



Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

The background of the slide is a photograph of a modern, multi-story building with a glass and metal facade. The building is partially obscured by a blue overlay. In the foreground, there are trees and a street with a few people walking. The overall color scheme is blue and white.

Kapitel 2: Grundlagen

Cyber Resilliance Act (CRA) von der EU verabschiedet

- EU verabschiedet am 10.10.24 den CRA
 - Tritt 20 Tage nach Veröffentlichung in Kraft
- Cybersicherheit von vernetzten Produkten soll erhöht werden
- Ab Nov. 2027 müssen Produkte mit digitalen Elementen grundlegende Anforderungen erfüllen
 - Risikobasierter Ansatz
 - TR-03183 - Cyber Resilliance Requirements for Manufacturer and Products
 - Meldepflicht für Schwachstellen
 - Dokumentationspflichten - mehr Transparenz über Sicherheitseigenschaften
- Sicherheitsupdates über die Lebensdauer des Produktes (max. 5 Jahre)
- CE-Zeichen wird um Cybersicherheit erweitert

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

Ziele der Informationssicherheit

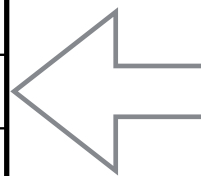
■ Hauptproblem:

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	C onfidentiality
Integrität	I ntegrity
Verfügbarkeit	A vailability



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

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

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

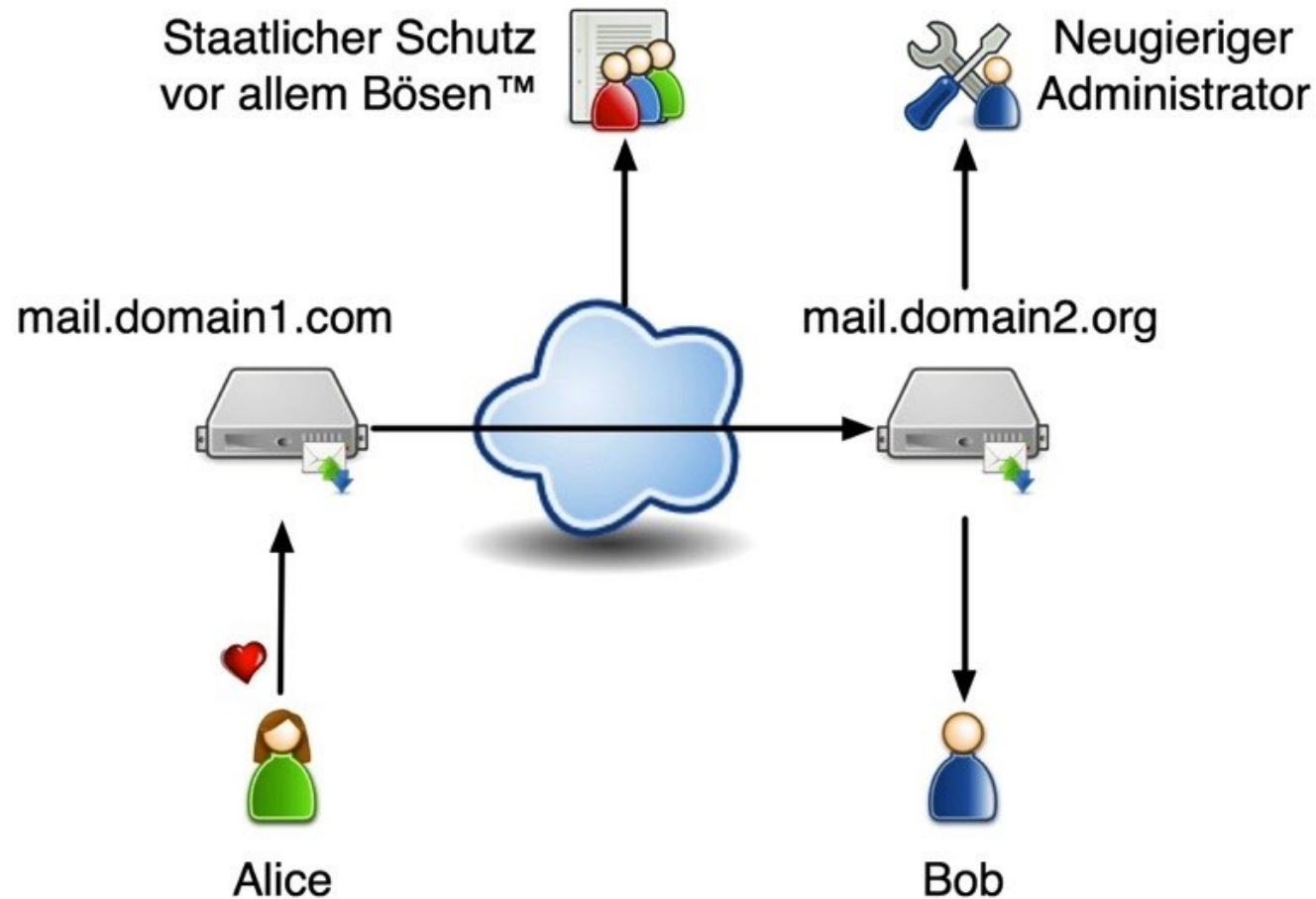
■ Typische Sicherheitsmaßnahme: Verschlüsselung

