windows 2000 system policies and access control lists (ACL) ineffective.
- One or more Exchange 5.5 *sites* could be inadequately mapped onto an Exchange 2000 *routing group*, as this can entail restructuring the Exchange server. The primary danger here is that erroneous protocol settings or other configuration mistakes could induce a functional failure.
- Administration of the system might not be professionally planned and the administrative boundaries not defined clearly, as the administrative boundaries can change compared with Exchange 5.5 as a result of the introduction of administration groups in Exchange 2000. The Exchange 5.5 Administrator role no longer exists in Exchange 2000, and appropriate domain users have to be configured. If the granting of permissions for this user group is poorly planned, this can lead to security weaknesses and also impede administration of the system.
- The organisation-wide security policies required could be inadequately implemented as a result of poor planning of the migration of the security settings. This affects the possibilities for accessing both the server and the data held on the server.
- Data and information could be lost during the migration, especially if the system crashes during the migration phase.
- The remedial work to the configuration of the productive systems that this would necessitate could result in a loss of productivity.

T 2.92 Poor control of browser access to Exchange

Like Exchange 5.5, Exchange 2000 offers the possibility of accessing one's own e-mail account via a browser. One feature that is new in Exchange 2000 is support for the *WebDAV* protocol, which is based on the HTTP protocol. This enables access to the *Installable File System* (IFS), thus supporting the functionality of the *Web Store* and *web forms*. This is achieved using *Internet Information Services* (IIS), which is a fixed element of the installation of Exchange 2000 Server.

In principle, there is a danger that if this functionality is not professionally planned and properly regulated, the internal network could be accessed from the outside in an uncontrolled manner.

The prime areas where mistakes in the configuration can be made are the authentication of the web client to the Exchange 2000 server and the protection of information transmitted over the IP network. If the authentication methods defined are too weak, it could be possible for unauthorised persons to access e-mail data and system resources. If the encryption mechanisms used are not sufficiently strong, there is a danger that data could be intercepted. If the authentication and encryption mechanisms are not strong enough, connections could be taken over by unauthorised third parties. There is also a danger that viruses or other harmful code could get onto the e-mail server over the OWA channel.

There is a whole array of other areas of concern. Examples of other possible consequences are:

- e-mail addresses could be spied out;
- unauthorised persons could gain access to e-mail functions;
- spam attacks could be enabled;
- unauthorised persons could gain internal information about the company or agency;
- there could be opportunities for direct attacks on the internal network.

T 2.93 Inadequate contingency planning concept with outsourcing

Failings in the area of contingency planning can rapidly have serious consequences where business processes are outsourced. Additional difficulties are caused by the fact that problems generally can be spread over three critical areas. These are:

Different responsibilities

1. IT systems at the customer's
2. IT systems at the outsourcing service provider's
3. Interfaces between customer and service provider, e.g. network connection, router, telecommunications provider.

If a fault occurs, first of all it must be correctly localised, but, depending on the type of fault, this may be difficult as different faults can induce the same symptoms, e.g. failure of the communications link and failure of a system at the service provider's. Appropriate contingency measures cannot be initiated until the fault has been identified.

In the case of a partial or total failure, shortcomings in the contingency planning concepts for the customer's and the service provider's IT systems and the interfaces always result in unnecessarily long downtimes, with associated consequences for the customer's productivity and service.

T 2.94 Inadequate planning of the use of IIS

Microsoft Internet Information Server (IIS) can be used in a number of different ways. For example, it can be used as a simple information server in the intranet or as the basis for complex web applications on the internet. These operational environments result in different requirements regarding the security of IIS. The protection of a server accessible over the internet is generally a much more resource-intensive exercise than the protection of a server in the LAN, which is accessed only by trusted users.

Unless proper planning is carried out prior to installation, for example covering the system environment into which the server is to be integrated, the protocols to be used and how access is to be controlled (authentication), there is a danger that some potential risks will be overlooked.

Availability and performance are critical to the success of an internet website. No user will accept sustained long waiting times, so an internet server must always be available and its response time must be as short as possible. If resource planning is inadequate and does not take network capacities and system resources into account, then user acceptance for a website may be adversely affected.

T 2.95 Inadequate concept for linking other e-mail systems to Exchange/Outlook

Most IT environments are heterogeneous, as regards both the operating systems used and also the applications. Frequently this reflects a background in which the organisational structure within the company or agency has grown or mergers have take place.

Exchange 2000 is tightly dovetailed with the Windows 2000 operating system and is cumbersome to operate with other systems. To interact with other e-mail systems, Exchange 2000 offers *connectors* as a means of connecting the Exchange system to other systems.

From a security point of view there is a danger that security settings made under Windows 2000 which affect the Exchange 2000 e-mail system might not work outside the homogeneous Microsoft environment.

Naturally there is also a risk that security policies adopted for the outside systems will not work in the Exchange 2000 system. When different subsystems are administered separately, it is easy for inconsistencies to occur.

Connection of outside e-mail systems by a non-expert could, moreover, result in the loss of data or a blockade of the system.

T 2.96 Outdated or incorrect information on a website

The accuracy and currency of the information that an organisation publishes on a website does not just influence the success of the web offering. If incorrect information is published on the web, then the public reputation of the organisation may be damaged.

In many cases, there is a risk of financial loss or legal consequences (for example, cautions) if incorrect information is published. The consequences can be even worse if by mistake internal (confidential or even secret) information which should not be published at all gets on to the web server.

Even if particular information on the web server is only outdated, this can have negative effects. If, for example, out-of-date contact information is published, this can result in disruption of the business processes concerned.

Example:

- In 2002, reporters found a file containing the quarterly report of a Swedish company which should only have been published a few days later on its web server. Amongst other things, this led to a temporary fall in the share price of the company.

T 2.97 Inadequate contingency planning with an Apache web server

When an Apache web server is operated, inadequate contingency planning can significantly accentuate problems that occur and prolong downtime following a failure.

In addition to general errors that are frequently made in the area of contingency planning, certain special errors can occur with an Apache web server that make it difficult or impossible to respond rapidly to incidents. Some of these errors are described below.

- Should it be necessary to reinstall an Apache web server after an emergency (for example, a hacker attack), recovery can be significantly delayed if packages used during the installation (source text or distribution packages) are no longer available. If the installation packages are available, but, for example, they are stored on the web server computer itself rather than on another computer or a write-protected data medium, then they must be viewed as insecure after a hacker attack.

Installation packages not available

- If it is not clear which compilation and installation options were selected during installation of the Apache web server, it can be very difficult to restore a functionally equivalent installation. This applies especially where, for example, external modules have been included in the compilation.

Undocumented installation options and procedures

- If the configuration has not been documented at all or documentation is inadequate, then it can be very difficult to restore a functional configuration at all after an emergency. Poor documentation can also mean that configuration errors are not discovered immediately so that when problems occur troubleshooting is time-consuming.

Undocumented or poorly documented configuration

- When restoring the system after an emergency, there may be reasons for wanting to restore an older version of the configuration. However, if no version control has been implemented for the configuration files, especially the file httpd.conf, this can be difficult or even impossible.

Poor version control for configuration files

T 2.98 Incorrect planning and design of the use of routers and switches

The aspects of functionality and performance generally predominate when planning the use of active network components. If the operation of routers and switches, which act as central elements in networks, is not incorporated in the organisation-wide security concept, the secure use of these components cannot be ensured.

The errors in the planning of the use of routers and switches mostly fall into one of the following categories:

Insufficient consideration of the intended purpose of the devices

During the planning of the use of routers and switches, it is crucial that attention is paid to the intended purpose of these components. Often the intended purpose of the components is insufficiently considered during planning, for example on the use of VLANs. Contrary to statements often made in advertising, VLANs were not developed to meet security requirements on the separation of networks. VLANs provide a large number of possible points of attack, such that additional measures must always be taken particularly on the separation of networks requiring protection.

Errors can also be made during the planning of the use of router protocols. If routers are used in demilitarised zones (DMZs), the use of dynamic routing protocols can jeopardise the availability, confidentiality and the integrity of the network to be protected.

Insufficient consideration of security mechanisms

During planning, the existing security mechanisms (both in the existing network and also in the network components it is planned to use) are often not taken into sufficient consideration. For example, additional measures may be necessary, if a device does not support certain security mechanisms. If this situation is not taken into account during the planning phase, problems may arise later when the necessity is recognised.

An important point that, for instance, is often not taken into account during planning is the setting up of a separate administration network (out-of-band management). If the selected or existing devices only support insecure protocols such as SNMPv1, SNMPv2 or Telnet, it is imperative that an administration network is set up. In many cases this aspect is not addressed with the consequence that, in some circumstances, there are difficulties setting up the administration network later because the necessary connections are not available.

Missing or inadequate information and documentation

Occasionally, information needed is not available during the planning phase, as no related documentation has been made available by the provider

or the related documents are not taken into account. Incorrect decisions made due to inadequate documentation can often only be corrected with difficulty, if, for instance, it is found later that a device does not support certain functions, or only supports them inadequately.

T 2.99 Inadequate or incorrect configuration of the zSeries system environment

The resources provided by the zSeries architecture permit the operation of several production and test systems on a single physical computer. This configuration results in a high threat potential because incorrect definition of the boundaries for the zSeries system environments can permit unintentional access to other resources in certain circumstances.

Shared DASD (Direct Access Storage Device)

- When using LPAR it is possible to configure a disk for a z/OS operating system such that it can be used by all z/OS systems on the computer (by configuring appropriate sub-channel addresses using the *host configuration definition process*). Associated with this configuration is the risk that the separation of data between the LPARs is no longer ensured.
- It is possible to place disks for a logical partition, LPAR1, *online* on another logical partition, LPAR2. The data on the new disk are then available on LPAR2 and can be processed as per the RACF definitions on LPAR2. If the RACF definitions on LPAR2 are less strict than the definitions on LPAR1, in some circumstances unauthorised tampering or reading of the data may be possible.

Improper separation of test and production

Security problems can also be produced by improper separation of test and production environments. If test and production are operated on different LPARs (different zSeries systems would be even better), it is easier to define the boundaries. The operation of test and production on the same LPAR is, in principle, possible (here threat T 3.70 *Insufficient z/OS system file protection* must always be taken into account), however, the separation in this case is considerably more difficult. If boundaries between environments are not correctly defined, it is possible for test data to be included in production or for production data to be used for testing. Both involve a high threat potential.

Example:

An outsourcing service provider operated in his computer centre the applications for two competing organisations in the car industry on the same z/OS system. Due to an insecure configuration, it was possible for customer B to place the disks for customer A online. Customer B used this configuration to obtain competitive advantages over customer A by accessing the data.

T 2.100 Errors on applying for and managing Internet domain names

Internet domain names (mostly simply referred to as "domains") cannot be chosen arbitrarily, but must be registered with registration authorities (*registrars*). A registration authority can grant names for one or more so-called "top level domains" (for example DeNIC GmbH manages the top level domain *.de*). Domains are not "bought"; they are only registered for a specific period. Once this period has elapsed, the registration must be extended by paying a fee. During the registration and the extension of the registration of domain names, errors are often made that, in some circumstances, may result in significant costs and a loss prestige for the institution. Some of these errors are briefly explained below:

Failure to take "related" domain names into consideration

Often only the "right" domain name that the organisation actually wants to use (for instance *organisation name.de*) is registered. Here it forgotten that "related" domain names (for example *organisation name.com* or *organisation name.info*) will often be simply tried by Internet users who do not know the "right" domain for the organisation.

Domain grabbers

"Related" domain names are often registered by untrustworthy providers who then, for instance, run websites with pornographic content under the name. Although such presences can often be stopped by court action and the website shutdown, as such a process often takes a long time, the prestige of the organisation can suffer considerably in the meantime.

For example, in the year 2000 a German university had to take court action against a pornography provider who was using the "*com* domain name" of the university. In 2004, an adolescent managed to have the German domain for an online auction house transferred to him for a short time due to a "procedural error"; this story caused a considerable stir in the press.

Theft of access data and credit card information

The consequences can be worse than just damage to the image if a "related" domain name is used to setup a web presence that is almost identical to the real web presence and entice the innocent user into entering access data for the real web presence or credit card information for making payments. This data can then be used to obtain access to the real web server or to make purchases with the stolen credit card information. Such incidents have been announced on a number of occasions.

Trademark infringements

During the registration of domain names, it is often not checked whether the name selected infringes registered trademarks belonging to other organisations. Such trademark infringements are mostly noticed very quickly. Trademark owners or lawyers and organisations specialised in cautions regularly undertake research to identify new domains that may infringe trademarks and, in the majority of cases, send cautions with demands for compensation. In addition, the owner of a trademark can take the issue to court and demand the return or deletion of the domain. Along with significant costs, this situation can bring significant image damage.

Errors on the extension of domain names and on changing the registration authority

Domain names must be regularly "extended" at the related registrar by paying an administration fee. If the fee is not paid in time, the right to the domain name is lost and other organisations can register the domain name. If the related domain name is not company-specific, in the worst case there is no possibility of getting back the lost domain. The additional damage to the image that may be caused by the registration of this type of "orphaned" domain by a pornography provider or a radical organisation that then uses the domain to publish offensive or even illegal content can be considerable.

Sharks, touts, con men

Less trustworthy registration authorities have also rung up organisations that are customers of their competition and claimed that the registration has expired and must be renewed by making a further payment to them. When surprised customers then paid the fee to the related authority, at the same they changed registration authority.

Incorrect arrangement of the *primary name servers*

On the registration of a domain name, at least two name servers must be given; these act as *primary name servers* for this domain. If these two name servers are located in the same network segment, on the failure of the network switching element that links this network segment to the Internet, name resolution for the complete domain may be disrupted. This situation will result in it no longer being possible to access any of the services covered by the domain name such as a web server or e-mail.

For example, in 2001 a large software organisation’s domain was practically completely disrupted for several hours by a DDoS (Distributed Denial of Service) attack on the router that connected the domain’s primary name servers to the Internet. As a reaction to this attack, the name servers were moved to different network segments.

T 2.101 Inadequate contingency planning for a security gateway

When a security gateway is operated, inadequate contingency planning can significantly accentuate problems when they arise and prolong downtime following a failure.

In addition to general errors that are frequently made in the area of contingency planning, a number of specific errors can be made on a security gateway that will make it difficult or impossible to respond rapidly to incidents. Some of these errors are described below.

- If there are no plans covering the procedure in the case of emergencies and no related instructions, an efficient reaction is not possible in the majority of cases. On complex systems such as multi-level security gateways, additional problems can arise if the dependencies between individual components are unknown or not documented, or if they were not correctly taken into account during planning.
- If no replacement parts or devices are available for important hardware components and no related agreements (for example service level agreements or on-site replacement within a guaranteed time) have been made with the manufacturers or suppliers, significant downtimes and costs may be incurred.
- If the configuration and the key operating parameters have not been documented at all or documentation is inadequate, then it can be very difficult to restore a functional configuration after an emergency. Poor documentation can also mean that configuration errors are not discovered immediately so that when problems occur, troubleshooting is time-consuming.
- If tools and programs necessary for troubleshooting are not available or the administrators are not capable of using them correctly, considerable delays can be caused.
- If important data is not included in logging, the correct assessment of the nature and severity of an incident may be rendered very difficult or impossible.
- When restoring the system after an emergency, there may be reasons for wanting to restore an older version of the configuration. However, if no version control has been implemented for the configuration data, especially for the packet filter rules, this action can be difficult or even impossible.

T 3 Threats Catalogue Human Failure

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 3.46	Error in the configuration of a Lotus Notes server
T 3.47	Error in the configuration of browser access to Lotus Notes
T 3.48	Incorrect Configuration of Windows 2000 computers
T 3.49	Incorrect Configuration of Active Directory
T 3.50	Errors in the configuration of Novell eDirectory
T 3.51	Errors in the assignment of access rights in Novell eDirectory
T 3.52	Errors in the configuration of intranet client access to Novell eDirectory
T 3.53	Errors in the configuration of LDAP access to Novell eDirectory
T 3.54	Use of unsuitable data media for archiving
T 3.55	Violation of legal requirements regarding the use of archive systems

T 3.56	Incorrect integration of IIS into the system environment
T 3.57	Incorrect configuration of the operating system for IIS
T 3.58	Incorrect configuration of IIS
T 3.59	Inadequate knowledge of security loopholes and test tools for IIS65
T 3.60	Incorrect configuration of Exchange 2000 servers
T 3.61	Incorrect configuration of Outlook 2000 clients
T 3.62	Incorrect configuration of the operating system for an Apache web server
T 3.63	Incorrect configuration of an Apache web server
T 3.64	Incorrect configuration of routers and switches
T 3.65	Incorrect administration of routers and switches
T 3.66	Incorrect character conversion on the use of z/OS
T 3.67	Inadequate or incorrect configuration of the z/OS operating system
T 3.68	Inadequate or incorrect configuration of the z/OS web server
T 3.69	Incorrect configuration of Unix System Services in z/OS
T 3.70	Insufficient z/OS system file protection
T 3.71	Incorrect system time on z/OS systems
T 3.72	Incorrect configuration of the z/OS security system, RACF
T 3.73	Incorrect use of the z/OS system functions
T 3.74	Inadequate protection of the z/OS system settings against dynamic changes
T 3.75	Inadequate control of the batch jobs in z/OS
T 3.76	Errors during the synchronisation of mobile devices

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

Inappropriate actions on the part of IT users can 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.
- Data media are sent out without the prior physical dilution of data previously stored on them.
- Documents are published on a web server without checking whether these are actually intended and cleared for publication.
- Due to incorrect administration of access rights, an employee is able to modify data without realising the critical impact of such a violation of integrity.
- New software is tested using data that has not been anonymised, giving unauthorised members of staff 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.

If an outsourcing service provider looks after several customers, it is possible for data belonging to one outsourcing organisation to be made accessible to other clients of the outsourcing service provider due to human error.

Possible causes include the following:

- incorrect routing of a print job
- selection of the wrong e-mail address from the address book
- database errors
- careless "copy and paste" operations (e.g. copying and pasting of configuration files for the systems of different customers)
- mailing of items (e.g. backup media, contracts etc.) to the wrong address

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. The same results can be caused by the 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 closing all the applications that are currently running in the proper manner or else 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.
- In a z/OS system, a system programmer had permission to call the *ICKDSF* program to format hard disks. When he urgently needed a hard disk to perform his work, he selected a free hard disk from the existing pool, but, due to a typing mistake, he entered the wrong address. He only read the reply that appeared in the system log very hastily and answered it immediately. The result was that a hard disk already full of data was released and important production data was destroyed.
- 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 safeguards

It is a relatively common occurrence that, due to negligence and insufficient checks, people fail to implement, either wholly or partially, IT security safeguards that have been recommended to them or prescribed. This can cause damage which otherwise could have been prevented, or at least minimised. Depending on the function of the person in question and the importance of the safeguard overlooked, the resulting damage could even be quite serious.

IT security safeguards are frequently disregarded due to the lack of security awareness. A typical sign of this is the disregarding of recurring error messages after a certain habituation period.

Examples:

- Keeping floppy disks in a locked desk does not adequately protect them against unauthorised access if the key is kept in the office e.g. on top of a cupboard or inside a card index.
- Passwords which need to be kept secret are kept on a piece of paper near a terminal or a PC.
- Although it is widely known that the purpose of data backups is to minimise potential damage, cases of damage involving the unintended deletion of data which could not then be restored due to inadequate backups are very common. This is suggested by cases of damage caused, for example, by computer viruses that are reported to the BSI.
- Entry to a computer centre is supposed to be exclusively via a door protected with an entry control system (e.g. magnetic strip reader). However, the emergency exit door is used as an additional entrance and exit, even though it is only supposed to be opened in an emergency.
- In a z/OS system, batch jobs are run on a daily basis to back up the RACF database. The correct execution of these procedures should be checked daily by the responsible Administrators. However, as the backups have run for several months without any problems, no one checks any longer that everything is proceeding as it should. Only after the RACF databases of the production system develops a fault and there is a need to load the backups is it established that these batch jobs have not run for several days. The result is that there are no up-to-date backups available and the changes made during the last few days have to be entered manually after the event. In addition to the considerable extra administrative work, this incident also introduces an uncertainty factor, as it is not possible for all the definitions to be reliably reconstructed.

T 3.4 Illegal connection of cables

In addition to technical defects, the main cause of illegal 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 unintentional errors in the set-up and complicates the detection of deliberately incorrect assignments.

Due to illegal connections, data may be transmitted additionally or exclusively to wrong addressees. The normal line can be disrupted.

T 3.5 Inadvertent damaging of cables

The less protection is afforded to cables when laid, the greater the risk of inadvertent damage. Such damage does not necessarily result in an immediate failure of connections. It is also possible that unauthorised connections could be established accidentally. Typical examples of such damage are:

Within the building:

- Loose cable on a device is yanked out with the foot;
- Concealed (buried) cables damaged by drilling or nailing;
- Incursion of water into windowsill ducts;
- Incursion of water into conduit subways (floor ducts) during cleaning of the building;
- Exposed lines (on walls or floors) damaged during the transportation of bulky or heavy objects.

Externally:

- Damage during underground construction, caused either by manual excavation or by an excavator;
- Incursion of water into underground lines/buried cables.

Examples:

- In a pedestrian precinct, the cleaning lady employed by a small shop had made a habit of pouring waste water into the PTT-cable inspection manhole directly outside the shop door. Although the water evaporated, it took a lot of time and effort to remove the dirt and soap residue deposited on the cables.

- Damage to cables caused by rodents;
- Damage caused to ducts and cables by roots (the roots of a tree are strong enough to crush cables);
- Damage caused by the traffic loads exceeding the permitted limits (e.g. causing pipes to burst or cables to 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.
- In one computer centre, painting work was to be carried out in the machine rooms. By mistake, the painter knocked his ladder against the central emergency switch of the power supply and triggered it. The entire power supply of the z/OS systems in this computer centre was immediately interrupted. As a result of the power failure, several hard disks were not available immediately (*DASD - Direct Access Storage Device*). It took the technician who was called in several hours to get the system working again.

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 safeguards.

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 unnecessarily raises the risk of loss or damage due to viruses and Trojan horses.

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. The danger of configuration errors is especially serious in complex security systems, such as RACF under z/OS. Many system functions mutually influence each other.

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.

- In a z/OS system the users files were protected through RACF profiles via *Universal Access*, so that no one was able to access them unchecked (*UACC = NONE*). Due to carelessness on the part of the Administrator, an entry in the *Conditional Access List* of the profile allowed *READ* access to all IDs (***** entry). As a result, despite the definition *UACC=NONE*, every user in the system could see the files via the *Conditional Access List*.

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 legal force 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

inappropriate password protection under WfW

When using the file or print manager or the clipboard on a computer running Windows for Workgroups, operational errors are possible when sharing directories, printers or pages of the clipboard. This can result in resources being shared unintentionally. The required 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.

Also, a shared directory will be shared automatically, without the user noticing, if the "*Share during next start-up*" option is activated.

