Introduction to cybersecurity

> Note: *pdf version in document root may not be up to date*

Concepts

Information security

> Other names: *data security, cyber security*

Information security consists of three independent branches:

- information availability
- information integrity
- information confidentiality

Each of these three branches must be maintained for all information (data).

Availability

Data availability ensures the timely and convenient access to data for all authorised entities.

Integrity

Data integrity ensures that the information comes from a legitimate source and hasn't been altered, deliberately or accidentally, after its creation.

Confidentiality

Data confidentiality ensures that data, or the information carried by the data, can be accessed only by authorised subjects.

Security of data

Security of data is achieved by securing the IT assets surrounding the data. These assets include

- IT equipment
- data communication channels
- software

and must take into account

- the organisation (structure and operating principles)
- personnel
- data carriers

- infrastructure

Standard model of harm

Threats influence the data and exploit the **vulnerabilities** of IT assets or components of the systems. Threats in conjunction with vulnerabilities determine and pose the **security risk**.

When a risk is not mitigated, a **security breach** may happen. Therefore, to minimise risks and avoid breaches, **safeguards** or **security measures** must be set in place.

Security and planned residual risk

No matter the amount of safeguards set in place, absolute security can never be achieved. Implementation of safeguards merely minimises the probability of a breach.

Acceptable residual risk

Instead of absolute security, the concept of acceptable residual risk is followed.

Acceptable residual risk means the situation where the total price of all implemented safeguards is approximately equal to the forecast of loss caused by a security breach.

Security threats

A threat represents a potential violation of security by an external element. It may consist of

- violation of availability
- violation of integrity
- violation of confidentiality

or any combination of those. A threat is always considered an external influence.

Classification

Threats can be classified by

- the target: availability, integrity, confidentiality
- the source: subject causing potential harm
- the type of IT asset
- the extent of potential danage

Generally the first two classifications are used.

Threats classified by source

Threats classified by source can be separated in two groups:

Spontaneous or accidental threats

such as environmental threats (Force Majeure), technical failures or human error,

Deliberate acts or attacks

in case the damage is intentional or the motives are clear.

It is worthy of note that in practice, accidental or spontaneous threats cause in general more harm than deliberate attacks, due to neglicence.

Attacks

Attacks or deliverate acts are always based on humans making deliberate actions to harm an entity's security.

Sources of attacks

- Authorised users of IT systems
- Intelligence agents
- Crackers
- Other criminal elements

Channels of attack

- Direct contact with the target system
- Networks
- Portable data carriers such as external memory devices

Attack classifications

- physical attacks
- mis-use of resources
- blocking of resources
- interception
- fabrication
- system manipulation
- attacks to security mechanisms
- attacks via software / malware

Physical attacks

Physical attacks mainly harm the integrity and availability.

- attacks on infrastructure
- vandalism
- trespassing / break-in
- theft
- manipulation or destruction of equipment

Mis-use of resources

Mis-use of resources harms all branches of security.

- unauthorised use of IT systems

- mis-use of user rights
- mis-use of administrator privileges
- theft of services (such as mobile services)

Resource misuse is susceptible to happen during the conversion, maintenance, repairing and/or upgrade tasks performed by external parties.

Blocking of resources

Blocking of resources mainly harms availability.

- overloading of network
- mass-execution of tasks
- filling quotas

The most common implementation of resource blocking are distributed denial of service (DDOS) attacks.

Interception

Interception or eavesdropping is an attack to confidentiality by any unauthorised subject.

- voice interception in rooms
- interception of calls
- unauthorised reading or copying of data
- reading of residual information (ex: from printers)
- wiretapping
- inappropriate deletion of data or destructuring with subsequent reading

Fabrication

Fabrication or faking consits in fake data inputs or propagation, which harms integrity.

- playback of recordings out of context
- masquerade attacks (phishing)
- social engineering
- denial of authorship

System manipulation

Manipulation consists in unauthorised changes made to an IT system, which mainly harms integrity. It has some overlaps with fabrication.

- manipulation of data or software
- manipulation of communication lines
- manipulation of data during transfers
- attacks via service ports

Attacks to security mechanisms

Attacks to security mechanisms can harm all three branches of information security.
The main attack targets are authentication systems and cryptosystems.

