IT-Security

Prof. Dr. Reiner Hüttl

Content

- Motivation, Goals
- Encryption
- Checksums and Digital Signatures
- Authentication, Authorization
- Application Security
- Secure Software Engineering
- Secure Communication
- Privacy

Organization

- Exam: Oral exam, 15 minutes
  - You can choose the language (English/German)
- The slides are not a complete script!
  They are partly subjective opinions that should be discussed
- The following are necessary for the examination:
  - Participate in the lectures
  - Make additional personal notes in the script
  - Make own research (books, web, videos) when you don't understand something or ask
  - Execute the online task (exercises, tests, ...)
  - Participation in the exercises
    English exercise for AAI
    German Exercise for INF/WIF

Literature

- Foundations of Information Security, Jason Andress, O Reilly, 2019
- Real-world Cryptography David Wong, Manning Publications Company, 2021
- Applied cryptography, Bruce Schneier, Wiley, 2015
- Modern Cryptography for Cybersecurity Professionals, Lisa Bock, Packt Publishing, 2021
- The Cyber Security Handbook - Prepare for, Respond to and Recover from Cyber Attacks, Alan Calder, IT Governance Ltd, 2020
- The Art of Invisibility, Kevin Mitnick, mitp, 2017
- Hacking, The Art of Exploitation, Jon Ericson, No Starch Press, 2008
- Cryptography Engineering, Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, Wiley Pub, Inc, 2010

Aditional German Literature

- Claudia Eckert: IT-Sicherheit, De Gruyter Studium, 2018
- Jörg Schwenk: Sicherheit und Kryptographie im Internet, Vieweg, 2020 **(E-Book)**
- Pohlmann, N: Cyber-Sicherheit, Springer Vieweg (2019) **(E-Book)**
- Klaus-Rainer Müller: IT-Sicherheit mit System, Vieweg, 2018 **(E-Book)**
- Wolfgang Ertl: Angewandte Kryptographie, Hanser Verlag, 2019 **(E-Book)**
- Matthias Rohr: Sicherheit von Webanwendungen in der Praxis, Springer Vieweg, 2018 **(E-Book)**
- Inge Hanschke: Informationssicherheit & Datenschutz - einfach & effektiv, Hanser, 2019 **(E-Book)**
- Steffen Wendzel: IT-Sicherheit für TCP/IP- und IoT-Netzwerke, Springer Vieweg, 2018 **(E-Book)**

Web sites

- http://www.bsi.de (Federal Office for Information Security)
- http://www.cert.org/ (U.S. Computer Readiness Team, analyzing and publishing vulnerabilities)
- http://www.teletrust.de/ (Association for the Promotion of Trustworthiness in ICT Technologies)
- http://www.heise.de/security/ (Alerts, Articles, Tools, Forums)
- http://www.nsa.gov/ (National Security Agency/Central Security Service in USA)
- https://www.nist.gov/ (National Institute of Standards and Technology)
- https://www.sans.org/ (information security training, certifications, research)
- https://attack.mitre.org/ (globally-accessible knowledge base of adversary tactics and techniques)

IT-Security

Chapter 1: Motivation, Goals

Prof. Dr. Reiner Hüttl, TH Rosenheim, © 2023, 15.03.2023

Shell-Schock: Bash-Vulnerability (2014)

- Allows execution of malicious code
- Code can be inserted into environment variables which will be executed unchecked when a new shell is started
- Test with the following statement
  `env x='() { :;}; echo vulnerable' bash -c "`
  Output: vulnerable
- Programming error: Fault in parser of function definition of environment variables
- How to protect yourself?