When using Windows 95, access rights have to be granted explicitly for sharing, so that every user has to decide whether and who is to have access. In Windows NT/2000, only an administrator or main user can share files or directories.

different protocols under UNIX and Linux

Unix- and Linux-based IT systems provide a range of possibilities for making resources available to other IT systems through the network, for example installing SAMBA, setting up NFS-Shares or activating the FTP-Daemon. As a rule, this can be done only with supervisor rights, although some services can be configured so that they use so-called non-privileged ports and can therefore be started by normal users. This carries the risk that resources are inadvertently made available through the network.

misuse of shared resources

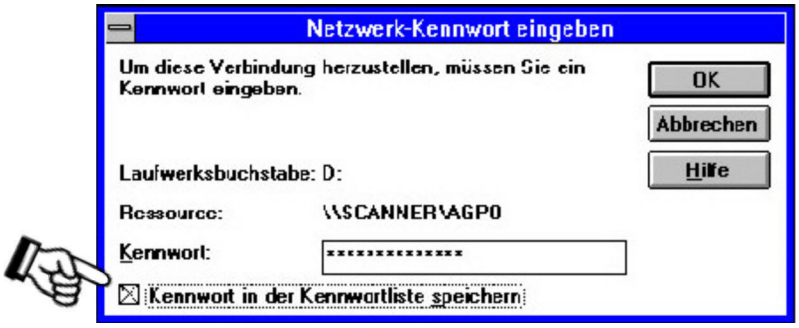
As shared resources (except for the pages of the clipboard) are generally visible to all users, other users can detect and abuse this situation. It is possible for confidential data to be read, changed or deleted without authorisation. For instance, if a directory was shared with write access and without password protection, it would be possible to store files in that directory until the capacity of the hard disk was exhausted.

Example:

After the WfW user interface had been introduced within a server-based LAN without accompanying user training, about 10% of 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. 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 encrypted 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 encryption products which are strong in themselves is often intentionally reduced (by reducing the diversity of the keys). 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 keys is reduced to only 40 bits. Some export rulings even require parts of the keys 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 encrypted 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 person related 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 encrypted before transmission because the plain-text mode in the cryptomodule was activated accidentally.
- When cryptographic keys are entered, parts of the keys 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 key) can decrypt the data with the incorrectly-entered key.
- The electricity supply is accidentally cut off during the process of encrypting the data. This has the result that only parts of the data are encrypted while other parts are not. In such a case, it may no longer be possible to decrypt the data because the process was interrupted in an inconsistent state.
- Some of the encryption parameters are entered incorrectly. This can result in an insufficient secure cryptoalgorithms or insecure cryptographic keys being used.
- If the users are involved in producing the keys, 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 encrypted or no longer encrypted, even though it may be necessary to encrypt it to preserve confidentiality.
- Encrypted data can no longer be decrypted because improper use has made it impossible to use the cryptomodule in accordance with the rules.
- Data is either intentionally or unintentionally encrypted in such a way that it can no longer be reconstructed because the necessary cryptographic key is not known.
- Correctly-encrypted data is changed in such a way that the data can no longer be decrypted.

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 Switching off the server while in operation

If a network is managed through a management system, then servers with special tasks will exist (especially in the area of system management). Databases containing management information are normally kept on what are known as management servers. If such servers are simply switched off while in operation, then any data held in the computer's memory, for example, will no longer be written to the file system. As a result, inconsistencies in the management data may occur when the computer is next booted up. Large management systems therefore normally utilise databases which use what are known as transaction mechanisms to ensure that the information can be restored to an (old) consistent state. This reduces the risk but does not completely eliminate it and can even be used by an aggressor seeking to exploit an earlier configuration with less restrictive access rights.

Switching off of archive systems

Errors can also occur with electronic archiving, if the archive system is switched off either wholly or partially during ongoing operations. Switch-off can mean that documents are deemed to have been archived, whereas in fact they have not been completely written or have not been written at all to the storage medium, and therefore can no longer be reproduced.

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 specified 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.

Untested software

Examples of current configuration or operation errors are storing passwords on a PC on which software from the internet is run without being checked (such software was used in the spring of 98, for example, to spy out T-Online passwords), or loading and implementing defective ActiveX controls. These programs, one of whose purposes is to make web sites more attractive through dynamic contents, are run with the same permissions that the user has, and can therefore delete, alter or send data at will.

Disclosure of information

Many programs which were intended to relay data in an open environment without restrictions can, with the wrong configuration settings, 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. Web browsers also transmit a series of information to the web server (e.g. the version of the browser and the operating system in use, the name and the internet address of the PC) whenever a query is made. Cookies should also be mentioned in this context. These are files in which the operators of web servers store data concerning the web user in the users 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 web pages on the server that the user has already visited.

The use of a Domain Name System (DNS), which is responsible for transcribing an internet name such as *computer1.university.edu* 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 the data traffic.

Active content

Executable contents in e-mails or HTML pages is another serious threat. This is referred to as a content security problem. Files that are downloaded from the internet can contain a code which is executed 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 on the internet, also have the potential to cause damage if the control function is used incorrectly.

Defective RACF databases

In z/OS operating systems, the availability of the RACF security system is of central importance to the availability of the entire system. This could be restricted through improper use of z/OS utilities during the backup of the RACF database or incorrect use of the RACF commands.

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

Incorrectly configured components for communication

- 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.

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 one public agency it transpired that users whose offices faced the road frequently had the same password. that this was the name of the hotel opposite the building, which dominated the view from the building with its large illuminated letters.

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 3.46 Error in the configuration of a Lotus Notes server

Errors in the configuration of a software system are frequently the cause of successful attacks. Because of the complexity of a Notes server, there is a real possibility that the Notes system might not satisfy the security requirements if configured incorrectly. Due to the large number of variables requiring configuration and the fact that a lot of parameters interact with other parameters, a number of threats can arise. Some typical incorrect configurations are listed below:

- **No restrictions on access to the server**. The basic settings generally allow anyone to access a Notes server. If there are no restrictions on access to a server, this first hurdle is wasted. Especially when combined with weak or incorrect access authorisations for other services or databases, security problems can arise.
- **Flawed access control lists (ACLs) or insecure standard ACLs.** Every database is given an access control list complete with standard entries following creation. This ACL will be based on the appropriate database template. Depending on the particular template, normally these do not offer adequate protection for the database as normally operated. This applies particularly where the database has to be initialised or further configuration settings have to be made following creation. Often generous privileges which are not necessary for ongoing operations are nevertheless initially necessary. If the standard access lists are not amended, this can result in unauthorised persons being able to access the database or users being granted excessive privileges.
- **No encryption is used**. Encryption of network communication (port encryption) and encryption of databases and database fields are normally disabled by default. To use the encryption facilities, they must be explicitly enabled. If this is overlooked, then the data will be unprotected.
- **Insufficient authorisations for server or administrative processes**. The correct functioning of a Notes database depends on its being administered and maintained from a dedicated server. The administrative and maintenance tasks of a server include updating database copies (data, access control lists etc.). If insufficient privileges are granted to the responsible server, the administrative actions cannot succeed. This can lead to security problems, for example, because changes to access authorisations cannot be passed on to the copies of a database.
- **Acceptance of cross-certificates**. Trust relationships between different certificate hierarchies (without a common certification entity) can be registered by effecting cross-certification (recognition of certificates issued by other bodies). Cross-certificates can generally be automatically generated when an unknown certificate is "discovered". This applies both to Notes certificates and also to X.509 certificates. It is also easy for users to create cross-certificates in personal local address books. On the other hand, only an authorised Administrator may create cross-certificates in the Name and Address Book. Ill-considered recognition of certificates as

trustworthy can lead to security problems (e.g. in the case of active content which is signed with the certificate that is now viewed as trustworthy).

The problem areas listed are examples of possible threats which could come about as a result of incorrect configuration. Depending on the particular operational environment, there could be additional threats.

Example:

A server is configured in such a way that anonymous access is not permitted. On the Web interface only SSL connections are allowed. Therefore, when configuring the database ACLs no "Anonymous" entry is created. Moreover, SSL-protected Web access is not enforced as the server only accepts SSL connections to the Web interface. The "default" privileges defined in the database templates have not been changed in order to minimise the administrative effort involved in modifying the templates. A new database which contains public information is subsequently added, and the server is now configured so that normal Web access is permitted to this database (on an anonymous basis, not SSL-protected). From now on it is possible to gain anonymous access to all the server databases, with the "-Default-" privileges, which often permit at least read access, in force. As a result there is a danger that unauthorised persons could see confidential data or tamper with information.

T 3.47 Error in the configuration of browser access to Lotus Notes

Web access to a Notes server is implemented with two different mechanisms which differ as to the protocol used, the authentication mechanisms and the control of access control. As a result, especially when Web access to the Notes server is introduced, it is possible for the wrong configuration settings to be made so that a given Web user is granted more extensive privileges than are in fact desirable. Typical causes are as follows:

- **The Web authentication mechanism is too weak**. Generally this is due to a combination of problems:
  - If a user name and password are used for authentication, but the authentication data is not protected with SSL, it is possible for the Internet password to be intercepted.
  - SSL client certificates are used, but the client computer is inadequately protected (e.g. no password on the certificate database). In this case there is a danger that the client certificates could be used by unauthorised third parties without the certificate owner being aware of this.
  - If the "anonymous access" option is enabled, this can, in combination with poorly configured access control lists (e.g. no "Anonymous" entry and "-Default-" entry gives " Manager" privileges), result in unauthorised access to databases.
- **The database does not enforce SSL-protected access**. Although a database contains sensitive data which should only be transmitted protected, the database configuration does not enforce the use of an SSL connection. As a result the data may be transmitted unprotected if SSL is not enforced on the server or the configuration of the server is amended.
- **Inadequate authorisation restrictions**. Additional authorisation restrictions can be configured on servers and databases for Web access. If these are not applied consistently, it could be possible, for example, through direct entry of a URL to access databases, database masks or agents.

The problem areas listed are examples of possible threats to a Notes system resulting from incorrect configuration of the Web interface.

T 3.48 Error on the configuration of Windows 2000 computers

Windows 2000 is a complex operating system whose security is essentially determined by the parameter settings. Risks to security can arise from this, especially from incorrect configuration of one or more components. These can range from malfunctions through to compromising of a Windows 2000 network.

Migration is more risky than new installation

- Where a Windows NT system is migrated to Windows 2000, the access authorisations set in Windows NT, which allow normal users extensive access to system files, are retained. As a result, the access security in migrated Windows 2000 systems is generally lower than in freshly installed Windows 2000 systems.
- If the NTLM authentication mechanism is not securely configured, it is possible to reconstruct user passwords by listening in on the network traffic. Especially in older versions of NTLM before version 2.0 this used to be a problem, but even version 2.0 of the NTLM protocol has since been compromised.

Incorrect configured encryption does not protect

- If EFS has been incorrectly configured (e.g. local user accounts are used without enabling of SYSKEY password), EFS encryption can be circumvented if an intruder has physical access to the computer.

As well as the pure operating system configuration, security problems can also arise from mistakes in the configuration of system-related components such as DNS, WINS, DHCP, RAS or IPSec. If an intruder succeeds in attacking the components, then the system security of the entire network is at risk.

T 3.49 Error in the configuration of Active Directory

Windows 2000 allows individual administrative privileges to be delegated to particular users, including for subareas of Active Directory. This delegation is effected through the assignment of detailed individual authorisations in Active Directory.

Wrong access rights

Because the assignment of rights is extremely complicated, e.g. many specific individual authorisations for each of the various object types, inheritance of access authorisations, inadequate documentation etc., it is possible for

- administrators to have access to areas of the Active Directory which they are not authorised to administer, or
- areas of the Active Directory to not be protected through access rights so that any user can access this data.

The danger of unauthorised access resulting from incorrect configuration of the AD access rights is all the greater because several access interfaces to the AD exist, e.g. ADSI, LDAP.

Special threats arise from actions which alter the database structure of the Active Directory.

Incompatibilities

- Changes to the Active Directory schema can render the existing Windows 2000 system incompatible with other software packages that use Active Directory. As some changes to the schema cannot be reversed, this can mean that the existing system has to be set up all over again.

Person related data

- When integrating a person-related attribute in the Global Catalog of the Active Directory there is a danger that personal data could also be accessible beyond the actual addressee group.

Example:

Within a company the internal telephone numbers of staff are stored in the Active Directory. If the company's computers constitute only one domain in the Active Directory tree of a larger corporate network, these internal telephone numbers would be distributed to every domain in the Active Directory tree upon entry in the Global Catalog.

T 3.50 Error in the configuration of Novell eDirectory

Errors in the configuration of software are one of the most common courses of successful attacks. The high degree of complexity and large number of parameters available in eDirectory mean that unintended side-effects can result in additional security problems.

Configuration mistakes may concern any of the following:

- creation and definition of the tree structure on its own
- configuration of the certificate server
- configuration of the objects to be mapped
- configuration of access mechanisms
- the assignment of access rights (see T 3.51)
- configuration of intranet client access to the directory service (see T 3.29)
- LDAP access to eDirectory (see T 3.53)
- configuration of partitioning of the directory database
- configuration of eDirectory replication
- configuration of the eDirectory events to be recorded
- configuration of the real-time alert mechanism
- configuration of the *iMonitor* tool for web-based remote monitoring
- configuration of an automated backup mechanism

Inconsistent implementation of the security policies

In principle, the configuration of the system must be consistent with the security guidelines. Where mistakes have been made in the configuration, there is a danger that these guidelines will be inconsistently implemented so that the objectives of the security requirements will not be achieved.

Unauthorised system access

eDirectory allows role-based administration of the directory system to be configured and also delegation of administrative rights. If these functions are incorrectly configured, this could result in serious problems due to unauthorised system access. Again, where mistakes have been made in the configuration settings, there is a danger that controlled administration may no longer be possible.

The list below provides a summary of the possible security-relevant consequences of mistakes in the configuration of Novell eDirectory:

- Chosen authentication mechanisms are too weak
- Incorrect assignment of rights for access to directory service objects
- Unauthorised system access via the administration interface
- Inadequate protection against attacks on the system
- Blocking of the means of administering the system
- Defective or slow replication of data between directory databases
- Inconsistencies in the implementation of the security guidelines

T 3.51 Error in the assignment of access rights in Novell eDirectory

As eDirectory contains a large amount of sensitive data relating to system users and resources and, moreover, it has a close relationship with the underlying operating system, the assignment of rights of access to eDirectory is particularly critical.

Access Control Lists

Rights of access to eDirectory objects are granted via *Access Control Lists* (ACLs). The access in question relates both to eDirectory objects themselves and also to the individual attributes of an object.

At object level, the following rights (privileges) are available for assignment: *Browse, Create, Delete, Rename* and *Supervisor.* At attribute level, the rights available are: *Compare, Read, Add Self*, *Delete Self, Write, Supervisor* and *Inheritance Control*. *Compare* is treated here as part of the *Read* right, i.e. if a *Read* right has been assigned, then a *Compare* right also automatically exists.

Inherited Rights Filter

Access Control Lists themselves are attributes (properties) for the relevant eDirectory objects. Rights of access to eDirectory objects are by default inherited by child objects from parent objects within the tree hierarchy. To prevent breaches in this inheritance mechanism arising as a result of partitioning of the eDirectory directory, an *inherited ACL* is attached to the root object of the partition. The inheritance process can be influenced with masks or *Inherited Rights Filters.*

The default setting is that access rights at attribute level are not passed on along the directory hierarchy. However, this can be configured via the *inheritance control* attribute right. The particularly critical *Self* right can also be controlled by this means.

Trustee assignments

The access rights are explicitly assigned by means of *trustee assignments.* Here, access rights (privileges) to the target object by other eDirectory objects (users, user groups, services, applications, servers etc.) are entered directly in the ACL of the target object.

Security equivalences

Access rights can also be indirectly assigned through *security equivalences.* Example: Target object X is given (at least) the same access possibilities as target object Y, i.e. the trustees of object Y automatically also become trustees of object X. This is likewise configured as an ACL entry of object X.

During specific eDirectory access, the actual *effective rights*, i.e. the end result of the configurations described above, are always worked out.

This variety of configuration options of eDirectory access rights carries the risk that inconsistent or incorrect access possibilities could be assigned. If access rights are incorrectly assigned in eDirectory, the security of the entire system will be compromised. This affects the confidentiality and integrity of data as well as possible backdoors for far-reaching system attacks.

Blocking the adiminstration

The assignment of Administrator rights is especially critical. eDirectory allows a role-based administration concept to be implemented, also delegation of individual administrative tasks, through the assignment of corresponding access rights. If these rights are incorrectly assigned, the entire administration

concept is called into question and it is even possible that administration of the directory system could be blocked.

T 3.52 Error in the configuration of intranet client access to Novell eDirectory

Where the eDirectory directory service is used in the intranet of an organisation, corresponding clients are needed for distributed user access to the system. Separate clients software is available for the various operating systems:

- Novell Client for Windows operating systems
- a client library for Linux
- a client library for Sun Solaris

Client access to the eDirectory directory service is effected with the proprietary NDAP protocol (Novell Directory Access Protocol). This in turn is based on the Novell NCP protocol, which can be operated with either IP or IPX.

When the eDirectory tree (or an eDirectory object) is accessed with the aid of Novell Client for Windows, the user name and password must be passed to the client. The client then searches in eDirectory for the corresponding object and sends its private key, which is encrypted with the user password. On the client side, the private key is then decrypted using the user password, and from this a *credential* and a signature are worked out. The private key is then deleted from the memory of the client and only the credential and the signature are kept. This means that these can then be used for other "background authentications" to other objects or services. The user no longer has to be involved and thus *single sign-on* is achieved.

From the credential and the signature a proof is generated using a *zero knowledge procedure*, and this is passed to the target system. The target system can verify the identity of the client with the aid of this. The advantage of this method is that the signature is not explicitly passed across the network so that there is less scope for attack.

Nevertheless, certain attack scenarios, referred to as *man-in-the-middle attacks*, are known, albeit more of a theoretical nature, as considerable technical effort is required to use them.

Nevertheless, serious security problems can arise if

- the authentication mechanisms for client access are unsatisfactory,
- unauthorised access to the eDirectory directory and its objects is possible, or
- Administrator rights for the directory service can be abused or gained illegally.

T 3.53 Error in the configuration of LDAP access to Novell eDirectory

LDAP access to the directory service of eDirectory is suited above all to two scenarios:

- user access to the directory service over the internet and
- access to the directory service by other applications.

In principle there are three different types of user access with LDAP from the point of view of eDirectory:

- as a [Public] object (*anonymous bind*),
- as a Proxy User (*proxy user anonymous bind*),
- as NDS user (*NDS user bind*).

Transfer of passwords in plaintext

It should be noted here that the [Public] object in eDirectory by default always possesses the *Browse* right over the directory tree unless this right has been explicitly withdrawn. Furthermore, it should be noted that unless suitable authentication mechanisms are configured there is a danger that user passwords could be transmitted in plaintext. Encryption of transmissions can only be relied on if communication between client and eDirectory server proceeds using SSL.

Incorrect SSL configuration

Again, there is scope for errors to be made in configuring SSL, and these too could lead to a reduction in the security level or performance.

It should also be noted which LDAP version is supported by the clients and what configuration options exist there. It is possible for misunderstandings to occur here and for the security of operations to be impaired.

In principle the same dangers exist where network applications are connected by LDAP to the eDirectory directory service as with access by clients, namely

- unauthorised access to the directory
- loss of integrity and confidentiality of data held in the directory
- unintended creation of a backdoor to the system.

T 3.54 Use of unsuitable data media for archiving

The data media on which data is stored have in each case a defined range of application and a finite period of usage. As a result it can happen that data media that do not satisfy the requirements are used either in the long-term or temporarily.

Typical reasons include:

- errors during the procurement or ordering of the data media;
- insufficient stockpiling, so that to avoid loss of data data media other than those earmarked for the purpose have to be used;
- incorrect identification of data media; or
- inadequate knowledge of the range of applications for which a given data medium is suitable.

Loss of data

During the routine procurement of new data media for an archived system, instead of WORM (Write Once Read Multiple) media, by mistake rewritable media were ordered and delivered. As a consequence of the mistake, some archival data was overwritten. As the original data had been archived a long time earlier, no copies of it were available any longer. As a result the originally saved documents were irrevocably lost, as they were no longer available in non-electronic form.

T 3.55 Violation of legal requirements regarding the use of archive systems

When electronic documents are to be archived, various legal requirements, infringement of which can result in civil action or prosecution, need to be considered. Especially common are:

- minimum periods for which documents must be retained for tax, budgetary or other reasons;
- requirements based on the data protection legislation regarding the maximum retention time;
- access rights that have to be granted to external parties, such as tax authorities;
- the legal situation with regard to digital signatures.

Some of the sources regarding the legal framework are listed in safeguard S 2.245 *Determination of the legal influencing factors for electronic archiving*.

T 3.56 Incorrect integration of IIS into the system environment

IIS is used in different environments all over the world. "Operational environment" refers here to the network topology (configuration of other hardware and software components and network components) in which IIS is operated. One important aspect that has to be considered here is the requirement for communication between IIS and other systems.

The protection of a public server accessible from the internet is generally much more complex than that of a server installed on an intranet. The secure use of suitable network separation devices is of critical importance here.

A poorly planned network structure, e.g. without demilitarised zone (DMZ). or an incorrectly configured peripheral control device (firewall) can be exploited for an attack from the internet or intranet.

Inadequate sizing of system resources (firewall, network connection) poses another risk. If these systems do not match the requirements for availability and performance of the actual web server, there is a danger of a single point of failure (SPOF).

Example

An e-business application is built on IIS and a database server. If the database server is in the same segment as the IIS, which can be accessed from the internet, there is a danger that an unauthorised person could also access the database and read or tamper with existing data assets.

T 3.57 Incorrect configuration of the operating system for IIS

Secure operation of an application depends on the security of the operating system used. As IIS is tightly dovetailed with the operating system and, for example, uses the user database and file authorisations in Windows, secure configuration of Windows NT/2000 is imperative for secure operation. Some typical configuration errors are listed below:

Too many, unnecessary services are offered. The more services a server offers, the more opportunity there is for attacking the availability of the computer and the confidentiality and integrity of the data to be handled. Every service can contain additional weaknesses that could be exploited for an attack. Especially in the case of the NetBIOS service, there is a danger that an attacker could retrieve information about existing users, shares etc.

Overgenerous configuration of network settings. The Windows Registry contains a number of parameter settings, for example, restricting the time limits of connections or limiting the number of simultaneous connections. Incorrect settings, especially of timer values, can enable a DoS attack on the server.

Inadequate protection of passwords. Another target for attack is passwords that are easy to guess or are not adequately protected. Windows provides various password protection tools which enforce adherence to a security policy over the choice of password (e.g. *passfilt.dll*) or make access to and reading of passwords difficult (e.g. *passprop, syskey)*.

The aspects listed are examples of possible security problems which could come about as a result of incorrect configuration of the operating system. Depending on the particular operational environment, there could be other potential security problems as well.

T 3.58 Incorrect configuration of IIS

Errors in the configuration of a software system are frequently the cause of successful attacks. Due to the complexity of IIS and the many different ways of using it in combination with other server systems, there is a danger that the system will be inadequate for the security requirements due to incorrect configuration. Due to the large number of variables requiring configuration and the fact that a lot of parameters interact with each other, many security problems can arise. Some typical incorrect configurations are listed below:

Too many, unnecessary services are offered: the more services a server offers, the more opportunity there is for attacking the availability of the computer and the confidentiality and integrity of the data to be handled. Every service can contain additional weaknesses that could be exploited for an attack. For example, the FTP service can be used to transfer data onto the server.

Confidential information is not adequately protected since, for example, it is held in directories that are widely accessible. Depending on the function and operating environment, there could be personal information on the server, e.g. as a result of the evaluation of forms. If this data is not adequately protected against unauthorised access, e.g. through access control lists (ACLs), it might be possible for an aggressor to read it.

