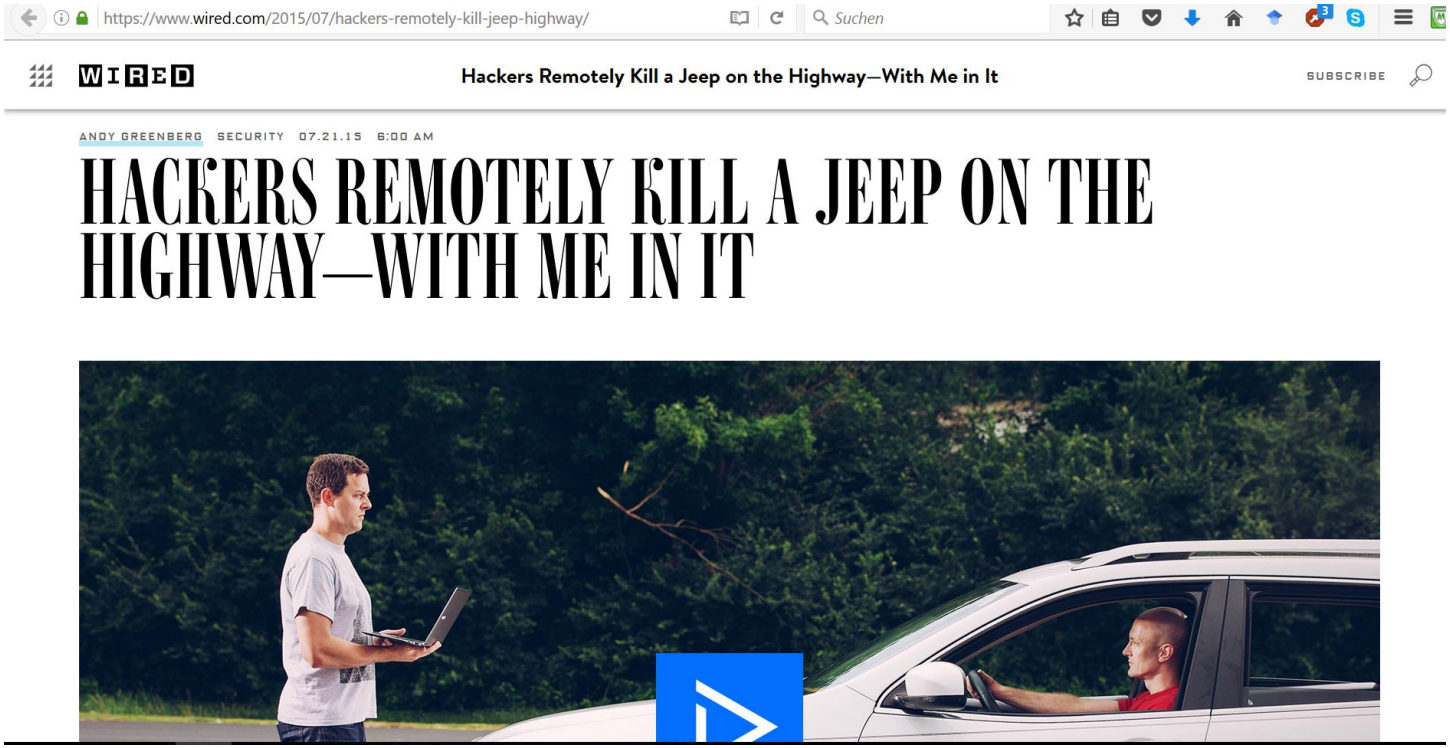
Computersystemsicherheit

Prof. Marc Fischlin, WS 2018/19

01

Einleitung

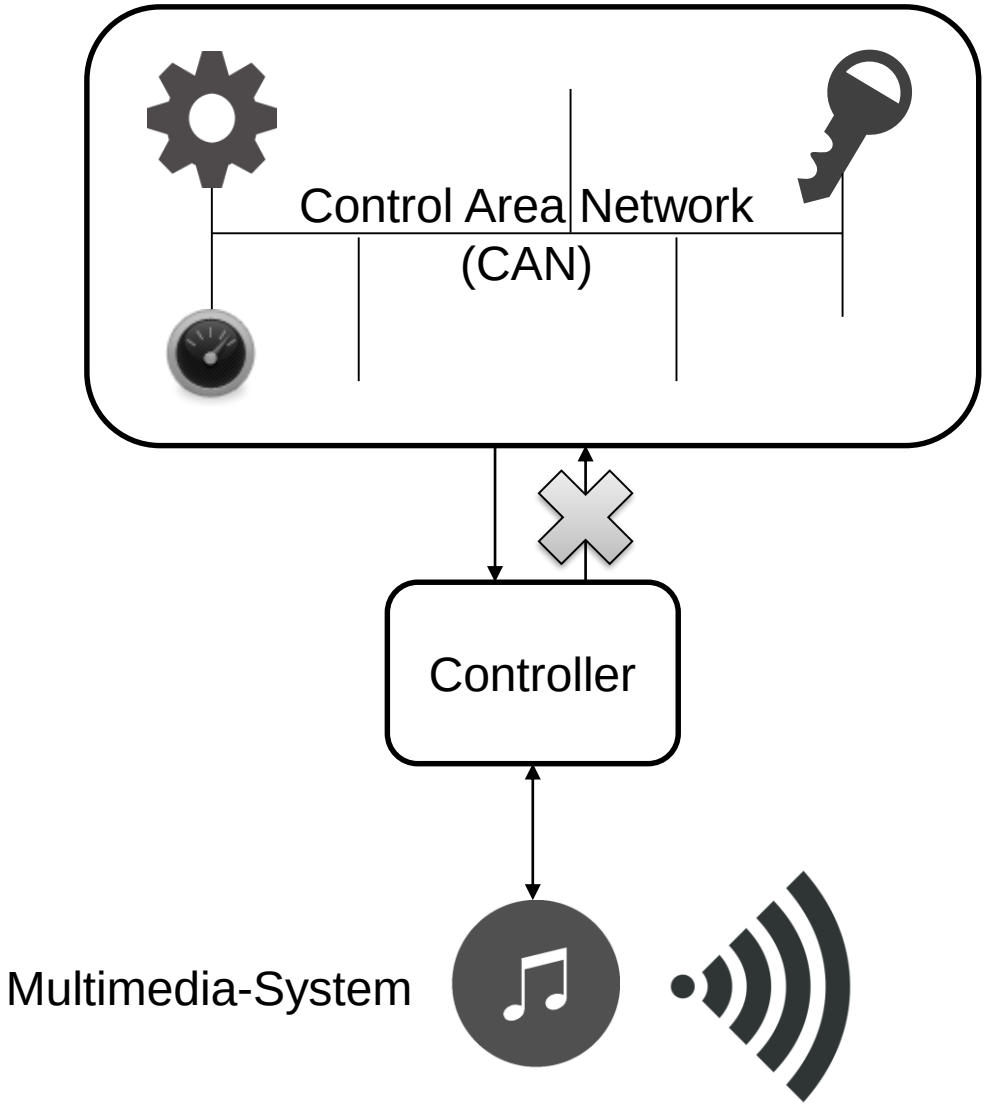
(Un)Sicherheit ist überall

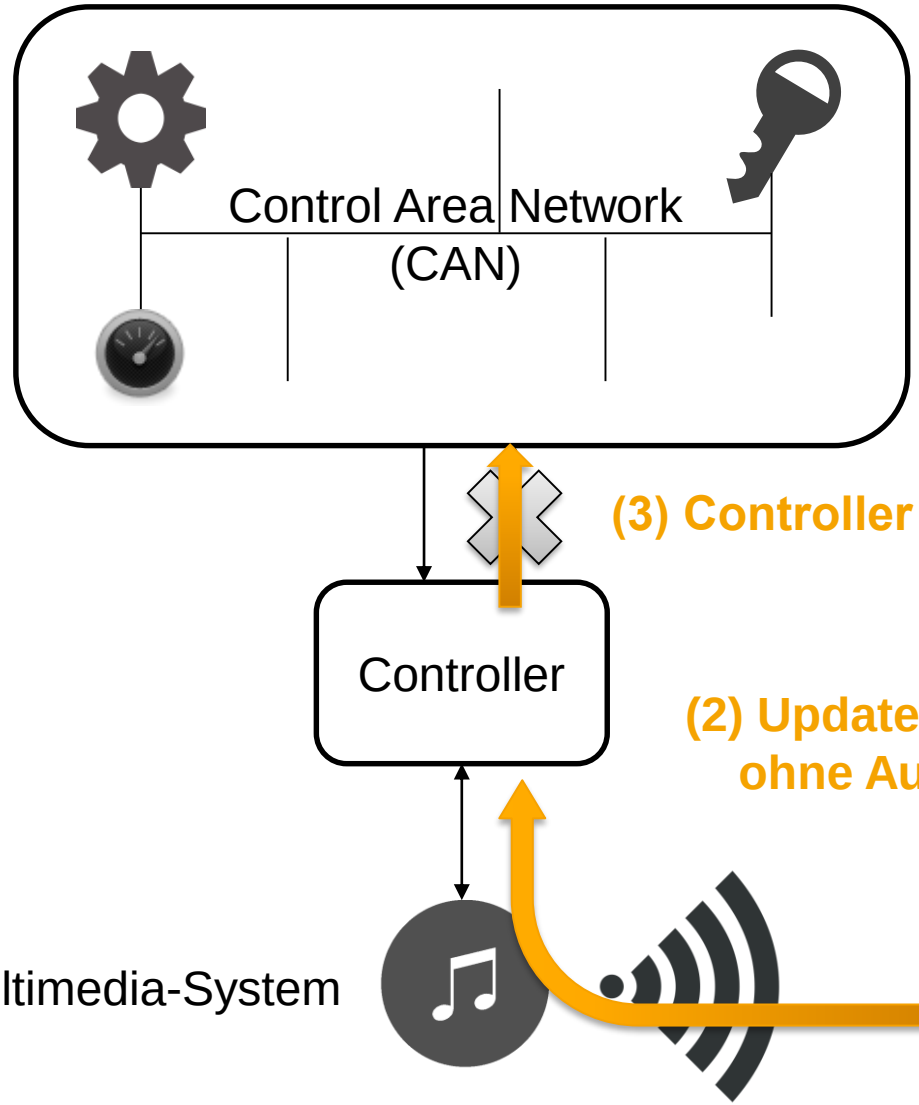


Video

Dokumentation

Schematische Darstellung
Auto-Komponenten





(4) Klimaanlage an,
Musik laut, bremsen,…

