INDUSTRY 4.0 for VET

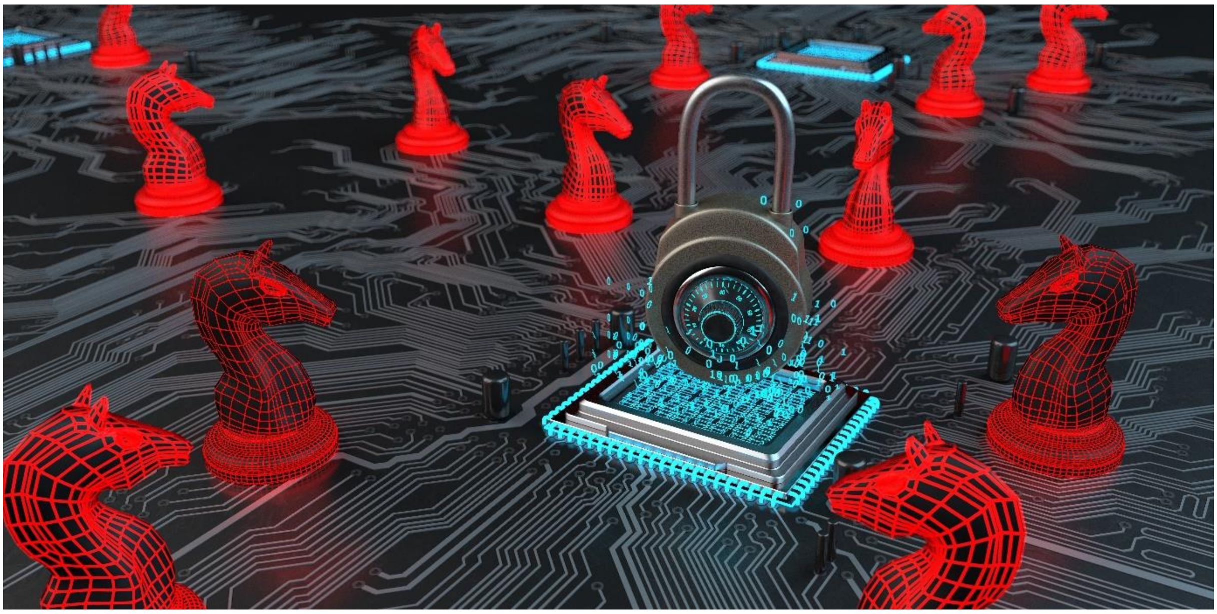
5. IT-SECURITY

5.1 The topic

The first introduction

Backing up data has been easier before. In the past, important documents such as contracts or savings books were usually locked away in safes or simply hidden. This ensured that unauthorized persons could not gain access at all or only with great difficulty.

Today, it is no longer that simple. Documents and data are now digitalized and often no longer physically available. Think, for example, of your online banking, important contracts that are signed electronically and sent by e-mail, or private data such as photos. Just as analogue documents used to be "locked away", nowadays data must also be digitally backed up. Because potential data theft or illegal processing or manipulation of data can carry high risks and serious consequences - both for private individuals and for entire companies and organizations.



IT security, also “information security”, is not a new topic - but it is becoming increasingly important due to the rapid digital developments in recent years. We should be familiar with it, because digital information, whether we are aware of it or not, is simply the basis of modern life.

The practical relevance - for this you will need the knowledge and skills

From private life to work, from individual companies to global corporations - data and information are present in all areas of life and are a valuable asset. Whether it's cybercrime, data loss or data forgery - IT security should really concern everyone. This learning unit will help you to ensure the security of your private data and make a valuable contribution to data security in your company. You will be sensitized for IT security to act confidently in this regard.

