INDUSTRIAL SECURITY

COPADATA

DOES IT AFFECT ME?

The gates of the production facilities are open.
Can unauthorized people easily gain access?

My colleagues in production work with PCs.
Are there guidelines, relating to password creation, for example?

I use mobile devices.
Are they used to access production data?

Production IT and office IT are two different systems.
How is the data exchanged between them?

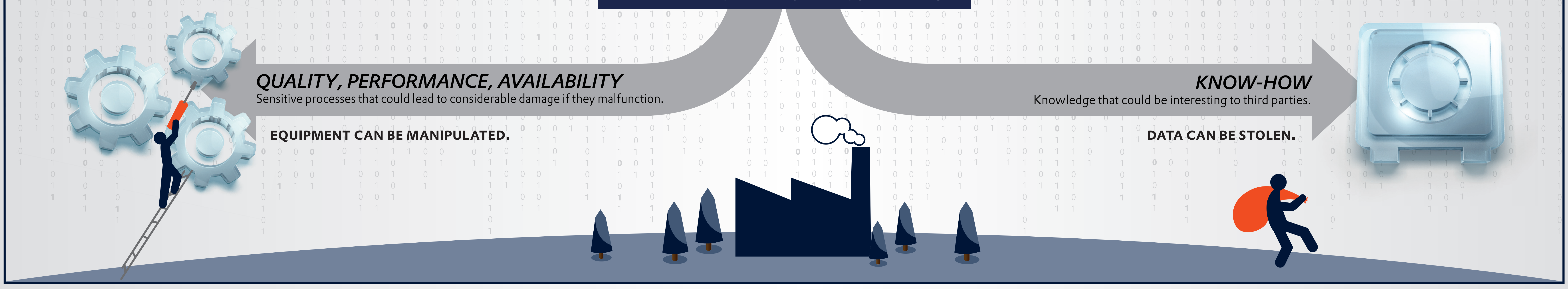
I am networked to my external customers and suppliers.
Are these connections secured appropriately?

PCs are connected to the Internet.
How can I protect them from malware?

UPDATES

In my company, widely-distributed software licenses are used.
Is there an effective software update policy to minimize security vulnerabilities?

AM I AN INTERESTING TARGET FOR ATTACK?



THE PRIMARY CAPITAL OF MY COMPANY IS ...

QUALITY, PERFORMANCE, AVAILABILITY
Sensitive processes that could lead to considerable damage if they malfunction.

EQUIPMENT CAN BE MANIPULATED.

KNOW-HOW
Knowledge that could be interesting to third parties.

DATA CAN BE STOLEN.

WHAT POTENTIAL WEAK POINTS DOES MY COMPANY HAVE?

HUMAN

- Unauthorized access to sensitive areas of equipment, switching cabinets, network components
- Unauthorized access to production data
- Careless use of the IT system