(3) Controller erlaubt nun „Senden“ an CAN

(2) Update Controller-Software
ohne Autorisierung möglich

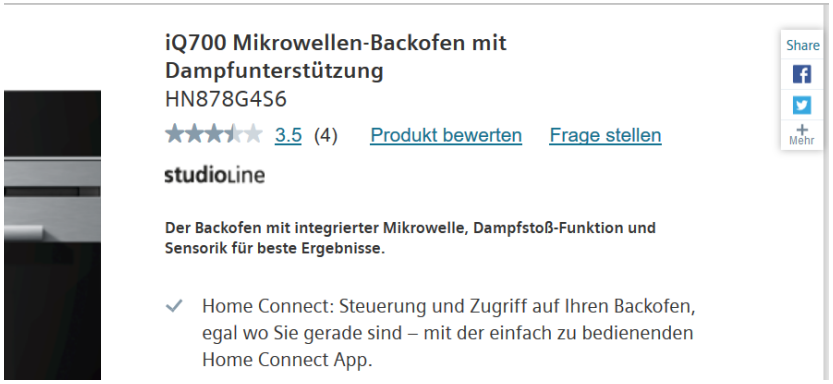
(1) WLAN Passwort
≈ Herstellungsdatum erraten

Lessons Learned

Komplexität ist der (erste) Feind der Sicherheit

Je komplexer ein System, desto schwieriger ist es, das System sicher zu machen.

Systeme werden immer komplexer, also:



Sicherheit ist in Zukunft (noch) schwieriger zu erreichen.

Lessons Learned

Sicherheit selbst ist komplex

Sicherheit besteht aus vielen Komponenten
und ist meistens nur so gut wie das schwächste Glied.

Quelle: 9gag.com

Um was geht es in der Veranstaltung „Computersystemsicherheit“?