Learning objectives and competences at a glance

In this chapter you will learn about the term IT security in its most important facets. You will learn more about its meaning and goals, but also what threats and measures currently exist in the area of IT security. You will learn how you can personally contribute to a more secure information environment - both privately and professionally.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Learning Objectives
Know and understand the general definitions and application areas of IT security.
Being able to name and explain the goals and tasks of IT security.
Get to know current IT threats and be able to assign them to IT security in the areas of application.
Know measures and defense mechanisms of IT security in the application

5.2 Definitions and areas of application

Right away: **IT security is not just information security** – although often both terms are used in the same way (especially if not exactly translated from English into another language), there is a subtle difference which will help you to define the term.

In principle, this difference is the "T" in the name - because IT security stands for "Information Technology Security". But that sounds rather bulky - that's why we prefer to stick with "IT security".

Definition

Information security vs. IT security

The term **information security** means protective measures for ALL systems that process or store information in any way. It does not matter whether these are digital or "analogue". So the computer is meant as well as a stack of handwritten, confidential documents.

IT security is a subarea of information security. In fact, only the protective measures of so-called "socio-technical" systems are meant here. Socio-technical systems are nothing more than systems in which humans use information technology to store and process data.

Incidentally, according to the dictionary, **information technology** is defined as "technology for the collection, transmission, processing and storage of information by computers and telecommunications equipment".

So far so good. However, since nowadays only in very few exceptional situations no IT is used at all, IT security covers a very large part of information security.
An example of an IT-less application of information security might be the hand-written secret recipe in the safe of your favourite restaurant. But that is not what this unit is about.
There are also other sub-concepts in IT security whose initial overview is worthwhile - especially how they are connected:

- **Computer security:** This refers specifically to the security measures of local and networked computer systems themselves. How safe is a computer from unauthorized access or manipulation? What happens if a computer "crashes"?

- **Data protection:** The term is a real buzzword – quite rightly, because "data protection is personal protection". This aspect is the most important one for the private person, because it is about the protection of one's own personal data from misuse. Privacy and anonymity are a sensitive issue in a digitalised world.

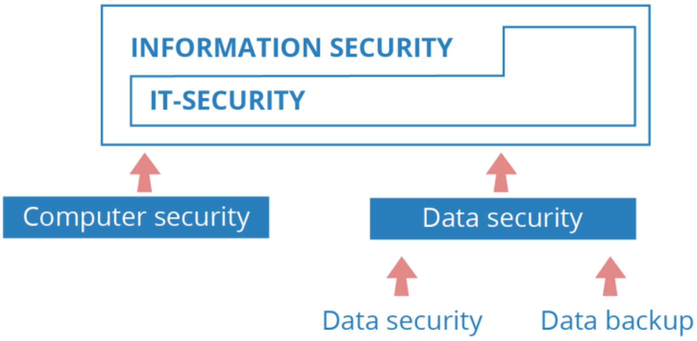
- **Data security:** This is again, of more technical nature. It is not so much a question of legal issues, but simply how to protect data from manipulation or loss. Data security can be understood as the technical preliminary stage for successful data protection.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Data backup:** This is specifically about (multiple) backups of data - you are most likely familiar with the term "backup". And nothing else is data backup too: the correct duplication of data to prevent its loss.

The following diagram makes the context of all the terms learnt clearer:



IT security makes up a large part of information security and consists mainly of computer security and data security. Data security is the basis for successful data protection and data backup.

Important

Data and information

Now you have read the terms "data" and "information" so often, you will surely want to know the difference:

- Data are actually useless signs and symbols - without context, this data remains empty and there is nothing to do with it. Let's just take the sequence of numbers 19081974, for example.

- Information is data that is placed in a context. This data then becomes meaningful and transports information, for example Date of birth 08-19-1974 - it is already clear what was meant by the sequence of numbers.

By the way, this is also the basic idea behind encryption, no matter whether it is done on the computer or by hand. You leave data without context, maybe even mix it up. Only someone who also understands the context can understand the meaning of the sequence of numbers.

For whom is the implementation of IT security now important?

Actually, for everyone with a computer - whether as an individual or in an organisation. Nevertheless, it helps to classify the implementation areas of IT security a little more precisely, also in order to be able to later assign the threats and corresponding measures to the correct area of application.