Attacks via software

- malware
- undocumented features of legitimate software
- special purpose software

Malware

- logical bombs
- trojan horses
- worms
- viruses
- droppers (trojan installers)

Vulnerabilities

Vulnerabilities are all properties of a system which can be exploited by threats. They can be divided in four main classes:

- infrastructure vulnerabilities
- IT vulnerabilities
- personal-related vulnerabilities
- organisational vulnerabilities

Infrastructure related vulnerabilities

- unfavourable physical locations of devices
- primitive or deprecated infrastructure solutions

IT related vulnerabilities

- limited resources
- improper installation of equipment or connection lines
- errors, defects and undocumented features of software
- shortcomings of protocols
- shortcoming of data management
- inconvenience of safeguards

Personnel related vulnerabilities

- incorrect procedures
- ignorance and lack of motivation
- ignoring of safeguards and protocol (intentional and negligence)

Organisational vulnerabilities

- deficiencies of work organisation

- shortcomings of resource management
- incomplete documentation
- incomplete implementation of safeguards
- shortcomings of safeguard management

Interaction between threats and vulnerabilities

Threats exploit vulnerabilities.

Security diminishes as the probability of threats increases and so does the number of exploitable vulnerabilities. The reciprocal stands as well.

Digital data

Securing digital data

Cryptography is essential for achieveing both confidentiality and integrity, which differs significantly from paper based data.

Authentication itself becomes essential and availability is often ensured by the network.

Role of cryptography

Encryption or cyphering is a technique where data is converted to a non human readable or device interpretable form. The conversion process uses a certain piece of data called a key to achieve the encryption.

Cryptography is used both for

- ensuring confidentiality: data cannot be deciphered without the key
- ensuring integrity: data cannot be changed without having access to the decryption key or leaving a permanent mark that data was altered

Availability of digital data

- regular backups
- reliable IT systems
- digital record management system
- transmission of data via networks

Integrity of digital data

- data and its carrier are permanently tied together (excludes network based applications)
- client-server techniques where interacrtions are logged
- usage of e-signatures to cryptographically associate data and its creator

Confidentiality of digital data

- secure storage and transport of plaintext data
- encryption of data and public handling

Encryption adds the **key management** problem. Additionally, encryption should be mandatory for any confidential information transfers over the common network.

Safegurads

Safeguards minimise vulnerabilities and the residual risk.

Classification of safeguards

- their purpose
- their security area
- the type of assset
- the means of implementation
- strength of security

Purpose divided safeguards

- preventive safeguards
- identifying safeguards
- reconstructive safeguards

Safeguards may also be polyfunctional.

Preventive safeguards

Preventive safeguards are used to prevent security incidents such as

- to minimise vulnerabilities
- to prevent attacks
- to minimise risk probabilities
- to decrease the potential damage of attacks
- the facilitate reconstruction

Preventive safeguards can further be divided into three subcategories

Reinforcable safeguards

which have the purpose of minimising the impact of spontaneous threats

- order or systematicness (standards, procedures, ...)
- working conditions (micro-climate, ergonomics, social climate, corporate hierarchy)
- preventive checks (verification and testing, monitoring, auditing)
- security awareness (training of employees, security drills, ...)

Deterring / scaring safeguards

which have the purpose of minimising the probability of attack attempts,

Separative safeguards

which fend off the attacks by taking care of different security aspects. They can further be divided into

- spatial isolation
- temporal isolation
- logical isolation (access control, service broker, securing)

Identifying safeguards

Operative identification

Involves methods which are able to identify security incidents as soon sa they occur and allow for immediate response.

Post-event identification

Is based on logging of events and later analysis of the logs for future improvement or proof and action taking.

Evidence-based identification

Is based on security elements integrated to IT assets which allows to check for integrity and/or confidentiality of data.

Reconstructive safeguards

After a security incident, it is necessary to restore the normal operation of impacted IT systems. This can be achieved via

- backups (data redundancy)
- renovation (removing of defects and errors)
- replacing (substitute for corrupted or damaged data)

Classification by IT assets

German BSI IT Baseline Security Method and Estonian ISKE standard distinguish the following categories:

- generic aspects
- infrastructure
- IT systems
- networks
- applications

Classification by implementation

Organisational safeguards

which include the security of administration, of system design, management and security incident handling activities and operations.

They should be implemented in the first order and beginning with security policies formulation, risk analysis and security plan creation.

They also should include four main components:

- activities a person must do
- activities which are prohibited for a certain person
- consequences of frobidden actions
- consequences of negligence

Physical safeguards

which involves the infrastructure, mechanical components, guards, etc...

IT-related safeguards

which are mainly used for performing logical separations and identifications of security incidents.

Two main branches include software-based access control and cryptographic means.