

# Kapitel 2: Grundlagen



1. Ziele der Informationssicherheit
2. Systematik zur Einordnung von Sicherheitsmaßnahmen
3. Technik & Organisation - ISO/IEC 27000
4. Abgrenzung: Security vs. Safety

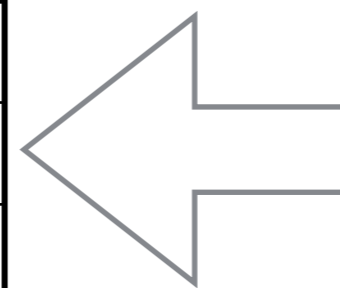
## ■ Hauptproblem:

Informationssicherheit (IS) kann nicht gemessen werden

- Es gibt keine Maßeinheit für IS
- Sicherheitskennzahlen (security metrics) quantifizieren nur Teilaspekte; organisationsübergreifend einheitliche Definitionen sind noch Mangelware.

## ■ Lösungsansatz: Indirekte Definition von IS durch (Teil-)Ziele:

|                 |                         |
|-----------------|-------------------------|
| Vertraulichkeit | <b>C</b> onfidentiality |
| Integrität      | <b>I</b> ntegrity       |
| Verfügbarkeit   | <b>A</b> vailability    |



*jeweils bezogen  
auf Daten und sie  
verarbeitende  
IT-Systeme*

Akronym **CIA** häufig in **englischer** IS-Literatur

# 1. Teilziel: Vertraulichkeit

## ■ Definition im Kontext *Daten*:

Vertraulichkeit (engl. confidentiality) ist gewährleistet, wenn geschützte Daten nur von Berechtigten genutzt werden können.

## ■ In vernetzten Systemen zu betrachten bezüglich:

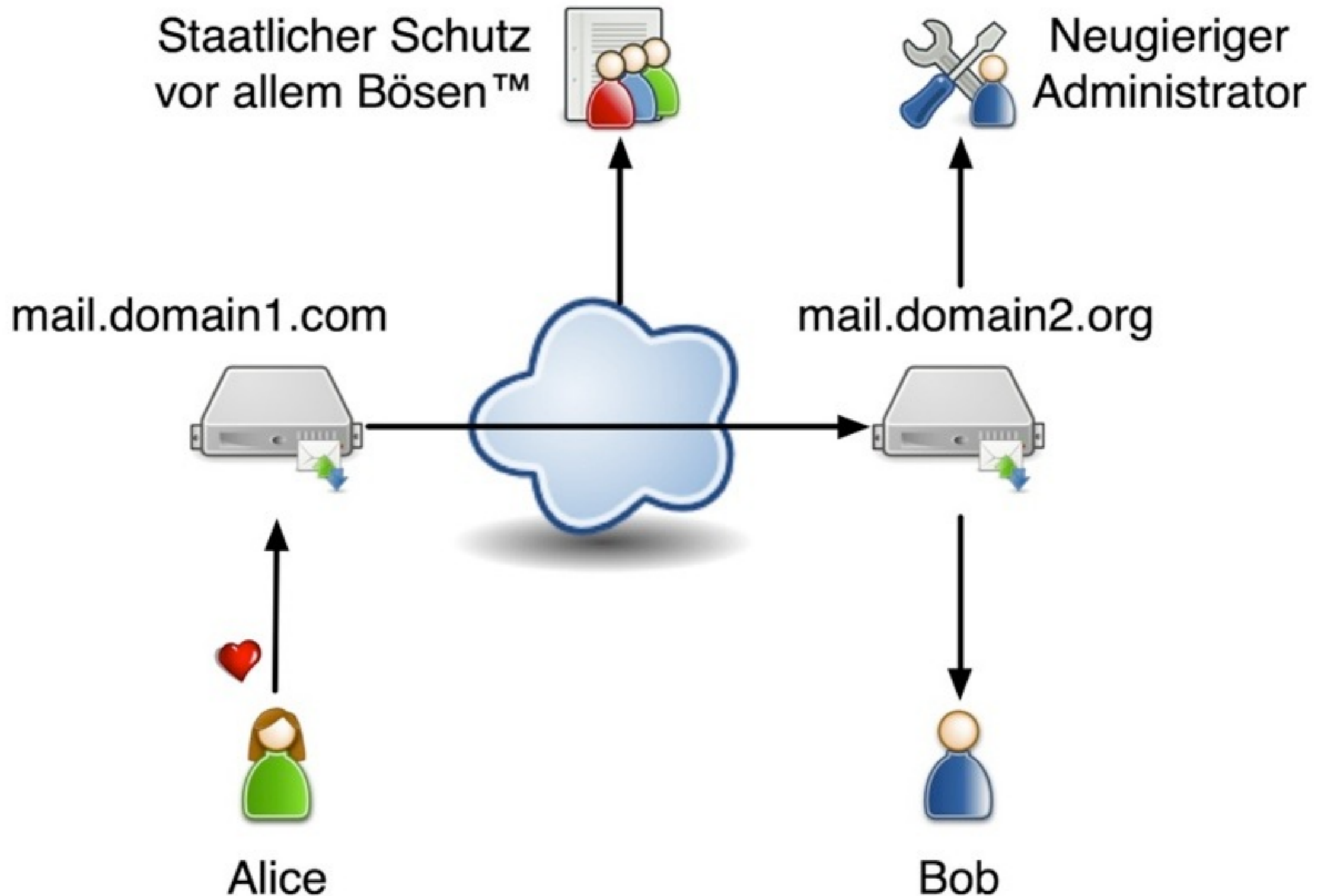
- Transport von Daten (über Rechnernetze)
- Speicherung von Daten (inkl. Backup)
- Verarbeitung von Daten