Ziele der Veranstaltung

1. Sicherheit von Computersystemen „verstehen“

2. Auswahl für weitere Themen im Gebiet IT-Sicherheit

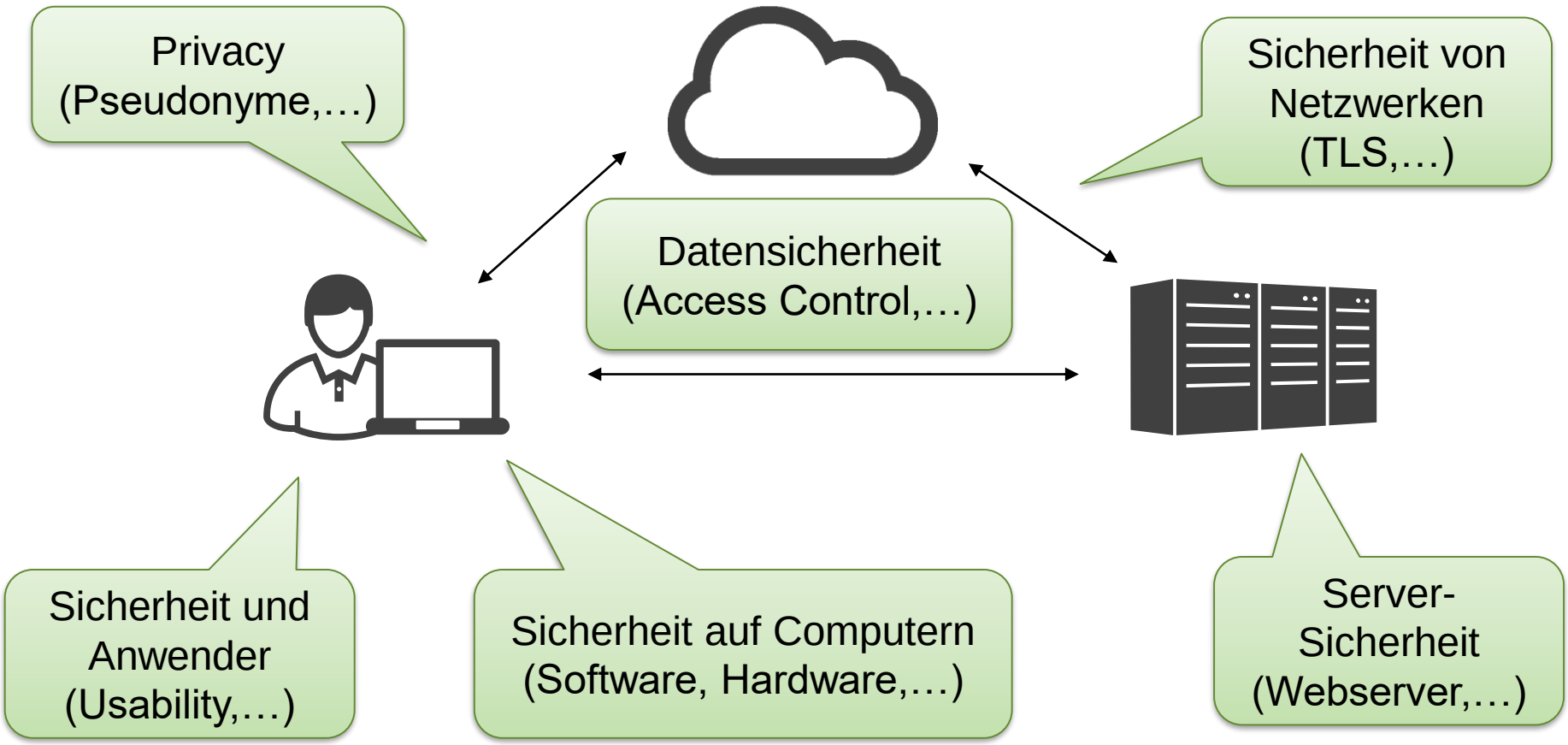
Warnung!

Sie werden in der Vorlesung auch einige Angriffsmöglichkeiten kennenlernen, um die Sicherheit von Computersystemen besser zu verstehen.

Sollten Sie diese Möglichkeiten außerhalb des in der Veranstaltung vorgesehenen Rahmens anwenden (z.B. gegen Kommilitonen, die TU Darmstadt, oder sonstige Dritte) kann dies rechtliche Konsequenzen für Sie haben!

Siehe insbesondere §202 StGB.

Um was geht es in der Computersystemsicherheit?

