Threats Catalogue – Elementary Threats

Table of Contents

T 0.1 Fire

Fire can cause severe damage to people, buildings and their facilities. In addition to damage resulting directly from fire, consequential damages can be identified, which can assume catastrophic proportions in their damage effect especially for Information Technology. Damage resulting from fire-fighting water, for instance, does not occur only at the location of the fire. It can arise also in lower lying areas of the building. During incineration of PVC, chlorine gases are produced, which form hydrochloric acid when combined with moisture in the air and water for fire-fighting. When hydrochloric acid vapour is disseminated via the air-conditioning system, damage can thus be incurred to sensitive electronic devices, located in a very remote part of the building from the scene of the fire. However, “ordinary” fire smoke can also have a damaging impact on IT-equipment in this way.

Not only negligent handling of fire (e. g. unattended open flames, welding and soldering works), but also improper use of electrical appliances (e. g. unattended coffee machine, overloading of multi-socket adapters) can result in an outbreak of fire. Technical defects of electrical equipment can lead to a fire as well.

The propagation of fire can be promoted by:

– keeping fire-proof doors open using wedges,

– inappropriate storage of combustible materials (e. g. waste paper),

– failure to follow relevant fire protection standards and instructions,

– lack of fire detection and alarm systems (e. g. smoke detectors),

– missing or unprepared hand-held or automatic fire extinguishers (gas extinguishing systems),

– inadequate fire prevention facilities (e. g. lack of fire insulation in cable routes or use of unsuitable insulating materials for thermal and acoustic

insulation).

Examples:

- At the beginning of the 90s a mainframe computer centre in the Frankfurt area suffered catastrophic fire damage leading to a complete failure.
- It often happens that small electrical appliances, such as coffee machines or table lamps, are improperly installed and therefore cause fires.

T 0.2 Unfavourable Climatic Conditions

Unfavourable climatic conditions like heat, frost or high humidity can lead to a wide variety of damage, like malfunctions in technical components or damage of storage media. Frequent fluctuations of climatic conditions amplify these effects. Unfavourable climatic conditions can also lead to a situation where people are no longer capable of working or where they are injured or put to death.

Every human being and every technical appliance has a temperature range, within which normal operation or proper functioning is guaranteed. Whenever the ambient temperature exceeds the lower or the upper limit of this range, it may cause absences from work (stoppages), operational disruptions or device failures.

IT systems as heating

For example, electrical energy is converted into heat in a server room owing to the devices inside and thus heating the room up. In cases of insufficient ventilation, the permissible operating temperature of the devices inside can be exceeded. Under solar exposure, the temperature in the room can reach 50 degrees Celsius.

For the purpose of ventilation, windows in server rooms are frequently opened without permission. In seasonal transition periods with major temperature fluctuations (spring, autumn), this can result in exceeding the permissible air humidity due to severe cooling.

Defects in long-term storage media

When storing digital long-term storage media, excessive fluctuations of temperature or a too high humidity level can lead to data errors or a reduced data retention period. Some manufacturers state that the optimum storage conditions for long-term storage media are temperatures ranging from 20 to 22°C and an air humidity of 40%. Also, analogue media like paper or microfilms require certain storage conditions. If, for instance, paper is stored in too humid a place, it can get mouldy or disintegrate.

Examples:

- In cases of high temperatures during the summer and inadequate cooling of IT equipment, temperature-dependent failures can occur.
- Too much dust in IT systems can lead to a build-up of heat.
- Too high temperatures can cause demagnetisation of magnetic data storage media.

T 0.3 Water

Water can affect the integrity and availability of information stored on analogue and digital data storage media. Also information in the RAM of IT systems is at risk. An uncontrolled admission of water into a building or into rooms can, for instance, result from:

– disruptions in the water supply or sewage disposal,

– defective heating system,

– defective air-conditioning systems with a water supply,

– defective sprinkler systems,

– water used during a fire-fighting operation and

– water sabotage e. g. performed by opening taps and blocking drains.

Regardless of how water enters into the building or into rooms, it entails the risk that supply facilities or IT components will be damaged and taken out of operation (a short circuit, mechanical damage, rust, etc.). Especially if central supply facilities of the building (main power distributor, telephone, and data) are housed in basement rooms without automatic drainage, The ingress of water can cause extremely high losses.

In addition, problems resulting from frost can arise. For example in frost-endangered areas, pipes can start to leak if water stands still inside them, accompanied by persistent frost. Even existing thermal insulation will also be overcome by frost in time.

Example:

– In a server room, there was a water pipe running beneath the ceiling which was covered with plasterboard panels. When a coupling in the water pipe started to leak, this was not recognised in time. At first the leaking water collected in the deepest point of the cladding, before it flowed out and caused a short circuit in the power distributor attached underneath. As a consequence until it was finally repaired, both water and power supplies of the corresponding part of the building had to be switched off completely.

T 0.4 Pollution, Dust, Corrosion

Dust interferes with electronics

Besides electronics, many IT devices contain mechanical components, such as hard drives and removable disks, DVD drives, printers, scanners etc. and coolers for CPUs and power supply units also. With increasing quality and speed requirements, these devices must function more and more precisely. Even small amounts of pollution can lead to disruption of a device. Dust and pollution in significant amounts can for example be generated by the following activities:

– repairs on walls, raised floors (double floors) or other building parts,

– hardware upgrades or similar work

– packaging (e. g. Styrofoam particles)

Existing safety circuits in the equipment usually ensure a timely switching off the device. This restricts the direct damage to the affected device, keeps the repair costs low and the downtimes short, but the affected device remains unavailable during down-time.

In addition, equipment and infrastructure can be damaged by corrosion. This can have a negative impact not only on IT but even on the safety of buildings.

Corrosion can also indirectly lead to further risks. For example, when water flows out of corroded water pipes (see T 0.3 Water).

Altogether, pollution, dust or corrosion can therefore lead to failure of or damage to IT components and supply facilities. As a consequence, proper information processing can be impaired.

Examples:

– After installation of a server in a media room, together with a photocopier and a fax machine, errors within the CPU cooler and the power supply fan occurred successively due to the high dust level in the room. The breakdown of the CPU cooler led to sporadic server crashes. The breakdown of the power supply fan finally led to an overheating of the power supply unit resulting in a short circuit, which eventually entailed a total failure of the server.

– To hang up a blackboard in an office, holes were drilled into the wall by the site technical service. During this, the office employee had left his office for a short time. After he returned to his workplace he noticed that his PC no longer functioned. The reason for this was the ingress of dust from drilling into the PC power supply unit through the ventilation slits.

T 0.5 Natural Disasters

With natural disasters natural changes are meant which have a devastating impact on people and infrastructures. Causes for a natural disaster can be seismic, climatic or volcanic phenomena such as earthquakes, floods, landslides, tsunamis, avalanches and volcanic eruptions. Examples of extreme meteorological phenomena are thunderstorms, hurricanes or cyclones. Depending on its location, the institution is exposed to these risks stemming from various types of natural disasters to a greater or lesser degree.

Examples:

- In the case of computing centres in flood-endangered areas, there is a particular danger of water entering into the building in an uncontrolled manner (flooding or phreatic rise).
- The frequency of earthquakes and hence the risk accompanying them depends strongly on the geographical location.
- Extremely high solar activity has in the past repeatedly led to impairments of telecommunications infrastructures and the energy supply.

Independent of the type of natural disaster, even in areas not directly affected by it, the danger exists that supply facilities, communication links or IT components will be damaged or put out of operation. In particular, the failure of the central supply facilities of the building (main power distributor, telephone, data) can cause very high losses. Access to the infrastructure by the maintenance and service staff can be impeded due to extensive restricted areas.