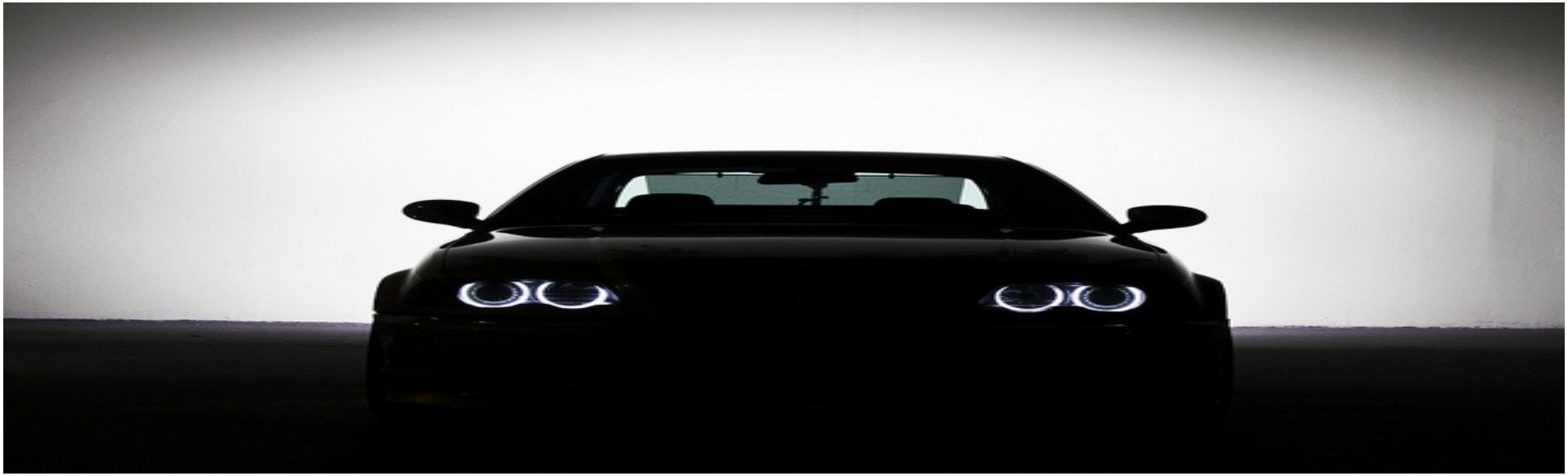
https://www.heise.de/security/meldung/ShellShock-Standard-Unix-Shell-Bash-erlaubt-das-Ausfuehren-von-Schadcode-2403305.html

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=2ahUKEwjm-ZbT0qzoAhViRBUIHcfpBiMQFjADegQIBhAB&url=https%3A%2F%2Fwww.owasp.org%2Fimages%2F1%2F1b%2FShellshock_-_Tudor_Enache.pdf&usg=AOvVaw1o9Chco8_W946RsItbrmsY

Security vulnerability in BMW Connected Drive (2015)

- **Use Case:** The door of the vehicle can be unlocked by the owner via Remote App

- **Misuse Case:** A hacker can use a portable cellular base station to send data to the vehicle to unlock the door



Weaknesses in the security concept enables the attack

- At the time of the investigation, ConnectedDrive had six vulnerabilities that compromised its security:
  - BMW uses the same symmetrical key in all vehicles.
  - Some services do not demand transport encryption when transferring data to the BMW backend.
  - The integrity of the ConnectedDrive configuration is not protected.
  - The Combox reveals the VIN of the vehicle with error messages.
  - Data sent by SMS is encrypted using the insecure DES method.
  - The Combox has no protection against replay attacks.

- Source: http://www.heise.de/ct/ausgabe/2015-5-Sicherheitsluecken-bei-BMWs-ConnectedDrive-2536384.html

It can be even better: Jeep Cherokee (2015)

- A vulnerability in the infotainment system allowed safety researchers to take control of a Jeep
  - Radio, climate, ...
  - Brake
  - Steering wheel
  - Reverse gear
  - …
- The attack goes over the Internet.