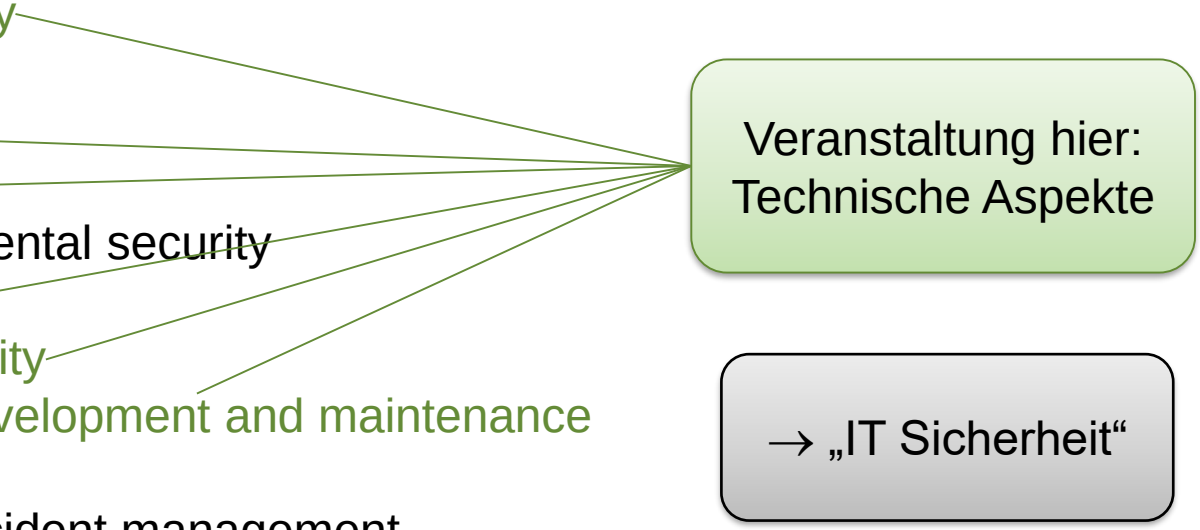


Die „ISO/IEC 27002“-Sicht

ISO/IEC 2700x ist Serie
von Standards zur IT-Sicherheit

14 Bereiche von Maßnahmen zur IT-Sicherheit:

A.5: Information security policies
A.6: Organization of information security
A.7: Human resource security
A.8: Asset management
A.9: Access control
A.10: Cryptography
A.11: Physical and environmental security
A.12: Operations security
A.13: Communications security
A.14: System acquisition, development and maintenance
A.15: Supplier relationships
A.16: Information security incident management
A.17: Information security aspects of business continuity management
A.18: Compliance; with internal requirements, such as policies,
and with external requirements, such as laws



„Sicherheits-Sprache“

Begriffe

zum Teil aus:
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Glossar der IT Grundschutz-Kataloge

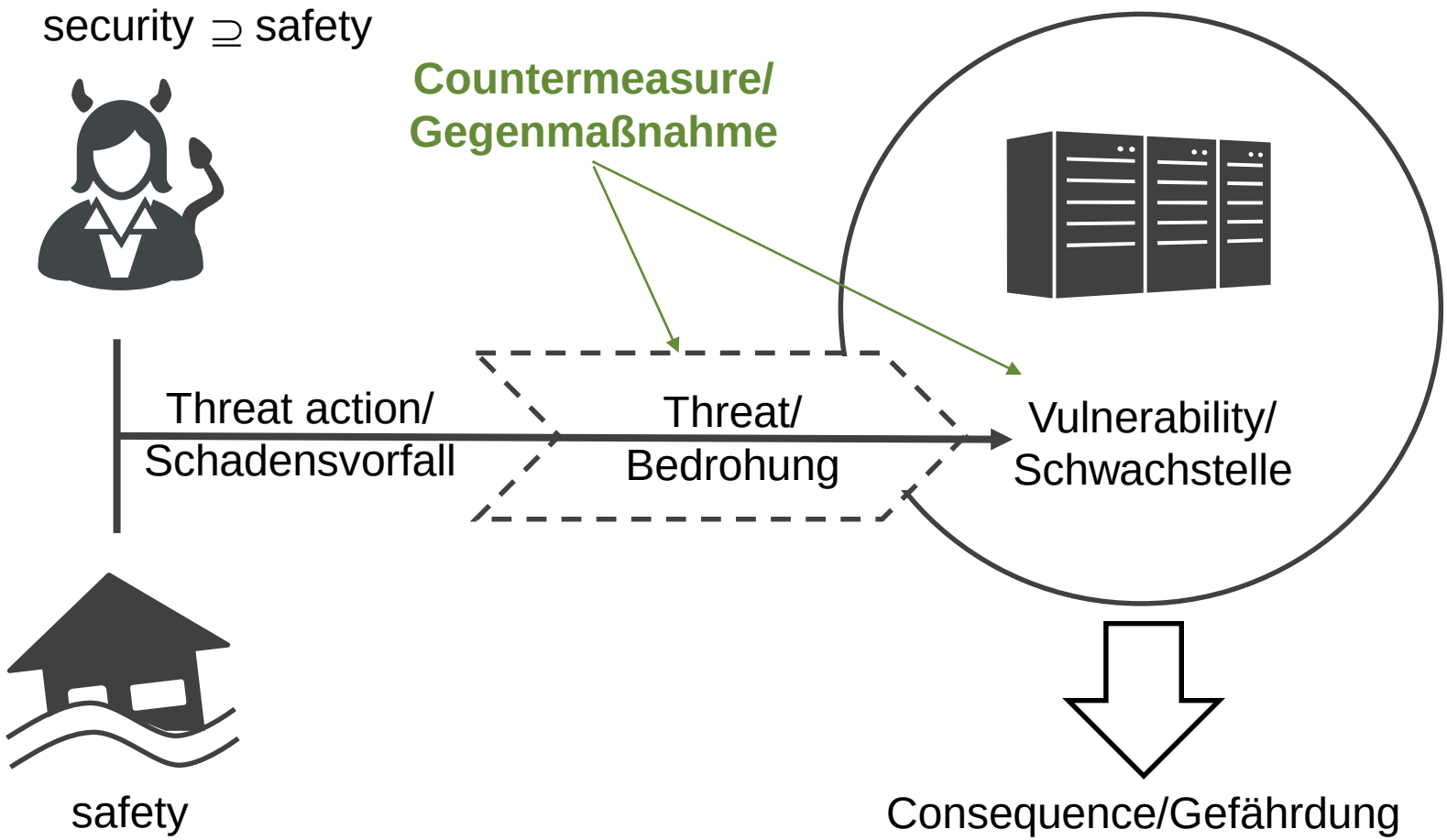
Vulnerability – Schwachstelle des Systems