■ 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

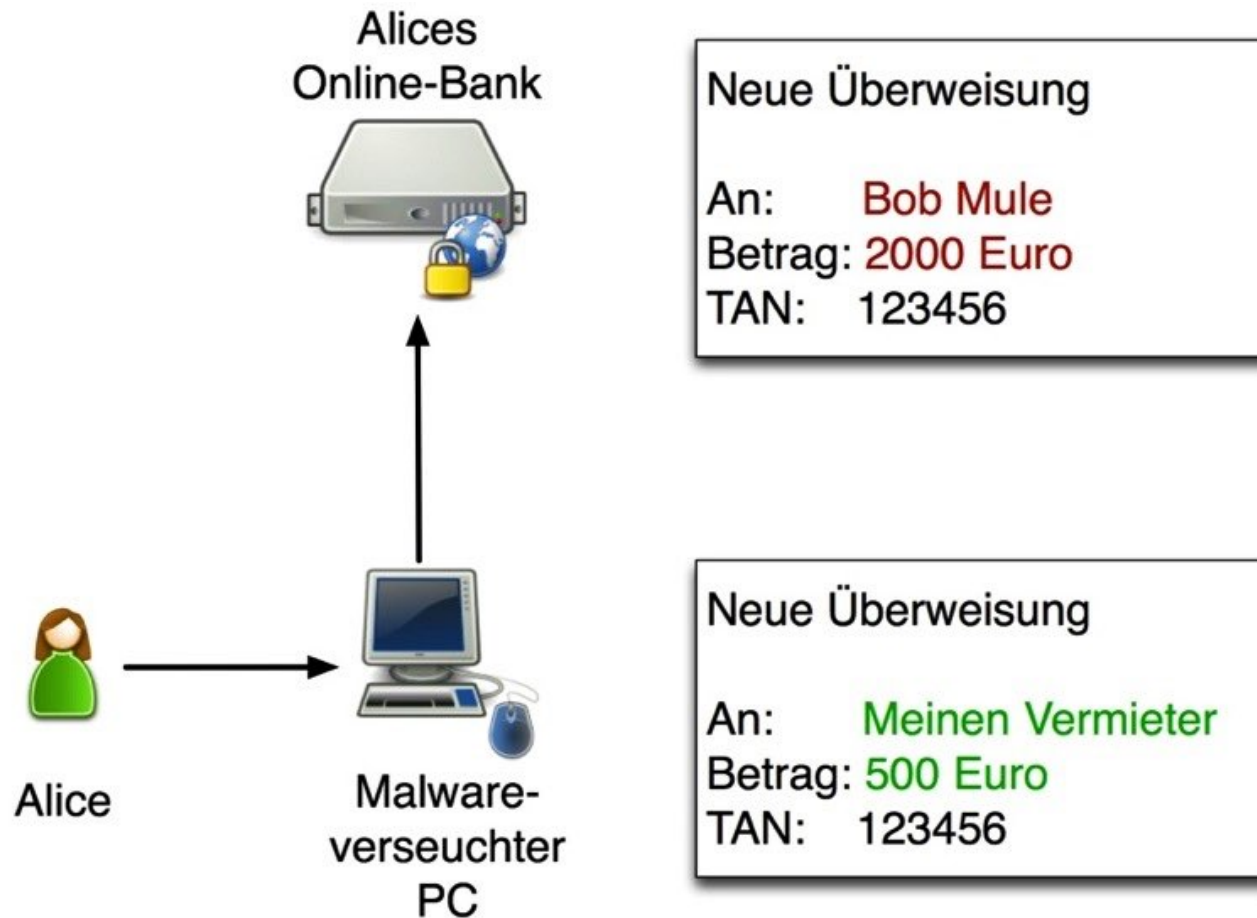


- Definition im Kontext *Daten*:

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.