The main distinction is whether devices and data are used privately or within an organization.

Private sector: This concerns individuals and devices that are used privately. This includes your own laptop or smartphone, for example. Whether you use it publicly, for example in the WLAN of a university, is of secondary importance - the important thing is that you use the device to manage your private data.

Companies and organizations: These are devices that can be used to access the data of companies or organisations - for example, company laptops or company telephones. This refers to both commercial enterprises and state companies and organizations it is about *shared data*, that belong to an organization.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

What exactly are the differences between these two areas of application?

- **Private area**

  Almost every software always has programming errors in some way or another. This can be due to inaccuracy, but also simply due to ignorance - because nobody can know by which "backdoor" or by which special feature in the software code unwanted access can be gained.

  This is particularly problematic because most devices are constantly connected to the Internet. These include the private computer, the smartphone, the smartwatch, but also the television or the voice assistant. In most cases, the "break-in" or unauthorized access to personal data is then carried out via the Internet. Data theft can also take place physically, e.g. by breaking in and stealing the computer.
  It should be noted: it can happen quickly and passwords for online banking are stolen, important documents are lost, or private photos are public.

  IT security is an important topic in the private sector - yet the applied means of IT security are less pronounced in this area - be it due to a lack of awareness on the part of the persons using the system or also due to fewer technical possibilities.

- **Companies and organisations**

  When it comes to IT security in companies, the main focus is of course on economic interests. Although the technical implementation of IT security is usually better than in the private sector, the criminal energy behind possible IT attacks is much higher.

  One thinks of banks and insurance companies that manage a lot of money. Or technical high-tech companies that want to secure their prototypes and ideas from the competition.
  Here too, IT systems are now connected via the Internet. An example of this would be the use of a cloud service from several company locations: a cloud server provides storage space for documents that can be read and edited over the Internet from all locations. Here, it must above all be ensured that only authorized persons can access these documents.

  Large companies now have their own departments that only deal with IT security and invest a lot of money to stay up-to-date. Because here, too, the following applies: HOW an IT attack will happen is not known beforehand - so the main thing is to be able to react quickly IF an attack occurs.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

By the way, there are standardised documents for IT security, so-called basic protection catalogues, which present detailed IT security models. However, IT is developing so fast that following these catalogues alone is not enough and some of them quickly become outdated.

Remember
IT security is a subarea of information security and means all protective measures in the processing and storage of data with the help of information technology systems. This includes computers as well as all other means of telecommunication in private and business environments. IT security can also be defined in sub-areas that are linked together: • Computer Security • Data protection • Data backup • Data security The areas of application of IT security can be assigned to the private as well as the corporate and public sector. Since most devices are connected to the Internet, the dangers of IT attacks and the measures for IT security are quite similar in all areas - differences can be found in personal awareness and technological factors.

5.3 Goals and tasks of IT security

The most important task in IT security is **to follow the technical developments.** The digitalising and networking world is progressing very rapidly in terms of technology. New technologies require new software, new areas of application require new security measures.

Whereas in the past a few large computers simply took over tasks for entire companies and were operated by a few people, today there are a myriad of small devices that are all interconnected.

It can be quite tricky to even explain what exactly is to be protected from what, what threats there are and what gaps in security systems could be exploited.

However, so-called **protection goals** are defined - these are considered the "main goals" of any IT security. These are:

confidentiality - integrity – availability

If you consciously take these three protection goals to heart, you have already implemented half of the IT security! This is what they look like in detail:

- **Confidentiality**
  Data, information and resulting knowledge should be hidden from persons who have no right to view them.

- **Integrity**
  Data, information and resulting knowledge should be protected against unauthorized changes and manipulation.

- **Availability**
  Data, information and resulting knowledge should be accessible to those who have permitted access, if necessary.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

These three objectives are so important and central because they are equally important in the private and business context. Take a look at the following examples:

Examples

The three protection goals in a private context using the example of "online banking”
You use the online access to your bank account. This is a sensitive issue, because your money is at stake. How are the protection goals fulfilled here?