Examples:

- Many commercial enterprises, also large companies, do not take the threat of floods into account adequately. There is a company which has been "surprised" by flood damage in their computing centre several times already. The computing centre literally swam away after flood damage for the second time within 14 months. The loss incurred amounted to several hundred thousand Euros and this has not been covered by insurance.
- An IT system has been installed at a site with a geographic location well-known for a volcanic activity (intermittent phenomenon, where volcanic emission phases alternate with somewhat long resting phases).

T 0.6 Environmental Disasters

A public body or a company can suffer damage when a serious accident happens in its environment, for instance, a fire, an explosion, a release of poisonous substances or a dangerous radiation leak. Therefore, the danger is not only due to the event itself but often to activities resulting there from, for example access restrictions and rescue measures.

The property of an institution can be exposed to a variety of threats originating from the environment, among other things from traffic (streets, rail, air, and water), neighbouring companies or residential areas.

Even preventative or rescue measures can affect the property directly. Such measures can also lead to a situation where employees cannot reach their workplace or staff must be evacuated. However, the complexity of site technical service and IT infrastructure can also give rise to indirect problems.

Example:

– Due to a fire outbreak in a chemical plant in the immediate proximity of a computing centre (approx. 1000 m as the crow flies), a large cloud of smoke arose. The computing centre had an air conditioning and ventilation system which did not have any external air monitoring. Thanks only to the attention of an employee (the accident happened during working hours) who observed the emergence and spreading of the cloud, the external air supply could be manually switched off.

T 0.7 Major Events in the Environment

Major events of every kind can impede the proper operation of a public body or a company. They include amongst other things street festivals, concerts, sporting events, industrial action or demonstrations. Riots in connection with such events can have additional consequences, like intimidation of employees up to the use of force against the staff or the building.

Examples:

- During the hot summer months, a demonstration took place nearby a computing centre. The situation escalated resulting in violence. In a side street, a window of the computing centre area was still opened, through which a demonstrator gained access and used the opportunity to steal hardware with important data stored on it.
- During the construction of a big funfair, electric cables were cut by mistake. This led to a failure in a computing centre connected through it. This failure however, could be backed-up by the emergency power supply.

T 0.8 Failure or Disruption of the Power Supply

In spite of high security of supply in the electricity sector, interruptions to the power supply on behalf of the distribution network operators or energy supply companies continue to occur. The majority of these disruptions are so short, with times of less than one second, that a human does not notice them. But interruptions of more than even 10 ms are capable of disrupting IT operation. However, besides disruptions in the supply networks, also shut-downs caused by unheralded works or cable damage due to civil engineering work, can lead to power failures.

It is not only those obvious, direct consumers of power (PC, lighting etc.) which are dependent on the power supply. Many infrastructure facilities depend on electric power today, e. g. lifts, air-conditioning devices, alarm systems, security gates, automatic door locking and sprinkler systems. Even the water supply in skyscrapers is power-dependent because of pumps in the upper floors required for producing pressure. Prolonged power outages resulting in failure of the infrastructure facilities can lead to a situation where no activity can be undertaken on these premises any more.

Besides failures, other disruptions of the power supply can impair the operation also. Voltage spikes can, for example, lead to malfunctions or even damage of the electrical equipment.

In addition it has to be taken into account that sometimes failures or disruptions of the power supply in the neighbourhood can affect one's own business processes, if access routes are blocked for instance.

Examples:

- Due to an error in the uninterrupted power supply unit of a computing centre, the unit was unable to return to normal operation after a short power failure. After discharging of its batteries (which took about 40 minutes) all computers in the respective server hall failed.
- At the beginning of 2001 in California there was a power supply crisis for more than 40 days. The power supply situation there was so tense that the Californian Independent System Operator ordered rotating power cuts. Not only households but also the high-tech industry was affected by these power cuts which lasted up to 90 minutes. Since during the power failure alarm systems and surveillance cameras were also turned off, the energy suppliers kept their shut-down schedule secret.
- In November 2005 many communities in Lower Saxony and North Rhine-Westphalia remained without a power supply for days after intense snowfall, because many pylons were knocked over by the load of snow and ice. The recovery of the power supply took several days.

T 0.9 Failure or Disruption of Communication Networks

Many business processes nowadays require at the very least intact communication connections, be it telephone, fax, email or other services using local or wide area networks. If one or more of these communication connections are not available over a longer period of time, the result can, for example, be that:

- Business processes cannot be continued any longer because the required information cannot be retrieved,
- Customers cannot contact the institution for inquiries any more,
- Orders cannot be commissioned or completed.

If time-critical applications are run on IT systems which are connected via wide area networks, the possible losses and consequential damages due to a network failure are correspondingly high if no alternatives (e. g. connection to another communications network) are available.

Similar problems can arise if the required communications networks are disturbed even though they have not completely failed. Communication links can show increased error rates or other quality shortcomings for example. Wrong configuration parameters also can lead to impairments.

Examples:

- For many institutions the Internet has become an indispensable communication medium today, for the retrieval of important information, for representation purposes and for communication with customers and partners, amongst other things. Companies specialising in Internet-based services are of course eminently dependent on an operating Internet connection in particular.
- Benefiting from convergence of networks, voice and data services are frequently transmitted over the same technical components (e. g. VoIP). This however, increases the danger that at a disruption in communication technology leads to a failure of both voice and data services.

T 0.10 Failure or Disruption of Mains Supply

In a building there are a variety of networks used for basic supply and disposal services and, as such, form a basis for all of an institution's business processes, including IT. Examples of such supply networks are:

– power,

– telephone,

– cooling,

– heating or ventilation,

– water and sewage,

– supply of fire fighting water,

– gas,

– alarm and control systems (e. g. for burglary, fire, housekeeping control engineering) and

– intercoms.

A failure or disruption of a supply network can lead to a situation where, amongst other things, people cannot work in the building any more or IT operation and hence information processing is impaired.

Certain networks are dependent on each other to varying degrees so that operational disruptions in individual networks can also have an effect on others.

Examples:

– A failure of heating or ventilation can have the consequence that all concerned employees must leave the buildings. This can, under certain circumstances, result in high losses.

– The failure of a power supply does not only directly affect IT but also all other networks which are equipped with electrical automatic controls. Even in sewage lines, electrical lifting pumps are used in some circumstances.

– A failure of the water supply may affect the proper function of air-conditioning systems.

T 0.11 Failure or Disruption of Service Providers

Hardly any institution today operates without service providers like subcontractors or outsourcing providers. If organisational units are dependent on service providers, their performance can be impaired due to the absence of external services. A partial or complete outage of an outsourcing service provider or a subcontractor can have a considerable effect on operational continuity, particularly in the case of critical business processes. There are different reasons for such outages, for example insolvency, unilateral termination of contract by the service provider or subcontractor, operational problems due to forces of nature or shortfall of personnel for example. Problems can also arise if the services rendered by the service provider do not correspond to the quality requirements of the contractor.

In addition, it has to be taken into account that service providers also frequently resort to subcontractors to make their services available to the contractor. Disruptions, quality defects and failures on the part of the subcontractors can thus indirectly lead to impairments in relation to the contractor.

The contractor's business processes can also be impaired by failures of the service provider's IT systems or communication connections.

Ceasing to outsource service processes, if it proves necessary, can be considerably complicated, because the outsourced procedures are not adequately documented or because the former service provider does not support this realignment, for instance.

