Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

German-American IT Security Forum
→ Greetings

Prof. Dr. (TU NN)
Norbert Pohlmann

Professor** for **Cyber Security
Director** of the **Institute for Internet Security – if(is)

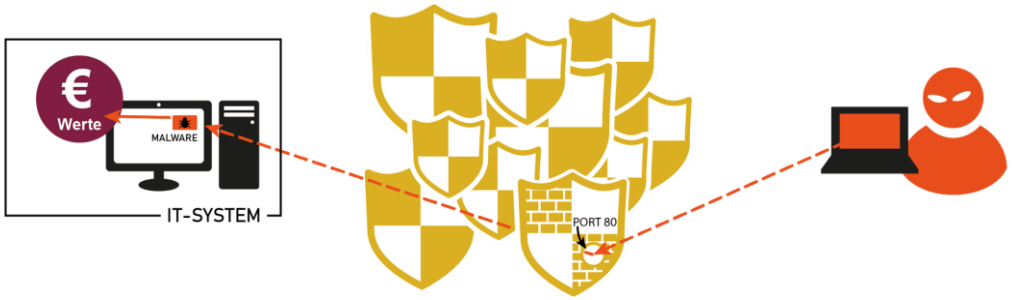
Chairman of the board** of the **IT Security Association TeleTrusT
Member of the board** of the **Internet industry association eco.

if(is) internet security.