- Confidentiality: Your access and account data and passwords should only be accessible to you.
- Integrity: No one, but you should be allowed to make unauthorised online transfers.
- Availability: You should have unlimited access to your account at any time and from anywhere.

The three protection goals in the corporate context using the example of "product development
A company develops a completely new product that should revolutionise the market. Of course, this should happen without the competition profiting from it. How could the protection goals be fulfilled here?

- Confidentiality: All information about the development of the new product can only be viewed by authorized persons.
- Integrity: Data obtained from the development of the product is protected against sabotage and manipulation from outside.
- Availability: All involved and authorized persons have secure access to the development of the new product and the resulting data.

In addition, there are also extended protection goals that have to be considered according to requirements. These do not necessarily have to be anchored in IT security and can vary greatly in the private and corporate context.

- **Accountability** or **Anonymity**
  An action in the IT environment can be clearly assigned to a person - or not. In the corporate context, the person responsible for internal sabotage, for example, can be identified. In private life, by the way, the opposite is more likely to happen, namely that the person enjoys the greatest possible anonymity in connection with his or her data - for example, when researching health-related topics on the Internet.

- **Authenticity**
  Data, information and resulting knowledge should be verifiable for authenticity, for example whether transmitted research results are original or have been manipulated by a third party.

- **Non Repudiation**
  Actions in an IT environment should not simply be denied - this is particularly important for electronically processed contracts. Here, for example, electronic signatures are used.

How are these goals to be achieved in practice?

This question is all about **weaknesses**. Or rather, it's about finding and eliminating vulnerabilities. As you have already learned, all software has weaknesses. These are not clearly identifiable as such in advance. Often it is due to poor programming of the software used or the design of the IT system. This does not necessarily mean that "wrong" programming has been done, but simply that not all known IT threats have been considered in the programming. However, weak points can also be the human being or the wrong handling of IT systems.

Important
Of course, IT security can **also bypass via the hardware** not only via the software. But this is more "impractical" - because in order to manipulate or steal data via the hardware, you have to be physically present, for example with a USB stick in your hand or by stealing the entire computer. So, accessing the software via the Internet is already more convenient - and above all more difficult to track if you get caught in the middle.

In order to achieve the protection goals of IT security, it is therefore of enormous importance to identify these weaknesses and possible threat scenarios. And this is where it becomes difficult, because a 100-percent representation of all weak points is not possible at all due to the constant development of the systems and the general inability to look into the future - one can only approximate as closely as possible.

Remember
IT security **strongly depends on the current technological developments** – new areas of application of information technology also involve new dangers. Here, a quick reaction is required to be able to offer appropriate countermeasures. There are **three protection goals** that must be met in all areas of application: • Confidentiality • Integrity • Availability

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

There are three additional protection goals, which vary according to the area of application and should be considered accordingly:

- Attributability or anonymity
- Authenticity
- Commitment

To achieve these protection goals **the core task of IT security to identify weak points of systems** and to eliminate them accordingly. This can also affect hardware, but currently rather software - this refers mainly to programming errors or unconsidered weaknesses in programming.

Perfect IT security can only be approximated, but not 100 percent fulfilled. That is why IT security must be treated as a whole.

5.4 Threats in IT

Threats in IT are manifold and do not necessarily have to be intentional or criminal in nature. IT can also be threatened by "force majeure" and/or technical failure - for example, an earthquake could cause a power outage that results in data loss.

But of course, human error is also conceivable. A classic example of this is: the password for online banking has been forgotten - so the information would then no longer be available.

You will now learn about the possible IT threats - always keep the protection goals of the previous chapter in mind.

Important

By the way, a potential threat or vulnerability does not automatically mean that the IT is at risk. An actual threat is only considered to be a threat if vulnerability (e.g. programming error or easily accessible WLAN) also meets a threat (e.g. hacker attack).