Examples:

- A company has installed its servers in a computing centre of an external service provider. After a fire in this computing centre, the finance department of the company was no longer capable of working. It resulted in considerable financial losses for the company.
- The just-in-time production of a company's products was dependent on the subcontracted supply of material from external service providers. After a provider's lorry failed due to a defect, the delivery of parts urgently required was drastically delayed. This way, a number of customers could not receive their deliveries, timely.
- A banking institute handled all monetary transports using a cash-in-transit company. The latter company surprisingly declared itself bankrupt. The agreement and route planning with a new valuables carrier took several days. This led to considerable problems and time delays in cash supply to and collections from the affected branches of the bank.

T 0.12 Interfering Radiation

Today, information technology consists of electronic components to a large extent. Although optical transmission technology is increasingly in use, computers, network coupling elements and storage systems, for example, still generally contain many electronic components. Due to electromagnetic interference having an effect on such components, electronic devices can be impaired in their function or even damaged. As a consequence, disruptions, wrong processing results or communication errors can occur, among other failures.

Wireless communication can also be impaired by interfering radiation. In this case, a sufficiently strong disruption of the used frequency bands is enough in certain circumstances.

Furthermore, information which is saved on data storage media of certain types can, when under influence of interfering radiation, be deleted or distorted. This refers in particular to magnetically sensitive data storage media (hard disks, magnetic tapes etc.) and semiconductor memory. Damage to such data storage media due to interfering radiation is also possible.

There are many different sources of electromagnetic fields or radiation, for example wireless networks (such as WLAN), Bluetooth, GSM, UMTS etc., permanent magnets and cosmic radiation. In addition, every electric device emits electromagnetic waves of varying strength, which can spread amongst others via air and along metallic conductors (e. g. cables, air conditioning ducts, heating pipes etc.).

In Germany, regulations in this subject area are stated in the Act for the Electromagnetic Compatibility of Resources (EMVT - Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln).

T 0.13 Intercepting Compromising Emissions

Electrical devices emit electromagnetic waves. In cases of equipment which process information (e. g. computers, displays, network coupling elements, printers) this radiation can also carry the information currently being processed with it. Such information-bearing radiation is called expositional or compromising emissions. An attacker, for example in a neighbouring house or in a vehicle parked in the proximity, can try to intercept this radiation and to reconstruct the processed information carried there. The confidentiality of the information is this way called into question. A possible motive for such an attack is industrial espionage.

The limiting values in the Act for the Electromagnetic Compatibility of Resources (EMVG) generally do not suffice to prevent interception of the compromising emissions. If this risk cannot be accepted, additional protective measures must therefore be taken.

Compromising emissions are not restricted to electromagnetic waves. Useful information can sometimes be retrieved from sound waves produced by printers or keyboards, for example.

In addition, it has to be taken into account that compromising emissions can be, in some cases, caused or amplified by the external manipulation of devices. If a device is exposed to radiation with electromagnetic waves, it may occur that the reflected waves carry confidential information.

T 0.14 Interception of Information / Espionage

Espionage is defined as attacks aimed at collecting, evaluating and presenting information about companies, people, products or other target objects. The presented information may then be used, for example, to provide certain competitive advantages to another company, blackmail people or build a copy of a product.

In addition to a variety of technically complex attacks, there are often also much simpler methods for gaining valuable information, for example by bringing together information from several publicly accessible sources, which looks like harmless information in isolation, but can be compromising in other contexts. Since confidential data is frequently not sufficiently protected, this can often be intercepted using visual, acoustic or electronic ways.

Examples:

uncrypted password

– Many IT systems are protected against unauthorised access by identification and authentication mechanisms, e. g. in the form of user name and password verification. If the password is transmitted over the wire in an unencrypted form, it is under certain circumstances possible for an attacker to retrieve it.

– To be able to withdraw money out of an automatic teller machine, the correct PIN for the used electronic cash card or credit card must be entered. Unfortunately, the visual protection available for this equipment is frequently insufficient, so that an attacker can look over the shoulder of a customer entering the pin without much effort. If the attacker steals the card afterwards, he can plunder the account this way.

– To receive access rights to a PC or to otherwise manipulate it, an attacker can send the user a Trojan Horse which he has enclosed within an email as a supposedly useful programme.

– In many offices, workplaces are not sufficiently protected in terms of acoustics. As a consequence, colleagues and also visitors could possibly listen to conversations and come to know information which is not meant for them or is even confidential.

T 0.15 Eavesdropping

Eavesdropping on conversations

Targeted attacks on communication connections, conversations, noise sources of all kinds or IT systems with the objective of collecting information are referred to as eavesdropping. It ranges from unnoticed, surreptitious eavesdropping on a conversation to highly specialised complex attacks in order to intercept signals transmitted over radio or transmission lines, e. g. with the help of antennae or sensors.

It is not only because of the low chance of discovery that wiretapping of lines or eavesdropping on wireless connections is a considerable threat for information security. In principle, there are no tap-proof cables. It is only the effort required by the eavesdropper that distinguishes the security of cables. Whether a line is actually wiretapped can only be ascertained through high metrological effort.

Particularly critical is the unprotected transmission of authentication data in plain-text protocols like HTTP, FTP or telnet, since they can easily be analysed automatically due to the clear structure of the data.

The decision to eavesdrop on information somewhere is in principle determined by the question of whether the information is worth the respective technical or financial effort and the risk of being discovered. The answer to this question essentially depends on the individual possibilities and interests of the attacker.

Examples:

- In the case of telephone calls, it is not only eavesdropping on conversations that can be of interest to an attacker. The information which is transmitted in signalling can be misused by an attacker as well e. g. due to an incorrect setting in the terminal resulting in the password being transmitted in plain text at the time of login.
- An attacker can easily eavesdrop on the entire communication if wireless transmission is unprotected or insufficiently protected (e. g. if a WLAN is protected only with WEP).
- Emails can be read throughout their entire journey through the network if they are not encrypted. Unencrypted emails should therefore not be compared with conventional letters but with postcards.

T 0.16 Theft of Devices, Storage Media and Documents

The theft of data storage media, IT systems, accessories, software or data, on the one hand results in costs for the replacement and restoring operational status. On the other hand, there are losses due to lack of availability. If confidential information is disclosed due to theft, this can result in further damage. Besides servers and other expensive IT systems, also mobile IT systems, which are unobtrusively and easily transported, are frequently stolen. However, there are also cases in which data storage media like documents or USB-Sticks were purposefully stolen to access confidential information stored there.

Examples:

- A notebook computer disappeared from the U.S. Department of State in the spring of 2000. In an official statement, it was not ruled out that the device could contain confidential information. Nor was there information given as to whether the device was protected by cryptographic or other measures against unauthorised access.
- A German Federal Office was repeatedly broken into through the same unsecured windows. Mobile IT systems disappeared along with other valuables. It could not be ruled out without a doubt that files were copied or manipulated.
- There were a number of data leaks in Great Britain, in which confidential documents were disclosed because data storage media were stolen. In one case, several computer hard disks were stolen from the British Air Force which contained personal information, collected by employees for security screening purposes.
- An employee of a call centre prepared copies of a large set of confidential customer data shortly before he had to leave the company. After leaving the company, he then sold this data to competitors. Since details about the incident were then published by the press, the call centre lost many important customers.

T 0.17 Loss of Devices, Storage Media and Documents

There are a variety of causes that can lead to a loss of equipment, data storage media or documents. Directly, availability is a concern. But it may also mean that confidential information falls into the wrong hands if the data storage media have not been completely encrypted. The replacement of equipment or data storage media incurs costs, but also if they emerge again, information can be disclosed or unwanted programmes can reside in them.