## ■ Typische Sicherheitsmaßnahme: Verschlüsselung

## ■ Teilziel gilt als verletzt, wenn geschützte Daten von unautorisierten Subjekten eingesehen werden können.

## ■ Kontext *Dienste*: Vertrauliche IT-Dienste können nur von autorisierten Anwendern genutzt werden.

# Beispiel: Vertraulichkeit von E-Mails

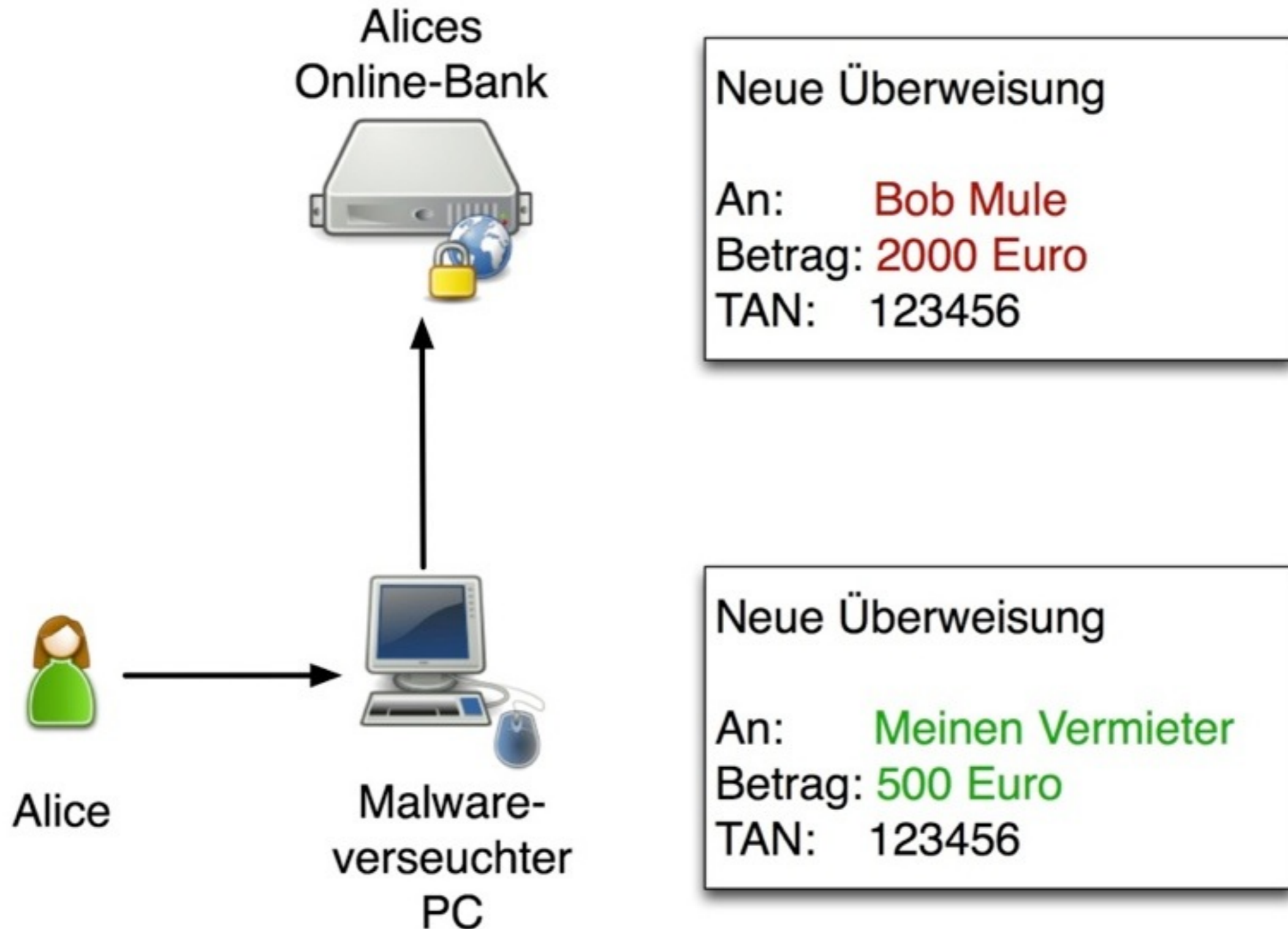


- Definition im Kontext *Daten*:

Integrität (engl. integrity) ist gewährleistet, wenn geschützte Daten nicht unautorisiert und unbemerkt modifiziert werden können.

- Wiederum bei Transport, Speicherung und Verarbeitung sicherzustellen!
- Typische Sicherheitsmaßnahme: Kryptographische Prüfsummen
- Teilziel verletzt, wenn Daten von unautorisierten Subjekten *unbemerkt* verändert werden.
- Kontext *Dienste*: Integre IT-Dienste haben keine (versteckte) Schadfunktionalität.