Targeted attacks by people or organisations

First and foremost, of course, it is attacks that are deliberately carried out that must be averted by IT security. Usually referred to as "hacking", an individual or even an entire organization gains unauthorized access to foreign data and tries to circumvent the protection goals. This can have various reasons: Theft of funds, sabotage of competing companies, political motivation, sometimes just "fun" - but it is always a matter of obtaining, manipulating or destroying foreign information via the network to which the target devices are connected.

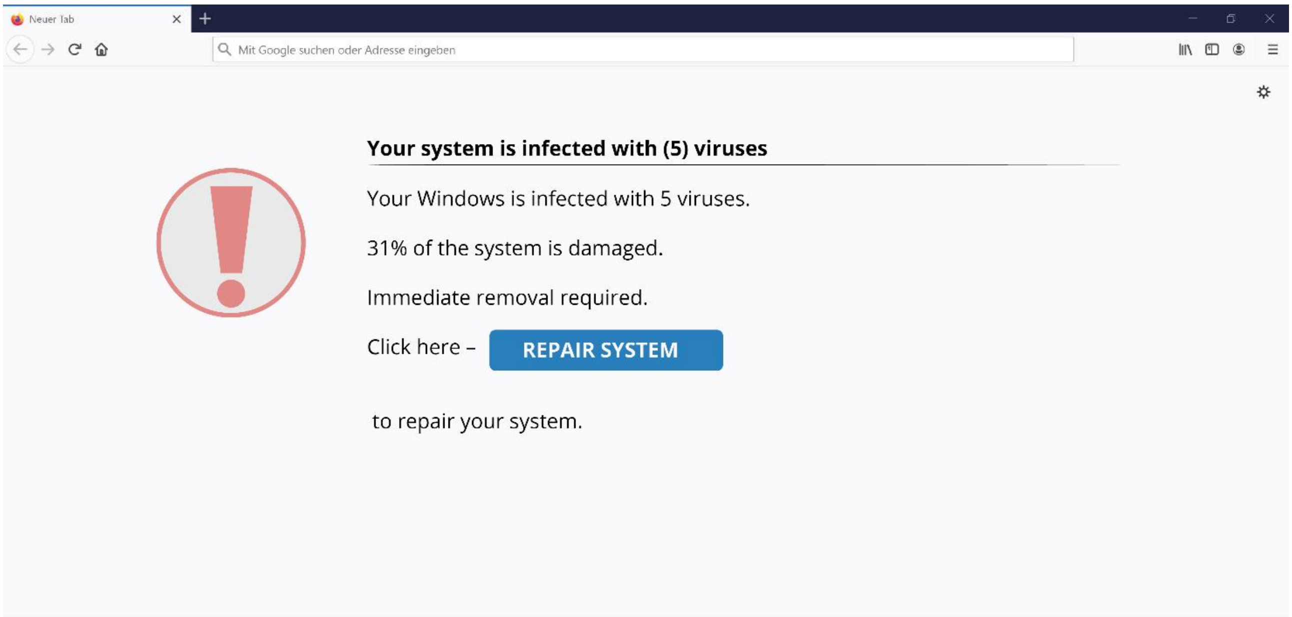
The most important tools of such hacking attacks are known from Hollywood movies of the turn of the millennium and usually have funny names - "viruses", "trojans", "worms", "spoofing", "phishing" and others. Let's take a closer look at some of these examples:

- **Virus**
  Computer viruses are quite simply programs that automatically perform their programmed task in the target systems: for example, to track down a password. Viruses need a so-called host to spread

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

them. This can be a mass email or a so-called "pop-up" - a self-opening website, for example, which points to an allegedly necessary update.



Your system is infected with (5) viruses

Your Windows is infected with 5 viruses.

31% of the system is damaged.

Immediate removal required.

Click here – REPAIR SYSTEM

to repair your system.

- **Worms**
  These are viruses that can actively spread themselves - this means that they actively detect weak points in systems and networks and forward themselves accordingly without a so-called "host" being present.