Mobile terminal equipment and mobile data storage media can be particularly easily lost. Today, on small memory cards, gigantic amounts of data can be stored. However, it also happens again and again that printed documents are inadvertently left somewhere, for example in restaurants or on public transport.

Examples:

- An employee uses the journey in the tramway to her workplace to read over some documents. When getting off the tram in a hurry at her destination stop, she leaves the documents inadvertently on her neighbouring place. Although the documents are not confidential, several signatures of high-profile executives must nevertheless be collected once again as a consequence.
- At a major event, while searching through his briefcase, an employee inadvertently drops a memory card with confidential calculations on the ground without noticing. The finder views its contents on his laptop and sells the information to the competition.
- A manufacturer sends CDs with software updates for bug fixing by post to his customers. Some of these CDs are lost in the post. Neither the sender nor the recipients are informed about it. As a consequence, the effected customers experience malfunctions in the software.

T 0.18 Bad Planning or Lack of Adaption

If organisational processes serving direct or indirect information processing are not properly designed, it can lead to security problems. Although every single process step is carried out correctly, damage often occurs because processes altogether are defined in an improper way.

Another possible reason for security problems is dependency on other processes which do not have any apparent relation to information processing. Such dependencies can be easily disregarded during planning and trigger impairments during operation.

In addition, security problems can arise when tasks, roles or responsibility are not clearly assigned. This may cause, amongst other things, processes to be delayed, security procedures to be neglected or regulations to be disregarded.

A danger arises when equipment, products, procedures or other means for implementation of information processing are not deployed properly. The choice of unsuitable products or weak points in application architecture or in network design for instance, can lead to security problems.

Examples:

- If maintenance or repair processes are not designed to meet technical requirements, unacceptable downtimes can occur as a consequence.
- An increased risk can arise from attacks on one's own IT systems if security requirements are not taken into account in the procurement of information technology.
- If required consumable material is not made available on time, the IT procedures dependent on it can come to a halt.
- Weak points can arise if, at the planning stage of an IT procedure, unsuitable transfer protocols are selected.

Information technology and the complete environment of a public body or a company continually change. Be it that employees leave or join, new hardware or software is procured or a supplier declares itself bankrupt. If the subsequent necessary organisational and technical adaptations are not taken into consideration or are considered only inadequately, threats may follow.

Examples:

- Due to structural changes in the building, existing escape routes have been changed. Since the employees were not sufficiently informed, the building cannot be evacuated in the required time.
- When transferring electronic documents, it has been disregarded to use a data format readable for the recipient.

T 0.19 Disclosure of Sensitive Information

Confidential data and information should only be accessible to the persons entitled to receive such information. Next to integrity and availability, confidentiality belongs to the basic parameters of information security. For confidential information (like passwords, personal data, official or trade secrets, development data) there exists an inherent danger that these are disclosed by technical failure, carelessness or also by deliberate actions.

This confidential information can be accessed in differing forms, for example:

– on storage media within computers (hard disks),

– on movable storage media (USB sticks, CDs or DVDs),

– in printed form on paper (print outs, files) and on transmission paths during data transmission.

The way how information is disclosed also can vary widely, for example:

– unauthorised access to read files,

– inadvertent dissemination e. g. in the course of repair orders,

– inadequate deletion or destruction of data storage media,

– theft of data storage media and subsequent data perusal,

– eavesdropping on transmission lines,

– infection of IT systems with malicious software,

– intercepting by viewing data on screen or eavesdropping on conversations

Disclosure of sensitive information can have serious consequences for an institution. Loss of confidentiality can among other things lead to the following negative impact on an institution:

– violation of laws, for example data protection and banking secrecy,

– negative interior effects, for example demoralisation of the employees,

– negative exterior effects, for example impairment of the relations to business partners, lost confidence of customers,

– financial consequences, for example claims for compensation, fines, litigation costs

– impairment of the informational right of self-determination.

A loss of confidentiality is not always immediately noticed. Often, it turns out only later that unauthorised persons have obtained access to confidential information, e. g. by press inquiries.

Example:

– Buyers of second-hand computers, hard disks, mobile telephones or similar equipment repeatedly find highly confidential information stored on them, like medical records or account numbers.

T 0.20 Information or Products from an Unreliable Source

If information, software or equipment is used which comes from unreliable sources or whose origin and correctness were not sufficiently verified, their deployment can pose high risks. It can lead to business relevant information resting in the wrong database, calculations providing wrong results or wrong decisions being made, among other things. Also, integrity and availability of IT systems can be affected thereby.

Examples:

- A recipient of emails, the origin of which has not been verified, can be encouraged to carry out certain actions which have an adverse effect on himself or others. For example, the email may contain interesting attachments or links, which when clicked upon install malicious software on the recipient's computer. The sender of the email can be falsified or it can imitate a familiar communication partner.
- An assumption that a statement is true because it is "published in the newspaper" or "was shown on TV" is not always justified. Wrong statements can be incorporated into business critical reports in this way.
- The reliability of information which is spread via the Internet differs greatly. If statements are accepted from the Internet without further source verification, wrong decisions can result from this.
- If updates or patches are downloaded and installed from untrustworthy sources, it can lead to unwanted side effects. There is an increased threat that IT systems get infected with a harmful code, if the origin of software is not verified.

T 0.21 Manipulation of Hardware or Software

Manipulation is defined as any form of targeted but secret intervention aiming to change target objects of all kinds in an unnoticed way. Manipulation of hardware or software can be performed, in, amongst other situations, when being influenced by desire of vengeance, to deliberately generate damage, to obtain personal advantages or gain. It can focus on all kinds of devices, accessories, data storage media (e. g. DVDs, USB sticks), applications and databases or the like.

Manipulation of hardware and software does not always lead to a direct loss. However, if such processed information is impaired, this can lead to all types of security implications (loss of confidentiality, integrity or availability). Manipulations can thereby be all the more effective the later they are discovered, the more extensive the knowledge the perpetrators have, and by how much more profound the effects on a work process would be. The effects range from the unauthorized inspection of sensitive data to even destruction of data storage media or IT systems. Manipulation can thus also result in considerable downtimes.

Examples:

- In a Swiss financial company, an employee had manipulated the software used for certain financial services. This made it possible for him to illegally gain large amounts of money.
- By manipulating ATMs, attackers succeeded several times to illegally read the data stored on payment cards. In conjunction with PINs spied out, this data was then misused to withdraw money at the expense of the cardholder.

T 0.22 Manipulation of Information

Information can be manipulated in various ways, e. g. by incorrect or intentionally false recording of data, any change to the contents of database fields or via correspondence. In principle, this concerns not only digital information, but for example documents in paper form also. A perpetrator can, however, only manipulate the information to which he has access. The more access rights to files and directories of IT systems a person has or the more possibilities to access information he has, the more significant manipulations he can carry out. If the manipulations are not detected early, the smooth progress of business processes and professional tasks can thus be seriously disrupted.

Archived documents usually contain sensitive information. The manipulation of such documents is particularly serious because, under certain circumstances, it may take years before the manipulation is noticed and verification will often no longer be possible.

Various motives

Manipulation of information can be performed when being influenced by the desire for vengeance, to deliberately generate damage or to obtain personal advantages or enrichment, amongst other reasons.

Example:

– An employee was so annoyed at the promotion of her roommate in the accounting department that during the short absence of her colleague, she illegally gained access to her computer. Here she has caused, by changing some figures in the monthly balance sheet, enormous negative impact on the published financial results of the company.