# Beispiel: Integrität im Online-Banking

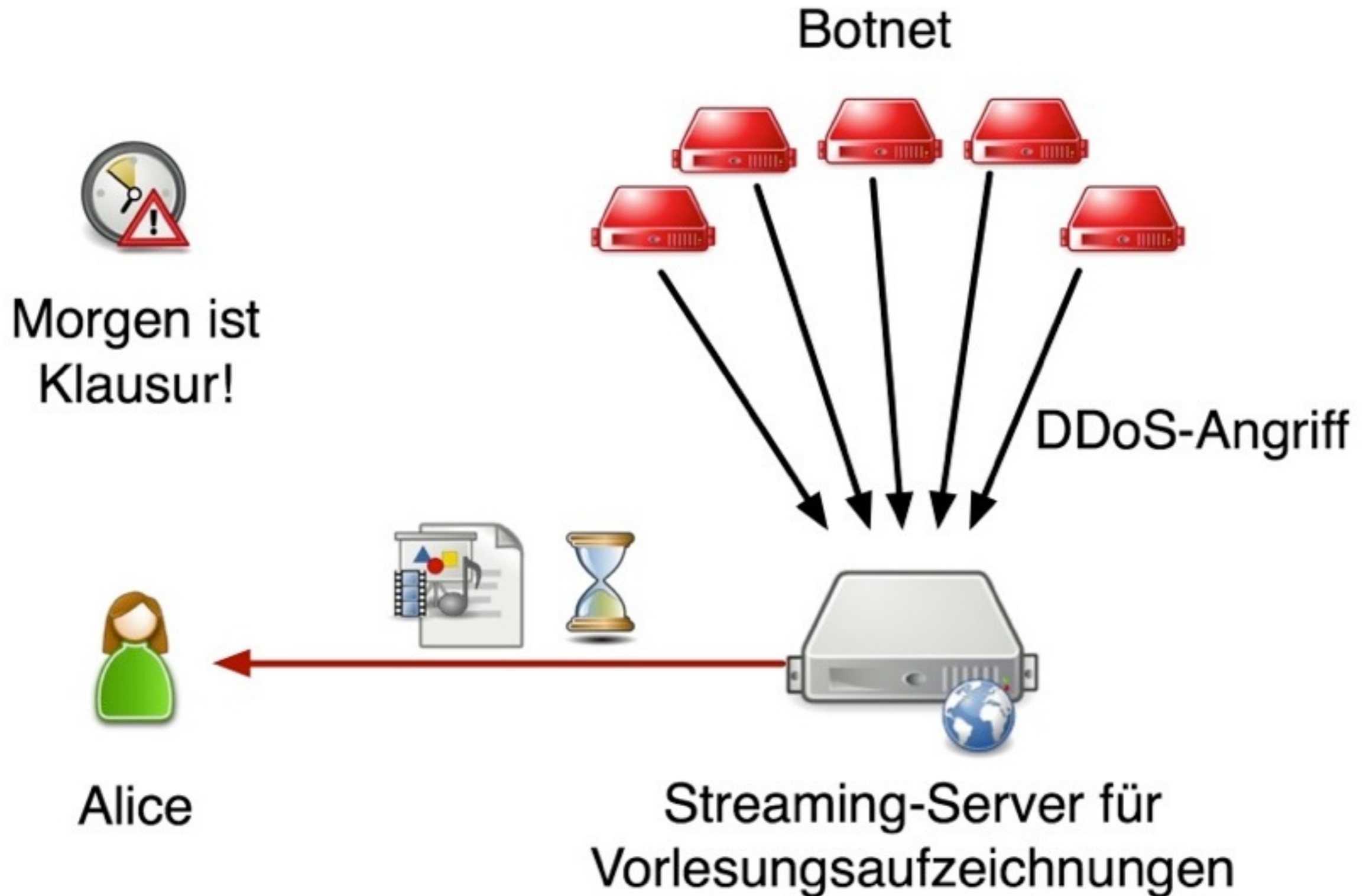


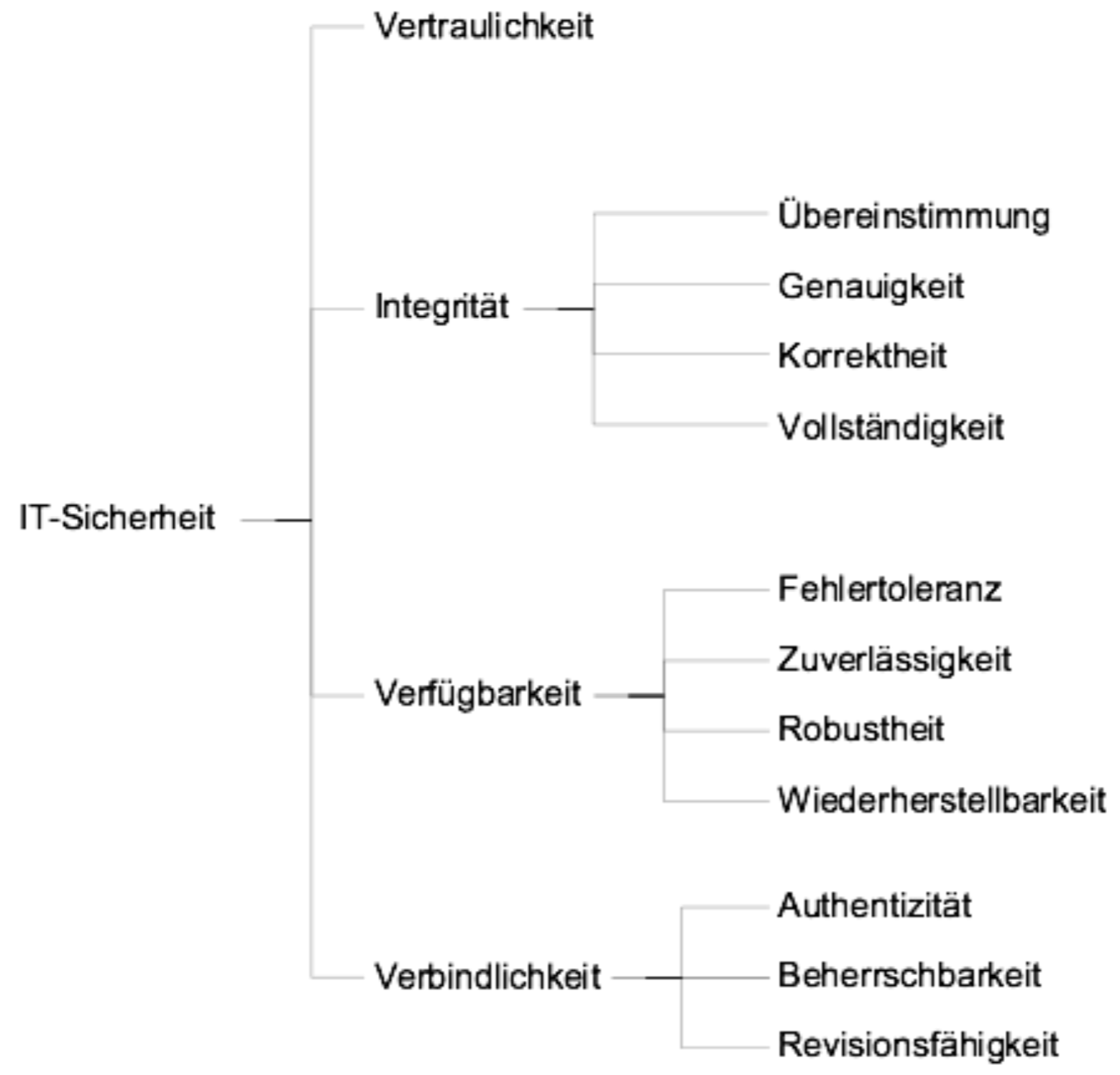
- Definition:

Verfügbarkeit (engl. availability) ist gewährleistet, wenn autorisierte Subjekte störungsfrei ihre Berechtigungen wahrnehmen können.

- Bezieht sich nicht nur auf Daten, sondern z.B. auch auf Dienste und ganze IT-Infrastrukturen.
- Typische Sicherheitsmaßnahme: Redundanz (z.B. Daten-Backups), Overprovisioning (z.B. mehr als genug Server)
- Teilziel verletzt, wenn ein Angreifer die Dienst- und Datennutzung durch legitime Anwender einschränkt.







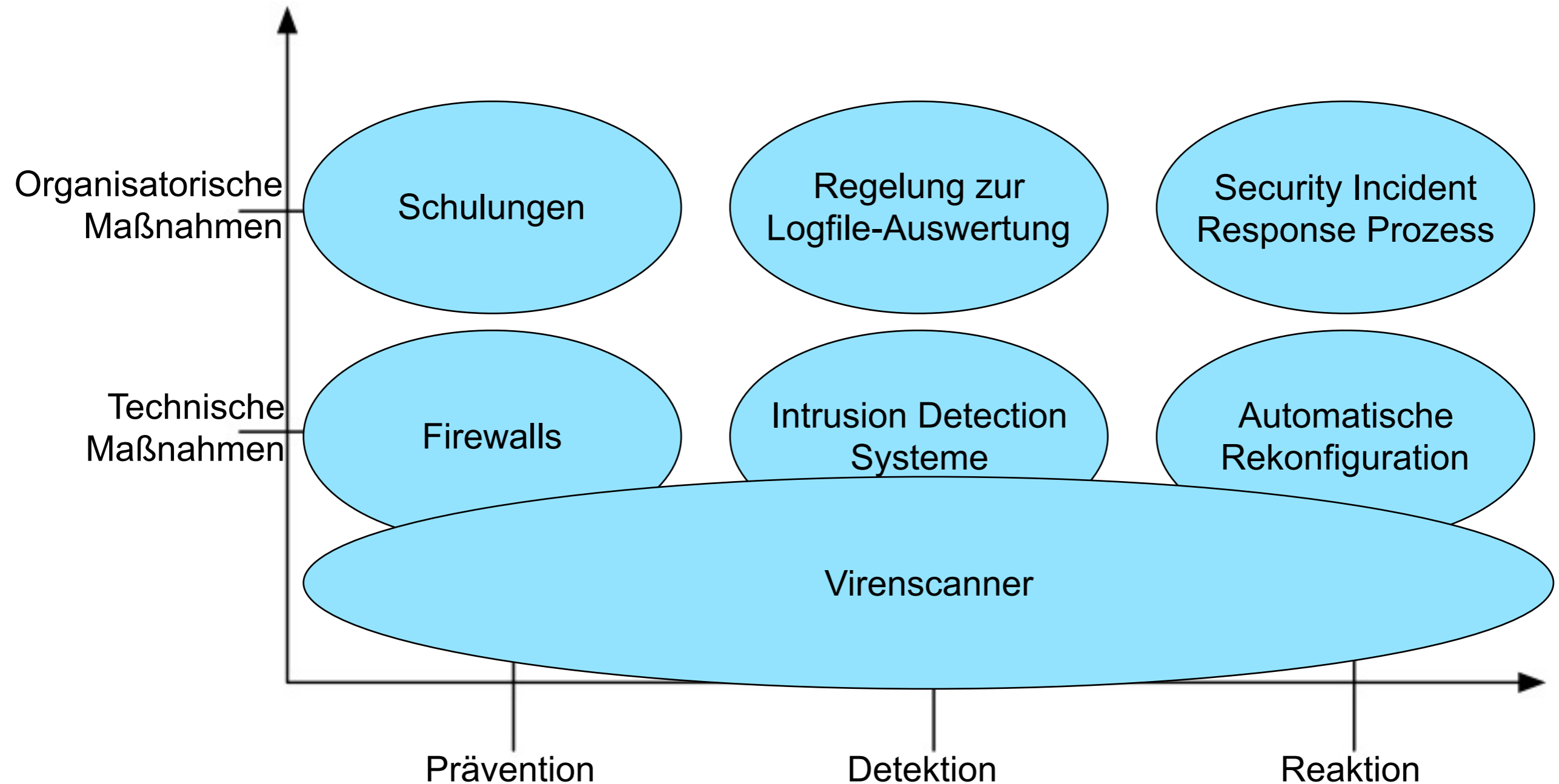
*Vgl. CIA in englischer Literatur:*

*Hier auch Verbindlichkeit (non-repudiation) als Top-Level-Ziel*

[In Anlehnung an Hartmut Pohl]