Input parameters not properly validated. Many programmers assume when they develop their applications that information requested from the user, e.g. in a form field or a URL, will always be entered correctly. Validation of user inputs is often confined to the conditions necessary for further processing. Checking of syntax or of the characters used is often neglected. This results in a danger that inputs that the system is not expecting, e.g. special characters or letters instead of numerals, could lead to unnecessary resource loads and buffer overflows so that security functions can then be circumvented.

Inappropriate access control lists (ACLs). IIS is tightly dovetailed into the operating system and also uses the security mechanisms of Windows for access to files and directories. Often access rights are assigned extremely liberally. For example, the account *IUSR_Computername*, which is automatically created when IIS is installed, belongs by default to the *Guest* group and as such possesses rights of access to directories outside the web root directory. Risks may also be associated with virtual directories if, for example, scripts or executable programs are used. If access rights are not assigned restrictively, there is a possibility that these programs could be read or altered.

T 3.59 Inadequate knowledge of security loopholes and test tools for IIS

Information technology is developing and changing all the time. Hardware and software solutions are becoming ever more capable, applications are updated and replaced by new versions. However, these changes impose new requirements on the administrators and those responsible for IT. They have an ongoing information duty to familiarise themselves with the latest state of the technology.

If an administrator has insufficient knowledge there is a danger that a system could be configured incorrectly, while on the other hand threats could be assessed incorrectly in a situation. In particular, because of the complexity of IIS and its interaction with other systems in a heterogeneous system environment, risks can arise which must be evaluated by the administrator.

Publications describing the latest vulnerabilities (bulletins) in the software used are an important source of information for the administrator. Although Microsoft does publish new service packs for Windows NT and Windows 2000 when necessary, newly identified vulnerabilities in Windows and IIS are not yet reflected in the service packs. The latest vulnerabilities discovered are published by Microsoft and other working parties and organisations.

If the responsible administrators are not aware of the latest security loopholes, obviously they will not be able to take the security measures needed to protect the system against the relevant attacks.

To simplify the administration of Windows and IIS, Microsoft offers a number of test tools which are part of the *Windows NT/2000 Resource Kit* or can be downloaded from the internet directly. For example, the *IIS Lockdown Tool* offers the possibility of implementing a number of security settings very quickly, especially as regards the restriction of access to important files and directories. Another Tool is the *Hotfix Check Tool*, which checks the patch status of Windows NT and Windows 2000.

The problem with many tools that affect administration is that they only undertake certain of the security-relevant settings and the individual functions are not adequately documented.

Example:

In July 2001 the *Code Red* worm infected over 350,000 computers around the world within the space of only 14 hours. The worm exploited a vulnerability for which a patch had been available from Microsoft for some time. However, even months later there were still a large number of infected computers because the appropriate security measures had not been introduced.

T 3.60 Incorrect configuration of Exchange 2000 servers

Generally-speaking, errors in the configuration of a software system are frequently the cause of successful attacks. Because of the complexity of an Exchange 2000 server, there is a real possibility that the Exchange system might not satisfy the security requirements if configured incorrectly. Due to the large number of variables requiring configuration and the fact that a lot of parameters interact with other parameters, a number of security problems can arise.

Some typical incorrect configurations are listed below:

- Exchange 2000 Server is installed on a domain controller, rather than as a member server within the network.

  This has considerable implications for administration permissions on the server and prevents the separation of different administrative roles. The background to this is that Exchange runs as a service under the *Local System* account and thus has complete control over the computer on which it runs. If Exchange were to run on a domain controller, amongst other things it would then have control of the Kerberos keys. There are further disadvantages as regards performance and reliability.

- The access restrictions to an Exchange 2000 server are inadequate.

  Especially when combined with weak or incorrect access authorisations for other services or e-mail databases, security problems can arise.

- Access control lists (ACLs) are poorly conceived or else insecure standard ACLs are used.

  Every Exchange 2000 object is given an access control list with standard entries at the time of creation. Depending on the particular template (system policy), these do not offer adequate protection for an e-mail database as normally operated. This applies especially when the e-mail database from Exchange 5.5 is migrated to Exchange 2000. Under Exchange 5.5, some objects have no *security identifier* (SID). This means that for these objects no ACL exists at all until the SIDs are then configured.

  Often a wide range of permissions is necessary to create or initialise an e-mail database, but these are not actually needed any longer once it is up and running. If the standard access lists are not amended, this can result in unauthorised persons being able to access the e-mail database or users being granted overgenerous permissions.

- No encryption is used.

  Encryption of network communication (port encryption) and e-mail communication is not activated under a standard installation. To use the encryption facilities, they must be explicitly configured. Otherwise the e-mail data is unprotected during the delivery process.

The problem areas listed are examples of possible security problems which could come about as a result of incorrect configuration. Depending on the particular operational environment, there could be additional problem areas.

T 3.61 Incorrect configuration of Outlook 2000 clients

The e-mail client Outlook 2000 is an important element of the e-mail system. Correct configuration of the client is important for the overall security of the system.

The following aspects require a special mention here:

- The choice of communications protocol can bring with it special security problems. This applies especially to the MAPI interface, over which a number of computer viruses and worms have been disseminated in the past.
- If a client PC is used by several users, then a separate profile is created and stored for each user. There is a danger here that this profile could be taken over by a colleague. This could mean that the user account of one person is taken over as far as the system is concerned, but without authorisation, with consequent risk to the confidentiality of data.
- If encryption and digital signatures are used at e-mail level, e.g. on the basis of S/MIME or PGP, the private key could be compromised if it is stored locally. This might then jeopardise the confidentiality of the data and allow third parties to assume permissions not intended for them, without authorisation.
- If encryption is used at network level, e.g. through the use of IPSec, SSL or TLS, there is a risk that these mechanisms could be rendered ineffective if the client PC is incorrectly configured.
- Moreover, incorrect configuration of the e-mail client Outlook 2000 could result in loss of data and blockading of the client PC. Again, an overflow could occur and, with it, overloading of the Exchange 2000 server.
- If automatic execution of risky file formats is not disabled in an appropriate way in the Outlook 2000 client, then there is a danger that viruses and malicious active content could be introduced or disseminated.

Appointments administration and the To Do list are further elements of the Exchange/Outlook system that are not used directly to process e-mail traffic but to support the workflow within an organisation.

Occasionally, however, these areas can contain information as sensitive and in need of protection as the electronic messages. If these subsystems are incorrectly configured, the following potential security problems arise:

- loss of confidentiality through unauthorised access
- loss of integrity of information through data manipulation (either random or deliberate)
- unauthorised assumption of the role or identity of another user
- loss of data and information caused by unprofessional data organisation and inadequate backup precautions

T 3.62 Incorrect configuration of the operating system for an Apache web server

Incorrect configuration of the operating system for an Apache web server can impair the secure and error-free operation of the server or aggravate the effects of problems.

Some of the operating system configuration errors found relatively frequently are as follows:

- If the partitions or file systems have not been configured large enough, then operational problems can occur when the file systems "fill up". If the file systems have been created on a single hard disk or are badly distributed over multiple hard disks, then the performance of the server can suffer noticeably.

Inappropriate file system layout

- If any unnecessary network services are running on the server computer, the effect can be to jeopardise the security of the entire system. Often too many users are configured in standard installations of operating systems or else users have too many or the wrong privileges.

Too many network services

- If compilers or interpreters for script languages have been installed on the server computer, these can be used by attackers who have managed to gain access to the server computer for further attacks. Often certain steps also require that files are downloaded from computers controlled by the attacker. For this purpose the attacker may need an SSH, Telnet or FTP client or download tools like *wget*, which are not necessary for normal operation of the server.

Too many programs installed

- Often the operating system-side access authorisations for the program and configuration files of an Apache web server and for *.htpasswd* files are chosen in such a way that too many local users have read or even write access to these files. As a result, unauthorised persons could gain information about the configuration of the server which might facilitate or actually enable an attack. If unauthorised persons are able to read *.htpasswd* files, then the passwords needed for access to protected areas of the website can easily be cracked via a brute force attack.

Overgenerous access authorisations

T 3.63 Incorrect configuration of an Apache web server

Although the default configuration of the source text distribution of an Apache web server is relatively secure, significant security loopholes can be created if a default configuration for the Apache web server is simply adopted as is or is only slightly changed.

During the configuration of an Apache web server, it is possible to make a variety of mistakes. Some of the mistakes most frequently encountered are outlined below:

- Apache distributions from operating system manufacturers or distributors often contain too many modules which are not required in the particular operational scenario in question. If an unnecessary module is loaded, this can endanger the security of the server in that the administrators do not respond when a security vulnerability in such a module is announced because they do not think it concerns them.
- If the log file paths are not modified, then these files will be stored in the *logs* subdirectory of the installation directory. As log files can rapidly growing to a considerable size, there is a danger that the relevant partition could "fill up". This could seriously disrupt operation of the server.
- The Apache configuration contains default values for certain settings that affect the performance of an Apache web server. If these settings are altered without accurate knowledge of the consequences, this can significantly impair performance. Often the effects of a change are not immediately apparent.
- If the *ScriptAlias* directive is used to mark directories for the Apache web server as directories containing executable programs that contain too many scripts or programs that are not actually needed, this can result in security vulnerabilities similar to the case of "forgotten" modules. If too many local users have write access to directories that are marked as program directories using *ScriptAlias*, then malicious users could put programs there which they could execute later on through access over the internet.
- Often the "global" defaults for directory options are not set sufficiently restrictively using a suitable *Options* directive. This particularly concerns the option *Includes*, which permits the execution of program code in Server-Side-Includes. However, other options like *Indexes* can also induce security vulnerabilities.
- The configuration of access protection for HTTP access (via the module *mod_access* and the various *mod_auth_* modules) can be wrongly set in many different ways, so that as a result either there is a loss of confidentiality when unauthorised persons gain access to confidential data, or the availability of information to authorised users cannot be guaranteed.
- Where *mod_ssl* is used, the server certificate can be inadequately protected as a result of various configuration errors. Often the server certificate is not protected with a passphrase, so that an attacker who makes a copy of the certificate file for himself can set up a "forged" server. If a passphrase is used, then problems can occur with the availability of the web server, as in

this case automatic unattended reboot of the server is not possible because the passphrase has to be entered.

T 3.64 Incorrect configuration of routers and switches

The configuration of active network components is heavily dependent on the intended purpose of the devices. In the following a few example are given that could jeopardise the secure use of the devices.

Operating system

Often out-of-date versions of operating systems are used on routers and switches. Exploits for attacking devices from various manufacturers and a number of operating system versions are available for download on well known sites in the Internet.

Password protection

The access to active network components is often inadequately protected by passwords.

Administration accesses

In practice administration accesses are often freely accessible. For example, no Access Control Lists (ACL) are set up.

Remote access

Active network components as a rule provide remote access with the aid of TELNET. When TELNET is used, the user name and password are transmitted as plain text.

Login banners

Login banners on active network components often give away the device's model and version number.

Unnecessary network services

Often there are unnecessary network services on routers and switches with the aid of which attackers could jeopardise the availability or confidentiality of the components.

Interfaces

Unused interfaces on routers are often not deactivated.

VLAN

Trunk ports can access all VLANs configured. This means that access to a trunk port provides access to all VLANs. The trunking protocols on terminal device ports are often not deactivated on switches. See also T 5.114 *Overcoming the boundaries between VLANs*.

Routing protocols

Routing protocols without authentication procedures can jeopardise the confidentiality, availability and integrity of complex networks.

T 3.65 Incorrect administration of routers and switches

Incorrect administration of routers and switches can jeopardise the availability, confidentiality and integrity of networks. There are various ways of accessing routers and switches for administration, which, if used incorrectly, could represent a security risk:

Remote administration

Remote administration is provided on numerous active network components using the service Telnet. The use of Telnet, however, involves risks of the unauthorised use of access rights, as the data traffic including the user name and password can be read in plain text.

Many devices enable administration tasks to be performed using the service HTTP. In this case a HTTP server is started on the router or switch, access is obtained from any client using a web browser. The standard settings for the access to the web interface are not the same for all manufacturers. Although the access can be deactivated, it is also possible for this service to be used unprotected without the entry of user information.

In the same way as on the use of the Telnet service, with HTTP the user name and the password are transmitted in plain text. In addition, a whole series of exploits are known that utilise weak spots in HTTP servers from various manufacturers.

SNMP

With SNMPv1 and SNMPv2 authentication is performed using only an unencrypted "community string". In the standard settings from almost all manufacturers the read community string is set to the value "public", while the write community string is set to the value "private". The SNMP community strings are transmitted over the network in plain text. SNMP is often used in unprotected networks such that an attacker is able to work out the SNMP community strings by reading data packets (sniffing). Once the community strings are known, an attacker can take control of the network components.

Logging

Security-related events on routers and switches are often only inadequately logged. Furthermore, a missing alarm component can have a negative effect on the availability, confidentiality and integrity of the systems.

Missing backup and documentation

Configuration changes on routers and switches are often not backed up and not documented. On the failure of components, the most recent changes are not available when the replacement system is restarted.

T 3.66 Incorrect character conversion on the use of z/OS

EBCDIC *(Extended Binary Coded Decimals Interchange Code)* and ASCII *(American Standard Code for Information Interchange)* are coding tables that define which letters, numbers and other characters are represented with the aid of 8 or 7 bits.

z/OS systems use EBCDIC *code*. Only HFS and zFS file systems (*Hierarchical File Systems*) used with USS (*Unix System Services*) permit data to be saved in both ASCII and EBCDIC. On the exchange of data between z/OS systems and systems that use ASCII code (e. g. also from USS to MVS), there is a risk that information could be corrupted if incorrect translation tables (*code page translation*) are used. A particularly frequent problem here is the translation of special characters.

Examples:

- In an organisation data were transmitted between various OS/390 and z/OS systems using the FTP protocol without problems over an extended period. The same FTP job was used for an additional Unix system and the *EBCDIC-ASCII* translation performed using the default table. The transfer initially went without problems, however, on the further processing of the data records in the Unix system it was found that in some cases the German umlaut and special characters had not been correctly translated. Only after the preparation of a special *translation table* used only for this transfer was the error rectified.

Problem with German Umlaut and special characters

- On the transmission using the FTP protocol of a file from one z/OS operating system to a Unix operating system, the *Binary* option was used. If was not possible to further process the data on the target system as the *Binary* option suppresses the conversion from EBCDIC to ASCII.

Data errors possible

T 3.67 Inadequate or incorrect configuration of the z/OS operating system

Incorrect definitions

The configuration of a z/OS operating system is very complex and requires considerable intervention by the system administrator. Incorrect or inadequate definitions will rapidly produce weak spots that can lead to related security problems.

Authorised programs

Programs that are loaded from an authorised library and are correspondingly labelled, can run functions with a high level of authorisation. If users manage to authorise their own programs without permission, nearly the same functionality is available to these programs as is available to the system programs. It is therefore possible, e. g., to deactivate security barriers such as RACF at any time.

System programs

On the installation of the z/OS operating system and its components, it is necessary to define certain system libraries (*partitioned datasets*) such that the operating system can rapidly find programs to be run using internal tables. The libraries for these system programs are combined in so-called *link lists* and as a rule contain programs with a high level of authorisation that run in the *kernel mode*. Due to errors in the definition (or due to tampering), other user libraries, which it was not intended to add, can be added to these *link lists*. The programs in these libraries also have a high level of authorisation and enable functions to be run that can circumvent the security mechanisms.

Errors on the creation of system libraries

System libraries that have been created as a PDS (*Partitioned Dataset)* with the option *Secondary Space* can cause problems during operation. For reasons of speed the system places the *directory* for some system libraries in memory during the initialisation phase and only accesses the library using this directory on loading the program. If, during the expansion of a library during software maintenance, a new extent (dynamic expansion of the data area on the hard disk) is created, the old program may become active instead of the new program, as the internal directory still points to the old loading address. Furthermore, as a result the space required by a file can grow continuously without any controlled limiting.

Supervisor calls

Problems with SVCs

Supervisor Calls (SVCs) are calls to special z/OS utilities that run with a high level of authorisation in the kernel mode. Programs for this mode must be particularly robustly programmed (IBM specifies related guidelines). In certain circumstances insecure SVC programs can be used to circumvent z/OS security mechanisms. After a successful attack, an attacker will find himself with a high level of authorisation in the kernel mode. Today so-called *authorisation SVCs* are often still in use; these comprise a few instructions and, using *modeset*, switch on or off the kernel mode and therefore make it possible to run functions in the kernel mode without authorisation.

TSO commands

TSO commands with a high level of authorisation

Time Sharing Option commands (TSO) normally run in the application mode (with normal user privileges), i. e. they do not have special privileges. However, z/OS has commands that need a high level of authorisation to run specific functions (or subfunctions). Commands that do not have the authorisation needed to processed can produce errors in operation. On the other hand, the uncontrolled enabling of authorised commands results in a weakening of the security.

Restricted utilities

Special utilities

IBM and other software manufacturers provide additional *utilities* with the operating system components. These programs run functions that perform various actions such as the copying of files or the creation of catalogues (z/OS file list for managing files). The majority of these utilities only require normal user privileges to be run, however, some require a high level of system authorisation to run their functions. If these utilities are not correctly defined, there is a risk they will not function correctly. If these utilities are not adequately protected, then there is a risk that they may be misused by unauthorised staff. As a consequence the integrity of the z/OS system may be degraded.

z/OS commands with SDSF (System Display and Search Facility)

SDSF enables the user to view the output from batch jobs, the system log and other system options in a JES2 system, and also to enter MVS and JES2 commands. If no measures have been taken or only inadequate measures have been taken, in certain circumstances the SDSF user can tamper with the system, such as terminating batch jobs that are running, stopping or starting *initiators* or even re-defining the system configuration. Furthermore, the user may be able to view all system messages from the *syslog* and also all job logs (in some circumstances also customer data).

Enhanced MCS support

Beyond the MCS console (*Multiple Console Support*), z/OS supports the *enhanced MCS console*. This console represents an interface over which commands can be transferred to MVS (JES2/3) and messages can be received from MVS. The *enhanced MCS console* is available in *TSO*, *NetView* and applications - such as *CICS*. If appropriate protective definitions are not made, in some circumstances commands can be issued that could seriously degrade the integrity of a system.

Examples:

An open system

- In the past an *authorisation SVC* was used on an OS/390 system to use specific functions in *TSO/ISPF* in the authorised mode (*kernel mode*). Although this weak spot had been known for some time, the SVC was also installed in later z/OS environments and was available to every user.

Too many people responsible

- For historical reasons a z/OS system was operated with the RACF attribute *OPERATIONS*. Many users whose account had this attribute could read and alter almost all files. On this z/OS system it was only possible to ensure the integrity of the data content to a limited extent .

- In a z/OS system, the *SDSF* for *JES2* was made available without any protection. After only a short time staff discovered how they could increase the priority of their own user account in the system so that they could have their batch jobs processed quicker in the system. Control and efficient utilisation of the system were no longer possible.

No system control

T 3.68 Inadequate or incorrect configuration of the z/OS web server

Accepting the default settings or incorrect configuration of the z/OS web server can cause security problems.

- On the use of the standard settings (file *httpd.conf*) and incorrectly set *userid* rules, in certain circumstances the web server's *MVSDS* function may be used to display files that should not normally be available to the user, such as system files.
- Administration errors can result in z/OS web server processes running with the *started task* ID. If this ID has high level rights in the system (e. g. *super user)*, security problems may result. File accesses and commands are then made and run using the authorisation of this ID. As a consequence, in certain circumstances it is possible to access files with customer data or, as described above, system files using the *MVS dataset display* function.
- The z/OS web server supports encrypted data communication using the SSL protocol. On the incorrect configuration of the parameters, there is a risk that the encryption will be deactivated or that the processes will be run using a different RACF ID.

Other threats are listed in module 7.5 "Web server".

Example:

- The use of the standard definitions for a z/OS web server enabled an external attacker to view sensitive data. In addition, the web server was configured such that the service ran with high level rights using its own *started task* ID. As a result it was possible for an external attacker to display the files *SYS1.PROCLIB* and *SYS1.PARMLIB* from the Internet. From these files the attacker was able to draw information that made it easier to attack the entire z/OS system.

T 3.69 Incorrect configuration of Unix System Services in z/OS

Unix System Services

Unix System Services (USS) is a z/OS subsystem that must be customised prior to putting the system into operation.

During the customisation of the USS parameters there is a series of problems that must be taken into account to ensure that there are no security problems in the z/OS system or parts of the z/OS system.

Depending on the type of error in the configuration, certain subfunctions in the *Unix System Services* may not be available after starting the z/OS system, or the *USS subsystem* will not start:

- If USS subfunctions fail, important subsystems such as TCP/IP may be missing.
- If the entire *USS subsystem* does not start, the z/OS operating system is also not available.
- If *HFS files* are not *mounted* during the start phase, applications that need these files cannot be used.

Some typical errors in the configuration of the USS are given in the following:

- The complex layout of the *BPXPRMxx member* can result in administration errors. Errors will result in an incorrect system start during the *Initial Program Load (IPL)*. This issue is question of the order in which the individual member definitions are run through.
- Certain parameters in the *BPXPRM00 member* must be matched to the system's capacity limits. Otherwise there is a risk that more Unix processes will start than the system can handle.
- Errors may occur in the *sysplex* definitions, e. g. in the *VERSION* information.
- Errors in the definition of the *mount policies* for HFS and zFS files (type, mode and mountpoint) are possible.
- Variables may have used incorrectly in the *BPXPRMxx member*.

Examples:

Inappropriate thresholds

- Calling a recursive Unix command continuously generated new processes on a z/OS system until the z/OS swap files (*page disks*) were exhausted. Despite the presence of further *page disks*, it was not possible to recover the system as it was only possible to make a few system entries. It was only possible to solve the problem by restarting (*IPL*) the system.

Complex sequences of parameters

- On a z/OS system with several *BPXPRMxx members* a parameter change was made in the wrong member. The change was not taken into account by the system because the parameter was read from a preceding member during the *IPL*.

T 3.70 Insufficient z/OS system file protection

In the z/OS operating system, a security system like RACF controls and monitors file access. Incorrect administration of the file protection may enable an attacker, under certain circumstances, to access important files without authorisation, e. g. operating system programs, configuration files or application data.

RACF enables user accounts to be granted comprehensive rights using special attributes (e. g. *Special* or *Operations*).

It should be taken into account that data to which a user has read access can also always be copied by the user in z/OS.

In this context the threat T 3.16 *Incorrect administration of site and data access rights* should also be taken into account.

Examples:

- The files for the salary data were copied using the ID of a member of staff with a user account defined in RACF with the attribute *Universal Access UPDATE*. As a result all staff had not only read access, but could also alter the data. **Unintentional viewing and tampering**
- Due to careless handling of the RACF attribute *Operations*, a user was able to read or copy nearly all system data and customer data. **Operations attribute**

T 3.71 Incorrect system time on z/OS systems

Incorrect time

The system time (date and clock time) is an important variable for a whole series of applications and system programs on which the correct execution of numerous actions and the reliable preparation of results and data is dependent.

Due to incorrect date/time information, among other aspects the following security problems and resulting damage can occur:

- Applications that make decisions based on the current date provide incorrect results. The rework of entire days of production can be consequence. This applies particularly for online applications and their transaction data. Corrections are often no longer possible if, e. g., customers access the system online.
- The analysis of security incidents that takes into account time information can be made significantly more difficult or even produce incorrect results.
- Differing system times in interconnected systems are a problem if, e. g., log data are to be used for a common evaluation.
- Applications that receive data from several individual systems and process the data as a function of the time stamp will produce corrupted results.