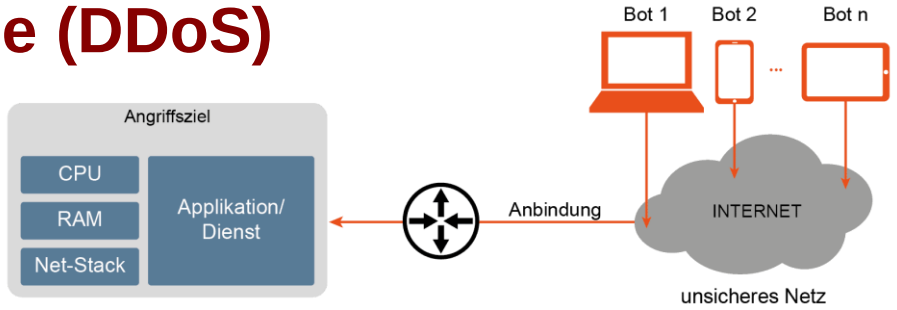
→ Actually Attacks

Advanced Ransomware

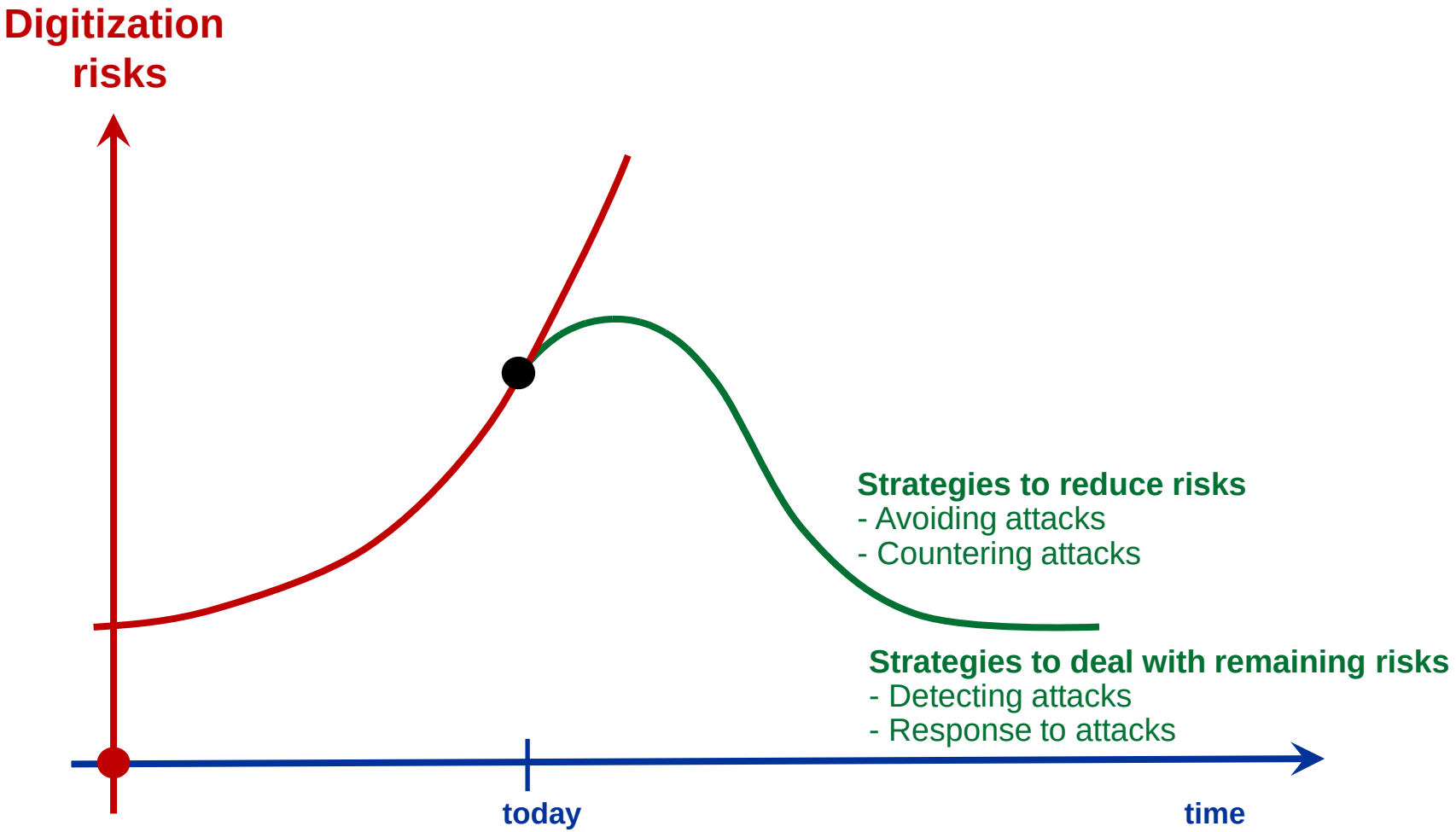
Advanced Persistent Threat



Distributed Denial of Service (DDoS)



Cyber Security Strategies
→ Overview



Principal Cyber Security Strategies
→ Avoiding Attacks

- A general cyber security strategy **for protecting the assets** of a company is the idea of avoiding damage from attacks - **avoidance strategy**.
- This approach **reduces the attack surface** and thus reduces the risks.
- The challenge is **to set up IT** in such a way that the company can do **everything necessary for the business** and **everything else is actively avoided.**

Cyber Security Mechanisms

- *Digital **data minimization***
- ***Focusing** (approx. 5% are particularly worthy of protection)*
- ***Only use secure IT technologies, products and services***
- ***Reduction of IT possibilities** (SW, rights, communication ...)*
- ***Security aware employees***

Principal Cyber Security Strategies
→ Countering Attacks

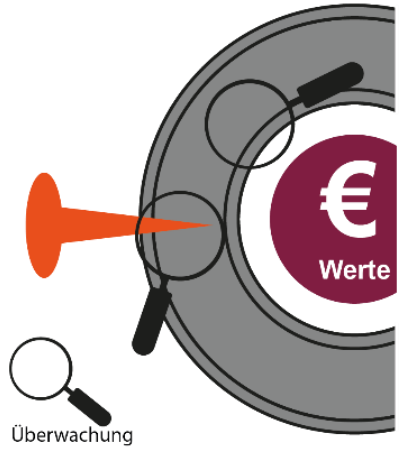
- Counteracting attacks is the **most commonly used** cyber security strategy to minimize the existing risk and thus avoid damage.
- For this purpose, cyber security mechanisms are used that provide a high level of **effectiveness against known attacks** and thus protect the assets appropriately.

Cyber Security Mechanisms

- *Encryption (in motion, at rest, in use)*
- *Multifactor authentication*
- *Anti-Malware solutions (New Concepts)*
- *Anti-DDoS mechanism (common infrastructures)*
- *Digital signature / certificates (e-mail, SSI ...) - PKI, BC*
- *Hardware security modules (smart card, TPM, HSM, smartphone)*

Principal Cyber Security Strategies
→ Detecting Attacks

- When attacks **aren't fully countered**, or avoidance doesn't sufficiently reduce the attack surface, the remaining strategy is to detect attacks and try to minimize the damage as quickly as possible.
- This involves identifying **attack signatures** or **anomalies** in a defined area of the IT infrastructure.



Cyber Security Mechanisms

- *Early warning and situational awareness systems*
- *Evaluation of security-related events (prioritization) - AI*

Principal Cyber Security Strategies
→ Response to Attacks

- If attacks are detected, appropriate actions should be taken as quickly as possible to **prevent the damage** or at least **reduce the magnitude** of the damage.

Cyber Security Mechanisms

- *Automated response (firewall, email service…) - AI*
- ***Definition** of authorities, information flows, decision-making process and communication strategies*
- *Digital forensics (optimize measures, close vulnerabilities)*
- *Emergency planning*

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

German-American IT Security Forum
→ Greetings

I wish us a successful security forum

Prof. Dr. (TU NN)
Norbert Pohlmann

Professor** for **Cyber Security
Director** of the **Institute for Internet Security – if(is)

Chairman of the board** of the **IT Security Association TeleTrusT
Member of the board** of the **Internet industry association eco.

if(is) internet security.