Threat – Bedrohung. Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann.

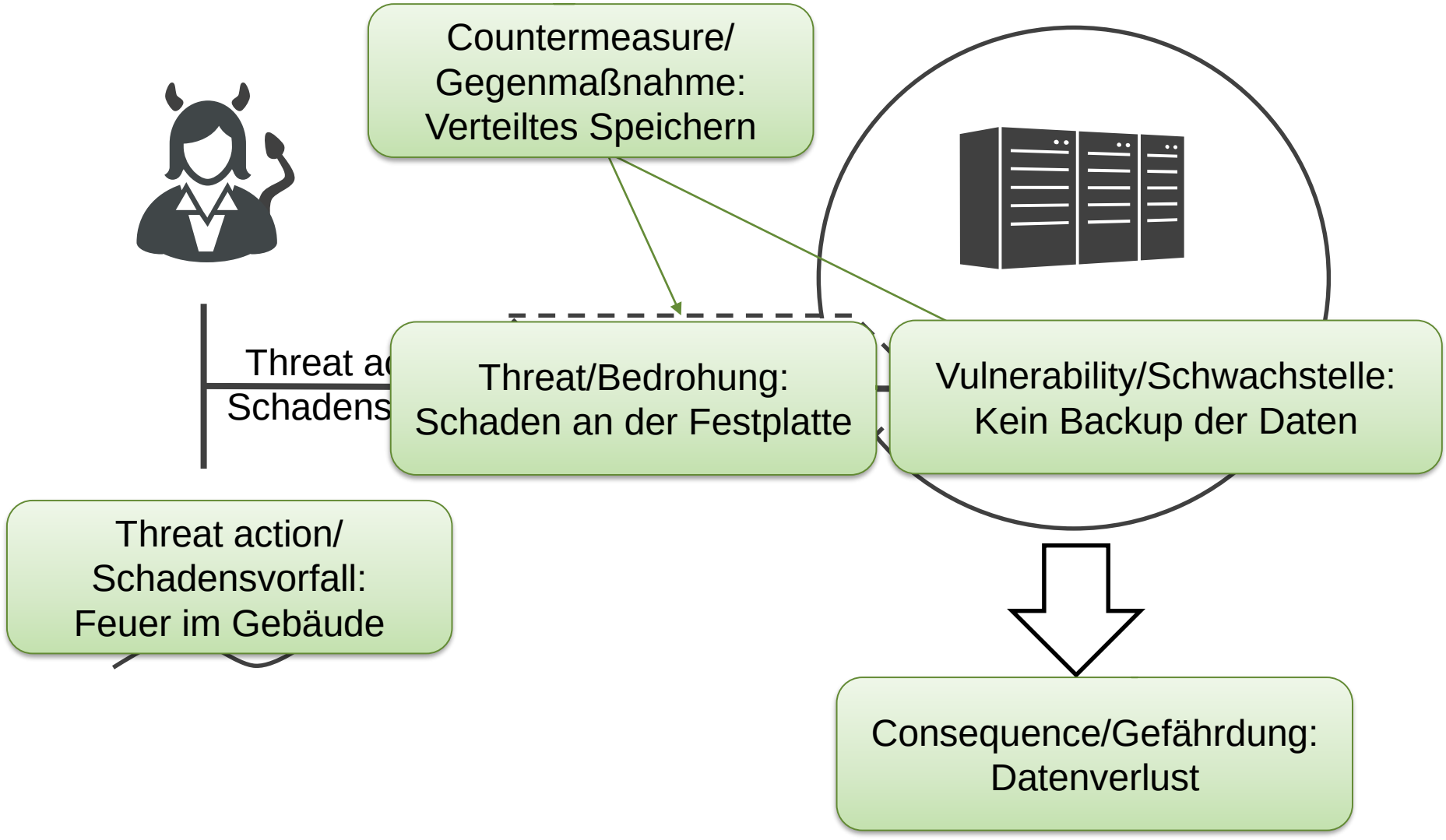
Threat Consequence – Gefahr/Gefährdung. Folge, wenn Bedrohung auf Schwachstelle trifft.

