Network Security

Current and Future Threat Landscape

Prof. Dr. Henning Trsek, Institute Industrial IT

Agenda of todays lecture

- **What is Security and why do we need it?**
- **Cyber attacks and their impact**
- **Examples for Security Incidents**
- **Common threat actors and attack patterns**
- **Threat intelligence**
- **Targeted attacks**

What are your past experiences and points of contact with Security?

- **Information Security**
  - Protection of information processing technical and non-technical systems against threats and damages
- **IT-Security**
  - Protection of IT and ICT against threats and economical damage
- **Computer Security**
  - Protection of single systems against outages/ manipulations

Information security

Ensures that the security objectives **Confidentiality, Integrity** and **Availability** of all information assets of an organization are always met.

Information assets are

Information and information processing systems, which have a certain **value** for the organization

Also business processes are concerned, as long as they depend on the previous systems and information.

Information in **all possible types and formats** are concerned: printed, spoken, audio, video, IT-Systems

- **Impossible to measure**
- **No metric available**
- **KPIs are very specific and are able to quantify only parts of the whole system**
- **Indirect definition of common security objectives**
  - Confidentiality
  - Integrity
  - Availability

Security objective: Confidentiality

- **Definition**
  - Information assets are only available and disclosed to authorized persons and systems
- **Considered in terms of**
  - Transport, storage, processing
- **Typical control**
  - Encryption
- **Objective violated, if information assets are disclosed to unauthorized persons/systems**

Security objective: Integrity

- **Definition**
  - Information assets are always complete and correct, an unoticed modification by unauthorized persons and systems is impossible
- **Considered in terms of**
  - Transport, storage, processing
- **Typical control**
  - Check sums
- **Objective violated, if information assets are modified by unauthorized persons/systems**

Security objective: Availability

- **Definition**
  - Information assets can be accessed and used by authorized persons and systems as intended
- **Considered in terms of**
  - Data, services, infrastructures, etc.
- **Typical control**
  - Redundancy, over provisioning
- **Objective violated, if information assets are only limited or not at all useable as intended due to an attacker**

Information Security concerns not only technical (IT) aspects!

Definition of ISO 27005

- Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

Key concepts of risk management

Governance, risk and compliance