System time on z/OS systems

If z/OS systems are not operated in a *parallel sysplex cluster*, as a rule it is necessary for the operator to enter the system time manually during the *IPL* (Initial Program Load). Here mistakes in the date or time can easily be made.

It is also possible to change the system time when the system is in operation. Here the risk of incorrect entries is even greater than during an IPL.

In the *member clock00* the time zone or the difference in relation to Greenwich Mean Time (GMT) is set. An incorrect time zone setting will produce the same result as if the system time itself was set incorrectly.

Examples:

Incorrect time information

- During operation the time setting in a z/OS system was to be corrected by 5 minutes. A typing error on the entry of the *SET* command resulted in a system time that was in the evening. Accordingly the *job scheduler* started the evening batch production during the day. Because the batch jobs required exclusive access to the application data bases, data entry online was no longer possible.

T 3.72 Incorrect configuration of the z/OS security system, RACF

Incorrect security settings in RACF

In the z/OS operating system, a special security system is responsible for the protection of access to resources. Here RACF (*Resource Access Control Facility*) is often used. The configuration of RACF as supplied does not, as a rule, match the security requirements in the related operational scenario.

The problem areas most often found in the RACF configuration are described in the following.

Validity rules for passwords

SETROPTS definitions

Using the SETROPTS command, it is possible to define security settings applicable across the z/OS system in RACF, in particular for passwords. The parameters include the minimum password length, the number of log-on attempts allowed, the maximum period of validity, the password history, audit settings and the class activations.

Misuse of standard passwords

As supplied, there are standard passwords in z/OS for the ID *IBMUSER* and the RACF command *RVARY*. Even in operation, the system monitors with functions critical for security are often still accessible using standard passwords.

The ID *IBMUSER* is used as an initial ID for setting up a new system and has *Special* and *Operations* privileges. As the *IBMUSER* ID is not allocated to any specific user, it is almost impossible to find out who is using or has used this ID.

Using the RACF command *RVARY*, the RACF database can be activated and deactivated, i. e. also changed.

The standard passwords are given in the product documentation and therefore generally known.

Warning mode

RACF resources can be protected in the *warning mode*. This means that access to the resources is always granted, even though the RACF definitions would actually deny access to the resource. As a result of the warning mode, in certain circumstances considerably more messages are written to the *syslog* and, in addition, more SMF records (*System Management Facility*) generated. As a consequence the amount of disk space required can increase significantly.

Erroneously granting access to resources via the warning mode can result in a loss of data confidentiality.

Protection of z/OS system commands

The z/OS system commands are protected using special classes in the RACF. If these classes are inadequately defined, it is possible for users to issue system commands that could degrade stable system operation in certain circumstances. Examples here are the starting and stopping of *started tasks* or placing disk systems online.

Global Access Checking table

If files are entered in the *Global Access Checking table (GAC)*, access is not checked using the RACF database. The user has direct access as per the rules defined in the *GAC*. If incorrect files are entered in the *GAC*, they will no longer be protected by the RACF profiles. These files can, e. g., be read by all users if they are entered in the *GAC* with *READ*.

RACF database

The RACF database contains, in encrypted form, all user passwords and must, like any other file in the z/OS operating system, be protected using appropriate definitions. If the access protection to the database is defined such that every user can read (and therefore also copy) the file (e. g. using the definition *Universal Access(UACC) = READ*), a brute force attack on the passwords is possible.

Examples:

- It is possible to change the RACF database using the *RVARY* command. A system programmer found that the password for the *RVARY* command was still the same as the standard password as supplied. The programmer was then able to place a different, specially prepared RACF database in the system and activate it. The programmer then had access to data that he could not view before.

Use of the RVARY command

- After setting up a new RACF database, an operator forgot to disable the ID *IBMUSER*. A clerk discovered this carelessness and was able to copy, from the system, data to which he was not allowed to have access.

Use of the IBMUSER

- The backup copy of an RACF database was only protected using the definition *UACC(READ)* due to an administration error. An attacker utilised this error to copy the database to his PC. On the PC he used freely available programs to carry out a brute force attack on the passwords in the RACF database and was successful in several cases. The attacker then used the other users' IDs and passwords so obtained to change production data. The suspicion fell initially on the owner of the ID logged for the access to the log files, and not on the person responsible for the damage.

Brute force attacks on RACF database

T 3.73 Incorrect use of the z/OS system functions

When the z/OS system is in operation, *operators* need to make changes from time to time, such as customising RACF settings or other system definitions.

Due to the complexity of the z/OS operating system and its components, it is not possible to fully exclude the possibility of incorrect actions by the operators. Depending on the nature of the incorrect action, individual components or the entire system may fail. A few typical examples of incorrect actions are given in the following.

Inadvertent restart using the Hardware Management Console (HMC)

A system restart can be requested using the HMC. To select the system it is sufficient to simply click the system icon, then it is only necessary to select the function (e. g. *Initial Program Load*). After accepting a corresponding prompt, this action will result in an immediate restart of the selected system. All processes that are running will be stopped in an uncontrolled manner. As a result a mistake on selecting the system can have serious consequences.

As groups of systems can also be set up in the *HMC*, including all z/OS systems in a computer centre, large areas of information processing could be affected.

Errors in the JES3 DSI (Dynamic System Interchange)

The *Job Entry Subsystem* JES3 permits the operation of a system group comprising a *global* computer and various *local* computers. Predominantly batch jobs are distributed across all computers in the group (*global* and *local*) under the control of the *global* computer and can be run (similar to a *parallel sysplex cluster*, but limited to JES3). The *global* computer takes over the central control of the entire life cycle of the batch job, such as interpretation of the job control language, system allocation, resource control, output management, etc.

To take over the function of the *global* computer on a *local* computer, a series of system questions must be answered. In an extreme case incorrect entries can result in an IPL (*Initial Program Load*) on all systems in the group.

Disabling z/OS IDs

IDs with the *Special* attribute generate a console message (*reply*) if the password is entered incorrectly several times during login. The *operator* can decide whether this ID is to be disabled. If, in an extreme case, e. g. during a DoS attack, all IDs with the *Special* attribute are disabled (e. g. by automatic means), on this system there is then no longer an ID that can operate the RACF. The security system is then completely locked.

Setting disks offline

Accidentally *setting* a disk *offline* can have serious consequences and even lead to the total failure of the system.

Deleting the default program class in RACF

If the star profile for the *program* class is deleted accidentally (e. g. by a typing error), the system may come to a halt. An IPL will not help, as the cause of the error will not be rectified. First the RACF database must be corrected. Such an error can result in a system failure lasting hours and considerable effort to rectify the error.

Forwarding of incorrect RACF commands

If a system is included in a RACF command synchronisation (e. g. *RACF Remote Sharing Facility* - RRSF), an incorrect RACF command can affect all other systems in this group. If, for instance, the deletion of the *Default Program Class* is transmitted via RRSF, all systems in the related RRSF group may come to a halt.

Incorrect operation of pre-defined program function keys

The use of pre-defined program function keys can also cause security problems in certain circumstances. Particular care is required, e. g., if function keys are allocated commands that require the addition of specific values prior to execution. Here there is a risk of the operator pressing the function key accidentally without entering the supplementary information. If the related command is syntactically correct even without the supplementary information, it will be executed and may cause undesirable effects or even massive damage in certain circumstances.

Incorrect input in general

In general there is always the risk of incorrect input. If, e. g. a system task (or a batch job) is to be stopped and the operator makes a typing mistake, the wrong job may be stopped if job names are similar. The same applies for the use of system commands.

If, e. g., on deactivating SNA nodes, the *cross domain* manager name is accidentally entered instead of a specific terminal name, all *SNA sessions* in this domain will be lost. After the node is restarted, the user must login again and re-establish the *SNA* connection to the system.

Locking of resources

On mutual locking of resources (*enqueue contention*), functions may not be available until the lock is removed. Often a series of system prompts (*displays*) and considerable experience are necessary to remove the mutual locks with the aid of the right MVS commands.

Inadvertent entry of the "Z EOD" command

If the *Z EOD* command is entered on an MVS master console during operation, this system will be shutdown in a controlled manner. All processes

will be stopped and must be restarted. This action and the related system failure will last, as a rule, at least 30 minutes.

T 3.74 Inadequate protection of the z/OS system settings against dynamic changes

Dynamic z/OS customisation

Many z/OS system settings can be changed during operation without the need to perform an IPL. After an existing parameter file (member of the *parmlib*) has been changed or a new file added, an activation command triggers the change process.

The security of z/OS systems can be impaired if certain commands are used incorrectly or they are misused by unauthorised persons. The most important, critical parameter files and system commands that can be changed by dynamic settings during operation are listed in the following.

Extension of the APF files

Files that must be authorised using the *Authorized Program Facility* (APF) can be defined in a *definitions member* (*PROGnn*) and then activated using the command *SET PROG=nn* (*SET* command and parameter *PROG=m*). As an alternative, using the command *SETPROG APF* (*SETPROG* command and parameter *APF*) individual libraries can be incorporated in the APF mechanism. If the *parmlib* definitions or the corresponding commands are not correctly protected, security problems may arise as third parties may be able to give their programs a high level of authorisation and activate them during operation.

Extension of the *LINKLIST* mechanism

Programs that are to be available in a batch job without a *Steplib* or *Joblib DD statement* can be defined in the *LINKLIST*. These definitions are saved in a *PROGnn member* in the *parmlib*. Files can be added dynamically using the *SETPROG LNKLST* command via a member that must be defined. If the *LINKLIST* is defined in the system definition (*IEASYSnn*) using *LNKAUTH=LNKLST*, all programs loaded using this mechanism are automatically APF-authorised. The integrity of the system is also jeopardised here if the command is available without protection.

Deactivation and modification of the *user exits*

Using the *SETPROG EXIT* command it is possible to deactivate *exits* or replace them with others. If the command is only inadequately protected, an attacker may be able to run his own *exits* on the system in certain circumstances. In this way it is possible, e. g. to prevent the writing of SMF records (*System Management Facility*) and to affect the auditing of the system (covering up).

Modification of the Message Processing Facility (MPF)

A large number of programs evaluate system *messages* for the automation of processes. By setting different MPF versions (*Message Processing Facility*) using the command *T MPF=nn*, automation can be disrupted or even completely disabled (*T MPF=NO*).

Exchange of parmlibs

Parameter files (*parmlibs*) are the central point for the z/OS system definitions. With the aid of the *SETLOAD* command, existing *parmlibs* can be replaced with new *parmlibs*.

Other critical z/OS commands for dynamic changes

Along with the commands described above, a series of other commands for changing z/OS system settings is available, such as *SETSSI* for adding or deleting subsystems or *SETSMS* for changing the SMS definitions.

Security problems can be caused by all these commands that dynamically change the z/OS definitions if they are available in the system without control. The misuse of these commands can result in problems similar to those on tampering with critical definition files.

Examples:

- A member of staff in an organisation was able to authorise his own program file due to inadequate protection of the *SETPROG APF* command. With the aid of a further program loaded by this file, it was possible for the member of staff to corrupt important financial data.

Unauthorised access to APF files

- Using the command *T MPF=NO* (T is a short form for the SET command), an operator disabled the *z/OS message processing*. This action resulted in a console overload (message flood) and some *exits* defined there were disabled such that the automation of the system was seriously impeded.

Tampering with the automation

T 3.75 Inadequate control of the batch jobs in z/OS

z/OS operating systems are still used to a large extent for running batch jobs. A batch job comprises one or more single steps (job steps).

The inputs to a batch job are either one/several file(s) or corresponding control cards, which are added using the *Job Entry Subsystem (JES2/3)*. The output is also managed using the *Job Entry Subsystem*.

The control of the batch jobs primarily comprises *starting*, *monitoring* execution and *checking* the result (mostly in the form of a *return code*). Depending on the *return code*, it is often necessary to start other batch jobs. The greater the number of jobs and the complexity of executing the jobs, the greater is the probability of an error.

Manual control

During the manual execution of batch jobs there is always a risk that problems will occur during the execution of the batches due to human error. Along with the sequence of execution in time, the dependencies of the batch jobs on each other are affected. With an increasing number of batch jobs to control, the complexity of the entire batch chain therefore increases drastically and will result in an ever increasing number of errors. Manual control therefore has its natural limits.

Time delays, e. g., can result in an online process running after the batch job not starting at the right time, or file backups colliding with the online process.

Computerised control (job scheduler)

If a computerised process (*job scheduler*) is used, the execution of the jobs will be ensured. However, errors can occur if the instructions to this *job scheduler* have not been properly tested and there are errors in the instructions. Incorrect reactions from the *job scheduler* can also be caused by incorrectly defined automation during the batch processing.

Example:

Degradation of online operation

The abort of a batch job during batch processing was not noticed. Only online processing the following day showed that there were errors in the data. To correct the errors, it was necessary to stop the online processing, reload data and then repeat the batch processing. During this time it was not possible to process data online.

T 3.76 Errors during the synchronisation of mobile devices

Data that is held on mobile IT systems, such as laptops, mobile phones and PDAs, is often synchronised with fixed-location IT systems. For example, this is sensible for appointment and address administration.

However, data can also be destroyed during synchronisation. Generally it is necessary to lay down rules as to how to proceed in cases of conflict, for example, whether if two files have the same name either the PDA file or the one held on the other device should be adopted without question or whether the user should be asked to confirm which file to use. This action is often configured when the docking station is used for the first time and is then conveniently forgotten. If data is then changed in a sequence different from that originally intended, important data can be lost very quickly. This situation can occur as an unpleasant side effect, if, for example, several users synchronise their PDAs using the same terminal device without considering the possibility that files with the same name could be overwritten.

T 4 Threats Catalogue Technical Failure

T 4.1	Disruption of power supply	
T 4.2	Failure of internal supply networks	
T 4.3	Failure of existing safety devices	
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	**dropped**
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 storage space
T 4.30	Loss of database integrity/consistency
T 4.31	Failure or malfunction of a network component
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 operational environment
T 4.41	Non-availability of the mobile communication network
T 4.42	Failure of the mobile phone
T 4.43	Undocumented functions
T 4.44	Failure of Novell eDirectory
T 4.45	Delayed access to archive information
T 4.46	Poor synchronisation of index data during archiving
T 4.47	Obsolescence of cryptomethods
T 4.48	Failure of an outsourcing service provider’s systems
T 4.49	Insecure default settings on routers and switches
T 4.50	z/OS operating system overload
T 4.51	Inadequate security mechanisms on PDAs
T 4.52	Loss of data when using a portable device

T 4.1 Disruption of power supply

However supposedly secure a power supply is, power failures are actually a regular occurrence. In most cases of power failure, the power is down for less than a second so that it can escape notice. However, IT operations can be disrupted even by failures lasting as little as 10 ms. During measurements carried out at some 60 measuring points in Germany in 1983 approximately 100 power dips of this type were recorded. Of these, five failures lasted for up to 1 hour, and one had a duration of more than one hour. These interruptions were due solely to failures in the mains supply. Interruptions can also be caused by shutdowns for unannounced maintenance work or by cables damaged during underground engineering work.

It is not only direct users of electric power (PC, lighting, etc.) that depend on the power supply. All infrastructure installations nowadays are either directly or indirectly dependent on electric power, e.g. lifts, pneumatic post systems, air conditioning, alarm systems and telephone private branch exchanges. Even the water supply in high-rise buildings relies on electric power due to the use of pumps to generate pressure in the upper storeys.

Liberalisation of the electricity market has resulted in some industrial countries in a worsening of the level of supply. In Germany also the danger could arise of problems due to power supply failures or to switching operations at a national level.

Examples:

- In a large industrial plant in southern Germany, 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 departments that had no auxiliary power supply.
- Due to a fault in the uninterruptible power supply of a computer centre, this did not switch back to normal operation after a brief power failure. Following discharge of the batteries, after around 40 minutes all computers in the server room affected crashed.
- At the beginning of 2001 there was a power emergency in California that lasted over 40 days. The power supply situation was so tight there that the Californian Independent System Operator (ISO) mandated rolling blackouts. These outages, which lasted up to 90 minutes, affected not only households but also high-tech industry. The power utilities did not publish timetables as to when the power would be down and where, because alarm systems and surveillance cameras were switched off during the power failures.

T 4.2 Failure of internal supply networks

In a building, a variety of networks exist for supply and disposal and thus serve as a basis for IT processes 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 Failure of existing safety devices

Technical defects or external factors (e.g. ageing, improper use, deficient maintenance, manipulation, power failure) can cause safety devices to fail, with the result that their protective effect is greatly reduced or entirely lost. It can also happen that in problem areas, e.g. due to major environmental influences or especially high usage, controls and maintenance intervals are not modified as required. Once again this can result in failures of safety devices.

Examples:

- Door locks can become damaged due to age or improper use.
- Fire extinguishers which are incorrectly serviced do not work properly.
- Dirty fire alarms fail to detect fires or are triggered unnecessarily.
- Keys or identity passes can become damaged due to failure to look after them in the proper manner or through wear and tear.
- Bolt contacts in doors can get stuck.
- Still images in surveillance cameras can become burned in.
- Fire protection doors are often carelessly wedged into an open position.
- Sometimes smoke alarm systems are tampered with in non-smoking zones.

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

Fluctuations in the supply voltage may result in malfunctions and damage to IT assets. Such fluctuations range from extremely short and minor incidents which have little or no effect on IT systems, to total failures or destructive overvoltages. These can be induced in any part of the electricity supply system, ranging from the mains supply of the power company through to the power circuit to which the devices concerned are connected.

Overvoltages can also occur outside the electric power supply system, on all the other electrically conducting networks (e.g. telephone connections, building services management system, water or gas pipes etc.).

T 4.7 Defective data media

Failure of, or faults in, individual data media due to technical defects or damage are relatively common. Such media include mass storage devices like 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 impact. Again, CD's can be rendered useless by surface scratches. Diskettes are particularly vulnerable to failure: it is not uncommon to find that reading from, or writing to, a diskette is suddenly 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 headcrash, as a result of which some data was destroyed. **Dust particles**
- A field service employee's laptop started inexplicably developing faults, despite always being 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. **Magnets**
- Some ZIP diskettes were temporarily stacked on the speakers of a multimedia PC while it was being backed up. The magnets in the speakers destroyed parts of the data media.
- Bit errors on archival data media could mean that encrypted documents can no longer be decrypted. By a similar process it is possible that digital signatures could no longer be verified. **Bit errors**

T 4.8 Disclosure of software vulnerabilities

Software vulnerabilities are understood to refer to 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 checking of limits on 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 were 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 accessing networked IT systems

Unlike stand-alone systems, on which access is essentially controlled by the log-in process, so that the only way of corrupting access is through the use of poor passwords or failure to enforce password entry, network computers have many complex processes allowing multifarious forms of access. Thus under UNIX, for example, *sendmail* allows for the introduction of texts (e-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 plaintext passwords. However, this security mechanism is circumvented when services such as FTP or Telnet, which use plaintext passwords, are used.

All these processes can constitute a security vulnerability if incorrectly configured, but there is also, of course, a much greater probability that a security-related programming error could exist in one of the processes due to its size.

There are many different ways of connecting a z/OS system to internal and public networks. Access is possible over SNA and TCP/IP, e.g. FTP, TELNET or via the browser. Many of the network functions familiar to UNIX installations can be used under the *UNIX System Services* of z/OS. This diversity of connection possibilities makes it very difficult to achieve a secure network configuration for z/OS systems.

Example:

Non-authorised data access via FTP

An external aggressor succeeded in working out the user ID and password for an application under z/OS that required a high level of authorisation. Although the ID did not have a *TSO segment*, the attacker was able to bring a batch jobs directly into the *JES2* via FTP and execute it there. As the job output could also be read via FTP, access to confidential data was possible.

T 4.11 Lack of authentication possibilities between NIS server and NIS client

If the NIS domain name is known, any computer can be logged on as a client, and all the NIS maps can be retrieved, in particular the *passwd* map.

If Administrator privileges can be gained on a computer, a NIS server process (*ypserv*) can be started on a privileged port. If the client process *ypbind* is now restarted on the computer to be infiltrated and the own server process can be made to respond before the correct NIS server, any arbitrary information can be transferred 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. 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 could delay or even prevent the performance of administrative 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)
- Exposure of magnetic data media to external magnetic fields
- Destruction of data media by force majeure, e.g. fire or water
- Inadvertent deletion or overwriting of files
- Intentional or accidental setting of deletion flags in archive systems (see also T 5.106 *Unauthorised overwriting or deletion of archival media*)
- Technical failure of external storage (headcrash)
- Faulty data media
- Uncontrolled changes in stored data (loss of integrity)
- Deliberate destruction of data through 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 involvedAs 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 4.18 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 failureIf 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 the exhausting of storage medium capacity

Every storage medium has a finite capacity to hold data. When this limit has been reached, data could be lost and/or services could cease to be available, so that, for example,

- Users cannot save any more data;
- Incoming e-mail is rejected and it may not be possible to send out any more e-mails either;
- Incoming or outgoing fax transmissions are rejected;
- Logging of data is no longer possible, or log data which has not yet been analysed is overwritten;
- Documents can no longer be archived electronically.

The capacity of the storage medium can suddenly become exhausted due to a variety of reasons, e.g. due to errors in the application program, an increase in users storage requirements or a malicious attack intended specifically to reduce the existing storage space, thus preventing audit trails from being kept.

Large quantities of data to be archived

Where electronic archiving is used, usually large quantities of data have to be backed up. Data is generated firstly due to the large number of documents that have to be archived under defined processes. And secondly, every newly created version of a document is stored with a newly assigned version number.

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 Vulnerabilities or errors in standard software

The more complex it is, the more frequently programming errors will occur - this applies both to standard software and to all other software. High expectations on the part of the user coupled with the release of standard software at inordinately short intervals can have the result that the manufacturer sometimes launches a product before it is ready and all the bugs have been fixed. If these software errors are not detected, the errors resulting from the use of the software can have serious consequences.

Examples:

- A software error in the RACF security software of the z/OS operating system can mean that not only does RACF suspend the service but that as a result the entire system can no longer function and needs to be restarted.
- Users frequently overestimate the strength of the security functions in standard software (such as passwords or encryption algorithms). These security functions often cannot survive 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. This has the effect of consuming additional IT resources, while at the same time it is makes clear that the full functionality of the product cannot be checked down to the last detail during software testing.
- 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 that arise 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 arbitrary 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 fault 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 can be carried out manually. In the case of tasks which entail the use of a database and depend on IT support, depending on the nature of the tasks, the following consequences are possible:

- financial loss
- security risks which might be severe enough to cause personal injury (for example, in the case of medical databases)
- loss of confidence because archived documents cannot be furnished
- partial or complete disruption of operations

Examples

- Electronic archives are based on a database in which all the archived documents are indexed. If this index database were to fail, it would no longer be possible to find or search for archived documents The result could be that the archive cannot be operated at all or only with severe restrictions

Index database of archives

- The content and all the supplementary information for a publication that appeared at regular intervals were moved to a database. Since, as a minimum, read access to this database is necessary for all work in the responsible section, unless it functions properly then it is no longer possible to perform any content work. The database was out of action for some time for the purposes of carrying out maintenance work. As a result, for a whole week the section was only able to perform very limited work.

Maintenance work

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. Then the old data have to be converted and mounted into the changed tables. 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 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 4.30 Loss of database integrity/consistency

A loss of database integrity or consistency means that, although data may still exist in a database, it has become corrupted or unintelligible. As a result, the data cannot be correctly processed any more. This could be due to a variety of causes, for example, inadvertent data manipulation (e.g. unintentional modification of data), inadequate synchronisation control of transactions or deliberate attacks.