T 0.23 Unauthorised Access to IT Systems

In principle, each interface of an IT system includes not only the possibility to legally use particular services of this IT system pertaining to this interface, but also the risk of unauthorised access to the IT system via this interface.

Examples:

- If a user ID and password have been spied out, any unauthorised use of the applications or IT systems protected by them is well possible.
- Using inadequately safeguarded remote maintenance access, hackers could gain unauthorised access to IT systems.
- When interfaces of active network components are inadequately safeguarded, it is possible that an attacker gains unauthorised access to the network component. If they also manage to overcome the local security mechanisms, e. g. obtain administrative privileges, they could perform all administrative activities.
- Many IT systems have interfaces for the use of interchangeable data storage, such as extra memory cards or USB storage media. In an unattended IT system with the corresponding hardware and software, there is a risk that large amounts of data can be retrieved or malicious software can be introduced this way.

T 0.24 Destruction of Devices or Storage Media

Various motives

External and also internal perpetrators can, for different reasons (revenge, malice, frustration), try to destroy equipment, accessories, documents and other data storage media (e. g. DVDs, USB sticks) or similar media. The destruction of data storage media or IT systems can result in significant downtimes for business processes.

Due to negligence, improper use and also by untrained handling, destruction of devices and data storage media may occur which seriously impairs the operation of IT systems.

There is also a risk that, along with destruction, important information will be lost, which cannot be reconstructed at all or only with great effort.

Examples:

- In a company an internal perpetrator used his knowledge about an important server being sensitive to too high operating temperatures and blocked the ventilation slits for the power supply fan using an object hidden behind the server. Two days later, the hard drive in the server suffered a temperature-caused defect, and the server was down for several days.
- An employee was upset about the repeated crashes of his system so much that he let out his anger on his workstation. Here, as the computer was being kicked, the hard drive was so badly damaged that it was useless. The data stored there could only be partially reconstructed from a backup made the previous day.
- Humidity ingressing into an IT system, due to knocked-over coffee cups or watering the flowers can cause short circuits.

T 0.25 Failure of Devices or Systems

Failure of central components

The failure of a single component of an IT system can lead to a failure of the entire IT operation and hence to the failure of critical business processes. In particular, key components of an IT system for example, servers and network coupling elements, are likely to cause such failures. A failure of individual components of the technical infrastructure, such as air-conditioning or power supply facilities, may contribute to a failure of the entire information network as well.

Technical failure / Human error

The reason for a failure of an IT system is not always technical malfunction (e. g. T 0.8 Failure or disruption of the power supply). Failures can often be attributed to human error (e. g. T 0.24 Destruction of devices or storage media) or intentional acts (e. g. T 0.16 Theft of devices, storage media and documents, T 0.41 Sabotage). Also, lack of maintenance, for example due to absence of maintenance personnel, can lead to technical failure. Force majeure (such as fire, lightning, chemical accidents) can also cause damage, but this damage is usually many times higher.

If time-critical applications run on an IT system without any alternatives, the consequential damages after a system outage is respectively high.

Examples:

- Firmware has been installed on an IT system which is not designed for this type of system. The IT system will then no longer start without errors and must be made operational by the manufacturer.
- A power failure in a memory system at the site of an Internet Service Provider (ISP) resulted in having to switch it off. Although the actual error could be corrected quickly, the affected IT systems could not start again due to inconsistencies in the file system. As a result, several Web servers operated by the ISP were not available for days.

T 0.26 Malfunction of Devices or Systems

Devices and systems that serve for information processing, today often have many functions and are therefore of accordingly complex design. This applies generally to both hardware and software components. Due to this complexity, there are many different sources of error in such components. As a consequence, it happens that devices and systems do not function as they were intended to and this gives rise to security problems.

There are many causes of malfunctions, such as material fatigue, manufacturing tolerances, design weaknesses, exceeded limits, unintended conditions of use or lack of maintenance for instance. Since there are no perfect devices and systems some residual probability of malfunctions must always be accepted.

A malfunction of a device or system can affect all the basic parameters of information security (confidentiality, integrity, availability). In addition, malfunctions may under certain circumstances remain unnoticed for a longer period. It may therefore happen that, for example, calculation results are false and not corrected in time.

Examples:

- A blocked ventilation grid causes overheating of a storage system, which does not fail completely, but just malfunctions sporadically after that. It has been noticed only a few weeks later that the information stored there is incomplete.
- A scientific standard application is used to perform a statistical analysis of previously collected data stored in a database. According to the documentation, the application does not support the database product concerned. The analysis seems to work, spot-checks however show that the calculated results are wrong. The reason for the problem was identified as incompatibility between the application and the database.

T 0.27 Lack of Resources

If the available resources in a given area are insufficient, bottlenecks may occur in the supply serviced by these resources or even congestion and failures. Depending on the type of resources concerned, even a small event that was actually predicted to happen, can in the end affect a large amount of business processes. Lack of resources may occur in IT operations and communications, but also in other areas of an institution. This can lead to a variety of negative effects if for certain tasks, insufficient personnel, time and financial resources are made available. It can happen, for example, that the necessary roles in projects are not filled with qualified people. If resources such as hardware or software do not sufficiently meet the requirements, under certain circumstances technical tasks cannot be successfully processed.

Personnel, time, financial, technical and other shortages in normal operation can often be compensated for, for a limited period however. Under extreme time pressure though, for example in emergency situations, they become even more obvious.

Resources can also be deliberately overloaded, if someone intentionally generates an intense need for a resource and thus provokes an intense and persistent impairment of this resource (see also T 0.40 Denial of Service).

Examples:

- Overloaded electrical wires heat up which, in an unfavourable installation layout, can lead to smouldering.
- When new applications in the network have higher bandwidth requirements than it was assumed at the time of planning, this can result in loss of availability of the entire network, if the network infrastructure does not scale in an adequate measure.
- If due to overwork, the administrators only sporadically check the log files of the equipment they administer, possible attacks will not be detected promptly.
- Web servers can become so overloaded by a large amount of simultaneous incoming requests that controlled access to data is almost impossible.
- If a company is subject to insolvency proceedings, it may happen that there is no money for urgently needed spare parts or those essential service providers cannot be paid.

T 0.28 Software Vulnerabilities or Errors

For all software the following applies: the more complex it is, the more likely errors will occur. Even after intensive testing, not all errors are usually detected prior to delivery to the customer. If software errors are not detected early, the crashes or errors of the application can result in far-reaching consequences. Examples for this include incorrect calculation results, wrong decisions at management level or delays in the workflow of business processes.

Due to software vulnerabilities or errors, serious gaps in the security can occur in an application or an IT system or all IT systems networked with it. Such gaps in the security can under certain circumstances be exploited by attackers to introduce malicious software, to access data in an unauthorised manner or to perform manipulation.

Examples:

- The most frequent warnings of the Computer Emergency Response Teams (CERTs) in recent years were related to security-relevant programming errors. These are errors made during programming of software which allow attackers to misuse it. A large proportion of these errors are caused by buffer overflows.
- Internet browsers are nowadays an important software component on clients. Browsers frequently do not only access the Internet but are also used for internal web applications in companies and public bodies. This is why software vulnerabilities or errors in browsers can impair information security overall particularly strongly.

T 0.29 Violation of Laws or Regulations

If information, business processes and IT systems of an institution are insufficiently safeguarded (for example, by inadequate security management), this can lead to violations of laws relating to information processing or of existing contracts with business partners. Which laws must be observed there, depends on the type of institution and of its business processes and services. Depending on where the sites of an institution are located, a number of national regulations may also have to be observed.