Video: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

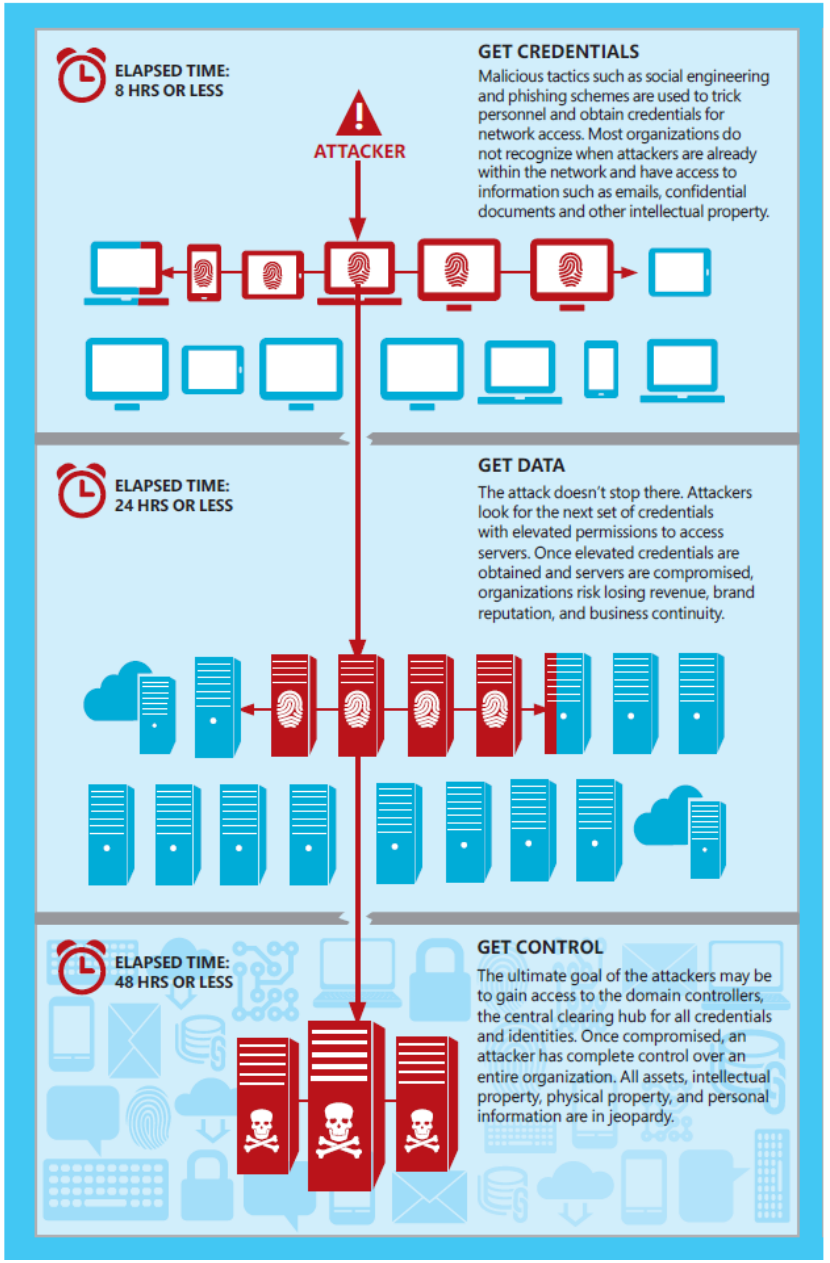
States are also under attack: Bundestag-Hack (2015)

- Attack on parliamentarians' computers with e-mail attachment and **Drive-by-Download**
- Theft of credentials for domain administrator nodes with open-source tool **mimikaz**
- **Pass-the-Hash (PtH) Attack**
  Attacker does not try to calculate password from hash, but can use hash itself to gain access to systems (usually via vulnerabilities in Single-Sign-On systems)
- Propagation in the internal network with common methods and public available tools

https://de.m.wikipedia.org/wiki/Datei:Bonn_Bundestag_Plenarsaal1.jpg

Anatomy of a PtH Attack

- Attack Activities
  - **Privilege escalation**
    attackers try to gain higher-level permissions on a system or network
  - **Lateral movement**
    attackers tries to enter and control remote systems on a network and subsequently gaining access to it
- Mitigations
  - Restrict and protect high privileged domain accounts
  - Restrict and protect local accounts with administrative privileges
  - Restrict inbound traffic with firewalls