- **Trojans**
  Also known as "Trojan horses", these are apparently useful programs that the victim installs himself - but in the background, Trojans independently open backdoors in the system, forward data and information and can, for example, record passwords that are entered.

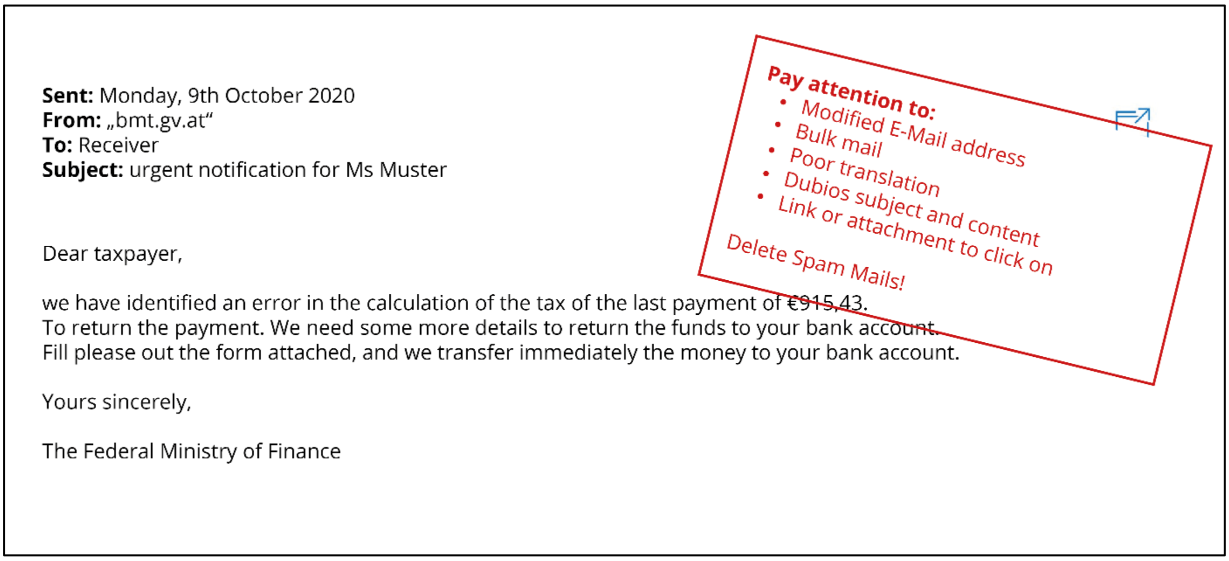
- **Denial-of-Service-Attacks**
  Here, the availability of the data is more likely to be manipulated - by deliberately overloading the system from outside (this can be done, for example, by automatically repeatedly calling up a website), the system is brought to a standstill. Sometimes this happens until the affected organization pays a ransom, for example. By the way, software for blackmailing methods is also referred to as "ransomware".

- **Spoofing/Phishing**
  This is mainly about identity theft. Fake websites on the Internet and emails that link to them entice the victim to actively share passwords or account information. These are mainly found in the private sector of IT security.

- **Spam**
  By the way, the probably best-known term in IT security describes nothing more than unsolicited emails - these can be annoying newsletters, but of course also hosts of viruses or phishing attempts.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



Sent: Monday, 9th October 2020
From: „bmt.gv.at“
To: Receiver
Subject: urgent notification for Ms Muster

Dear taxpayer,

we have identified an error in the calculation of the tax of the last payment of €915,43.
To return the payment. We need some more details to return the funds to your bank account.
Fill please out the form attached, and we transfer immediately the money to your bank account.

Yours sincerely,

The Federal Ministry of Finance

Pay attention to:

- Modified E-Mail address
- Bulk mail
- Poor translation
- Dubios subject and content
- Link or attachment to click on

Delete Spam Mails!

The above-mentioned malware can of course also be personally "injected" into the computer system - information can be stolen or manipulated by physically breaking into the company building or home. Due to the networking of computer systems, however, this is usually no longer necessary.

