TECHNISCHE HOCHSCHULE
OSTWESTFALEN-LIPPE
UNIVERSITY OF
APPLIED SCIENCES
AND ARTS

Cyber Security in IoT

Katharina Pilar von Pilchau

Prof. Dr. Stefan Wolf

TH OWL, Höxter, Germany

Cyber Security

- Security
- Safety

pixabay.com

- Confidentiality
- Integrity
- Availability

CIA

Fundamental values of Cyber security

- Data privacy

Cyber Security – current situation

- The overall situation is getting worse

Ransomware

Cybercrime

IT supply chain disruption

DDoS-Attacs

Data theft

Blackmailing

Cyber-Sabotage

Perimeter systems come into focus

IoT in the Water Sector

- IoT in the facilities
- IoT in public areas
- IoT in the private sphere of customers

Special challenges in the IoT

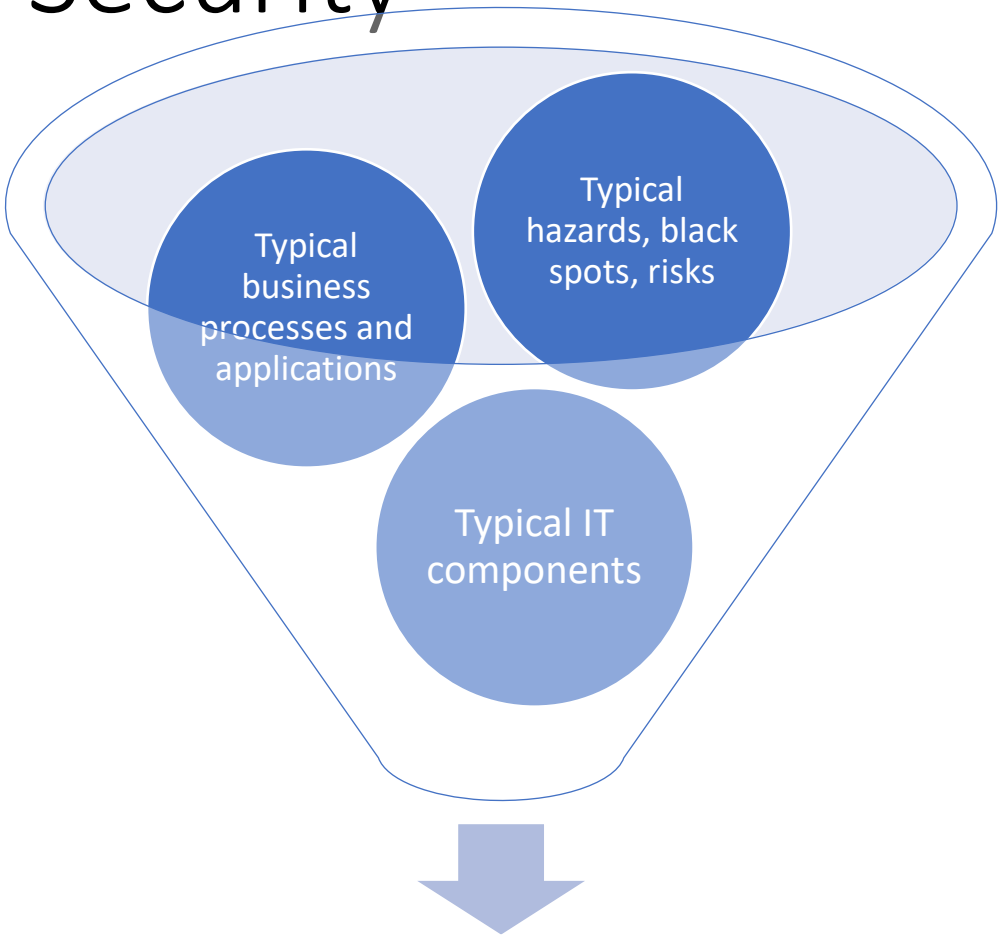
- Lack of awareness
- Up-to-dateness of the software
- Software dependencies
- Often part of the critical infrastructure
- Shortage of skilled staff

=> Checklist

Threats to cyber security

- Force majeure
- Organisational shortcomings
- Human error
- Technical failure
- Deliberate acts

Better Cyber Security



Framework for cyber security management

https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

Example

SYS.4.4.A15 Restrictive Granting of Access Rights (S)

Access authorisations for IoT devices SHOULD be granted as restrictively as possible. If this is not possible using IoT devices themselves, it SHOULD be considered via the network.

SYS.4.4.A16 Elimination of Malware on IoT Devices (S)

The IT Operation Department SHOULD regularly obtain information as to whether the IoT devices used could become infected with malware and how it can be removed. Malware SHOULD be eliminated immediately. If the cause of an infection cannot be eliminated or a new infection cannot be effectively prevented, the affected IoT devices SHOULD no longer be used.

SYS.4.4.A17 Monitoring Network Traffic on IoT Devices (S)

Whether IoT devices or sensor systems communicate only with IT systems that are necessary for their operation SHOULD be monitored.

SYS.4.4.A18 Logging Security-Relevant Events on IoT Devices (S)

Security-relevant events SHOULD be logged automatically. If this is not possible using IoT devices themselves, routers and logging mechanisms of other IT systems SHOULD be used. The log data SHOULD be evaluated appropriately.

SYS.4.4.A19 Protection of Administration Interfaces (S)

Depending on whether IoT devices are administered locally; directly using the respective network; or using central, network-based tools, appropriate security precautions SHOULD be

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf

What to do?

- Build a security policy, a security concept and a CISO
- Establish a security process