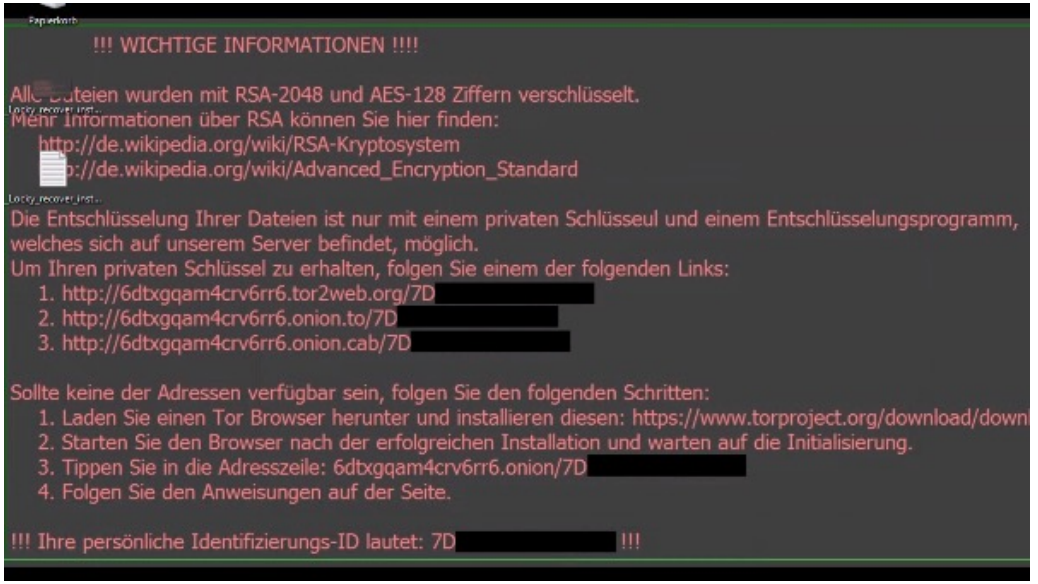


https://de.m.wikipedia.org/wiki/Datei:Bonn_Bundestag_Plenarsaal1.jpg

https://www.microsoft.com/en-us/download/details.aspx?id=36036

This can affect anyone: Locky Ransomeware (2016)

- In an e-mail is an attachment that contains a macro
- Macro saves a file that reloads malware
- Malware encrypts files on computer and accessible drives
- Malware also deletes all shadow copies of files
- How can you protect yourself?



https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/

Hardware also causes problems (2018)

- Cause
  - Out-of-order execution in Processor
  - Speculative execution
  - One page table for user processes and kernel
- Attacks
  - **Meltdown**
    - Access to memory (cache) of foreign processes provoked by exception
  - **Spectre**
    - Interpreted scripting languages such as JavaScript extract information from the address space of the web browser
- How can you protect yourself?
  - Kernel-Page-Table-Isolation (KPTI)
  - Browser Patches
  - Problem: Processor performance will drop

Weitere Details siehe:
https://www.heise.de/security/meldung/FAQ-zu-Meltdown-und-Spectre-Was-ist-passiert-bin-ich-betroffen-wie-kann-ich-mich-schuetzen-3938146.html

Computer viruses and malware

- **Overview:** https://www.youtube.com/watch?v=n8mbzU0X2nQ&t=4s
- **Computer virus**
  - program code that only works as a program part within a host program
  - when the host program expires, the virus code is also executed and can spread and have a harmful effect
  - variants: Program-, File-, Boot-, Macro-Virus
- **Worm** ("the Autonomous")
  - independent program that creates copies of itself and executes them
  - mostly occur in networks
  - reproduction by copying and sending the duplicate to other systems
  - difference to computer viruses: Worms are independent programs.