Threat action (**Exploit**) – Schadensvorfall. Konkreter Umstand oder Ereignis, durch das Schaden entsteht.

Countermeasure (**Control**) – Gegenmaßnahme, um Schwachstelle oder Bedrohung zu mindern oder zu beseitigen

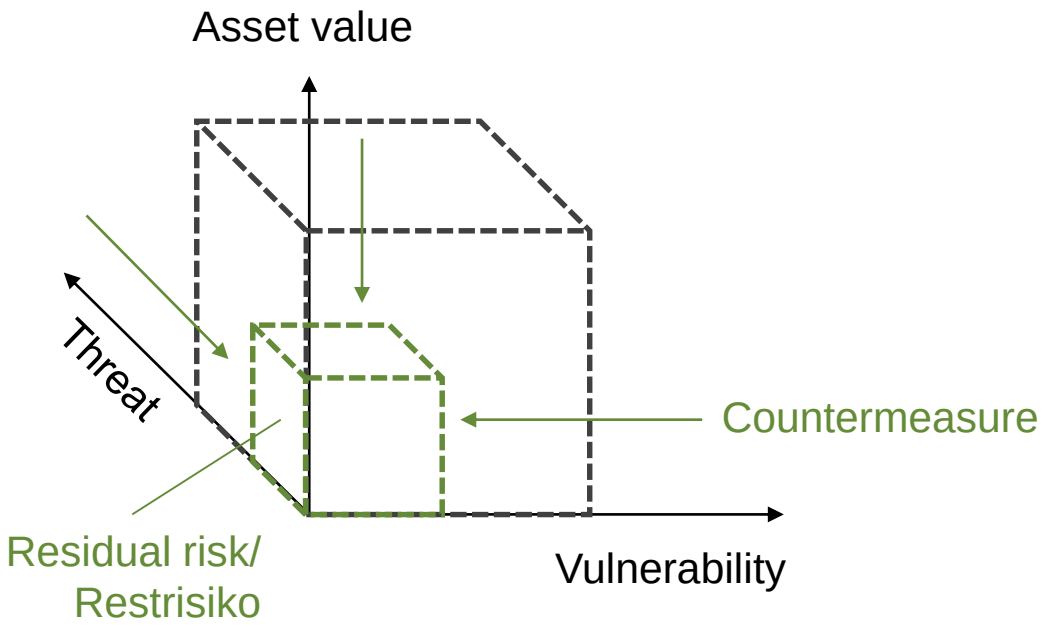


Gegenmaßnahme verhindert Ausnutzen der Schwachstelle durch Bedrohung.