TECHNOLOGY

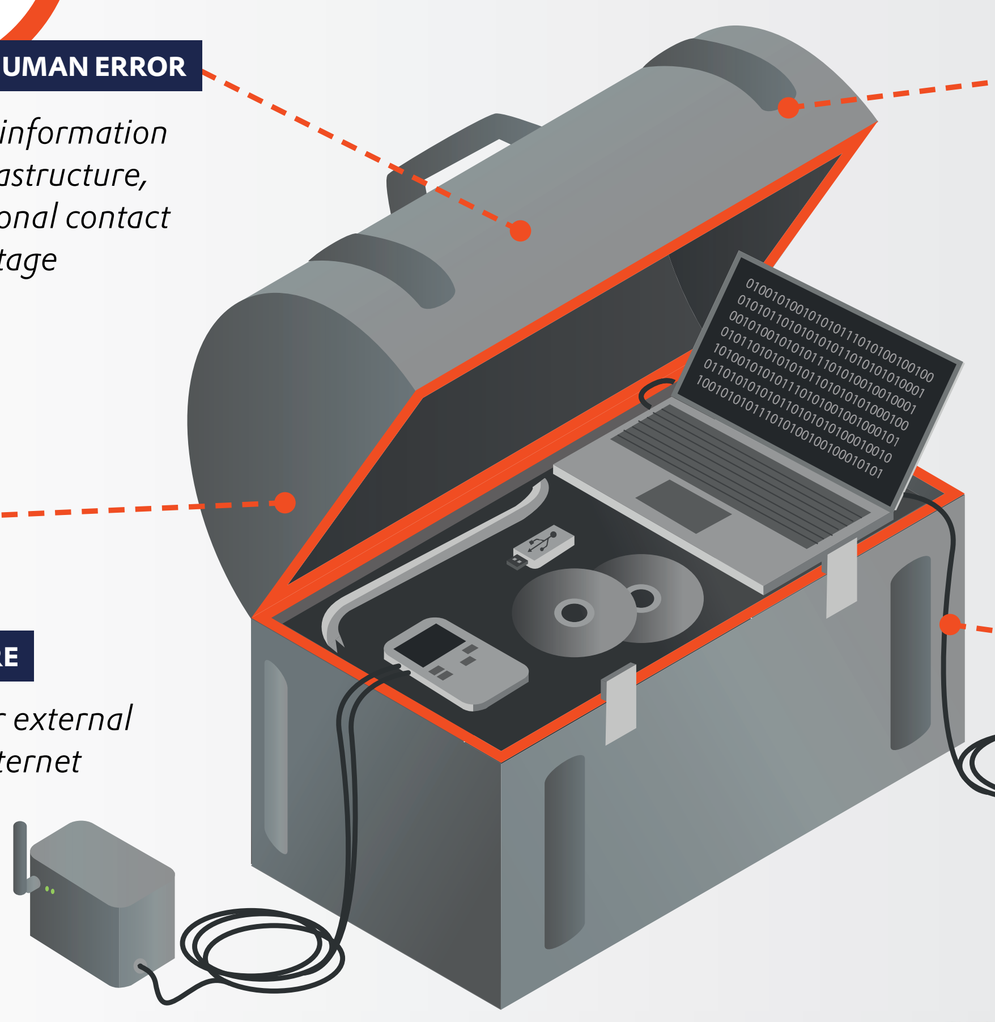
- Unencrypted protocols
- Access to data and processes via smartphone
- Outdated software systems and a lack of security updates
- Control components directly connected to the Internet
- Non-secure exchange of data inside the business networks
- Connections for remote maintenance systems

ORGANIZATION

- Unsecured configurations of network components (routers, firewalls, switches, etc.)
- Insufficient patch management
- Insufficient awareness of and too little expertise in IT security in the company

WHICH TOOLS AND TECHNIQUES DO POTENTIAL HACKERS USE?

The attackers' toolbox



SOCIAL ENGINEERING OR HUMAN ERROR
Unauthorized access to information or to the technical infrastructure, for example due to personal contact or internal sabotage

EXPLOITATION OF EXTERNAL ACCESS
For example, by means of remote maintenance systems, or networking with suppliers or consumers

INFECTION WITH MALWARE
Office networks, intranet and/or external hardware captured via the Internet

COMPROMISATION
From smartphones in the production environment, extranet and/or cloud components

What standards & guidelines are there?

USA
NERC CIP (North American Electric Reliability Corporation / Critical Infrastructure Protection)

IEC 62443

Germany
German IT Security Act (often also called the KRITIS Act)

...

ISO 27000

WHAT TYPES OF HACKER ARE THERE?

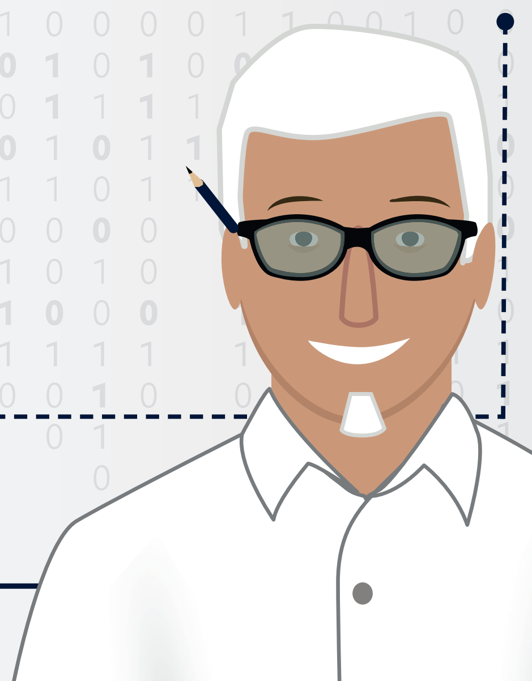
HACKER TYPES

BLACK HAT

Criminal intent,
elite training,
experts in their field.

GRAY HAT

Want to make people
aware of security loopholes,
operate in a legal gray area.



WHITE HAT

No criminal motivation,
searching for security loopholes,
considered security researchers.