Malware

- **Trojan horse ("the secret one")**
  - Standalone program that contains an undocumented routine that performs an unexpected, mostly destructive, additional function.
  - popular technique for illegally collecting passwords
  - Difference to computer viruses and worms: Trojan horse shows no multiplication or movement, but mostly remains in the same place in the same system.
- **Spyware:** monitors user activity on a computer, collects sensitive data and sends it to the originator or third parties to harm the user
- **Ransomware:** Encrypts the data and demands ransom money for decryption
- **Adware:** Aggressive advertising software, which can collect browser data or compromise security by creating an open door for malicious programs

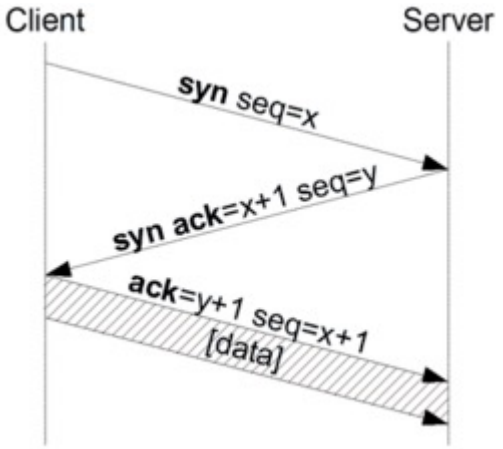
Malware

- **Bots:** software application that runs automated tasks over the internet, a network of hijacked computers form a botnet
- **Rootkit:** type of malware to give the attacker administrator rights and remote access to the infected system while hiding its presence
- **Keylogger:** records the user's keystrokes and clipboard and sends them to the attacker
- **Exploit:** Malware that takes advantage of vulnerabilities. It is used to perform attacks on vulnerable software and systems.
- Sources:
  - https://www.youtube.com/watch?time_continue=4&v=n8mbzU0X2nQ&feature=emb_logo
  - https://www.heise.de/tipps-tricks/Was-ist-Malware-4614964.html
  - Steffen Wendzel: IT-Sicherheit für TCP/IP- und IoT-Netzwerke, Springer Vieweg, 2018 (E-Book)

Denial of Service Attacks

- **DoS** is a type of cyber attack designed to disable, shut down or disrupt a network, website or service

- Example: TCP SYN-Flooding



https://deacademic.com/dic.nsf/dewiki/1221679

- **DDos Distributed DOS Attacks**: Attack coordinated by a larger number of other systems
  - Phase 1: Install agents on unprotected machines
  - Phase 2: Start attack from all agents

The difference between Security and Safety

- **Security:** (information security): no unauthorized information modification or extraction
  - Protection against intentional, targeted, and malicious attacks
  - Detect and defend against attacks
  - Minimizing the vulnerability of assets and resources
  - Example: DDOS, spam, eavesdropping, data manipulation
- **Safety:** System works and avoid accidents
  - Protection against accidental events (human and technical error)
  - Detection and defense of malfunctions that affect the correct functionality and operational safety
  - Specification of the desired functionality and detection of deviations from the desired behavior
  - Example: System failures, network failures, operating errors
- Secure systems are obtained through a combination of security and safety aspect

Core values of information security: CIA

Security Objectives

CIA = Confidentiality, Integrity, Availability

Verfügbarkeit (Availability)

Data and features are always available when they are needed and for those who need them.

Integrität (Integrity)

No unauthorized manipulation of data and functions

Vertraulichkeit (Confidentiality)

No one receives unauthorized access to data, messages and functions.