1. Ziele der Informationssicherheit
2. Systematik zur Einordnung von Sicherheitsmaßnahmen
3. Technik & Organisation - ISO/IEC 27000
4. Abgrenzung: Security vs. Safety

- Zum Erreichen der IS-Teilziele müssen Sicherheitsmaßnahmen umgesetzt werden (vgl. IS-Risikomanagement in Kapitel 3).
- Sicherheitsmaßnahmen gibt es zuhauf; sie entwickeln sich wie Dienste und Angriffe ständig weiter.
  - In der Vorlesung werden wichtige “klassische” und diverse aktuelle Sicherheitsmaßnahmen behandelt, aber bei Weitem nicht alle.
  - Systematische Einordnung ist Basiskompetenz bei der Analyse und Bewertung neuer Sicherheitsmaßnahmen.
- Wir orientieren uns an **zwei** bewährten **Dimensionen**:
  - **Lebenszyklus potentiell erfolgreicher Angriffe** auf Dienste/Daten
  - Unterscheidung zwischen **technischen und organisatorischen** Maßnahmen (=> Faktor Mensch nie zu unterschätzen!)



Einige Sicherheitsmaßnahmen können mehreren Kategorien zugeordnet werden, d.h. es liegt keine Taxonomie vor!

- Die Kombination aller in einem Szenario eingesetzten **präventiven** Maßnahmen dient der **Erhaltung** von *Vertraulichkeit, Integrität und Verfügbarkeit*.
- **Detektierende** Maßnahmen dienen dem **Erkennen** von unerwünschten Sicherheitsereignissen, bei denen die präventiven Maßnahmen unzureichend waren.
- **Reagierende** Maßnahmen dienen der **Wiederherstellung** des Soll-Zustands nach dem Erkennen von unerwünschten Sicherheitsereignissen.

## ■ Grundidee:

- **Maßnahmenauswahl** ist immer szenarienspezifisch
- **Risikogetriebenes** Vorgehensmodell

## ■ Kernfragestellungen:

- Welche Sicherheitsmaßnahmen sollen wann und in welcher Reihenfolge ergriffen werden?
- Lohnt sich der damit verbundene Aufwand (Investition/Betrieb)?

## ■ Voraussetzung **Risikomanagement** (hier nur Überblick):

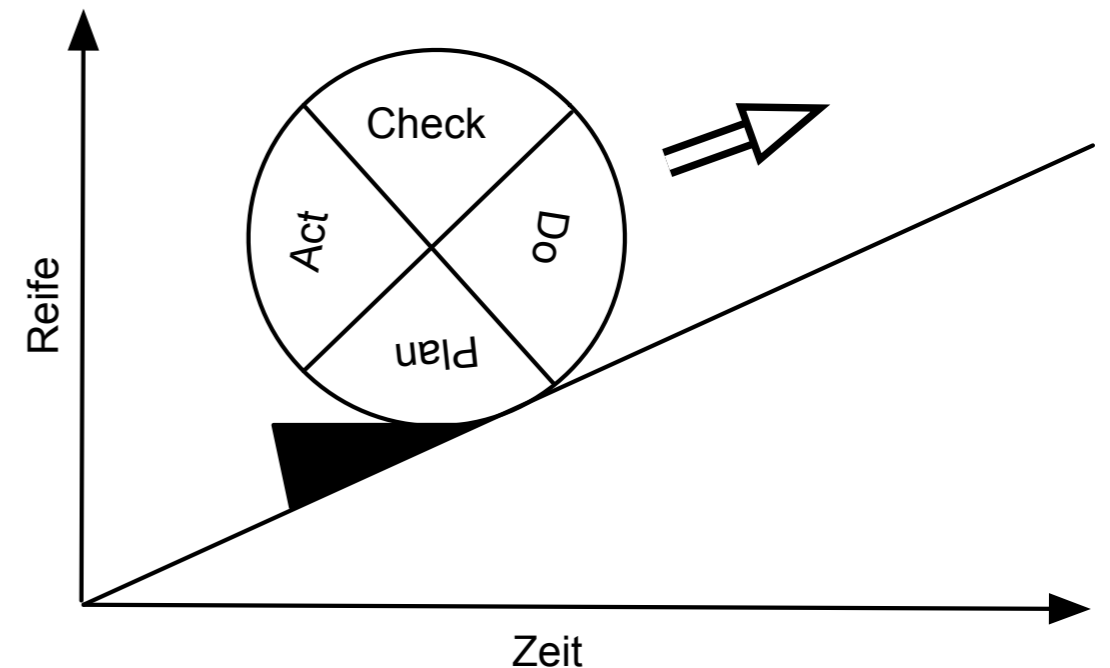
- Analyse des Schutzbedarfs
- Überlegungen zu möglichen Angriffen und deren Auswirkungen
- Ermittlung / Evaluation passender Lösungswege
- Entscheidung möglichst auf Basis quantitativer (d.h. nicht nur qualitativer) Bewertung

1. Ziele der Informationssicherheit
2. Systematik zur Einordnung von Sicherheitsmaßnahmen
3. Technik & Organisation - ISO/IEC 27000
4. Abgrenzung: Security vs. Safety



- Informationssicherheit Anfang der 1990er Jahre:
  - Stark technikzentriert
  - Kosten-/Nutzenfrage kommt auf
  - Führungsebene wird stärker in IS-Fragestellungen eingebunden
  