But sometimes such physical manipulation happens simply internally. For example, when your own company personnel steal customer data or product secrets without authorisation in order to sell them externally.

Unintentional threat of human error

But threats to IT security do not always have to be highly criminal and deliberate. Sometimes it is simply ignorance in dealing with IT that poses a threat:

- **Passwords**
  A good password is at best hard to remember - this is of course impractical. Many people still use passwords that are far too weak. 12345 for example is a weak password. UfNS3-?ßsDa-hUdk& - it looks quite different - the more different symbols, special characters, numbers and letters, the better. But not if the password is then only noted down again on a piece of paper directly on the screen.

  So you see - finding a suitable and secure password that the person concerned can remember is not that easy. Especially since many systems regularly prompt you to change passwords and it is not recommended to use the same password more than once.

Excursus
There are so-called **password manager** which can be used both privately and in companies. These are programs that can generate and store secure passwords for websites or programs. The program itself is secured with a so-called **master key**, i.e. ONE main password. The advantages and disadvantages are obvious: You can use a variety of different, secure passwords and do not have to remember them individually. But if the main password is cracked, all stored passwords can be accessed. A password manager is only secure if the main password is strong and preferably changed regularly.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

However, the passing on of passwords is also a problem. This does not have to be intentionally negligent. You want to help a colleague and quickly give him your own access to the system. Or the system administrator requests the password for a check. This can lead to critical situations - especially when people are involved who deliberately steal passwords in this way.

- **Bring your own device**
  "Bring you own device" - this does not mean a wild Christmas party in the company, but rather taking your own devices, such as external hard drives, USB sticks, smartphones and the like. If company-internal information is stored or edited on these devices, then internal IT security cannot really help. This is especially critical when so-called "home office" is the practice, i.e. working for an organisation from home.

  Sometimes, by the way, storage media are deliberately "prepared" with malware by third parties and then deliberately distributed to people who work for certain companies, for example. This happens, for example, at professional trade fairs, where USB sticks are often given away.

- **Installing unauthorized applications**
  The company laptop is too slow, so you "take care of it yourself" by installing antivirus programs and other stuff. Or you like to play a game in your spare time at work and download malware onto your company PC. This can also lead to threats to IT security due to a lack of awareness.

These are essentially the greatest threats to IT security. As already explained, completely unforeseeable events can of course also threaten IT - natural disasters such as fire, lightning strikes or floods can completely paralyse or destroy computer systems.

Remember

One speaks of an actual threat in terms of IT security **when an internal vulnerability meets an external threat.**

Such a threat can be a deliberate attack, unintentional by humans or by "force majeure" like natural disasters.

Deliberate attacks:

- Malware such as viruses, worms and trojans
- Physical intrusion and the stealing or manipulation of information or computer systems
- Identity theft or extortion through phishing, ransomware and denial of action attacks

Unintentional hazard

- Weak or passed on passwords
- Using private devices in corporate environments
- Installing unauthorized applications

Force majeure

- Natural disasters
- which subsequently lead to the destruction or paralysis of the computer systems.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5.5 IT security measures

IT security offers various measures, not only on the technical side. **To make people aware of malware or harmful, unconscious behaviour in the company or in their private lives** is usually already worth a lot.

To that effect, training courses and workshops are often offered, which can prevent the one or another IT problems in your private life. Within companies, sometimes entire strategies are designed to integrate IT security holistically and as comprehensively as possible into processes. However, this cannot work without first raising awareness among the staff.

Nevertheless, investments in information and awareness raising are of course not enough - so what else does IT security do?

Software
The obvious first: there is so-called **anti-virus software** that automatically scans your IT system and checks for malware. This should happen in short, regular intervals and is useful in both private and business environments. Security gaps and malicious programs that want to be downloaded from the Internet can thus be detected and banned.

You already know it, but you still can't rely on it 100 percent. Sometimes malware is simply not detected as such - or secure software is identified as malware, automatically removed, and then the computer stops working. Blindly trusting an antivirus program is therefore not advisable.