Integrität im Online-Banking



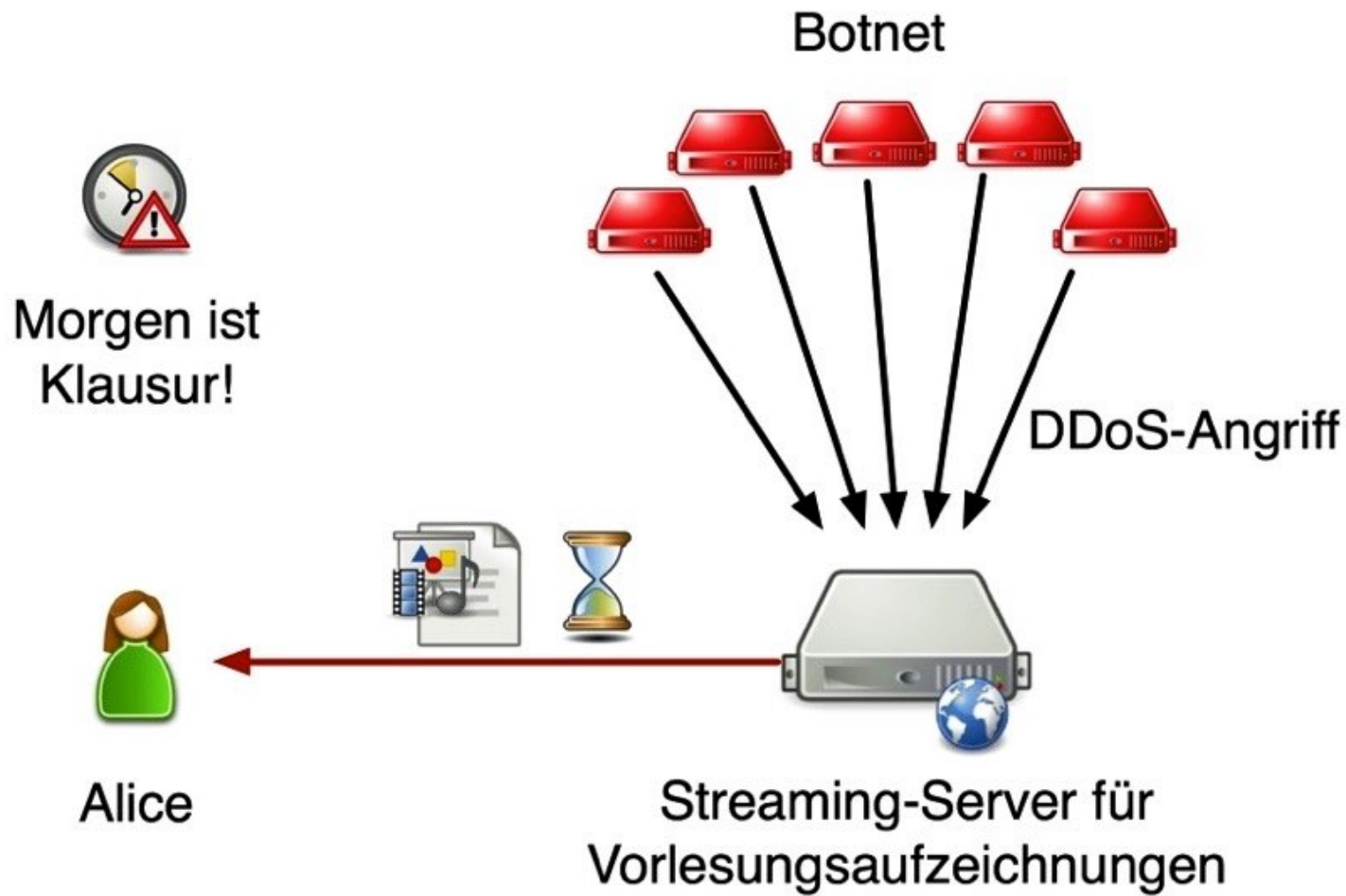
Verfügbarkeit

■ Definition:

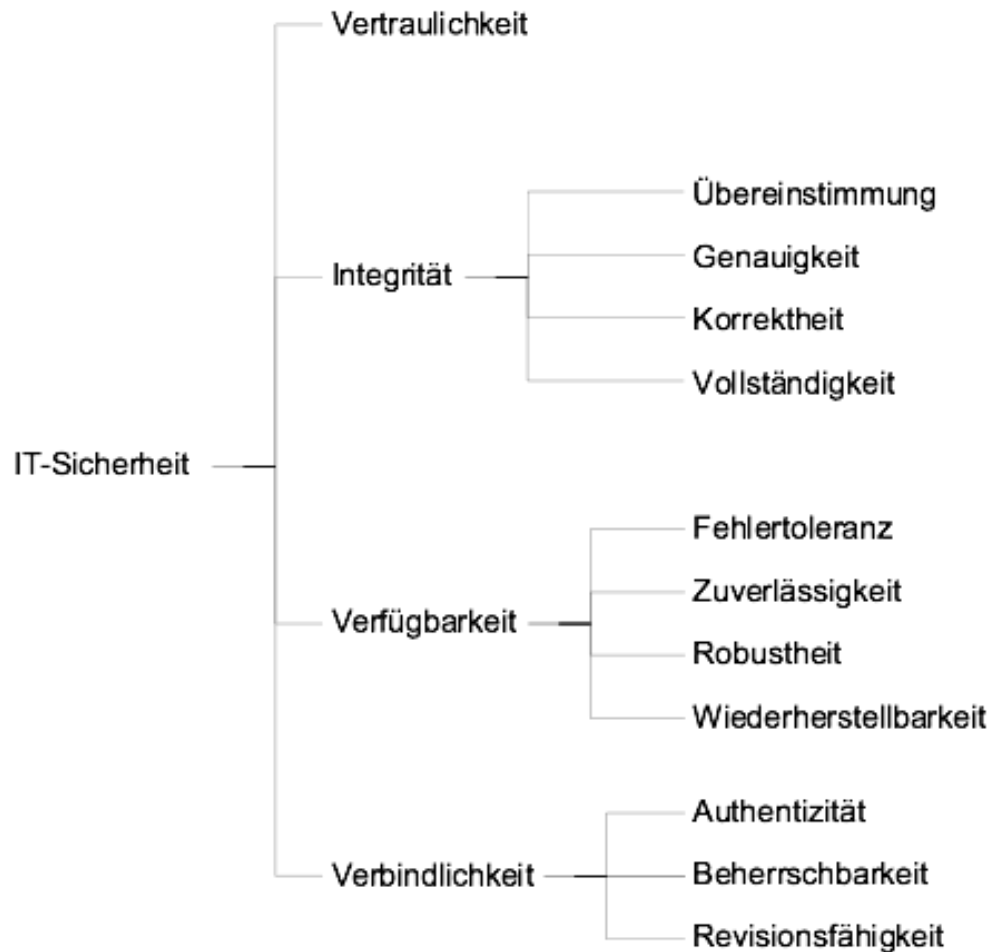
Verfügbarkeit (engl. availability) ist gewährleistet, wenn autorisierte Subjekte störungsfrei ihre Berechtigungen wahrnehmen können.

- 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.

Verfügbarkeit von Webservern



Ziele und abgeleitete Ziele in deutscher IS-Literatur



*Vgl. CIA in
englischer
Literatur:*

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

[In Anlehnung an Hartmut Pohl]