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 could be difficult or even impossible to determine exactly which data was modified. This could lead to further financial losses and security risks.

Examples

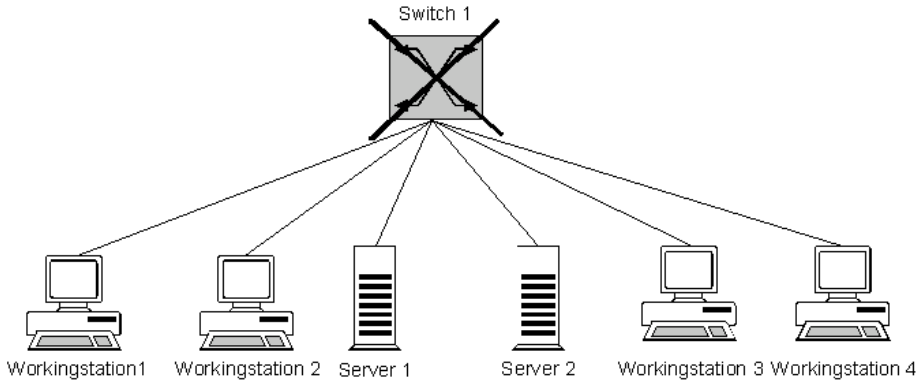
- To save space and time, a database file is created in the */tmp* file system on a UNIX server. This file is deleted subsequently during an overnight *cron* job, as a result of which the entire database is rendered unusable.
- Electronic archives are based on a database in which all the archive documents are indexed. If the indexing or referencing to individual documents is lost, it may not be possible to find them again without an inordinate amount of effort. Considerable financial or legal damage could result at a later date from such a loss of the database integrity.

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:

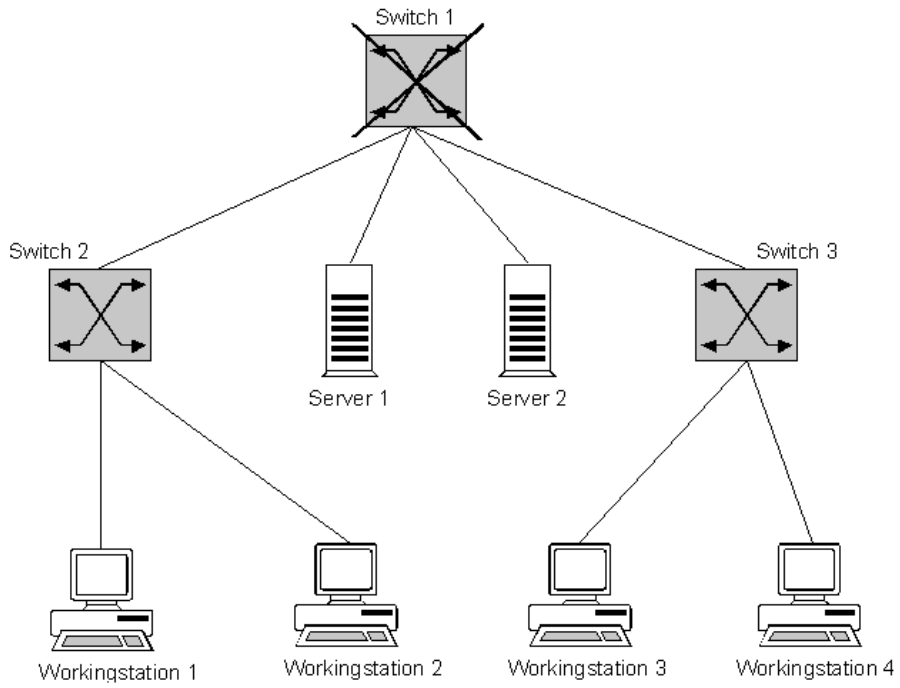
- With a failure or malfunction of the entire network component, the network is rendered inaccessible for all the stations connected to it. With such a failure or malfunction of just a single port, only the station connected via this port is no longer able to access the network.

  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.



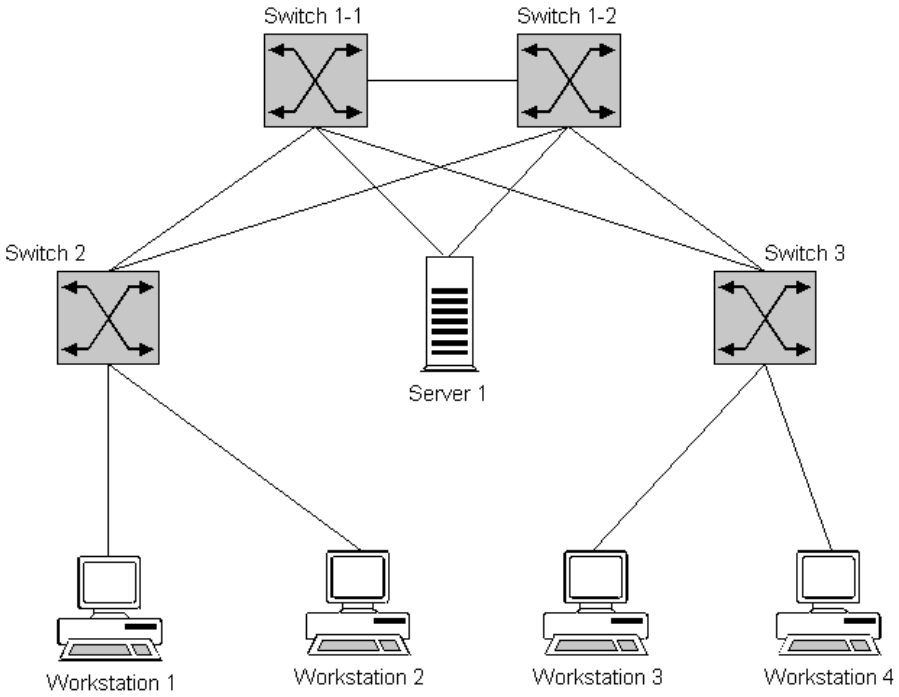
- Another situation involves active network components which are not connected directly to the network segments of mutually communicating workstation and server systems, but which are located in the signal path between these systems. If no redundant signal paths are present between the workstation and 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.

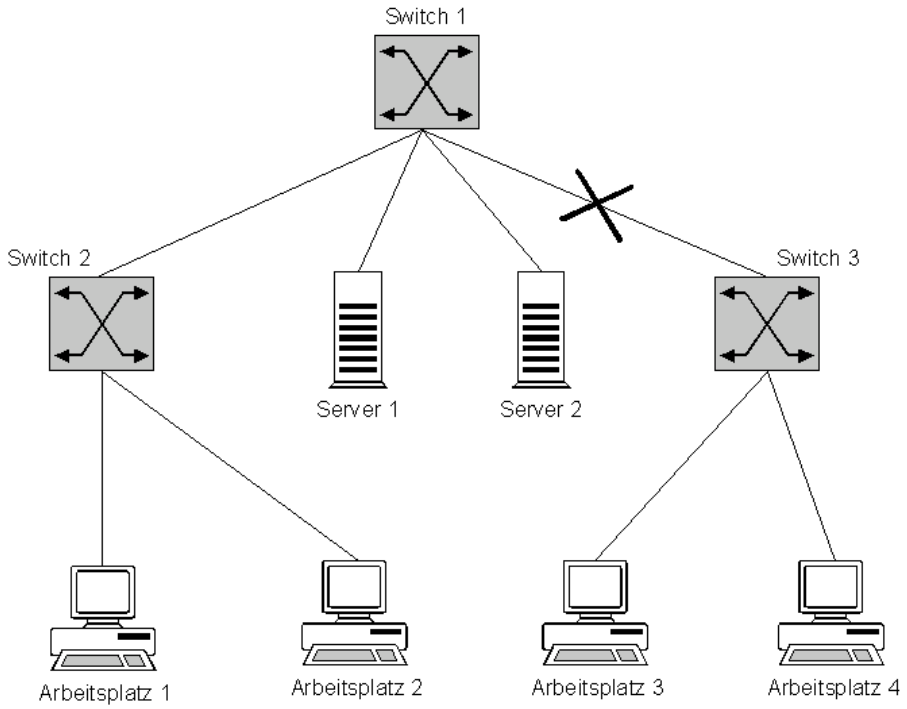
  Example: Failure of one of the redundant switches 1-1 or 1-2 as shown in the diagram below can restrict the available bandwidth for communications between the workstations and the server.



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. 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. The power supply units of components constitute a frequent source of errors, as all active network components 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. 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.


Switch 1
Switch 2
Switch 3
Server 1
Server 2
Arbeitsplatz 1
Arbeitsplatz 2
Arbeitsplatz 3
Arbeitsplatz 4

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 keys stored in volatile memory are deleted, so that the cryptomodule is no longer able to encrypt 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 encrypted, although the users rely on the cryptomodule to guarantee that the data is confidential.
- Encrypted data can no longer be decrypted until the required cryptomodule becomes available again. This can lead to problems in the availability of IT applications which process the decrypted data.
- If the cryptomodule ceases to work correctly but does not completely fail, data is encrypted 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 decrypt 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 keys see T 5.83).

Insecure cryptographic algorithms are characterised by the fact that a potential perpetrator with justifiable resources is able to break the cryptographic process. In the case of encoding algorithms, this means that it is possible to ascertain the original plain text from the encrypted text without any additional information. Here, you must take into account that relevant resources for the perpetrator include available computing power, 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 keys 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 key. 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 key 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 encryption, which is used frequently world-wide. This uses an effective key length of 56 bits. The so-called triple DES algorithm, carried out three times in a row with two keys, has an effective key 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 key length of less than 512 bits, potential insecurities are to be expected. For the next few years, a key 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 encryption algorithm there is, if the data to be encrypted 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 encrypted data

If data which is in an encrypted form is changed, it may no longer be possible to decrypt the data correctly. According to the mode of operation of the encryption routines, this can mean that only a few bytes are decrypted incorrectly or that all data following the error is decrypted incorrectly. If there is no data backup, this can cause the data to be lost entirely.

Errors in the encrypted data can occur in various ways:

- When the encrypted 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 encrypted 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 key used for encryption.

An error in the cryptographic keys used can be even more serious. Even if a single bit of a cryptographic key is altered, the result is that all of the data encrypted with it can no longer be decrypted. If the cryptographic key has no data backup, this data is lost for good.

T 4.37 Lack of authenticity and confidentiality of e-mail

In many organisations, e-mail is taking the place of conventional communication by post. However, the fact that, in the absence of additional security precautions, "normal" e-mail offers no guarantees of the authenticity and confidentiality of messages is frequently overlooked.

Where e-mail is unencrypted, all the information can be read on every IT system over which the message passes on its way through the network. As the precise route that a message will take cannot normally be predicted and the underlying SMTP (*Simple Mail Transfer Protocol*) protocol does not offer any mechanisms for specifying one particular route, an e-mail can pass through a large number of systems.

Information that is not protected by digital signatures can be altered or deleted on any of the systems involved without the recipient being aware of this. Apart from alterations to the e-mail text or any file attachments, information such as sender and forwarding data or even the sender's address itself can also be altered (see also T 5.73 *Impersonation of a sender*).

It is therefore a mistake to view e-mails as the equivalent of classic letters received by post. A more apt comparison would be with postcards.

Examples

- An employee sent out e-mails containing work assignments to various colleagues, using the sender details for his boss's e-mail address.
- Virtually all of the huge quantity of spam e-mails that clog up e-mail inboxes on a daily basis carry a false sender address.
- Normally the local system time on the sender's computer is registered as the send date. However, as this often can be altered even by ordinary users, a particular date in an e-mail is no proof that the e-mail was really sent at that point in time.

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 physicallIt 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 design errors

When programs and protocols are planned, mistakes that affect security can be made in the design. 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 design errors include the open transmission of data on 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 other errors in the internet protocols which will be published in the future.

Another example of a design error is *DNS spoofing* (see also T 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 design 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 *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 or PDA

A mobile phone or a PDA 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 energy.
- The user has forgotten the access password or PIN so that he cannot use the device any more.
- Components such as the display, keypad or SIM card are faulty.

If a mobile phone or PDA is exposed to harmful environmental conditions, its functional performance can be impaired. Mobile phones and PDAs can sustain damage through exposure to excessively high or low temperatures, as well as to dust or moisture.

Examples:

- An employee embarking on an extended business trip took a mobile phone plus accessories from a mobile phone pool with him. While on the road it transpired that he had unfortunately packed the wrong battery charger. As he was unable to recharge the mobile phone he could not use it any more during the rest of his trip.
- The mobile phone or PDA is left in a parked car. 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 60°C behind the window glass. A similar problem exists in winter, in that the temperature in a parked car can drop to below freezing. Such extreme temperatures can result in damage to the battery or the display.
- During a business trip, a PDA stopped working because the spare batteries were inserted too late. However, when it was switched on again, many of the configuration settings had been lost as these were not automatically saved by the operating system. As a result, some applications such as e-mail and Internet access no longer functioned correctly.

T 4.43 Undocumented functions

Many application programs contain undocumented functions, i.e. functions which are not described in the documentation and which the users do not know about. For some operating systems and application programs there are now books which describe a large proportion of the functions which have come to light that had previously been undocumented and are generally more voluminous than the manuals that come with the products. Undocumented functions are not, however, confined merely to tools that have useful effects. As long as these functions are not out in the open the possibility that they could create problems cannot be excluded.

In particular this is a problem where the undocumented functions affect security mechanisms of the product, for example access control. Such functions often serve as "backdoors" during the development or distribution of application programs.

Examples:

- In a number of IT systems backdoors that were inserted and then forgotten about by the developers but were originally intended to facilitate maintenance have been found, which, however, also made it possible to obtain administrator rights with a trivial password.
- Many programs can (or even have to) be registered on line with the vendor. With some of these programs the act of online registration of software simultaneously permitted an insight into all the programs stored on the hard disk.

T 4.44 Failure of Novell eDirectory

Technical failure caused by hardware or software problems can result in the failure of an eDirectory system or of parts of it. The result could be that data held in the directory is temporarily no longer available, either to eDirectory users or to any network applications which access eDirectory. Exceptionally, loss of data can occur.

This can result in disruption of business processes, prevention of internal workflows and loss of productivity due to the diverse functions of eDirectory and strong integration into the organisation.

If there are functional replicas of failed parts of the systems, then access may still be possible, although, depending on the network topology, this may be at the expense of reduced performance.

T 4.45 Delayed access to archive information

Delays in the recovery of archived documents can disrupt or impede business processes involving querying of archives. The delays can have many different causes, for example,

- outdated archive server software
- poor choice of indexing and search criteria during the creation or search of archived data
- overloaded archive server or database server hardware
- delays on the network
- unbalanced ratio of storage media to drives

As regards the latter point, two cases should be distinguished:

One large medium

- If a drive with a single, high capacity storage medium is used for the archiving, response times can be very long as in each case only one user can access the archive at a time. All other queries have to be buffered and then processed in sequence.

Many small media

- A large number of small storage media is used and the ratio of drives to storage media is relatively low. This means that the data media have to be frequently changed during queries, resulting in longer response times. Moreover, the storage capacity of small storage media is exhausted more quickly (see T 4.20 *Data loss due to exhausted storage medium*).

Delays can occur in connection with the transfer of documents to the archive; acknowledgement of the archiving process may be delayed because of long transmission times on the LAN.

T 4.46 Poor synchronisation of index data during archiving

Indexing of the archive system ¿

Archiving entails the storage of very high data volumes. It must be possible at a later time to unambiguously access all the archived data at any time in a controlled manner and with an acceptable delay. This functionality is guaranteed by the archive system, which generates an index of the stored files for this purpose.

However, archive systems generally implement only simple file accesses. Often a higher-level document management system (DMS) that controls access to the archive and provides additional functionality, e.g. complex search requests, is used to make access user-friendlier.

... and of the document management system

The DMS generates the data referencing during archiving, controls data versions and, if required, creates a full text index, so that all the data archived on the storage medium can be uniquely identified at a later time.

There are thus two index databases (in the archive system and in the DMS) which have to be synchronised. If unilateral changes are made to the index data stored in the DMS or there are errors on the storage medium and these changes are not considered elsewhere in the system, it is possible for archived data to cease to be assigned to the references in the DMS.

T 4.47 Obsolescence of cryptomethods

The reliability of cryptosystems is directly linked to advances in the computing power of IT systems, the development of new algorithms and research in cryptanalysis. Increases in the capabilities of IT systems can have the effect of possibly compromising cryptoalgorithms and key lengths hitherto regarded as secure in the future.

This creates a danger that, if cryptomethods or key lengths were to be compromised, then

- encrypted data could be decrypted by a unauthorised persons;
- documents could be given a technically valid signature by unauthorised persons, so that
- it would then no longer be possible to differentiate between authentic, signed documents and forgeries.

Example

DES with 40-bit keys

Hospitals have to keep their patients' files securely for a long period after the completion of treatment. Accordingly, one German hospital began encrypting its electronically stored patient data in 1980. The procedure used for this purpose was based on DES, with 40-bit keys. As no one in the hospital knew anything about encryption, this method was still being used in 2001 although by then programs were already available on the internet enabling data encrypted by that method to be cracked. This only came to light during a data privacy protection compliance check.

T 4.48 Failure of an outsourcing service provider's systems

The outsourcing service provider's IT systems could fail partially or wholly, with obvious effects on the customer.

Even if the IT failure only affects a few systems or applications, this can mean that data processing is inconsistent or faulty.

Lack of multi-customer capability

It should also be borne in mind that if the IT systems of the service provider are inadequately structured or isolated, the failure of one system, which has nothing to do with the customer, could nevertheless have a negative impact on the customer's IT operations. This can be a problem if individual IT components (e.g. host computer, firewalls) are simultaneously used for more than one customer of the service provider's. An error in the data resources of any customer of the outsourcing service provider's can mean, for example, that batch processing has to be suspended for several customers if host processing is poorly or incorrectly configured.

Similar problems can occur if the connection between the outsourcing organisation and the outsourcing service provider fails.

T 4.49 Insecure default settings on routers and switches

Active network components are supplied by manufacturers with insecure default configurations that jeopardise secure use. Also in some devices, the system commands for displaying a configuration do not display all parameters.

The following aspects are often a problem:

Operating system

Active network components are often supplied with an out-of-date version of the operating system.

Host name

Factory set host names often give away the manufacturer of the devices.

Services

Devices are supplied from the factory with standard configurations in which a large number of services are activated. For example, these could be HTTP, Telnet, FINGER or other services.

User accounts and passwords

User accounts setup in the factory have documented and therefore generally known standard names and passwords. There exist web sites with lists of manufacturer-specific standard accounts and passwords available for download.

Insecure versions of SNMP

With SNMPv1 and SNMPv2 authentication is performed using only an unencrypted, so-called, community string. In the standard settings from almost all manufacturers the read community string is set to the value "public", while the write community string is set to the value "private". If the insecure versions of SNMP are used and a dedicated network has not been setup for administration, an attacker can easily take control of network components if these default settings are not changed.

Routing protocols

Routing protocols are activated as standard on routers and switches from various manufacturers.

Login banners

Login banners on various devices as configured in the factory often give away the model and version number of the device. This data can be used for the specific selection of known exploits and in this way make it easier for attackers to carry out attacks.

T 4.50 z/OS operating system overload

Even if a z/OS operating system is managed using the *workload manager* such that an overload should not actually occur, there exists a series of threats that could lead to an overload. An overload must not necessarily lead to a complete system halt. It is also possible for various system resources to be simply no longer available, even though the system itself is still responding. The following situations are typical, but not the only threats of this type.

***Spool full* situation**

The spool file in a *Job Entry Subsystem* (JESx) is only intended to be used for a certain volume of output data. It may occur that, e. g., unlimited data are written to the spool file in the JESx due to a program loop. This action can lead to a *spool full* situation, new batch jobs can no longer be started. Only the online processes actually running will remain, in some circumstances, active, provided no output files are written to the spool file. As many JES commands require a useable spool file for execution, this situation may mean that extensive (and time-consuming) recovery measures are necessary to rectify the problem.

Complete system halt

Unix processes in the USS subsystem (*Unix System Services*) are mapped to address spaces in z/OS. If sufficient memory is no longer available, these address spaces must be swapped to page disks using the *Auxiliary Storage Manager* (ASM). If these are also insufficient, it is no longer possible to add any address space.

If the number of Unix processes in the USS is not limited and there is insufficient space on the page disks, security problems can result from the starting too many Unix processes. The cause, for instance, can be a recursive function that incessantly starts new Unix processes. As a consequence the system may practically come to a halt.

z/OS (with 64 bit addressing) is considerably less affected by this problem compared to its predecessor, OS/390 (with 31 bit addressing), due to the increased addressing available. As a result of the increased addressing available, more memory can be provided to the z/OS system. This factor has the consequence that the page disks are required much later.

In general, commands or program routines that continuously start new processes can rapidly overload the system. In the end this situation can make an IPL (*Initial Program Load*) necessary.

System overload due to an excessive number of JESx initiators

The administrator controls the batch processing and its priorities based on the number of *initiators* started. If too few *initiators* are started, queues can be produced during batch processing. If too many *initiators* are started, resources may be overloaded. If too many batch jobs are started, there is a risk that the *page datasets* will be insufficient. This situation would require manual intervention by the operators in the system configuration.

If the *job entry subsystem* has been defined with a very large number of *initiators* that, however, are not activated immediately, it may occur that on

the entry of the JES2 commando *$SI* (instead of e. g. *$SI1-10*), all possible *initiators* are started. As a result more batch jobs than planned may run in certain circumstances. Although as a rule this situation will not lead to a system halt, response times may become significantly longer.

Delayed tape processing

If more tape units are requested simultaneously than there are stations present, the backup of the data to tape will be delayed. The backup jobs enter the *wait* status and wait for free tape stations.

Examples

- Too many *initiators* were started in a z/OS installation. This situation had the consequence that during the batch processing, too many batch jobs were activated simultaneously, resulting in a very heavy load on the system's CPU. Although the system was able to withstand the load, the situation led to long response times for the *Time Sharing Option* (TSO). **Too many batch jobs**
- In the USS basic definitions for a z/OS operating system, the values for *MAXPROCSYS* and *MAXFILEPROC* were set to very high figures. As a member of staff tried out in the *Unix System Services* a recursive function call that he had learnt about during a Unix training course, the system came to a halt after a short time due to an *auxiliary storage shortage*. **Excessively large USS basic definitions**

T 4.51 Inadequate security mechanisms on PDAs

An IT system that is employed for portable use can be connected to a LAN via a VPN such that the communication link is very well protected. However, in the case that this IT system itself is inadequately protected against unauthorised access, there is a risk that an authorised person may misuse this system as a "gateway" to access the internal network.

Typical terminal devices for portable use are mobile telephones or PDAs on which, in the majority of cases, it is not possible to distinguish between users. As a result, anybody who has access to the IT system can access all data and programs, and also internal data belonging to the organisation or very personal data belonging to the owner.

Other, unfortunately very typical weak spots on portable components such as PDAs are:

- Inadequate access protection and authentication mechanisms
- No facility or an inadequate facility for encrypting data
- Insecure synchronisation
- No logging facilities or inadequate logging facilities

A large number of different PDA models with a very wide range of operating systems are available. The security features on the different PDA platforms vary, secure protection against tampering is, however, not provided by any of the common commercial systems.