Risiko = Funktion (Vulnerability, Threat, Asset)

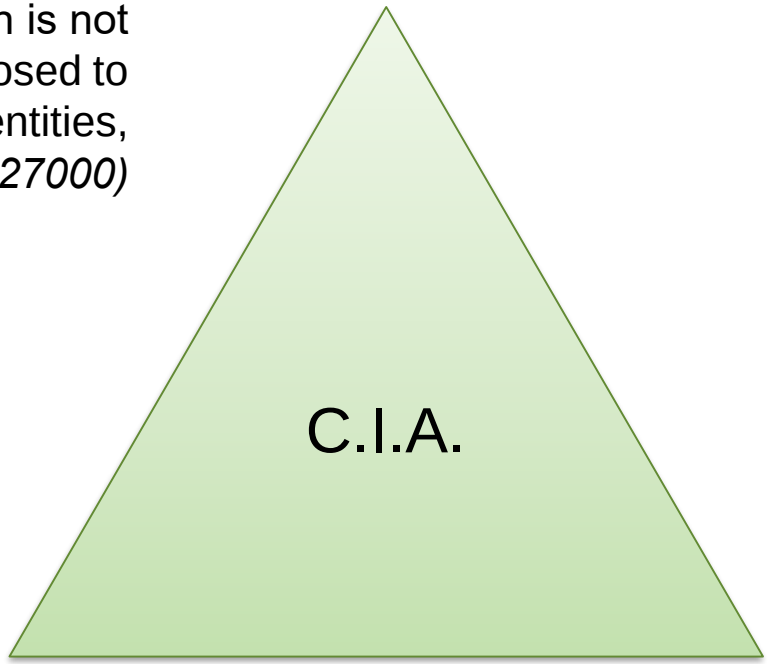
Asset/Wert – alles, was es zu schützen gilt



nach ENISA: „Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)“, Version 1.0, 2006

Schutzziele

Vertraulichkeit:
“property that information is not made available or disclosed to unauthorized individuals, entities, or processes“ *(ISO/IEC 27000)*



Unversehrtheit/Integrität:
“property of accuracy and completeness“
(ISO/IEC 27000)

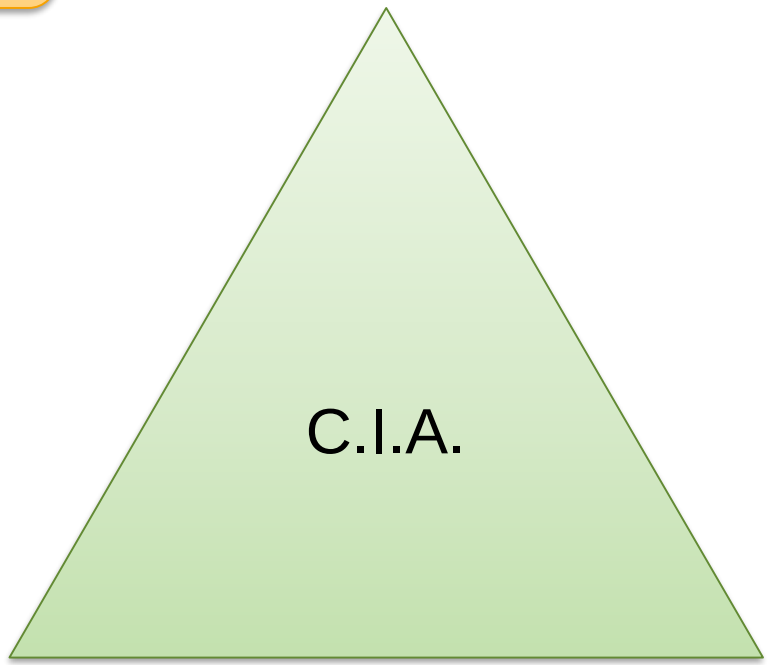
Verfügbarkeit:
“property of being accessible and usable upon demand by an authorized entity“
(ISO/IEC 27000)

nach ISO/IEC 27000 weitere möglich:
Authenticity (Authentizität), Accountability (Zurechenbarkeit), Non-repudiation (Verbindlichkeit), Reliability (Verlässlichkeit)

Mitlesen von Internetkommunikation

Confidentiality

Beispiel-Angriffe für Internetverbindungen



Integrity

Availability

Umleiten der Internetkommunikation

„Denial of Service“-Angriffe

Exerzieren Sie am Beispiel Vulnerability=
„Systemadministrator wählt Passwort 12345678“
die Sicherheitsbegriffe

Bennen Sie die drei großen Schutzziele.
Welche Ziele erreichen Sie z.B. mit
Festplattenverschlüsselung oder Backups?

Unter welchem Schutzziel würden Sie
Anonymität einordnen (und warum)?