- Wachsender Bedarf an Vorgaben und Leitfäden:
  - Kein „Übersehen“ wichtiger IS-Aspekte
  - Organisationsübergreifende Vergleichbarkeit
  - Nachweis von IS-Engagement gegenüber Kunden und Partnern
  
- Idee hinter ISO/IEC 27000:  
Anwendung der Grundprinzipien des Qualitätsmanagements auf das Management der Informationssicherheit

- ISO/IEC 27000 wird mehrere Dutzend einzelne Standards umfassen
  - Mehr als die Hälfte davon ist noch in Arbeit und nicht veröffentlicht
  
- Norm ISO/IEC 27001 legt **Mindestanforderungen** an sog. Information Security Management Systems (ISMS) fest
  - Zertifizierungen möglich für:
    - Organisationen (seit 2005)
    - Personen (seit 2010)
  - Inhaltliche Basis:
    - **Kontinuierliche Verbesserung** durch Anwendung des Deming-Zyklus (PDCA)
    - **Risikogetriebenes Vorgehen**
  - Seit 2008 auch DIN ISO/IEC 27001



- Begriffsdefinitionen (Verweis auf DIN ISO/IEC 27000)
- PDCA-basierter Prozess zum Konzipieren, Implementieren, Überwachen und Verbessern eines ISMS
- Mindestanforderungen u.a. an Risikomanagement, Dokumentation und Aufgabenverteilung
- Normativer Anhang A enthält:
  - Definition von Maßnahmenzielen (control objectives)
  - Definition von Maßnahmen (controls)
- Umfang:
  - DIN ISO/IEC 27001:2015 - 31 Seiten
  - DIN ISO/IEC 27002:2015 - 103 Seiten

A.5 Informationssicherheitsleitlinien (1/2) [ = 1 Objective, 2 Controls ]

A.6 Organisation der Informationssicherheit (2/7)

A.7 Personalsicherheit (3/6)

A.8  
Verwaltung der Werte  
(3/10)

A.9  
Zugangssteuerung  
(4/14)

A.10  
Kryptographie  
(1/2)

A.11  
Physische Sicherheit  
(2/15)

A.12  
Betriebssicherheit  
(7/14)

A.13  
Kommunikations-  
sicherheit  
(2/7)

A.14  
Anschaffung,  
Entwicklung von  
Systemen  
(3/13)

A.15  
Lieferantenbeziehungen  
(2/5)

A.16 Handhabung von  
Sicherheitsvorfällen (1/7)

A.17 Business Continuity  
Management (2/4)

A.18 Compliance (2/8)

**A.8.1 Verantwortlichkeit für Werte**

Inventarisierung

Zuständigkeit

Zulässiger Gebrauch

Rückgabe

**A.8.2 Informationsklassifizierung**Klassifizierung von  
InformationenKennzeichnung von  
InformationenHandhabung von  
Werten**A.8.3 Handhabung von Datenträgern**