The following examples illustrate this:

- The handling of personal data in Germany is governed by a variety of regulations. These include the Federal Data Protection Act, state data protection laws and a variety of sector-specific regulations also. If during communication between two business divisions, personal data (e. g. medical records) is transmitted unprotected over public networks, this can lead to legal consequences under certain circumstances.
- The management of a company is obliged to take all reasonable care in their business processes. This includes compliance with recognised security measures. In Germany, various laws are applicable, such as the Act for Corporate Control and Transparency (KonTraT - Gesetz zur Kontrolle und Transparenz im Unternehmensbereich), the Law on Limited Liability Companies (GmbHT - Gesetz betreffend die Gesellschaften mit beschränkter Haftung) or the Stock Corporation Act (AktT - Aktiengesetz), from which corresponding obligations and liabilities for the management or the board of a company can be derived in relation to risk management and information security.
- Proper processing of payment-relevant information is governed by different laws and regulations. In Germany they include among others, the Commercial Code (Handelsgesetzbuch HGB e. g. §§ 238 et seq.) and the Tax Code (AO Abgabenordnung). Proper processing of information implies their secure processing, of course. Both must be proven regularly in many countries, for example by auditors as part of the audit of annual accounts. If serious security deficiencies are identified, a positive audit report will not be issued.
- In many industries (e. g. the automotive industry), it is common that manufacturers commit their suppliers to meet certain quality and safety standards. Analogically, more and more requirements are placed on information security. If a contractor violates contractually regulated security requirements, this can result in penalties and even termination of contracts up to and including loss of business relations.

Few security requirements arise directly from laws. The legislation generally orientates itself however, on the standards in technology as a common basis for assessment of an achievable security level. If there is no healthy balance between the existing security measures in an institution and the sensitive information in the current state of technology, this can have serious consequences.

T 0.30 Unauthorised Use or Administration of Devices and Systems

Without appropriate mechanisms for entry, admission and access control, unauthorised use of devices and systems virtually can neither be prevented nor detected. The basic mechanism IT systems use for this is user identification and authentication. But even in IT systems with a strong identification and authentication mechanisms, unauthorised access is still conceivable, if the corresponding security features (passwords, chip cards, tokens, etc.) fall into the wrong hands. Also, when assigning and maintaining permissions, many mistakes can be made, for example, if authorisations are granted too liberally or given to unauthorised persons, or if they are not regularly updated.

When granted illegal access to devices and systems, unauthorised persons can intercept confidential information, carry out manipulation or cause disruptions.

A particularly prominent special case of unauthorised use is unauthorised administration. If unauthorised persons change the configuration or operating parameters of the hardware or software components, severe damage can be the consequence of such action.

Examples:

– When examining log files, a network administrator came across inexplicable events occurring on different days but often early in the morning and in the afternoon. After a closer examination, it turned out that a wireless router was not configured properly. People waiting at the bus stop outside the office building have used this access to surf with their mobile devices on the Internet while waiting for the bus.

T 0.31 Incorrect Use or Administration of Devices and Systems

Incorrect or improper use of devices, systems and applications may affect their security, especially when existing security measures are ignored or circumvented. This often leads to disruptions or failures. Depending on what types of devices or systems are used improperly, confidentiality and integrity of information may also be violated.

A particularly prominent special case of improper use is the improper administration. Errors in the installation, configuration, service and maintenance of hardware or software components can result in severe damage.

For example, too generously granted access rights, easy-to-guess passwords, inadequately protected data storage media containing backups or terminals not being blocked during a temporary absence can lead to security incidents.

In the same way, data can also be accidentally deleted or changed due to improper use of IT systems or applications. Confidential information can thus be available the public if, for example, permissions are set incorrectly.

If power or network cables are laid unprotected, they can be inadvertently damaged, which can cause an outage. A cable connection can be pulled out when staff or visitors stumble over it.

T 0.32 Abuse of Authorisations

Depending on their roles and tasks, people are granted corresponding entry, admission and access rights. In this way, the access to information is on one hand controlled and monitored, and on the other hand, people are enabled to carry out certain tasks. For example, individuals or groups need specific permissions to use applications or edit information.

A misuse of privileges occurs when intentionally legally or illegally obtained permissions are used outside of the scope of intended use. The aim is thereby often to gain personal benefit or to harm a specific person or institution.

In many cases, due to historical, system-related or other reasons, people have higher or more comprehensive entry, admission and access rights than they need to in order to perform their activities. These rights can be misused for attacks under certain circumstances.

Examples:

- The finer the granularity of access rights to information, the greater the effort required to keep these permissions up to date. There is therefore a risk that when granting the access rights, too little differentiation is being made among the various roles which facilitates the abuse of authorisations.
- In various applications, access permissions and passwords are stored in system areas, which can be accessed by other users. This would allow attackers to change permissions or retrieve passwords.
- Persons with too generously granted permissions can be tempted to access files belonging to other users, for instance to read another person's email if certain information there is urgently needed.

T 0.33 Absence of Personnel

Absence of personnel can have a significant impact on an institution and its business processes. Staff may be missing unexpectedly due to illness, accident, death or strike, for example. Furthermore, also the predictable personnel absences in cases of leave, training or regular termination of contract must be taken into account, especially if the remaining working time is reduced, for example, by a right to take annual leave. Absences of personnel may as well be caused by an internal realignment of resources.

Keyposition in the business process

In all these cases, critical tasks may in consequence no longer be performed due to absence of personnel. This is especially critical if the person plays a key role in a business process and cannot be replaced by another person due to lack of expertise. Disruptions in the IT operation may be the result. Thus, other areas and processes of the institution can be substantially impaired.

Loss of expertise and trade secrets

A loss of personnel may additionally include a considerable loss of expertise and trade secrets, which makes the subsequent transfer of activities to other people impossible.

Examples:

- Due to a prolonged illness, the network administrator of a company remained out of office. In the affected company, initially the network ran flawlessly. After two weeks however, after a system crash, no one was able to fix the problem because there was only one administrator familiar with operation of this network. This led to a network failure which lasted several days.
- During the vacation of an administrator, the institution needed to access the backup media in backup data safe. The access code to the safe was only changed recently and was only known to that administrator. The data recovery could only be performed after several days, because the administrator was not available earlier due to his vacation.
- In the event of a pandemic more and more personnel become unavailable in the longer term, either due to the disease or due to the necessary care for relatives or children. Also because of fear of contagion in public transportation or in the institution, some employees remain out of office. As a result, only the most necessary work can be done. The required maintenance of systems, be it the central server or the air conditioning in the computing centre, is not performed any more. Gradually, more and more system failures occur.

T 0.34 Attack

An attack can constitute a threat to an institution, certain areas of the institution or individuals. The technical possibilities to perpetrate an attack are numerous: throwing bricks, blasts by explosives, use of firearms or arson. Whether and to what extent an institution is exposed to the danger of an attack depends not only on the location and environment of the building but on the institution's activities and the socio-political climate. Companies and public bodies that operate in politically controversial areas are more at risk than others. Institutions close to the usual demonstration staging areas are more at risk than those in remote locations. To assess the level of threat or when suspecting the threat of politically motivated attacks, criminal investigation authorities or the Federal Bureau of Criminal Investigation (Bundeskriminalamt) can be consulted.

Many documents in a small room space

In the case of archives, threat assessment must take into account a special circumstance: They store a large number of documents and data in a relatively small space. This can be, for example, medical records, contracts, deeds or wills. Their destruction can have far-reaching implications, not only for the archive, but also for other users. For example, it may be necessary in such a case, that the lost data must be re-collected or newly recorded with great effort. Under certain circumstances some data will even be irrevocably lost. Attacks on paper-based and electronic archives can therefore cause substantial damage.