Nicht-Abstreitbarkeit (Non Repudiation)

Every action performed is verifiable exactly as it happened

Authentizität (Authenticity)

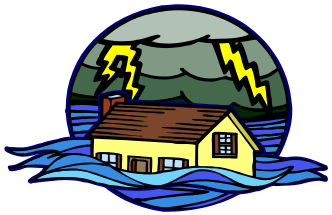
authenticity of data, accountability of messages

Details siehe z.B. https://www.kryptowissen.de/schutzziele.php

Widespread misjudgment

- Nothing has ever happened with us
- We are not in the focus of attackers, our data is not so valuable
- Our network is secure
- Our employees are trustworthy

IT security is ... endangered by threats



- **Higher Forces:** fire, water, lightning, illness, ...
- **Organizational shortcomings:** Missing or unclear regulations, missing concepts, ...
- **Human error:** "The biggest security gap often sits in front of the keyboard"
- **Technical failure:** system crash, disk crash, ...
- **Intentional acts:** hackers, viruses, Trojans, ...

Steps to IT Security: ISMS (Information Security Management System)

1. Set strategic security goals

   Availability **Integrity** **Confidentiality**

2. Create and communicate a security guideline
3. Distribute tasks and responsibilities
4. Identify critical applications and data
5. Make a risk assessment
6. Implement security measures and controls
7. Define policies and perform trainings
8. Perform regular audits (e.B. BSI, TÜV-IT, ISO 27001, TISAX)

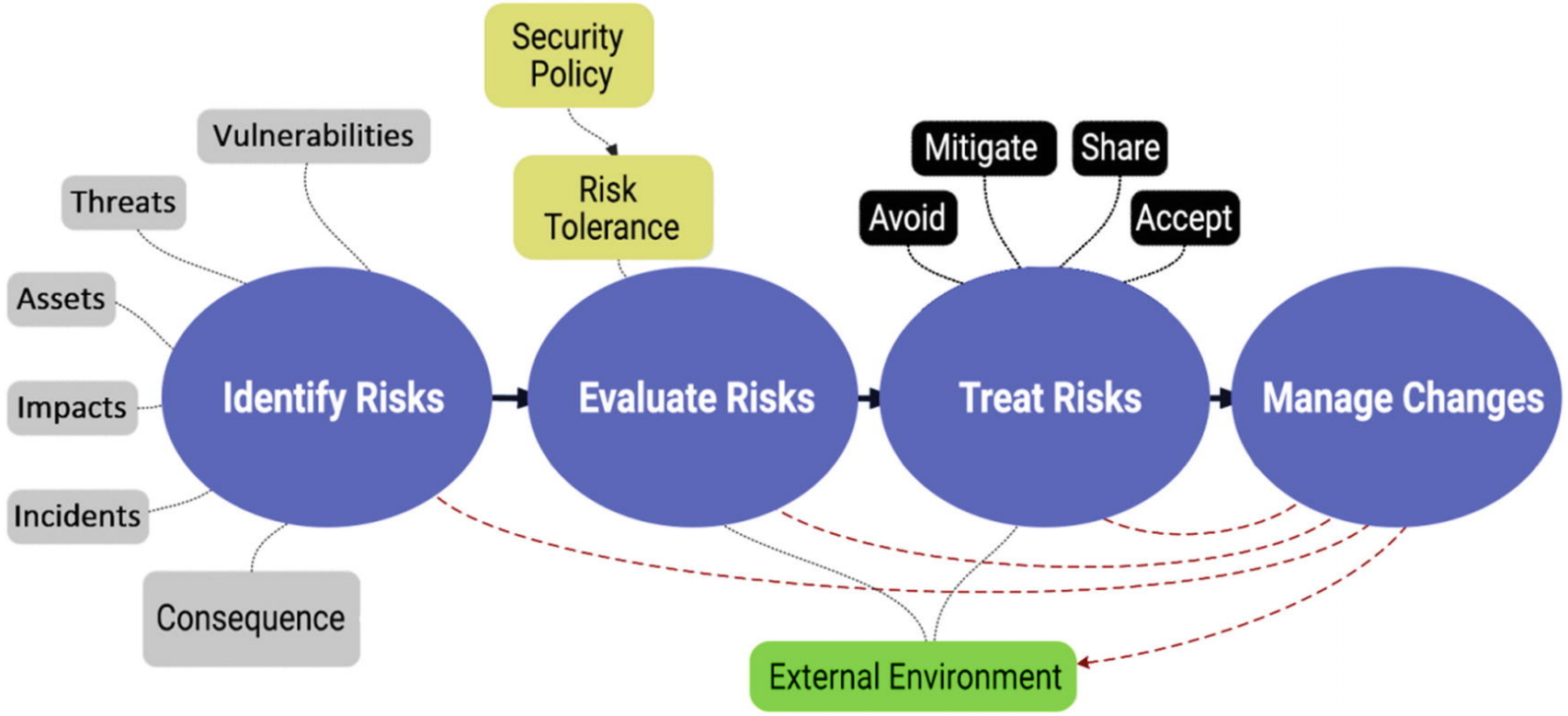
Source: Inge Hanschke: Informationssicherheit & Datenschutz - einfach & effektiv, Hanser, 2019