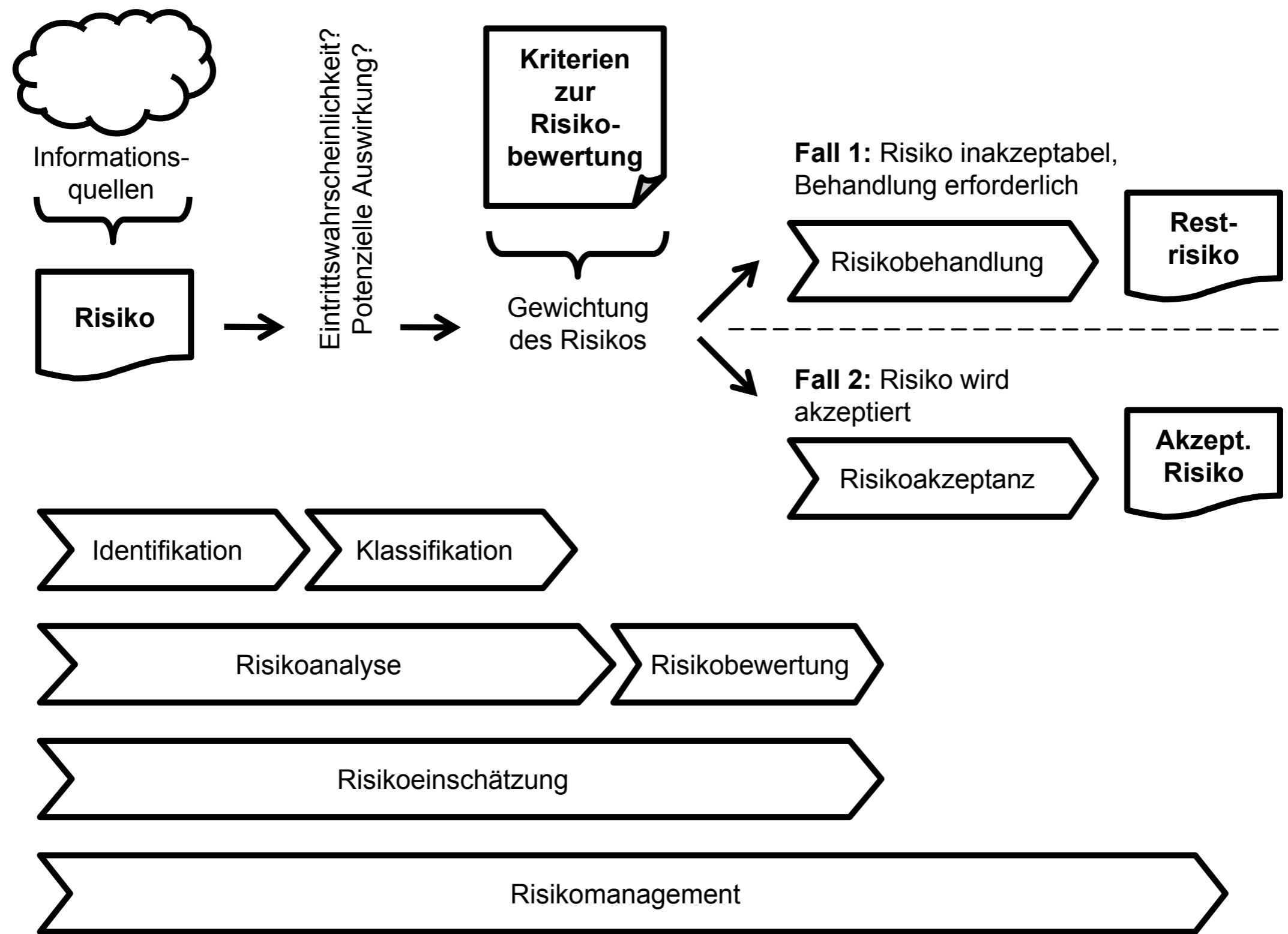
Wechseldatenträger

Entsorgung

Transport

## Beispiel A.8.3.2 - Entsorgung von Datenträgern:

Nicht mehr benötigte Datenträger werden sicher und unter Anwendung formaler Verfahren entsorgt. [\[DIN ISO/IEC 27001:2015-03, S. 19\]](#)

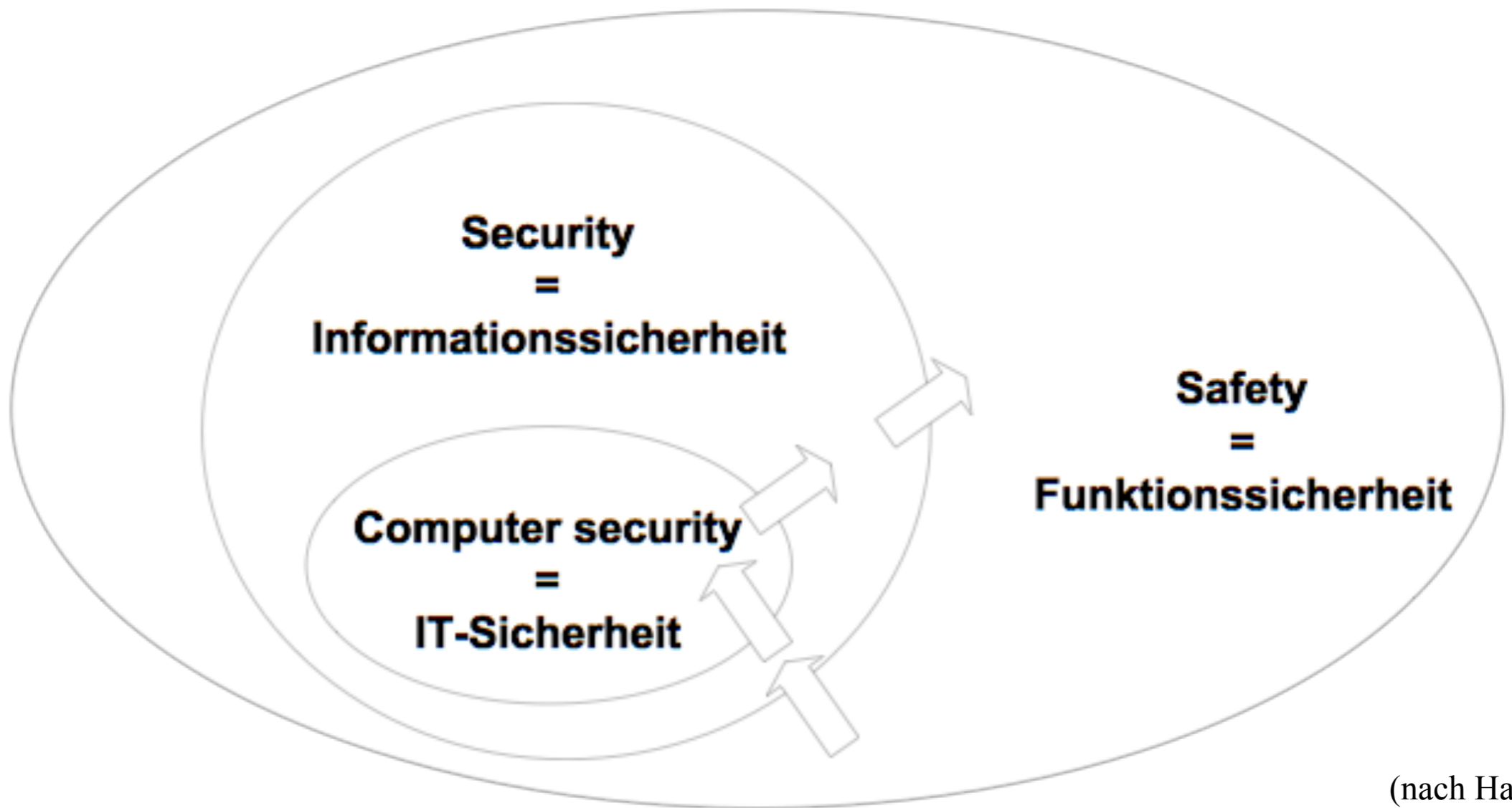
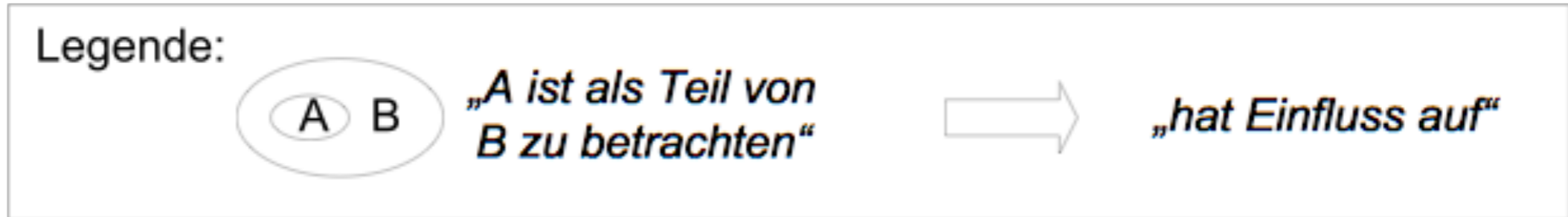