Examples:

- In the 1980s, a bomb attack was perpetrated on the data centre of a large federal agency in Cologne. Due to the large penetrating power of the explosive device, not only windows and walls, but also many information systems in the data centre were destroyed.
- In the attack on the World Trade Center in New York on the 11th of September 2001, not only were many people killed but also were a number of IT facilities destroyed. As a result, several companies had considerable difficulty in continuing their business activities.

T 0.35 Coercion, Extortion or Corruption

Coercion, extortion or corruption may affect the security of information and business processes. Using threats of violence or other detriments an attacker can, for example, try to make the victim disregard security guidelines, or to circumvent security measures (coercion).

Instead of threatening, attackers can also purposefully offer employees or other person's money or other benefits to make them an instrument for security violations (corruption). For example, there is a risk that a corrupt employee will forward confidential documents to unauthorised persons.

In principle, by coercion or corruption, all basic parameters of information security may be affected. Attacks can be aimed at, amongst other things, forwarding confidential information to unauthorised persons, manipulating business-critical information or disrupting the smooth execution of business processes.

Particular danger exists if such attacks are aimed against high-profile executives or persons in special positions of trust.

T 0.36 Identity Theft

In the case of identity theft, an attacker assumes a false identity, he takes advantage of information about another person, to act on his or her behalf. Here, data such as date of birth, address, credit card or bank account numbers are used in order, for example, to gain access to an Internet provider or to gain financial benefits in other ways. Theft of identity often leads directly or indirectly to damage of reputation, but also elucidating the causes and preventing the negative consequences for those affected is time-expensive. Some forms of identity fraud are also known as masquerade.

Identity theft occurs most frequently where identity verification is handled too carelessly, especially if expensive services are based on it.

A person who has been misled in respect to the identity of his or her communication partner can be easily persuaded to reveal sensitive information.

Examples:

- To register with various email providers or auction platforms on the Internet, it sufficed to invent a fictitious name and to provide a suitable address from the phone book with it. At first, attackers could register using recognisable fictitious names, for example, derived from cartoon characters. As stronger plausibility checks were later introduced for this purpose, names, addresses and account numbers of real people have been used. Those affected have only learned about a fraud, when the first claims for payment arrived.
- The sender address of emails can be easily spoofed. It happens again and again that users are this way fooled into believing that an email comes from a trusted communication partner. Similar attacks are possible by manipulation of caller ID for voice calls or by manipulating the sender identity for fax connections.
- An attacker may use a masquerade to try to enter into an already existing connection without having to authenticate himself, since this step has already been performed by the original communication participants.

T 0.37 Reputation of Actions

People can deny, for various reasons, to have committed certain acts for example, because these acts violate instructions, security guidelines, or even laws. But they could also deny having received a notification, for example because they have forgotten a deadline or an appointment. The field of information security is focused on accountability, a property predestined to ensure that committed acts cannot be denied without justification. Generally the term non-repudiation is used here.

In a communication there is a further distinction, whether a communication participant denies the receipt of messages (Repudiation of Receipt) or sending of messages (Repudiation of Origin). Repudiating the receipt of messages can be of relevance for, amongst other things, financial transactions when someone denies having received an invoice at a due date. Likewise, it may happen that a communication participant denies sending messages, e. g. denies having issued a purchasing order. Message sending or receiving mail can be repudiated in the case of post messages as well as fax or email messages.

Examples:

– An urgently needed spare part has been ordered electronically. After a week it is claimed still to be missing, in the meantime high losses due to production outage are incurred. The supplier denies having ever received an order.

T 0.38 Abuse of Personal Data

Personal data is almost always particularly sensitive information. Typical examples include information about personal or factual circumstances of an identified or identifiable natural person. If the protection of personal data is not sufficiently guaranteed, the danger exists that the person will be impaired in his or her social position or economic conditions.

An abuse of personal data takes place if an institution collects, for example, too much personal data, collects it without legal basis or consent, uses it for purposes different from the objective stated at the time of collecting, deletes personal data too late or discloses such data in an unauthorised manner.

Examples:

- Personal data may be processed only for the purpose for which it was collected or stored for the first time. It is therefore inadmissible to use log files for attendance and monitoring conduct, if they were designed to store information on users' logging on to an IT system and logging off merely for access control.
- Persons who have access to personal data could disclose them in an unauthorised manner. For example, an employee at the front desk of a hotel could sell the guests' registration information to advertising companies.

T 0.39 Malicious Software

Malicious software is software developed with the aim of performing unwanted and often harmful operations. Typical kinds of malicious software include viruses, worms and Trojan Horses. Malicious software acts usually in a secret way without the user's knowledge or consent.

Nowadays, malicious software offers an attacker comprehensive communication and control possibilities, and makes a variety of functions available. Amongst other things, malicious software can purposefully reveal passwords, remote-control systems, deactivate data protection software and spy on data.

The most significant damage here is loss or corruption of information or applications. But also the loss of reputation and financial damage, caused by malicious software, are of great importance.

Examples:

- In the past, the malicious software W32/Bugbear was spread in two ways: it searched in local area networks for computers with shares, where write access was possible, and made copies of itself on each share found. Moreover, it sent itself as an HTML-email to recipients in the email address books of infected computers. Due to an error in the HTML routines of certain email programs, the malicious software was executed upon opening the message without further action by the recipient.
- The malicious software W32/Klez spread in different variants. Infected computers sent the virus to all recipients in the email address book of the computer. After this virus had infected a computer, by continuous manipulation of the operating system it prevented the installation of anti-virus programs from most popular manufacturers and made it significantly more difficult to perform disinfection of the infected computers.

T 0.40 Denial of Service

There are a variety of different forms of attack, all aiming at disruption of the intended use of certain services, functions or devices. The generic term for such attacks is "Denial of Service". Often the term "DoS-attack" is used.

Such attacks can come, amongst others, from disgruntled employees or customers, but also from competitors, extortionists or politically motivated perpetrators. The aim of the attacks can be business-relevant values of any kind. Typical forms of DoS attacks are:

- Disruptions of business processes, for example, by flooding the order processing with improper orders,
- Damage to the infrastructure, for example by blocking the doors of the institution,
- provoking IT failures by e. g. purposeful overloading services of a server in the network.

This type of attack is often associated with distributed resources, the attacker generates such a high demand for these resources that they are no longer available for the actual users. In IT-based attacks, the following resources can be artificially made scarce: processes, CPU time, memory, disk space and transfer capacity.

Examples:

- In spring 2007 in Estonia strong DoS attacks on numerous Internet sites over a prolonged period of time took place. This led to significant impairments in the use of information services and Internet services in Estonia.

T 0.41 Sabotage

Sabotage is the deliberate manipulation of or damage to objects or processes with the aim of inflicting damage to the victim by acting this way. Particularly attractive targets can be data centres and the communication connections of public bodies or companies, since there a great effect can be achieved with relatively few resources.

Selective manipulation

The complex infrastructure of a computer centre can be affected by selective manipulation, when possibly external perpetrators but also primarily intruders from inside actively influence important components to provoke operational disruptions. In this regard, insufficiently protected technical building systems and communication infrastructure as well as central supply points are particularly threatened if they are left unobserved in organisational and technical terms and can be easily accessed by externals without being noticed.

Examples:

Power supply

– In a mainframe computer centre, a manipulation of the uninterrupted power supply led to a temporary total failure. The perpetrator had repeatedly manually switched the uninterrupted power supply to bypass mode and then manipulated the main power supply of the building. Altogether there were four failures within three years. Even hardware was partially damaged. The disruption took between 40 and 130 minutes.