Example:

With Palm OS 3.5.2 and all previous versions, using a combination of keys it is possible to change to either the so-called "Console Mode" or the "Debug Mode". Both modes provide direct access to system data bypassing all security mechanisms. Here it is irrelevant whether the PDA access is protected using a password or not: both modes can be activated by circumventing the access protection.

T 4.52 Loss of data when using a portable device

A portable terminal device is subject to considerably more risks that could lead to the loss of data than a stationary device. The loss of data can result from theft or the loss of the device, and also from technical problems or simply the lack of power.

Examples:

- The brand-new PDA falls out of the shirt pocket and breaks into pieces on the tiles, a handheld is carried by the dog instead of the newspaper, unfortunately with consequences. Transport damage in particular often results in the loss of data and device or component failures. Dust, dirt, moisture and dropping, in short "improper treatment", are the causes of irreparable damage to many portable terminal devices.
- The data may not be available temporarily because the battery is flat, as it was forgotten to put it on charge. However, the data may be lost completely if the backup battery is also flat and all data that have not been synchronised are lost.
- Data can also be lost on synchronisation. In general, prior to a synchronisation, it must be defined how conflicts arising during the data comparison are to be handled: whether for files with the same name, for example, the files from the portable device or the stationary terminal device are to be used without prompting, or whether a prompt is to be displayed. This action is often configured once when using the docking station for the first time and is then conveniently forgotten. If data are then changed in a sequence different to that originally intended, important data can be lost very quickly. This situation can occur as an unpleasant side effect, if for example several users synchronise their PDAs using the same terminal device without giving consideration to the fact that files with the same name may be overwritten.

Failure to keep up-to-date

Portable systems are naturally not always online. For this reason the data saved on them are not always up-to-date. This affects both calendar entries and also general information, however, it can also have security-related effects in certain circumstances. During the time in which there is no link to the organisation’s IT systems and information sources, it is also not possible to obtain information on current security problems, the virus scanner is not updated, etc.

T 5 Threats Catalogue Deliberate Acts

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	Web spoofing
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 phones
T 5.100	Abuse of active contents on access to Lotus Notes
T 5.101	Hacking Lotus Notes
T 5.102	Sabotage
T 5.103	Misuse of webmail
T 5.104	Espionage
T 5.105	Disruption of archive system services
T 5.106	Unauthorised overwriting or deletion of archival media
T 5.107	Disclosure of data to third parties by the outsourcing service provider
T 5.108	Exploitation of system-specific vulnerabilities in IIS
T 5.109	Exploitation of system-specific vulnerabilities with Apache web server
T 5.110	Web bugs
T 5.111	Misuse of active content in e-mails
T 5.112	Manipulation of ARP tables
T 5.113	MAC spoofing
T 5.114	Misuse of spanning tree
T 5.115	Overcoming the boundaries between VLANs
T 5.116	Tampering with the z/OS system configuration
T 5.117	Covering up tampering in z/OS
T 5.118	Obtaining high level rights in the RACF by unauthorised means
T 5.119	Use of other IDs in z/OS systems
T 5.120	Tampering with the Linux/zSeries system configuration
T 5.121	Attacks on z/OS systems using TCP/IP
T 5.122	Misuse of RACF attributes in z/OS
T 5.123	Bugging of indoor conversations using portable terminal devices
T 5.124	Misuse of information on portable terminal devices

T 5.125 Unauthorised transfer of data using portable terminal devices

T 5.126 Unauthorised photography and filming with portable terminal devices

T 5.1 Manipulation or destruction of IT equipment or accessories

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.

Various motives

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 input, changes to access rights, modification of accounting data or 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.

Various motives

Data or software can be manipulated out of revenge, to intentionally create some damage, for personal gain or for financial reasons.

Examples:

- In 1993, the application software for certain financial services in a Swiss financial institution was tampered with 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.
- Archived documents are usually particularly in need of protection. Manipulation of such documents is especially serious as it may be noticed only years later, by which time it may no longer be possible to investigate properly.
- In z/OS systems, the *System Management Facility* (*SMF* records) allows many security-critical user activities to be logged. If an unauthorised person can succeed in tampering with the SMF records, then he will be able to conceal unauthorised actions in the system.

Mainframe: covering up through SMF manipulation

T 5.3 Unauthorised entry into a building

A number of threats to IT systems, e.g. theft or tampering, are preceded by unauthorised entry into a building. Hence countermeasures directed at preventing break-ins are also effective against threats which depend on a prior successful break-in. In the case of professional criminals, the amount of time that the perpetrator has to pursue his objectives undisturbed is critical. The objective of a break-in could be the theft of IT components or other items that are easy to dispose of, but equally the intruder might be seeking to copy or tamper with data or IT systems. Tampering that it is not obvious can be far more harmful than direct acts of destruction.

Damage to property can occur simply as the direct consequence of unauthorised entry, as windows and doors are opened by force and damaged, so that they have to be repaired or replaced.

Examples:

- During a nocturnal break-in into an office building, the burglars could not find anything valuable to steal. Out of frustration they emptied the dry powder fire extinguishers in the office areas. The losses resulting from the break-in were trivial, but the damage due to vandalism was disproportionately high due to the costs of cleaning and the disruption to work. **Vandalism**
- During a break-in into a company over a weekend trivial damage was caused by forcing open the window and only a coffee cash box and some small items of equipment were stolen. However, it was later established during a routine check that a central server had been cleverly manipulated at precisely the time of the break-in. **Tampering**

T 5.4 Theft

Theft of IT equipment, accessories, software or data results not only in the expense of having to replace the equipment or to restore it to working order, but also in losses resulting from lack of availability. Loss of confidentiality and the results of this can also be damaging.

As well as expensive IT systems, mobile IT systems which are easy to transport inconspicuously are often targeted for theft.

Examples:

- During the spring of 2000 a Notebook disappeared from the US State Department. In an official statement the possibility that the device contained confidential information could not be excluded. Nor was it known whether the machine was protected against unauthorised access by encryption or other means. A warning had already been issued during security investigations about inadequate security checks.
- In a German government office several break-ins occurred through the same unprotected windows. In addition to other valuables some mobile IT systems disappeared. It was not possible to determine whether any documents had been copied or tampered with.

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

The technical possibilities for perpetrating an attack are varied: throwing bricks, causing an explosion with explosives, the use of firearms, arson etc. 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 the functions performed by the IT operator and 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 are at greater risk than those in remote places. When assessing the risk of politically motivated attacks, advice can be obtained from the State Office of Criminal Investigation or from the Federal Office of Criminal Investigation.

Many documents in a small amount of space

Where electronic archives are used, it is particularly important to bear in mind that a large number of documents are stored in relatively little space. This could include sickness data, contracts, certificates, and wills belonging to private persons, and documents and contracts belonging to companies, public agencies and other government offices. Their destruction could have far-reaching consequences, not just for the organisation where they are stored but also for a number of other users. Attacks on electronic archives can therefore cause considerable damage.

Examples

- During the 1980s, a bomb attack was committed against the computer centre of a large federal authority in Cologne.
- Almost every year, a tax office in the Rhine region was paralysed for several hours on account of bomb threats.
- In the late 1980s, there were reports of an attempted attack by the RAF terrorist group on the computer centre of a major German bank.

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 tap a line essentially depends on whether the information this could yield is worth the technical (financial) expenditure and the risk of detection. This question can only be answered by knowing what capabilities the attacker has and what his particular interests are. It is therefore impossible to know for sure what information, and therefore which lines, could be targets for interception.

It may take very little effort to intercept lines. On some kinds of LAN cabling, access to a LAN socket may be sufficient to eavesdrop all the network traffic on the local network. It is even easier to intercept network traffic on wireless networks (wireless LAN / radio LAN, IEEE 802.11). Moreover, the risk of discovery associated with the interception of wireless networks is virtually nil.

Automatic analysis of connections with plaintext protocols

The transmission of authentication data using plaintext protocols like HTTP, ftp or telnet, is especially critical, as in these cases it is easy to determine the position in the transmitted packet of the data entered by the user, thanks to the simple structure of the protocols (see also T 2.98 *Insecure protocols in public networks*). It is thus a relatively simple matter to perform an automatic analysis of such connections.

In a first step, password sniffer programs can be used to collect passwords during transmission to a system. This enables the aggressor to gain access to this IT system with a view to then carrying out further attacks locally on the computer.

Examples

- It is thus wrong to assume that messages sent by e-mail are the equivalent of letters in the classical sense. As e-mail messages can be read throughout their journey through the internet, a more appropriate comparison is with 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 virtually impossible. Even on IT systems that have identification and authentication functions in the form of user IDs and password verification, there is a risk of unauthorised use, if passwords and user IDs are obtained illicitly.

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 guessed by trial and error.

However, a much more efficient approach is to take a meaningful word as a password and try out all the user entries. 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 UNIX operating system concerned so as 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 Abuse of remote maintenance ports

Where remote maintenance ports are insufficiently protected, it is conceivable that hackers could gain access to the administration port of the IT system. In this way, having cracked the system password, they might be able to perform **all** administration tasks. The resulting damage could range from a complete system failure, a very serious disruption of service/operation continuity, loss of confidentiality of all data stored in the system, to a considerable direct financial loss.

Example

RSF function on z/OS systems

On z/OS systems, normally the *Remote Support Facility (RSF)* is used to notify the vendor of system errors. RSF can also be used by the vendor to implement patches to the microcode. Misuse of the RSF access of z/OS systems therefore constitutes a considerable threat.

Again, it is now common for manufacturers of hard disks for z/OS systems to solve problems via remote maintenance access.

T 5.11 Loss of confidentiality of data stored in 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 be used 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

Modern telecommunications systems generally feature numerous facilities to provide users with maximum convenience in their communications and to allow the system to be optimally adapted to its working environment.

Some of these facilities may, however, be misused by "inquisitive" staff members. Employees could, for example, try to

- divert calls intended for colleagues to their own telephone without permission;
- accept calls intended for others without permission;
- read other users' call and last-number re-dial memory without permission;
- tap telephone calls without permission.

There is a danger, therefore, that "inquisitive" employees may obtain information - perhaps even confidential information - that is not intended for them.

Example:

With the "Call pickup" function, a user could divert a call which is arriving at a colleague's phone but has not been answered yet to themselves. An employee of a company used the "Call pickup" function to take calls for an absent colleague. Apparently to save time, he answered these calls with only a brief "Hello?" without revealing his identity. Some of the callers therefore wrongly assumed that they were speaking to the person they had actually called and therefore talked about confidential matters. This allowed the nosy employee to obtain an insight into official projects and private affairs of his colleague.

T 5.16 Threat posed by internal staff during maintenance or administration work

Internal staff might during maintenance or administration work try to modify privileges (e.g. international dialling authorisation) or to activate user facilities, either to their own advantage, or as a favour for colleagues. As a result, system crashes could be caused through ignorance or other security loopholes could be opened up through configuration errors. Also, improper handling of hardware components could result in their destruction. In addition, maintenance staff may have full or restricted access to the stored data (read and write) and could pass this on without authorisation or tamper with it.

Manual control or temporary disabling of control technology or alarm systems could pose a serious threat as well. This also affects alarm and control systems.

Examples:

- A person employed temporarily to block accounts that were no longer used exploited his extensive permissions to download copyright-protected software from the central applications server for his own private purposes. In order to at the same time be able to distribute the program to his friends, he used the office CD-ROM writer and data media.
- To enable a colleague to carry out her private home banking transactions during office hours, as a favour she is given exclusive access to her Internet provider via ISDN as a favour. When she downloads a screen saver from the Internet at Easter, she infects her PC with a virus. As the computer is connected to the internal network, the virus rapidly spreads. The corporate network is out of action for several hours while the problem is sorted out.
- Intruder detection devices often have an integrated log printer. It is a common occurrence for the intruder detection device to be switched off in order to replace the necessary paper roll. When the machine is next turned on there is a danger that the system will not start up correctly so that it malfunctions as a result.

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 discovered by systematic trial-and-error. A distinction should be made here between simply trying out all possible character combinations up to a certain length (known as a *brute force attack*) and trying out successively every entry on a list of character combinations (a *dictionary attack*). The two approaches can also be combined.

Most operating systems have a file or a database (e.g. *passwd* file or *shadow* file under UNIX or RACF database under z/OS) that contains the IDs and passwords of the users. However, in many operating systems, rather than being stored in plaintext, at least the passwords are encrypted. If the file is inadequately protected against unauthorised access, it may be possible for an attacker to copy this file and perpetrate a brute force attack, using a powerful computer and without any restrictions as regards access time.

The time it takes to discover a password in a brute force attack depends on

- the time it takes to perform a password check
- the length of the password and
- the character composition of the password (e.g. letters and numbers).

The time it takes to check a password depends heavily on the relevant system and its processing and transmission speed. In the case of an attack, the method and technology of the aggressor are also relevant.

On the other hand, the length and character composition of the password will be influenced by organisational stipulations or even by technical safeguards.

Example

With a well equipped PC, currently around 400,000 password checks can be carried out per second using the standard password encryption function of UNIX or Linux. When the standard password encryption of Windows NT/2000/XP is used, this rises to a staggering 6 million checks per second (source: the Hamburg Data Protection Officer, 2003).

Assuming a character set of 26 characters, it would thus take around six days to work out an 8-character password under UNIX or Linux (standard password encryption). The same task could be completed in a mere nine hours under Windows.

T 5.19 Abuse of user rights

Misuse of user rights entails the deliberate exploitation of opportunities acquired either rightfully or illicitly to harm a system or its users.

Often, for systems engineering reasons users have higher-level or more extensive permissions than they actually need for their work. These permissions can be used to gather data illicitly, even if procedural instructions prohibit access.

Example

- On many UNIX systems, it is possible for any user to read the */etc/passwd* file and so gain access to 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 the granting of group privileges is overly generous, especially in the case of system groups such as *root*, *bin*, *adm*, *news* or *daemon*, it is easy to abuse these privileges, e.g. to modify or delete third parties files
- A Storage Administrator responsible for managing the hard disks in z/OS systems was able to view customer files by virtue of the attribute *Operations* which he had been assigned by the RACF Administrator to carry out his work. He used his access privileges to make unauthorised copies.

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

User programs, command tables and script languages

A Trojan horse, sometimes only called Trojan, is a program with a hidden, undocumented function or effect. The user therefore has no influence over the execution of this function, making its effect similar to that of a computer virus. However, unlike computer viruses, Trojan horses are not self-propagating. Any application program can serve as carrier for a Trojan horse. But script languages, like batch files, ANSI control sequences, *REXX Execs* and *ISPF Command Tables* in z/OS operating systems, PostScript etc., which are interpreted by the operating system or 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 could contain a Trojan horse which sends the users username and password to an aggressor over the network and then passes it to the actual log-in program. Such Trojan horses have appeared recently on several online services such as AOL or T-Online.

- **Screen savers**

  Screen savers, especially ones which have been downloaded from the internet, could contain a concealed function by means of which passwords entered by the user presently logged on are logged and sent to an aggressor.

- **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 could use the remote maintenance function of Back Orifice to gain access to the users 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 system programs like *ps*, *who*, *netstat* etc. to keep *backdoors* open for prolonged periods, allowing penetration of the system to go unnoticed, with all traces of the attack 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, by listing the contents of a directory, a superuser could unintentionally execute a modified "*ls*" program with root rights contained in it.

- **Implanting of program code**

  One possibility of obtaining high-level permissions in the z/OS operating system by devious means is where the attacker has *Update* access to files that either run during the logon process (e.g. a *REXX EXEC*) or are generally used during processing (e.g. *ISPF Command Tables*). The attacker can then replace the existing code with suitable code fragments.

T 5.22 Theft where an IT system is used from a mobile platform

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 around in cars or on public transport, set down in other peoples 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. A laptop locked up in a car boot could be stolen even though the original intention was to steal something else; if the car is stolen, the laptop too will fall into the wrong hands.

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.

T 5.23 Computer viruses

A computer virus is a *program with a damaging function*. The most serious damage that can be caused as a result is the loss or corruption of data or other programs. Such program functions can be triggered intentionally as well as accidentally.

The definition of a computer virus does not refer directly to the possibility that a damaging function has been programmed:

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 could also be programmed with damaging functions.)

As in the case of its biological equivalent, it is the property of reproduction that lends it is the name "virus". The manipulation possibilities are numerous. Overwriting or attachment of the virus code to other programs and sectors of the operating system are particularly frequent.

In principle, computer viruses can occur on all operating systems. However, the greatest threat is posed in the area of IBM-compatible personal computers (PCs). Around 20,000 viruses (including their variants) are currently known to exist world-wide on the operating systems most commonly used (MS-DOS, PC-DOS, DR DOS, NOVELL DOS etc.).

In practice, computer viruses directed at the Windows 3.x, Windows NT, Windows 95, OS/2 and UNIX operating systems are of little significance. 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 allows for booting from the floppy disk drives.

Around 100 computer viruses specific to Apple computers are known to exist. Corresponding virus scanning programs are also available for these.

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 camouflage mechanisms by means of which viruses are often protected against detection by users and scanning programs.

Boot viruses

"Booting" is the term used for 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 that 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 following execution of the

virus code during the start-up of the computer. This causes the computer to apparently start up in the normal way, but the boot virus is loaded into the computers main memory even before the operating system is loaded, and stays there the whole time that the computer is running. Consequently, the virus is able to infect the boot sector of every write-enabled floppy disk used while the computer is running. Boot viruses can only infect other computers during bootup 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, *multi-partite viruses* have gained in importance. 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 application programs under which not only single control characters, but also programs and other objects can be embedded in the files generated are affected. Microsoft Word and Excel files are especially 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 (see also T 5.43 *Macro viruses*).

Macros are programs with whose help the application program can be expanded with additional functions which have been tailored to the application (e.g. production of a fair copy from the draft of a text). These macros only run when the document is processed within the relevant application program (Word for Windows, Excel etc.), the macro being activated either by the user or else automatically. If, for example, a Word file is received over a web browser which automatically opens the document with Microsoft Word, a macro contained in the document 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 viruses and file viruses.

Examples of damaging 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 up to 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 the date reaches the year 2000. One of its effects is to alter the computers BIOS settings so that it no longer boots up correctly.

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 users 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 sender field or I/O address

Masquerading entails the assumption of a false identity by an aggressor. Thus, for example, he can obtain a false identity by spying out the user ID and password (see also T 5.9 *Unauthorised use of IT systems*) or by tampering with the sender field of a message or an address in the network (e.g. see T 5.58 *IP Spoofing* or T 5.87 *Web spoofing)*. Other ways of obtaining a false identity are to manipulate the call number display (Calling Line Identification Presentation) on an ISDN line or the originator ID of a fax originator (CSID - Call Subscriber ID).

Auser who believes he is communicating with a different person can be easily induced to disclose sensitive information.

Linking up to 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 carried out by the original communication participants. (On this point, see also T 5.89 *Hijacking of network connections.*)

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

A denial-of-service attack is intended to prevent IT users from using functions or devices that are normally available to them. This attack often takes place in conjunction with distributed resources, with the attacker using these resources to such a degree that other users are prevented from carrying out their work. For example, a shortage of the following resources can be artificially induced: processes, CPU time, disk space, inodes, directories.

This can be caused, for example, by:

- starting large number of programs simultaneously;
- simultaneously starting up many programs which use a lot of CPU time
- occupying all the free inodes within a UNIX system so that no new files can be created;
- uncoordinated usage of tape units in z/OS systems, such that applications have to wait for free tape units and online processing is restricted;

Blocking of tape units in the z/OS system

- deliberate entry of incorrect passwords (also using scripts) with the objective of blocking all IDs on a z/OS system;

DoS attacks on z/OS IDs

- 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 back on network connections.

T 5.29 Unauthorised copying of data media

When data media are replaced or moved, this can mean that the information to be transferred is transported from a secure environment via insecure channels to a possibly insecure environment at the receiving end. In such cases, unauthorised persons could copy this information more easily than in the original environment.

Due to the large concentration of information requiring protection on data media that is typically found in electronic archives (e.g. personal or company confidential data), these are a particularly attractive target for theft or copying by unauthorised persons.

Example

Confidential engineering results are to be transported from a development laboratory in town X to a production site in town Y. If the data media are mailed without any supervision or control, the possibility cannot be excluded that the information on them could be copied illegally and perhaps sold to a competitor, without detection of this disclosure 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 servers

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 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**

  Einige Geräte gestatten es, aus der Ferne über den Anrufbeantworter elektrische Geräte zu steuern (Ein- und Ausschalten).Some answering machines allow electrical equipment to be turned on and off remotely. Je nach Funktion und Bedeutung der angeschlossenen Geräte kann dies beliebig hohen Schaden nach sich ziehen.The damage arising from misuse of this feature depends on the function and significance of the connected equipment.

- **Turning off the answering machine**

  Einige Geräte können ferngesteuert abgeschaltet werden, so dass die Funktion des Anrufbeantworters nicht mehr zur Verfügung steht.Some answering machines can be turned off remotely so that their functions are no longer available.

T 5.39 Infiltration of computer systems via communication cards

A communications card (e.g. an ISDN card, an internal modem or 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 undetected.

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 a local terminal. This allows third parties with access to this computer to try out user IDs and passwords. The case where a user is not automatically logged off from the remote system if the connection is disrupted is even more dangerous. The next caller could then work with the same user ID, without any need to log on to the system. In this way he would gain full access to the IT system without identifying himself or being authenticated.

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 anyone with access rights to the relevant device files (e.g. */dev/audio* for UNIX, a Registry under Windows NT). Failure to exercise due caution over the granting of such access rights could result in persons other than the intended users gaining access and hence being able to misuse the microphone for eavesdropping purposes.

Example:

In March 2001 a television business programme showed how it is possible to bug a room using the microphone on a laptop that is connected to an ISDN telephone line. This was demonstrated using a laptop of a German politician. First of all she was sent a faked virus warning by e-mail, telling her to open a protection program enclosed as an attachment. But this program contained a Trojan horse which later established a connection to the outside over the ISDN line and transmitted the telephone number.

It was then possible for the computer to be telephoned from outside without the user having any visual or auditory information that this was going on. The microphone installed on the laptop was then activated over the open connection and the sounds in the room were transmitted to the outside.

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.

Where remote maintenance ports are insufficiently protected, it is conceivable that hackers may get access to the management program of the PBX system. Consequently, once they have mastered the system password they would, if necessary, be able to perform **all** administration tasks. The resulting damage could range from a complete system failure, a very serious disruption of service/operation continuity, a loss of the confidentiality of all data stored in the system, to a considerable direct financial loss, e.g. 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 and Windows 95. 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.

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 attack under which incorrect IP numbers are used to disguise ones true identity to the IP system being attacked.

With many protocols of the TCP/IP family, authentication of the IT systems communicating with each is effected exclusively via the IP address, but this is easy to falsify. If one also exploits the fact that the sequence numbers used by computers for synchronisation purposes when establishing a TCP/IP connection are easy to guess, it is possible to send packets using any sender address, so that any appropriately configured services such as *rlogin* can be used. In this case, however, an attacker may have to accept that he will not received any response packet from the computer that is being misused.

Other 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 control for TCP/IP networked systems. Unfortunately, the addresses used in Layer 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 LANs 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 response packet back with its hardware address. As the ARP response 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 way of perpetrating an attack. In an IP packet, it is possible to prescribe the route by which the packet should be transported to its target, or the route that the response packets should take. The route specification may, however, be manipulated during transmission so that instead of the secure routes provided for through the routing entries (e.g. via the firewall), other uncontrolled routes are used.

