IT Security

Jil Zerndt
FS 2025

01 - Intro

Business IT-Risks

- Ransom Demand
- Fraud
- Espionage
- Violation of Regulations
- Misuse of Computing Resources
- Reputation Loss
- System Outage
- Sabotage
- Data Loss
- Brand Misuse

Problems - Overview and their impact on data availability

Physisch

unabsichtlich

- Naturkatastrophen
- Feuer
- Ausfall
- Kaffee auf Server

absichtlich/bösartig

- Feuer
- Vandalismus
- Garantie läuft aus -> absichtlich langsamer
- Social Engineering

Virtuell

unabsichtlich

- Bitflip
- Config Fehler
- Bugs im SW
- Phishing klicken

absichtlich/bösartig

- DDoS
- Malware
- Ransomware
- Phishing senden
- Trojaner

Countermeasures - Overview

Disaster Recovery

- Offline backup solutions
- Restoring from images

Access Control

- Restricted Access Rights
- Multi-Factor Authentication
- Firewalls
- Traffic Management Solutions

Physical Protection

- Physical Access Control (locks, fences, etc.)
- Fire Protection (extinguishers, alarms, etc.)
- Monitoring (CCTV, Guards etc.)

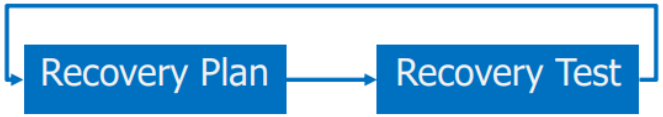
Training Processes

- Employee Training
- Four eyes principle
- Automation of routine processes
- Monitoring
- Preventive maintenance

Redundancy

- Uninterruptable Power Supplies
- High Availability setups
- Load Balancing
- Redundant data center
- Redundant network connections

Recovery Plan and Test



Recovery Plan - description of what to do if something goes wrong

- Roles and responsibilities
- Processes
- Contact details
- Technical instructions

Recovery Test - testing the recovery plan

- Theoretical dry run
- Practical tests
  - turn off a server or DC
  - restore data from backup

Goals of IT Security

Most measures in Information Security have one of the three following high-level goals:

- Ensure data is confidential
- Ensure data is not corrupted
- Ensure data and systems are available