Identify the risks to focus the activities to the right things

- Consider the threats and your assets, the vulnerabilities of your systems and estimate the risks for your information security
- A **vulnerability** is a security-relevant error of an IT system. A vulnerability can cause a threat to take effect and damage a system. A vulnerability makes a system vulnerable to threats.
- **Threat** is a circumstance or event that exploits one or more vulnerabilities in a system to compromise one or more protection objectives.
- The **risk** R of a threat is the probability of the occurrence of a damage event and the amount of potential damage that can result from it.

  Risk = Likelyhood * Impact

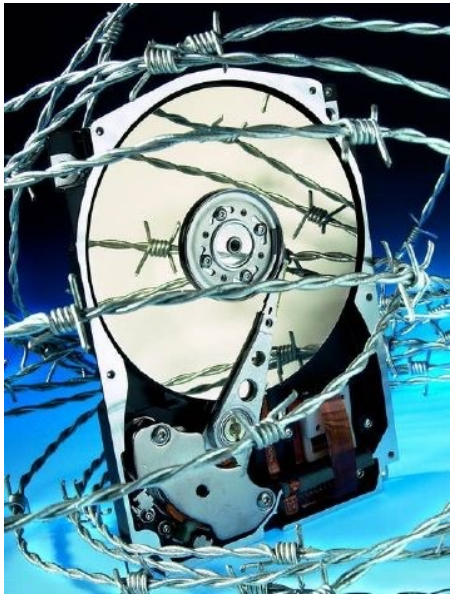
Risk management: Assesment and treatment of risks

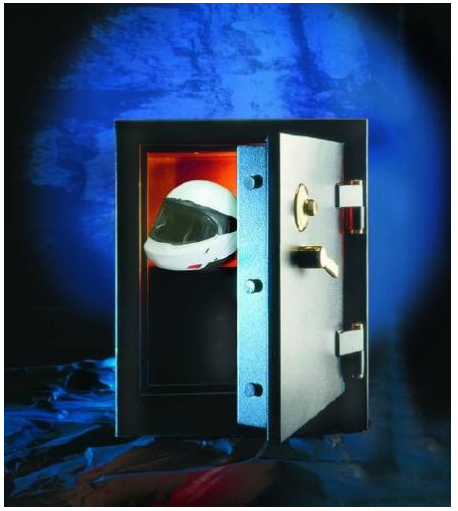


Source: Chopra A., Chaudhary M. (2020) Risk Management Approach. In: Implementing an Information Security Management System. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-5413-4_5

Measures and controls can reduce the risk

- Password Policy
- Virus protection, Firewall
- Emergency plan
- Outsourcing regulation
- Data backup concept
- Define responsibilities
- Rules for secure software development
- Training and information of employees
- Cryptography: encryption, signatures
- and so on.





(IX Thema 01 Security)

But this is not the end

- **Security is a continuous process !!!**
  - All measures must be reviewed regularly
  - New dangers must be identified
  - New measures need to be introduced if necessary
  - Everyone is affected and involved in this process
- **The greatest weakness is the human being**
  - Ignorance
  - Carelessness
  - Convenience
  - Cost, time and deadline pressure