T 5.50 Abuse of the ICMP protocol

As a protocol of the transport level, the function of the Internet Control Message Protocol (ICMP) is to transport error and diagnostic information. Through the abuse of ICMP messages, it is possible for an attacker not only to disrupt network operations but also to obtain information about the internal network that will assist him in planning an attack.

- ICMP *Redirect* messages can be used to tamper with the routing tables of computers.
- ICMP *Unreachable* messages can be used to disrupt existing connections or to completely suspend them.
- It is relatively easy to use the various ICMP *Request* message types (*Echo Request, Information Request, Timestamp Request, Address Mask Request*) to draw up a map of the internal network of an organisation (*ICMP sweeps*).
- Again, fake ICMP *Reply* messages can be used to obtain information about the internal network by inducing the destination computers to reply to these messages with an error message.
- Different operating systems differ as to the way in which they respond to certain ICMP messages. In addition to information that a particular address is active, ICMP responses can thus also betray the operating system under which the computer concerned is running (*fingerprinting*).
- Defective implementations of ICMP in some operating systems have led to security problems in the past:
  - Computers that ran under Windows 95 could be induced to crash by certain ICMP echo packets ("Ping of Death").
  - It was possible for excerpts from the working memory of the computer concerned to be contained in ICMP response packets of various operating systems. In the extreme case it was possible in this way for passwords or cryptographic keys to be passed to an external computer.
- Every type of ICMP message can also be used to create a covert information channel, on which data from the internal network can be transported to the outside.

T 5.51 Abuse of routing protocols

Routing protocols such as RIP (Routing Information Protocol) or OSPF (Open Shortest Path First) are used to pass on changes to routes between two networked systems to the systems concerned, thereby making dynamic changes to the routing tables possible. It is very easy 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 attacker can exploit this to change the transmission route in a particular way.

T 5.52 Misuse of Administrator Rights in Windows NT/2000 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:

Assuming ownership of files

By improper use of the right to assume ownership of any files, under Windows NT/2000 an administrator 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 detected 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/2000 no function is available to reverse this. Nevertheless, the administrator can gain access to user files without being noticed, for example, by having his name registered in the group of backup operators and then making a backup of the files he wishes to read.

Fälschung von Protokolldaten

There are a number of opportunities for exploiting Administrator privileges 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 log details through alteration of the system time, or through detailed tracking of the activities of individual users.

Booting of outside media

Depending on the underlying hardware, if 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 tampered with if the computer can be booted up using 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. 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 plain text with the help of network analysis tools or so-called sniffers. It must be taken into account that these sniffers are not always to be considered as "hacking software" since many products which serve as network-managers contain such a function.

Trace functions in the z/OS operating system

Trace functions in z/OS

So-called trace functions are available to the operator in z/OS. With the aid of the *Generalized Trace Facility (GTF)*, among other features terminal sessions can be monitored in SNA or TCP/IP networks. If the trace function is applied to the RACF administrator's session, in certain circumstances it may be possible to determine his password if the contents of the session are not encrypted. A similar trace function is included in the *Network Logical Data Manager* component (*NLDM)* in the product *NetView*.

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 on the Novell Netware Server.

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 the Novell Netware network 3.x

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, the 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 link cannot be prevented with available cable designs, which differ solely as regards 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
- the replaying 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 give the name of a false sender when sending an e-mail since, when SMTP-based e-mails are forwarded, generally no checks are carried out as to where a message comes from, only where it is to go to. Furthermore, many e-mail clients allow any sender data to be entered. This could be damaging if the recipient believes the information contained in the e-mail as authentic and binding.

Examples

- Most of the countless span e-mails which clog up users' mailboxes every day carry a false sender name.
- Some of the many e-mail worms that have been wreaking havoc on the internet for some years use an address from the e-mail address book of the user whose e-mail program they have just attacked as the sender address. Thus the next victims to receive an e-mail containing the worm find a familiar sender address on the e-mail and are thus more likely to open the e-mail or even the infected attachment.
- With many e-mail programs that are widely used, it is easy to forward an e-mail with false sender details to the e-mail server without any password check. If user authentication has not been performed on an e-mail, it is identified as "Unverified" in the "X-Sender" field. However, experience suggests that very few recipients pay attention to this. Besides, most mail programs do not include this field in their standard display 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 plaintext

E-mails are normally transmitted in plaintext. Data which has not been protected by cryptographic means can be read and modified on any IT system over which the message passes on its journey to the recipient. 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 loading and availability of gateways and network segments. In some cases, e-mail intended simply for transmission between two points in the same town 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 the e-mails that have been received. Depending on the configuration, it may contain not just e-mails which have not yet been read but 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 many cases copies of outgoing e-mails are also stored on the mail server. However, often the user mail program deposits these copies on the computer of the sender.

Examples

- A number of Microsoft internal e-mails were 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 customers by e-mail. If these e-mails are intercepted, an adversary could 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 on 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). Thus, the web 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 while processing the request.

The databases in which computer names are assigned the associated IP addresses and vice versa are located on name servers. Two databases are available for the 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 do not have to be mutually consistent! DNS spoofing is said to occur when an intruder becomes successful in faking 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 that *http://www.bsi.bund.de* was 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 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.

Examples

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 stored too. 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 intrusion 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/2000

Admin account cannot be locked

An Administrator account is created each time a Windows NT/2000 system is installed the standard way. This is true of both the Workstation and Server versions and also of domain controllers. Unlike user-configured accounts, this pre-defined Administrator account cannot be deleted or locked so as to prevent an administrator from being locked out intentionally or by mistake, which would make performance of administrative tasks impossible. One problem here is that the pre-defined Administrator account cannot be locked even if the maximum number of invalid passwords specified in the account policy before lockout is triggered is exceeded. This allows passwords to be tried out using cracking programs.

Admin password in plain text during tranfer

There are also other ways of obtaining a password assigned to an Administrator account so as to acquire Administrator privileges: if a computer is remotely administered under the Windows NT/2000 operating system, there is a danger that the logon password input during the authentication process could, depending on the authentication procedure used, be transmitted in plaintext, thus allowing an intruder to scan the password. Even if the system has been configured so that logon passwords are only transmitted in encrypted form, it is possible for intruders to record the encrypted password and decrypt it with the help of appropriate software. This applies especially to Windows NT, as the NTLM procedure is used here. Under Windows 2000 the default procedure used is Kerberos, which is more robust against such attacks.

Admin password on backup disk

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 repair disks or tape backups. An intruder who succeeds in gaining possession of this file could decode the necessary password with the help of appropriate software.

Malicious software

Finally, there is a special type of malicious code that 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 be a warning against computer viruses which can damage hardware or cause infections and damage when you just open an E-mail (not an attachment) and are not detected by any antivirus 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 is given for the sender, such as that of a well-known manufacturer.

A hoax is not a virus!

You should not confuse such a hoax with a computer virus which really can manipulate 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 keys, alter the keys 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 encrypts 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 encryption 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 keys, alter the keys 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.
- undocumented 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 keys,
- impairing the internal key 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 keys.

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 keys, 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 keys

When cryptographic procedures are used, the gain in security depends to a large extent on how confidential the secret cryptographic keys are. With knowledge of both the key and the cryptographic algorithm used, it is normally easy to revert the encryption and obtain plain text. A potential perpetrator will therefore attempt to ascertain the key used. Possible points of attack are:

- Unsuitable processes are used to produce the key, for example to determine random numbers or derive the key.
- The keys that are produced are exported before they are stored using a secure medium.
- During operation, keys from cryptomodules are exported through technical attacks .
- Keys left as backup are stolen.
- When cryptographic keys are entered, the keys observed by perpetrators.
- The cryptographic algorithms in use are broken. In the case of symmetric cryptographic techniques such as DES, for example, it is currently possible to determine the key using huge numbers of parallel computers (brute-force attack).
- Internal perpetrators give away cryptographic keys in use.

T 5.84 Forged certificates

The purpose of certificates is to link a public cryptographic key to a person. The link of a key 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 encrypted with the key 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 encrypted and sent with a key 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 key. 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 key which corresponds with the public key.
- Perpetrators produce a certificate and sign it with a key of their own. The forgery is only noticed if the certificate is checked 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 encrypted or compressed data records lose their integrity - and the alteration of just one bit is enough - they can no longer be decrypted or unpacked.
- The same applies to cryptographic keys, where the alteration of just one bit is enough to make the key useless. Likewise, this means that data can no longer be decrypted or checked for their authenticity.

Loss of integrity can occur in several ways:

- Information can be lost through the aging of data media.
- 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 on a Windows NT computer to query shared directories 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 T 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 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.

Unauthorised use of RAS access

- 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.

Passing on of passwords or token

- 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.

Unauthorised use in the private environment

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. 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 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.

T 5.100 Abuse of active contents on access to Lotus Notes

Often the implementation of functions within Lotus Notes databases entails the execution of active components following the occurrence of certain events (e.g. the input of data into a particular field). The active components here could be LotusScript or Java programs, for example, and are also known as agents. Execution of one agent can in turn trigger other agents (e.g. if an agent copies data to another database and this action triggers the execution of agents in the target database). Generally it is possible to distinguish between server-side and client-side execution of agents, but both variants are possible. In addition, when a database is accessed from the Web, the user interface may be implemented using active content (JavaScript, Java applets etc.) that is executed in the browser.

Incorrectly configured ECL

The Execution Control List (ECL) controls what active content can be executed in a Notes client and what authorisations are granted to active content. If the ECL is incorrectly configured, the active content could be used to attack the client. The same applies to the Web interface, for which no ECL exists but which is reliant on the security mechanisms of the browser.

If the ECL is incorrectly configured, it would be possible via active content, for example,

- for data held locally on the client computer (databases, files etc) to be accessed and data "stolen",
- for local data on the clients to be altered or deleted, and
- for harmful programs, for example computer viruses or Trojan horses, to be installed.

T 5.101 Hacking Lotus Notes

The data stored in the databases of the Notes server can also be made available for public access from the internet. This imposes special requirements on the security of the Notes server used for this purpose. In this case, security weaknesses could result in an adversary not only gaining unauthorised access to the Notes server itself but possibly also being able to penetrate the internal network which lies behind it.

Some of the problem areas and potential security weaknesses which need to be considered, particularly where public access is allowed from the internet to a Notes server, are listed below.

- The communication protocol of Lotus Notes is currently not published so that it is not possible to make any definitive statements about the security mechanisms. Even when appropriately configured, it must be assumed that there will be a residual risk.

Mechanisms not published

- A Notes server is complex system. A server network increases the complexity still further. This complexity (also the security-relevant settings) can result in mistakes being made during configuration and hence in the creation of security weaknesses.

High complexity

- With its wide functionality, it is possible for integration of a Notes server into appropriate background systems to permit the passing on of security weaknesses from a Notes server to the background systems. In such a case generally it is sufficient to exploit a single weakness in a single function package.

Effect on other systems

- There is no restriction as to the number of failed authentication attempts on the web interface. With the aid of browser clients, aggressors can thus attempt as many times as they like to log on to a Notes server with different usernames and passwords and in this way to gain unauthorised access.

Brute force attack

- Once web access to a Notes server is enabled, this affects *all* databases on that server. Unless secure access rights have been granted for every database, this can be easily exploited for deliberate attacks.

Direct database access

T 5.102 Sabotage

Sabotage refers to the malicious manipulation or damaging of objects with the aim of inflicting damage on the victim. Computer centres or communications links owned by an official body or company make particularly attractive targets, as a major effect can be achieved here with only slender means.

Selective manipulation

External aggressors and especially insiders can selectively manipulate the complex infrastructure of a computer centre through targeted attacks on important components, so as to induce equipment failures. Particularly at risk here are building-related or communications infrastructure that is inadequately protected and central supply points which are not monitored by organisational or technical means and are easy for outsiders to access unobserved.

Examples

Power supply

- In a large computer centre tampering with the UPS resulted in a temporary total failure. It was discovered that the perpetrator had several times manually switched the UPS to bypass and then tampered with the primary power supply to the building. The total failure - over a period of three years there were four blackout incidents - even resulted in hardware damage on two occasions. The outages lasted between 40 and 130 minutes.

Ingress of water

- A computer centre also contains wash facilities. By blocking the drains and simultaneously turning on the taps it is possible to induce water ingress into central technical components, resulting in damage that disrupts operation of the productive system.

Electronic archives

- Sabotage poses a special risk for electronic archives, as generally a lot of documents requiring protection are kept in a small amount of space. This means that it is possible is to cause extensive damage through selective tampering that requires little effort.

T 5.103 Misuse of webmail

Feigning a false identity

If user information is not sufficiently verified, attackers can obtain e-mail addresses containing another person's name and undermine that user's reputation by sending spam mail or obscene messages under that name. If a provider allows its customers to choose e-mail addresses freely, an attacker can select an address with which other users make particular associations and use that address to encourage users to act carelessly.

Test passwords

With many webmail providers, the mailbox access username is the same as or derived from the e-mail address. If the password has not been selected carefully enough, or if any number of incorrect password entries are possible without the account being locked, an attacker can find out the password through trial and error and gain full access to the user's account.

Forgotten passwords

Inappropriate "user-friendliness" often makes it easy for potential attackers to obtain a password and therefore full access to someone else's mailbox. A typical example is a mail provider whose start page already contains a "Password forgotten?" link, which opens a page that prompts the user to provide previously agreed, often easily guessable information. A popular code is the date of birth, which, if entered almost correctly, may even prompt with further advice, like "Incorrect month".

Examples:

- The example in T 5.40 *Monitoring rooms using computers equipped with microphones* describes how a German politician was asked in a forged e-mailed virus warning to open the attached virus protection program, which contained a Trojan horse. The sender address of this message was *support@xyz.de*, from the domain of her e-mail provider XYZ. She would probably not have opened the message if the sender address was unknown to her.
- In the Web-based e-mail service Hotmail, several security gaps have already been identified. A particular risk is represented by mail-embedded JavaScript that is run when the user reads the mail message. Malicious JavaScript could, for example, prompt the user to re-enter the password, which would then be sent to the attacker. Because JavaScript can be embedded in HTML-formatted messages in numerous ways, filtering of these active contents has, in the past, often been unreliable.

Insecure time window for virus protection

Following a virus warning, it can take several hours before the publisher of the virus protection program can provide the first effective updates and these updates are deployed across all IT systems. Messages arriving on the mail server during that time can be quarantined during that time. If safeguards are not in place to prevent messages being received through webmail accounts, PCs and servers in the LAN can be infected through this route.

Example:

- Late September 2001, the *Nimda* virus caused excitement. Nimda is a worm which performs a number of damaging actions: It distributes itself as an attachment to mail messages through a known weakness of Microsoft's Internet Information Server (IIS) and through shared drives. It took up to 24 hours before effective signatures for virus protection programs were

available after the worm was discovered. In some large companies, users infected their PCs with Nimda through webmail. Through these PCs, in turn, IIS web servers in the company network were then infected, which caused significant disturbance of LAN activities.

T 5.104 Espionage

In addition to the many complex attacks, there are much simpler methods of obtaining valuable information. Because sensitive data is often not sufficiently protected, it can often be obtained visually, audibly or electronically.

Examples:

- Most IT systems are protected against unauthorized use through identification and authentication functions, for example user ID and password verification. If a password is sent through the network unencrypted, an attacker could easily read it. **Unencrypted password**
- To withdraw money from a cashpoint, the user needs to enter the correct PIN. Unfortunately, the visual protection at these machines is often insufficient to prevent attackers from looking over the shoulder of a customer to watch them enter their PIN. If he then steals the cashpoint card, he can raid the account. The customer then has the additional problem of having to prove that he was not careless with the PIN, for example by noting it on the card. **Insufficient visual protection**
- To obtain access rights to a user PC, or to remotely manipulate a PC, an attacker can send a Trojan horse to the user as an attachment disguised as a useful program. Experience has shown that, despite user education, users open e-mail attachments even if they arrive unexpectedly or have strange names. As well as causing damage directly, Trojan horses can be used by outsiders to gather information about the computer to which it was sent and about the network to which it is connected. Trojan horses are often aimed at collecting passwords or other access data. **Trojan horses**
- In many offices, the workstations are not acoustically screened off well enough from each other. Colleagues and visitors may therefore be able to listen in on conversations at adjacent workstations to obtain information that is not intended for their ears and may even be confidential. **Listening in on conversations**

T 5.105 Disruption of archive system services

The services of an electronic archive consist of the following basic functions:

- acquisition and indexing of the documents to be archived
- administration and storage of the documents
- searching and finding of archived documents
- document display and reproduction
- maintenance and administration of the archive system

Disruption of the services of an archive system can be damaging, as illustrated by the following examples:

- If indexing of archived data is prevented or disrupted, e.g. through the entry of false context data, the result could be to make it time-consuming or even impossible to find data again later. **Indexing**
- If archiving of new data is prevented or blocked, for example through a denial-of-service attack on the network connection of the archive system, then, depending on the amount of data, this could result in the build-up of a significant backlog of data that has not been backed up. In the event of a system failure, the documents currently awaiting archiving could then be expected to be lost. If the archive system selected does not present the user with visible confirmation of archiving, there is a risk that any losses of documents could remain undetected for some time. If on the other hand the system used does issue confirmation of archiving, then if a confirmation fails to appear, downstream business or administrative processes will also be delayed. **Archiving**
- If reproduction of archived data is prevented, disrupted or delayed, the result can be that essential documents are not produced on time, which in turn could result in financial loss or damage or legal problems. **Reproduction**
- If administration of the archive system is prevented or delayed, e.g. through overloading of personnel with queries, it is possible that persons who are not supposed to have access could notwithstanding access the archive and store or recall documents in or from the archives without authorisation **Administration**
- Another damaging aspect of the obstruction of administration is that it might impair or delay maintenance of the archive system as a result. This in turn could cause security-relevant software updates to fail to be installed promptly or to not be sufficiently tested.

T 5.106 Unauthorised overwriting or deletion of archival media

Archival media are intended to store important data for long periods without undergoing any changes. Therefore this data must not be overwritten, deleted or otherwise changed without authorisation. Unauthorised deletion is possible if user rights have been incorrectly granted, e.g. if

- users have "delete" rights but on the basis of the information available to them they are unable to make proper decisions as to whether data records should be allowed to be deleted; or
- owing to administrative shortcomings, users are authorised to delete data without proper cause.

A distinction must be made here between rewritable media and WORM media:

- In the case of rewritable media, in principle it is possible to physically delete or overwrite data records.
- In the case of WORM media, physical deletion or overwriting of data is not possible. However, archiving systems generally allow data records to be logically flagged as deleted. These data records are then excluded during recopying to a new data medium. They are only removed from the dataset at the moment of copying to the new data medium.

In both cases, incorrect handling of the media can result in loss of integrity of the stored information and data (on this point see also T 5.85 *Loss of integrity of information that should be protected*).

T 5.107 Disclosure of data to third parties by the outsourcing service provider

Disclosure of data to competitors

Outsourcing service providers usually have several customers. It is therefore always possible that these will include one or more competitors of the customer organisation, especially if the outsourcing service provider is large or specialises in special requirements areas such as IT security services. If an outsourcing partner is working for two competitor organisations at the same time, conflicts of interest can occur unless strict separation is maintained between different projects (outsourcing service provider's multi-customer capability).

In such situations, it is possible that results and knowledge relating to a given project could intentionally be made directly available to the competitor by employees or subcontractors of the service provider. Generally there is no way of rectifying such a situation, even if individual persons or the entire outsourcing service provider can be taken to court later on.

Data protection

If the outsourcing project entails the handling or storage of personal data by the service provider, then additional data protection considerations must be borne in mind. If any information about the outsourcing organisation's own customers is compromised and published, then there is a danger that the relationship of trust between the outsourcing organisation and its customers will be permanently damaged.

T 5.108 Exploitation of system-specific vulnerabilities in IIS

As is the case with virtually all software, many minor programming and development errors only become apparent when the program is actually used. Again, system-specific vulnerabilities in Windows and IIS that are attributable to programming and development errors are always being discovered. Under certain conditions, for example, a buffer overflow can be induced. In particular, when the IIS software interacts with other software components, there is a danger that parameters could be insufficiently tested and affect the functioning of the system.

Security risks arise not only through programming and development errors, but existing sample applications and script files can be exploited for an attack on the system.

Under the standard installation of IIS, a number of sample applications and script files are installed along with the software. These samples are intended to illustrate application possibilities for the web server for the benefit of the administrator or developer or to serve as template for extended functions, e.g. search functions. Many administrators and developers are not aware of the full scope of functionality and possibly not even of the existence of such sample applications. As these applications and script files can be exploited by an attacker, they constitute a significant threat to the information system.

Example 1

Using an *escape sequence* in a URL it is possible to carry out a denial-of-service (DoS) attack on IIS. Escape sequences offer the possibility of inserting non-printable characters or special characters. These sequences consist of an escape character, e.g. "%" plus two hexadecimal characters. On the target system, these characters are converted to the appropriate ASCII code. For example, the character string *%20* means space or blank character.

If a lot of escape sequences are contained in a URL, the processor can be overwhelmed during conversion so that, for example, the IIS is no longer able to respond to regular queries. An example of this is illustrated in Microsoft Security Bulletin MS00-023 (*http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/fq00-023.asp*).

Example 2

The standard installation of IIS 4.0 contains an application that allows web users to alter the password of a user account on the web server. Every user who has access to this page (via HTTP) can find valid user accounts on the server through it. As the acknowledgements issued by the web server provide information on the user accounts tested, this interface can be exploited for brute force attack on the accounts.

Example 3

Due to a weakness in the *showcode.asp* web page, internet users are able to view files held on the web server. Unless steps are taken to exclude the

possibility of breaking out from the webroot directory with the aid of the character sequence /../, this script can also be used to read files from other directories, e.g. *WINNT*.

T 5.109 Exploitation of system-specific vulnerabilities with Apache web server

Like all software, the Apache web server is not free from vulnerabilities and programming errors. On the whole the Apache web server has been largely spared spectacular incidents such as the *Nimda worm*, but, for example, the *Slapper* worm which appeared in the autumn of 2002 exploited a vulnerability in the OpenSSL library to propagate itself over Apache web servers that used SSL. System-specific vulnerabilities in the Apache web server are found either in the actual web server or in modules like *mod_ssl*, *mod_dav*, *mod_rewrite, mod_php* and similar extensions.

By exploiting vulnerabilities (for example, buffer overflows) in the Apache web server or in extension modules, attackers may in extreme cases be able to compromise the server computer. As the Apache web server generally runs under a non-privileged account, it will not normally be possible to directly acquire root or administrator permissions, but nevertheless an attacker who has already gained access to the server computer may be able to gain additional permissions quite easily by exploiting local vulnerabilities of the operating system or other installed programs.

Even if there are no known instances in which a given vulnerability results in compromising of the computer because it allows an attacker to execute his own code on the server computer has been exploited, buffer overflows and similar vulnerabilities can be used to crash the Apache web server and thus to induce a denial-of-service attack.

Vulnerabilities in the Apache web server or in extension modules can also permit access restrictions to be circumvented so that confidential files are shown to unauthorised visitors. It is also possible for configuration information (such as installation paths or system path to web files) to escape to the outside world through a security loophole. Such information can facilitate attacks as in such a case the attacker does not have to try out a series of possible paths.

T 5.110 Web bugs

Web bugs are pictures that are embedded in e-mails or web pages that are loaded by a foreign server when opened. These pictures can be very small, for example a 1 x 1 pixel mini-graphic. The images are embedded in such a way that they are generally not visible, but when loaded from the original server, execution of a script or program is triggered.

E-mail

If web bugs are embedded in HTML-formatted e-mails, the originator can tell, for example, which e-mail was read when. This could be undesirable when combined with mass unwanted e-mails.