So-called **firewalls** are also popular means in both private and business contexts. They deal with the network connections of IT - for example with the WLAN. Here, unauthorized access from outside via the network can be detected and prevented. In most cases, such firewalls are already integrated in anti-virus software products.

Sandboxes are something especially exciting, not only for children. In IT security, a sandbox stands for a program that locks up malware. This relatively new concept is particularly effective for special data types. For example, PDF documents are opened in a separate "sandbox", separate from other programs. If the PDF is damaged, in the worst case only the sandbox program is attacked - the rest of the system is spared.

Using different software and sometimes trusting smaller providers can pay off, by the way – **the more "diverse" the IT is, the more difficult it becomes to crack the system as a whole.** Sometimes the best-known antivirus software companies are particularly affected by hacker attacks - simply because they are the most common.

Access control
Access control does not simply mean an overly long password. Companies help each other here with different user rights. **Only very few people in the company have access to all data** usually these are limited and divided according to the function in the company.

Restricted access to Internet pages or the prevention of external software on company computers can also be implemented. The company WLAN can also be designed so that only a very limited selection of applications and programs can be downloaded and used.

In addition, there is also the possibility of preventing "active content" - self-executing software (often these are utility programs) is turned off in this way. This can also be effective against potential malware. The measures mentioned here are of course more likely to be applied in a business context.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

However, **cryptography** can be used for business and private purposes. This means nothing else than an encryption of data. Not only is access to the data secured with a password, but the data itself is also "encrypted".

Excursus

Cryptography of data and information - end-to-end

End-to-end encryption is a common standard in data cryptography. Here, sender and receiver have a translator code. Messages or images are sent by the sender. However, the translator code automatically changes the message data into incomprehensible sequences of numbers and symbols. The recipient receives these and can in turn display and understand the message or image in its original form due to the translator.

This simply serves the purpose **that data possibly intercepted in the send process cannot be put into a context** and thus remain incomprehensible as information.

Backups and Updates

Regular updates of the software to keep it up to date also helps, of course. The older a software is, the sooner its errors are known. Especially operating systems and anti-virus programs should be updated promptly, as the greatest threats are posed by external access.

Of course, there is only one thing that can help against data loss (if, for example, the computer is broken or stolen): regular backups, i.e. copying the data and information yourself - preferably kept separate from the IT system on an external hard disk or in the so-called "cloud". Cloud systems are external servers and storage locations that are available via the Internet. Here, a backup can also be automated, but of course there is also the risk that the cloud provider itself becomes the victim of an IT attack.

Remember

Making people aware of the correct handling of IT security, both privately and in companies, is already worth a lot.

There is also a number of IT security measures:

Software

- Antivirus programs
- Firewalls
- Sandboxes
- Diverse deployment of the IT system

Access control

- Different user rights
- Restricted access to websites and programs on the Internet
- Cryptography

Additional measures

- Regular backups
- Latest updates

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5.6 Summary

IT security is a subarea of information security and means all protective measures in the processing and storage of data in an IT system - both in the private and corporate sector. This includes **computer security, data protection, data backup** and **data security.**

IT security depends heavily on **current technological developments**. Above all, it is necessary to react quickly in order to be able to offer appropriate countermeasures. There are **three core protection objectives** that must be met in all areas of operation:

confidentiality - integrity – availability

In order to achieve these protection goals**, the core task of IT security is to identify weaknesses in systems and eliminate them accordingly**. An actual threat in the sense of IT security is when an internal vulnerability meets an external threat.

Such a threat can be a **deliberate attack** to steal or manipulate data (e.g. with malware over the Internet or by physically breaking into the IT department of a company).

But an IT system can also be **unintentionally threatened,** for example, by a weak password or by natural disasters in which computer systems are damaged.

Making people aware of the correct handling of IT security, both privately and in companies, can already help. In addition, there **is protection software, restrictive access controls** and other IT security measures to minimize potential threats.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.