1. Ziele der Informationssicherheit
2. Systematik zur Einordnung von Sicherheitsmaßnahmen
3. Technik & Organisation - ISO/IEC 27000
4. Abgrenzung: Security vs. Safety

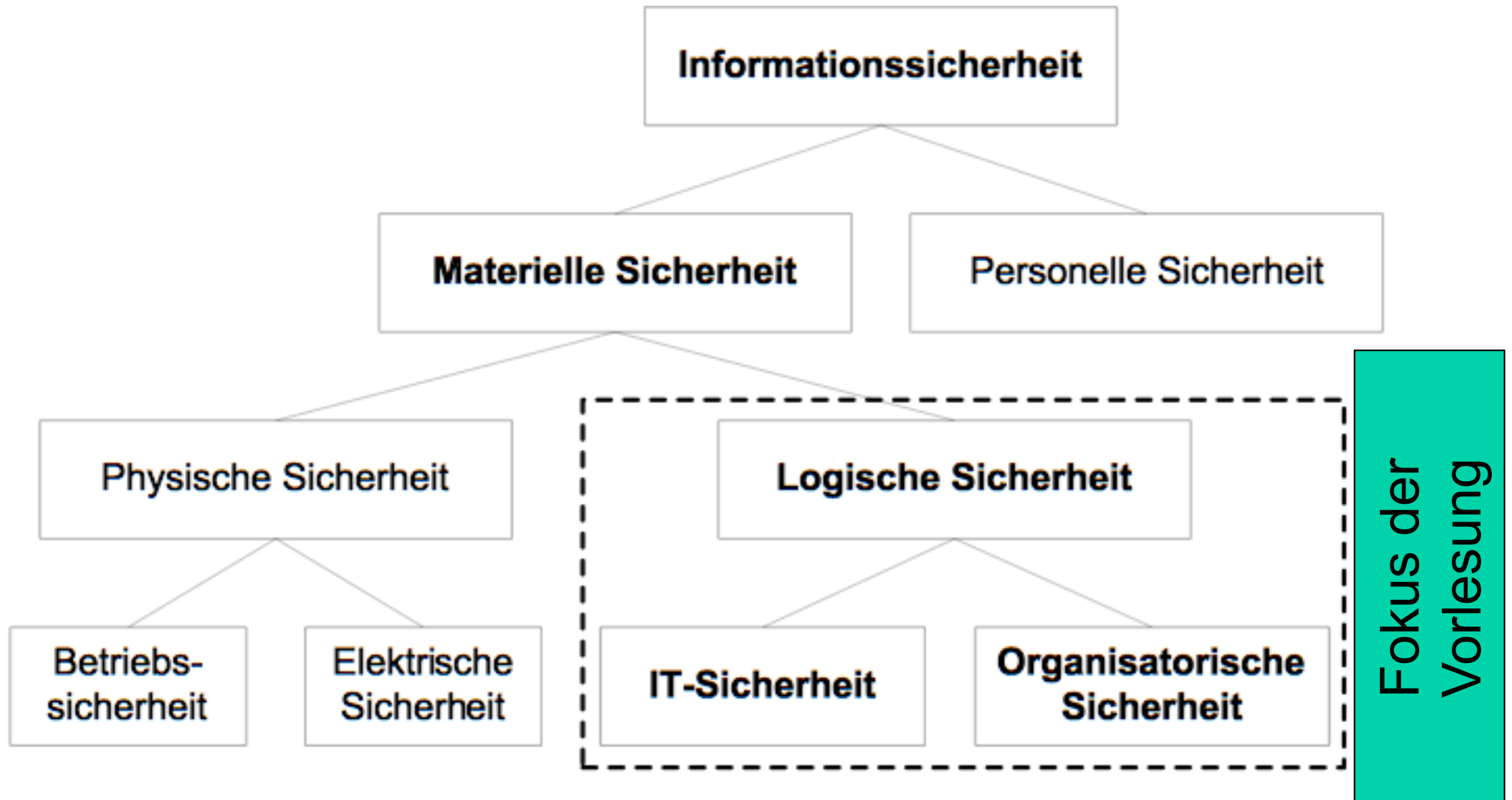
- Beide Begriffe werden oft mit „Sicherheit“ übersetzt
- Typische Themen der Safety („Funktionssicherheit“)
  - Betriebssicherheit für sicherheitskritische Programme, z.B. Steuerung und Überwachung von Flugzeugen, Kraftwerken und Produktionsanlagen
  - Ausfallsicherheit (Reliability)
  - Gesundheitsrelevante Sicherheitseigenschaften / Ergonomie
- Typische Themen der Security („Sicherheit“ i.S.d. Vorlesung)
  - Hardware-/Software-/Netz-basierte Angriffe und Gegenmaßnahmen
  - Security Engineering: Design und Implementierung sicherer IT-Systeme
    - Security Policies: Sicherheitsanforderungen und deren Umsetzung
    - Anwendung von Kryptographie, Hardware-Designmethoden, ... im Kontext „C I A“ von Daten und Diensten



# Einordnung Safety/Security (1/2)



(nach Hartmut Pohl)



(nach Hartmut Pohl)