The web

Where the web is used, users must basically expect that links will be established not only to the server whose web offering they are currently viewing, but also to other servers. This is the case, for example, when a link is contained on a web page to pictures that are located on a different server. Although in principle this is a normal process, it is possible for information to be unintentionally passed to third parties via this mechanism, as illustrated by the example described below. In particular, confidential data of the user or the server operator can be compromised as a result.

Example:

A university uses a software package that is freely obtainable on the internet to offer dynamic content on the web server (CGI scripts). Depending on the user's inputs, the software generates appropriate response pages on the web server and sends these to the user. As well as the actual content, the HTML pages generated also contain links to pictures that are not held on the university server but on a server belonging the person who programmed the CGI scripts. As a result, these images are called from the programmer's server whenever a user accesses the university's website. In this way the programmer obtains detailed information about the use of the software package he developed, but unfortunately he also gains information about the use of the university's web offering.

T 5.111 Misuse of active content in e-mails

Colourful, but also dangerous!

More and more e-mails are formatted in HTML these days. On the one hand this is often annoying as not all e-mail clients are able to display this format. On the other hand unwanted actions can also be triggered simply when such e-mails are displayed on the client, as HTML e-mails can contain embedded JavaScript or Visual Basic script code, for example.

There have been many cases in the past of HTML-formatted e-mails causing security problems through a combination of security loopholes in e-mail clients and browsers (see also T 5.110 *Web bugs*). One example of this can be found in CERT-Advisory CA-2001-06 (under *http://www.cert.org/advisories/CA-2001-06.html*).

T 5.112 Tampering with ARP tables

ARP spoofing

Unlike on a hub, on a switch it is not possible to intercept the communication between two stations from any of the other stations. For this purpose the switch maintains a table that allocates the MAC addresses of the stations on the various ports. Data packets or Ethernet frames that are addressed to a specific MAC address are only forwarded to the port to which the related computer is connected.

However, it is not only the switch that maintains an ARP table, but also the computers involved. The objective of ARP spoofing is to tamper with these tables (ARP cache poisoning). For this purpose an attacker sends an ARP reply to the victim in which the attacker uses the address of the router that acts as the standard gateway for the related subnet as his own MAC address. If the victim then sends a packet to the standard gateway entered, this packet ends up in reality at the attacker. In the same way the ARP cache on the router is also tampered with such that Ethernet frames, which were actually addressed to the victim, in reality end up at the attacker. A series of tools is available on related web sites that makes these methods of attack possible.

MAC flooding

MAC flooding is a method of attack that affects the function of a switch. Switches dynamically learn MAC addresses connected. The MAC addresses are saved in the switching table. In this way the switch knows to which ports the related MAC addresses are connected.

If a large number of packets with different source MAC addresses are sent with the aid of a suitable tool by one of the stations connected, the switch saves these MAC addresses in its switching table. As soon as the storage space for the switching table is full, a switch sends all packets to all switch ports. Due to this "flooding" of the switching table with meaningless MAC addresses, a switch can no longer determine to which ports actual destination MAC addresses are connected. This method of attack is used to make it possible to read packets in switched networks. On related sites in the Internet there are freely available tools that can generate 155,000 MAC address entries on a switch in a minute.

T 5.113 MAC spoofing

The MAC ("media access control") address for a device is an address assigned by the manufacturer and is used to address devices on OSI layer 2.

Various security mechanisms at the network level (for instance port security on switches) are based on the principle that a connection is only allowed to be established by a device with a specific MAC address.

With the aid of appropriate programs, an attacker can change the address of his device and send Ethernet frames in the network segment with a different ID. In this way it is possible to circumvent security mechanisms based solely on the use of a MAC address. However, the attacker must be in the same network segment or even have access to the same switch port as the device that he is attempting to mimic using MAC spoofing.

A threat due to MAC spoofing also exists on wireless networks (WLAN) on which related access control has been configured on the access point.

T 5.114 Misuse of spanning tree

The spanning tree protocol is specified in IEEE 802.1d. Spanning tree is used to prevent the formation of loops within a network comprising several switches. With this variant, redundant network structures are identified and a loop-free structure is formed. This measure reduces the active connection paths on any meshed network structure to a tree structure.

In the following illustration it can be seen that a port on the bottom switch has been disabled with the aid of spanning tree. By sending out Bridge Protocol Data Units (BPDUs), a root bridge is identified based on the priority set and MAC address of the switch. In the illustration the switch at the top right is the root bridge.

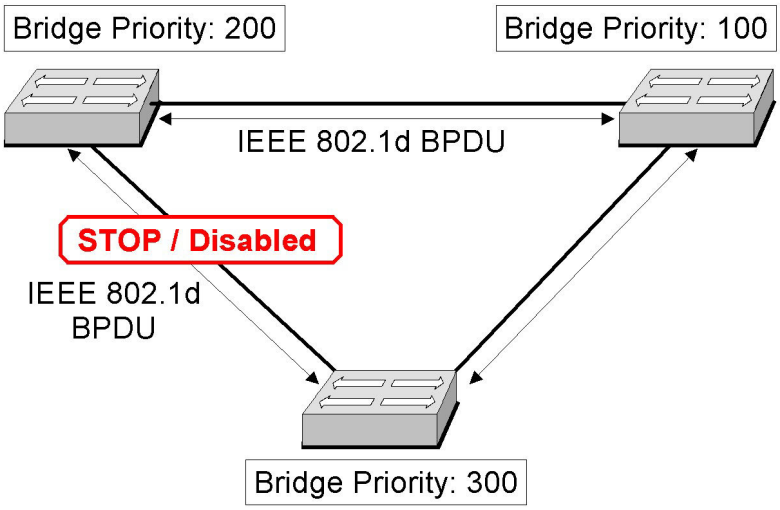


Figure 1: Spanning tree

Spanning tree does not provide any authentication on the exchange of BPDUs. This situation can be exploited by attackers in switched networks. If an attacker can send BPDUs from a station connected to a switch, the topology will be recalculated with the aid of the spanning tree algorithm. The convergence for the calculation of the topology change can be 30 seconds with spanning tree. In this way the availability of the network can be seriously affected by sending BPDUs.

T 5.115 Overcoming the boundaries between VLANs

Virtual LANs (VLANs) are used for the logical structuring of networks. In this case a logical network structure is formed within a physical network by combining functionally related workstations and servers to form a virtual network. At the same time a VLAN forms a separate broadcast domain. This means that broadcasts are only distributed within the VLANs. A VLAN can involve an entire switched network and does not need to remain restricted to a single switch.

The expansion of VLANs over several switches is realised using various so-called trunking protocols. Here a physical port is reserved per switch for the inter-switch communication, the logical connection between the switches is termed the trunk. An Ethernet frame is encapsulated in the trunking protocol for the exchange of information between the switches. In this way the destination switch is able to allocate the information to the related VLAN. IEEE 802.1q and the proprietary protocols ISL (Inter Switch Link) and VTP (VLAN Trunking Protocol) from the manufacturer Cisco are used as the standards.

If an attacker, who is connected to a switch, for example identifies himself as a switch by using the trunking protocol ISL (Inter Switch Link) or IEEE 802.1q, it is possible to obtain access to all VLANs configured and therefore to read data that belong to a VLAN; that is data to which the attacker would not normally have access.

Information on VLANs configured is exchanged between Cisco switches with the aid of the proprietary protocol VTP. Here it is possible to distribute the VLAN configuration on a central VTP server to all switches involved within a VTP domain. Although this simplifies the management of VLANs with several switches, at the same time it represents an additional security risk: although VTP supports authentication within a VTP domain, if a password is not set for the authentication of switches within a domain, an attacker (for example on a dedicated switch configured as a VTP server) can overwrite the entire VLAN architecture on switches in the VTP domain.

T 5.116 Tampering with the z/OS system configuration

Interaction with z/OS systems is possible using numerous interfaces, for example using the *hardware management console*, the *MVS master console*, the *enhanced MVS console service*, automation procedures, remote MVS console and remote maintenance ports. Some security problems that may be related with the use of these interfaces are listed in the following.

HMC (Hardware Management Console)

Unauthorised access to the HMC can lead to significant security problems. From the HMC it is possible to change the behaviour of the system during operation. Individual LPARs (*Logical Partitions*) and even an entire computer group can be re-initialised. Furthermore, using the HMC it is also possible to load new *input/output control datasets* that will become active on the next *Initial Program Load* (IPL). As a result there is a risk that disks not actually related to an LPAR are assigned to this LPAR.

MVS master console

z/OS operating systems are controlled, among other ways, via the MVS consoles. The standard consoles have a fixed connection to the system and do not require an ID or a password. This means that people who have physical access to an MVS console with a high level of authorisation (e. g. to the master console) can enter any MVS command. As a consequence, unauthorised *batch jobs* or *started tasks* can be stopped or started. Furthermore, disks on any system can be placed *online*, if they are generated there. In certain circumstances, it is also possible to generate channel paths later using MVS commands, and then to append disks that do not even belong to this LPAR.

Enhanced MVS Console Service

Beyond the normal MVS consoles, the z/OS operating system provides the EMCS (*Enhanced MVS Console Service*). This is also provided as a function by various applications, for instance TSO, CICS or NetView. Using EMCS, dynamic consoles can be created in a script; these consoles can support almost all commands that can also be used on the normal consoles. If EMCS is not protected or only inadequately protected using RACF profiles, in certain circumstances it will be possible to tamper with the z/OS operating system from any terminal.

Risks from automation

Automation procedures can be programmed such that they are triggered by messages. If the automation procedures are not specially protected, there is a risk that the generation of a fake message could be used to start automation functions.

Remote MVS console

z/OS systems in different locations can be controlled from a central console. Often a software tool is used for this purpose that enables, e. g., the LPARs in the z/OS systems to also be controlled over large distances. The software tool emulates an MVS console on a conventional PC. If the physical or the logical

access to such control consoles is inadequately protected, there is a risk of unauthorised tampering with remote z/OS systems from the console.

Remote maintenance ports

A further hazard for the z/OS system can result from incorrect configuration of the RSF console (*Remote Support Facility*). In certain circumstances, an external attacker can exploit the configuration and dial into this console (see also T 5.10 *Abuse of remote maintenance ports*).

Examples:

Obtaining the Special privilege by improper means

RACF was setup in a computer centre such that RACF commands could also be entered from an *MVS master console*. An unauthorised member of staff had access to the room in which these consoles were installed. As a consequence he allocated the *Special* privilege to his own user ID. This situation was not noticed for some time.

T 5.117 Covering up tampering in z/OS

By changing log files or shutting down log functions, it is possible to cover up tampering on the z/OS system.

The majority of components in the z/OS system generate logging information on system activities and system events. These data are regularly cleared and saved in the related log files (e. g. *system log*, *SMF data records*) that can be evaluated later.

Log files can be modified or tampered with if an appropriate access right to the file is held. This right may, for instance, have been granted unintentionally due to carelessness in the system administration, or an attacker may have obtained this right, for example by appropriate tampering.

A further possible method of attacking the system logging is preventing the generation of log data by means of appropriate tampering with the generating components. Which *SMF data records* are written is, for example, in z/OS entered in a *configuration member*. By making changes to this *member* or by setting *exits*, it is possible to ensure that certain *SMF data records* are no longer written. The usual security monitors are not able to detect suppressed violations and to report that no *SMF records* or no system messages are written.

Example:

Deactivation of SMF records

In a computer centre, a user managed to deactivate the writing of SMF data records. The user then tampered with the system in various ways and re-activated the SMF function afterwards. It was not possible to subsequently identify the changes made to the z/OS system during this period, as there were no log data. It was only possible to demonstrate in the system log that the commands were entered on a MVS console to which several people had access.

T 5.118 Obtaining high level rights in the RACF by unauthorised means

If a user manages to increase his rights in the z/OS security system, RACF, in certain circumstances the user will be able to access files without authorisation and tamper with the system.

Trace in the network

With a so-called *trace* (interception of the network traffic) on the TCP/IP or TPX protocols, an attacker may be able to obtain the ID and password of a user with *special* rights, depending on the protection in the network. Using this knowledge, the attacker will be able to increase his own permissions and even assign the *special* rights to his own ID.

APF, SVC

Two further possible ways to obtain higher level permissions as a user in the z/OS system are the APF (*Authorized Programming Facility*) and the SVCs (*SuperVisor Calls*).

If the user manages to place programs in APF-authorised files, or the user manages to install SVCs, then in this way he can obtain *special* or *operations* rights (tampering with his own ACEE control block). Although these may only be available temporarily for the related session, the program can be run time and again.

Accumulated rights

A further hazard are the so-called *accumulated rights* due to inadequate permission management. Here the following scenario is typical:

A user changes to a new post. The user receives the rights as necessary for the new post without the deletion of the old rights. In this way over a long period the user accumulates rights that are much wider than the permissions actually required.

Example:

Specialist knowledge in the z/OS environment is not widespread. As a consequence, z/OS consultants were employed in an organisation over a long period of time and accumulated rights. An administrator noticed this situation by accident when the permissions concept for the organisation was under complete revision.

T 5.119 Use of other IDs in z/OS systems

The *surrogat* permission in the z/OS security system, RACF, enables user A to run a batch job using a different user's ID, user B, without user A needing to know user B's password. All security checks are performed for user B's ID and the log and SMF data record user B as the user running the commands.

There is a risk that the *surrogat* permission could be misused if the necessary security precautions are not taken on granting and monitoring this permission:

- Users can, in certain circumstances, run unauthorised actions that they are not allowed to run with their own ID.
- Users can, in certain circumstances, make it appear that another user is responsible for their own (unauthorised) actions.

T 5.120 Tampering with the Linux/zSeries system configuration

Three different Linux operating modes are possible with zSeries:

- Linux native on zSeries hardware
- Linux in a zSeries LPAR
- Linux on a host system z/VM

Further information on the Linux operating modes in zSeries is given in the safeguard S 3.41 *Introduction to Linux and z/VM for zSeries systems*.

In all three Linux operating modes with zSeries, there exist the threats described in module 6.2 "Unix Server".

Mainframe-specific threats on the use of Linux

Beyond the threats described in module 6.2 "Unix Server", on the use of Linux on zSeries mainframes, the following security problems may exist, among others:

Linux in a zSeries LPAR

Mainframe-specific threats are produced by the possible effects on the zSeries hardware:

- By access to the *HCD* functions (*Hardware Configuration Definition*), members of staff can allocate hardware resources, such as hard disks, to the Linux partition without authorisation. As a result the Linux operating system has access to the hardware resources.
- The access to the *HMC* (*Hardware Management Console*) makes it possible to tamper with aspects such as starting, stopping and the allocation of resources to an LPAR. This aspect is described for the z/OS operating system in T 5.116 *Tampering with the z/OS system configuration*. Of similar criticality for security is the access to *SE*s (*Service Elements*). The Service Element is a component in the zSeries hardware providing the same functionality as an HMC.

Linux on a host system z/VM

In this scenario, Linux is operated on the emulated hardware of a virtual machine. The virtual machine's emulated hardware is realised by z/VM on the real zSeries hardware. The physical access to the real resources is performed only using z/VM.

The mainframe-specific threats result, on the one hand, from the possible effects on emulated hardware, and on the other hand, from the possible effects on z/VM.

- The access to *HCD* functions and to an *HMC* can, as described for the *Linux in a zSeries LPAR* operating mode, be misused.
- Members of staff who are allowed to issue critical z/VM commands can, in certain circumstances, significantly jeopardise the operational stability of the z/VM and with it the operational stability of the Linux operating systems running on it.

- Members of staff who obtain unauthorised access to the *DIRMAINT* utility can also, e. g. generate new virtual systems or allocate minidisks in one Linux system to another. If z/VM RACF is not used, user IDs can also be administered using *DIRMAINT*.
- If the security component z/VM RACF (Resource Access Control Facility) is used in the z/VM operating system, in z/VM the threats are comparable to those described in T 3.72 *Incorrect configuration of the z/OS security system, RACF* for the z/OS operating system. Members of staff who have high level RACF/VM authorisation (e. g. *SPECIAL*), can tamper with other z/VM IDs and permissions using RACF/VM.
- If the authentication in Linux is performed using an LDAP link to the PAM module (*Pluggable Authentication Module*) using a z/OS-RACF, Linux IDs and permissions can also be changed by members of staff with high level z/OS-RACF authorisation.

Example:

Unauthorised use of the z/VM administration

- For historical reasons, a member of staff still had the permission to use the DIRMAINT function in z/VM. The member of staff used this situation to generate and use a private Linux system. This situation resulted in the use of resources that as a result were no longer available to the proper processes on the zSeries machine.

T 5.121 Attacks on z/OS systems using TCP/IP

To attack a z/OS system over the network connection, it is often not necessary to have any special knowledge of the SNA network architecture or of MVS. Due to the TCP/IP connection to public networks and the *Unix System Services*, many z/OS systems can be reached by external attackers using standard protocols and services, such as HTTP or FTP.

External attackers can, in certain circumstances, carry out denial-of-service attacks against the services provided over the TCP/IP connection to public networks or read data transmitted without authority or tamper with data transmitted.

Internal attackers can try to increase their permissions using the TCP/IP connection to internal networks by obtaining, for instance, the ID and password for a user with *special* rights.

T 5.122 Misuse of RACF attributes in z/OS

In the z/OS security system RACF, the attributes *SPECIAL*, *OPERATIONS* and *AUDITOR* have special, high level permissions.

***SPECIAL* attribute**

The ID with the *SPECIAL* attribute is necessary for the administration of the RACF security system. The owner of this attribute can change settings in the RACF. This attribute gives the users, for instance, access to system resources and files. The owner of the permission can grant himself rights to all resources and files in the system. He can also assign the attributes listed below to all user IDs.

A possible weak spot is in the use of system monitors that, using program routines with a high level of authorisation can give their own ID the *SPECIAL* attribute. Users with access to the system monitors can exploit this situation, given appropriate RACF rights, to give their own ID higher level access rights.

***OPERATIONS* attribute**

The ID with the *OPERATIONS* attribute is primarily needed for the *space management* in the z/OS system. It includes the rights for copying, reading, deleting or the addition of files, without the need to have granted an explicit right for the file and the user ID. In principle, this situation makes it possible for a user to misuse the *OPERATIONS* attribute for unauthorised data access.

***AUDITOR* attribute**

Auditors are intended to be able to detect, track and check security-related events. With this permission, changes to RACF definitions are only possible for audit-related definitions (unlike *SPECIAL*), i. e. higher level authorisation cannot be achieved with this attribute. However, the *AUDITOR* attribute implies the risk that extensive information on the system, e. g. all RACF settings, could be obtained.

Examples:

- A system programmer did not have the *SPECIAL* attribute. He wrote a particular program and placed it in an APF-authorised file. He needed access to the APF files for his day-to-day work. Using the program he wrote, the system programmer was able to assign himself the *SPECIAL* attribute and make unauthorised changes to RACF settings.

Obtaining the Special attribute by improper means

- As it became known in an organisation that a competitor had drawn away customers, checks were made. It was found that a user's ID had the *OPERATIONS* attribute. With the aid of this attribute, the user was able to regularly copy customer addresses without authorisation and pass them on.

Exploiting the OPERATIONS attribute

T 5.123 Bugging of indoor conversations using portable terminal devices

A large number of portable terminal devices such as laptops, PDAs or mobile telephones are now equipped with a microphone or camera. Using these devices, it is not only possible to record ideas or snapshots when on the move, they can also be used for the surreptitious recording or bugging of conversations (see also T 5.95 *Bugging of indoor conversations over mobile phones*).

A PDA can be used for this purpose, for instance, by placing it inconspicuously in a room, e. g. during a meeting.

Can be activated inconspicuously

Participants in meetings will not normally expect the entire meeting to be recorded.

Example:

In a meeting almost all participants have their laptops with them and also use them incessantly during the meeting. One of the participants inconspicuously activated the microphone on his computer. Like the majority of portable terminal devices, here it is also inconceivable to the other users that the microphone is switched on. The participant recorded the entire meeting and cut small sections from the recording. As these were taken out of context, he was able to successfully create a different result for the meeting.

T 5.124 Misuse of information on portable terminal devices

Portable terminal devices are easily lost and are easy to steal (see also T 5.22 *Theft of a mobile IT system*). The smaller and more desirable such devices are, the greater is the risk. Along with the direct loss, in this case further damage can be caused by the loss and the disclosure of important data. This direct damage is in many cases more serious than the purely material loss of the device.

Examples:

Confidential data on the PDA

- Data such as notes from meetings or addresses that are saved in the PDA can certainly be of a confidential nature. Loss of the device may then mean disclosure of this stored information in certain circumstances.
- Many portable terminal devices have security mechanisms intended to provide protection from unauthorised access. These security mechanisms are mostly of weak design making it easy for attackers to overcome them. Even if they exist, they are often not used for reasons of convenience such that confidential data is not protected at all in case of loss.
- Portable devices often contain access data for other IT systems or the LAN in the authority or the organisation. If an unauthorised person comes into possession of a laptop or PDA with (static) access IDs, misuse of internal data becomes possible.
- On PDAs with a built-in mobile phone (smartphones), a dishonest finder or thief can make telephone calls at the expense of the rightful owner, provided he knows the PIN, he can guess the PIN easily, or if the security mechanisms on the device are easy to overcome.
- Many PDAs and laptops have interfaces for the use of interchangeable data storage devices such as memory cards or USB tokens. On an unattended PDA or laptop with the related hardware and software, there is a risk that large amounts of data can be quickly copied using these storage media. No traces whatsoever are left of the copying during this process.

T 5.125 Unauthorised transfer of data using portable terminal devices

Portable terminal devices such as notebooks or PDAs are in general designed so as to make possible the straightforward exchange of data with other IT systems. This feature may be a connecting cable or also wireless, e. g. infrared, Bluetooth or GSM.

Information can then be surreptitiously retrieved and transmitted in a place where IT systems can be accessed openly. The data collected can then be taken away unnoticed with the device or modified. A subsequent check or even the provision of evidence is not always possible, as often the accesses are not appropriately logged.

If the device has a wireless communication interface (for example an integrated WLAN card or an interface to a mobile telephone), the information saved can also be immediately transmitted anywhere in the world (see also T 5.97 *Unauthorised transfer of data over mobile phones*).

If a wireless network (WLAN) is operated internally in an organisation, a visitor can eavesdrop on WLAN traffic with his PDA. If the wireless network is inadequately protected, the attacker can straightforwardly "record" all data transmitted or even obtain direct access to the network in this way.

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 outside party uses the brief interval during which he is alone in the meeting room to link up the PC installed there with his portable terminal device. He then transfers all accessible data to his portable terminal device.

T 5.126 Unauthorised photography and filming with portable terminal devices

Candid camera!

Portable terminal devices are in the meantime increasingly equipped with built-in or plug-on cameras. In some cases it is even possible to film with such cameras. Such portable terminal devices can easily be used to take photographs or even to film in sensitive areas (for example in a development department). While the image quality may, in most cases, not be the same as "real" cameras, it is important to be conscious of this risk.

As for "general data theft" (see T 5.125 *Unauthorised transfer of data using portable terminal devices*) the images taken can be immediately transmitted to the exterior and then deleted from the device. In this case, even if somebody is suspicious, it practically impossible to obtain any evidence.

Example:

Mobile telephones with cameras are no longer allowed to be taken into many swimming pools and sports studios, as there have been numerous complaints about photographs taken surreptitiously in the changing rooms. This situation became known as some hobby paparazzi proudly published their photographs on web sites.