Flooding

– Sanitary facilities were also located within a data centre. Due to blockage of the drains and the simultaneous opening of the water supply, water penetrated into central technology components. Damage caused this way resulted in interruptions of operation in the production system.

Electronic archives

– Electronic archives present a particular risk of sabotage, since there, many sensitive documents are kept on a small floor space. Because of this aspect, by targeted unsophisticated manipulation a great deal of damage can be incurred under certain circumstances.

T 0.42 Social Engineering

Social engineering is a method to gain unauthorised access to information or IT systems through social action. In social engineering advantage of human qualities are taken of such as e. g. helpfulness, trust, fear or respect for authority. As a result, employees can be manipulated so that they act in an inadmissible way.

A typical case of attacks with the help of social engineering is the manipulation of people by phone calls where the attacker introduces himself as for example:

- a secretary whose boss must do something quickly, but has forgotten his password and needs it urgently now.
- an administrator, calling because of a system error, since he needs the user's password to fix the problem.

If such attackers are being asked critical questions in return, the enquirer is supposedly "just a temporary help" or an "important" personality.

Another strategy for systematic social engineering is to develop a longer relationship to the victim. Unimportant but numerous phone calls in advance serve the attacker to gain knowledge and build up confidence that he can make use of later.

Such attacks can also be multi-stage attacks, where in further steps knowledge and techniques are used, which have been acquired in the previous stages.

Many users know that they must not reveal their passwords to anybody. Social engineers know this and therefore must reach the desired aim using other ways.

Examples for this are:

- An attacker can ask the victim, to execute commands or applications unfamiliar to him or her, for example, because this will help to solve an IT problem. This may be a hidden command to change access rights. This allows the attacker to access sensitive information.
- Although many users are using strong passwords, they are however used for multiple accounts. If an attacker can provide a useful network service (such as an email address system), for which the user must authenticate him or her self, he can get access to the desired passwords and logins. Many users will use the same credentials they chose for this service also for other services.

If attackers gain passwords or other authentication features in an unauthorised way, for example by means of social engineering, this is often referred to as "phishing" (a portmanteau word from "password" and "fishing").

During social engineering the attacker is not always visible. Often the victim never recognizes that he or she was being exploited. If successful, the attacker does not have to face the risk of legal sanctions and also has a source for obtaining additional information later.

T 0.43 Replaying Messages

In this form of attack, attackers send specially prepared messages to individuals or systems with the aim of gaining an advantage for themselves or to cause damage to the victim. To construct the messages in a proper way, attackers use interface descriptions, protocol specifications, or records logging of the communication behaviour from the past.

In practice, there are two important special cases of message replay:

Replay

– In a "replay attack" (replay of messages) attackers record valid messages and play this information at a later time almost unchanged.Also only part of a message may suffice, such as a password, to enter into an IT system without authorisation.

Man-in-the-middle

– In a "man-in-the-middle attack" the attacker assumes unnoticed a mediating position in the communication among various participants. In general, the attacker pretends here to be the sender of a message to the intended recipient, and he pretends to the recipient that he is the actual sender. If successful, the attacker can receive messages, which are not intended for him, evaluate them and purposefully manipulate them before they are forwarded to the intended recipient.

An encryption of the communication does not protect against man-in-the-middle attacks, if no secure authentication of communication partners is performed.

Examples:

– An attacker records the authentication data (e. g. user ID and password) during a user’s login and uses this information to gain access to a system. In purely static authentication protocols a password, also if it is transferred in an encrypted way, can be used to illegally access a third party system.

– To cause financial harm to the employer (company or public body), an employee places an approved purchase order several times.

T 0.44 Unauthorised Entry to Premises

If unauthorised persons gain illegal entry into a building or individual premises, this can lead to various other dangers. These include theft or manipulation of information or IT systems. In qualified attacks time is crucial, in which the perpetrators can pursue their goal undisturbed.

Often the perpetrators want to steal valuable IT components or other goods that can be easily sold. However, the target of an intrusion, among other things, can be to gain access to confidential information, perform manipulations or disrupt business processes.

Unauthorised intrusion into premises can thus result in multiple types of damage:

- Damage can occur already due to the very entry into property in an unauthorised manner. Windows and/or doors are forced open and hence damaged, they must be repaired or replaced.
- Stolen, damaged or destroyed equipment or components must be repaired or replaced.
- Damage due to breach of confidentiality, integrity or availability of information or applications can occur.

Examples:

Vandalism

- During a night-time intrusion into an office building the perpetrators did not take a worthwhile trophy. Due to frustration about this, they emptied the powder extinguishers into the offices. The burglary damage was minor, however, the costs of cleaning and work interruptions disproportionately high.
- A break-in into a company during one weekend caused only minor damage due to levering a window open, only one coffee cup stolen and smaller pieces of furniture taken away. During a routine inspection, however, it turned out later that a central server has been skilfully manipulated exactly at the time of the intrusion.

T 0.45 Data Loss

Manipulations

Data loss is an event that leads to a situation where stored data cannot be used as required (loss of availability). A common form of data loss occurs when data is inadvertently or illegally deleted, for example by accidental misuse, malfunctions, power outages, pollution or malicious software.

Data loss may also occur due to damage, loss or theft of devices or data storage media. This risk is extremely high in case of mobile terminals and removable data storage media.

Furthermore, it should be noted that many mobile IT systems are not always online. The data stored on these systems is therefore not always up to date. When data is synchronised between the mobile and stationary IT systems, carelessness or malfunction may lead to loss of data.

Examples:

- A PDA falls out of a shirt pocket and shatters into pieces on the tiles, a mobile phone is retrieved by a dog instead of the newspaper, unfortunately with consequences. These and similar events are the causes of many total losses of data on mobile devices.
- There is malicious software that purposefully deletes data on infected IT systems. Some pests execute the delete function not immediately upon infection, but only when a defined event occurs, for example, if the system reaches a certain date.
- Many internet services can be used to store information online. If the password is forgotten, and is not stored, it may happen that the stored information cannot be accessed any more if the service provider does not offer a suitable method to reset the password.
- Hard drives and other storage media have a limited lifetime. If no suitable redundancy measures are undertaken, technical defects may result in loss of data.

T 0.46 Loss of Integrity of Sensitive Information

The integrity of information can be impaired by various causes, such as by manipulation, misconduct of individuals, misuse of applications, software failures of transmission errors.

– Due to the aging of data storage media, loss of information can occur.

– During data transfer transmission errors may occur. Transmission errors

– Malicious software can destroy or modify entire databases. Malicious software

– Due to incorrect input, undesired transactions may occur, which often remain unnoticed for a long time. Incorrect input

– Attackers may try to manipulate data for their purposes, e. g. to gain access to other IT systems or databases.

– Manipulating the index database can prompt electronic archives to archive or retrieve false documents.

If the information loses integrity, it can cause a variety of problems:

– In the simplest case, information cannot be read and hence further processed.

– Data can be accidentally or intentionally falsified to the extent that false information is passed on. In this way transfers with wrong amounts, for instance, or to the wrong recipient can be triggered, the sender data in an email can be manipulated and many more.

– If encrypted or compressed data loses its integrity (in this case it is enough to change just one bit), it cannot be decrypted or respectively decompressed under certain circumstances.

– The same applies to cryptographic keys, also here changing a single bit can make the keys useless. This also has a consequence that data can no longer be decrypted or their authenticity cannot be verified any more.

– Documents stored in electronic archives, lose their probative value, if their integrity can be questioned.