Seminar session 1

Cyber security challenges and solutions of international companies using the example of Shell Global.

About Shell Global:

- International company, operates on all continents worldwide
- 20 million customers per day
- Different payment methods (credit card, VISA, ect.)
- App provider (Shell app)
- Loyalty schemes

Challenges:

“For every action to store, secure, and use data, there is an equal or greater reaction to steal data.” - Leah VanSyckel

Because of the size of international companies, they are subject to greater cyber attack and vulnerability.

In the case of Shell Global, in addition to vulnerabilities in the software, it also affects its infrastructure (pipelines, oil bases, etc.).

Bruce Lindsay stated: “relational databases are the bedrock of western civilization.”

Responsible use of relational databases requires:

- efficient data management
- efficient access to stored data
- analytics knowledge

The CIA triangle model refers to the claims that are made of a software service:

- Confidentiality: The protection against access to private data by third parties.
- Integrity: The security that data is not manipulated.
- Availability: The guarantee of continuous access to the data by authorized persons.

Ethical and legal responsibilities:

Cyber laws are national and differ between countries.

A company must basically act according to the law of the country in which it operates, but also has to act according to the laws of the country in which the headquarters are located.

The General Data Protection Regulations (GDPR) represents the legislation of the European cyber law.

GDPR core regulatory principles:

- lawfulness, fairness and transparency
- purpose limitation
- data minimization
- accuracy
- storage limitation
- integrity and confidentiality

Consequences of ethical issues could be:

- Societal harm
- Physical and psychological damage to individuals
- violation against human rights

Solution approaches:

The following levels must be observed in cyber security:

- Hardware
- Software
- Databases
- Telecommunication (network)
- Procedures
- People

Security vulnerabilities:

1. Network security
2. Software security
3. Human factors