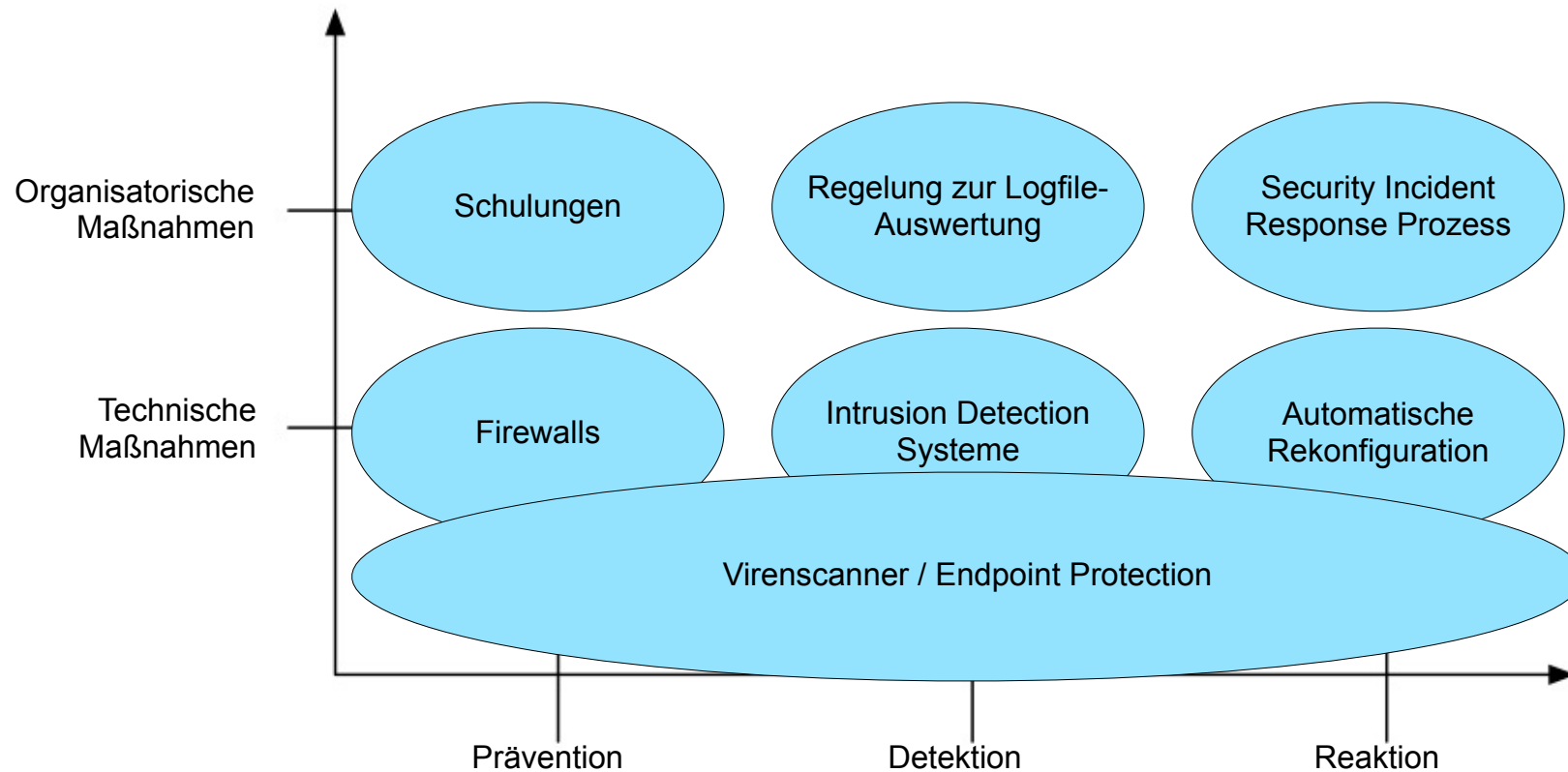
1. Ziele der Informationssicherheit
2. Systematik zur Einordnung von Sicherheitsmaßnahmen
3. Technik & Organisation - ISO/IEC 27000
4. Abgrenzung: Security vs. Safety

Warum Sicherheitsmaßnahmen einordnen?



- 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!)

Einordnung von Sicherheitsmaßnahmen



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.

Welche Maßnahmen werden benötigt?

■ 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

Motivation für Standardisierung

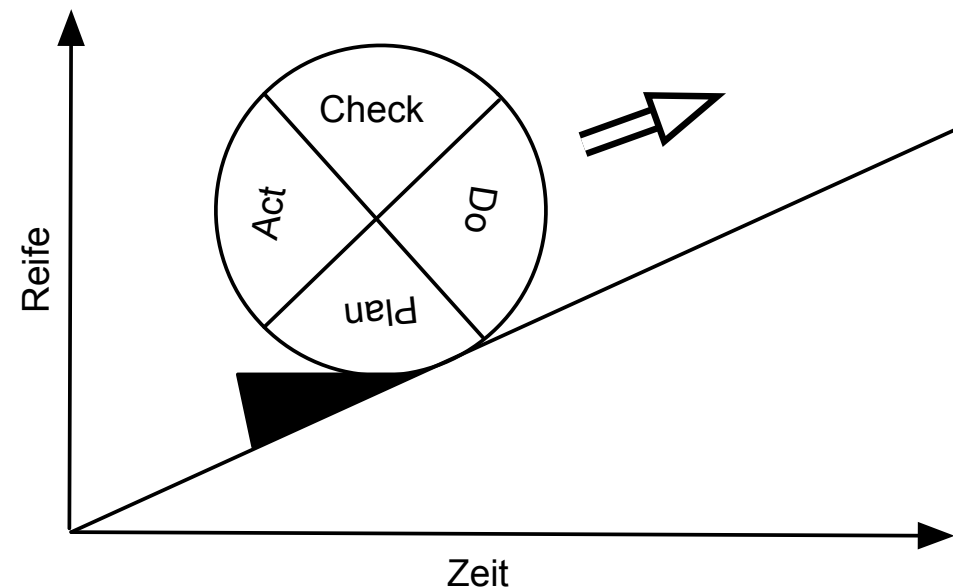


- Informationssicherheit Anfang der 1990er Jahre:
 - ❑ Stark technikzentriert
 - ❑ Kosten-/Nutzenfrage kommt auf
 - ❑ Führungsebene wird stärker in IS-Fragestellungen eingebunden

- 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

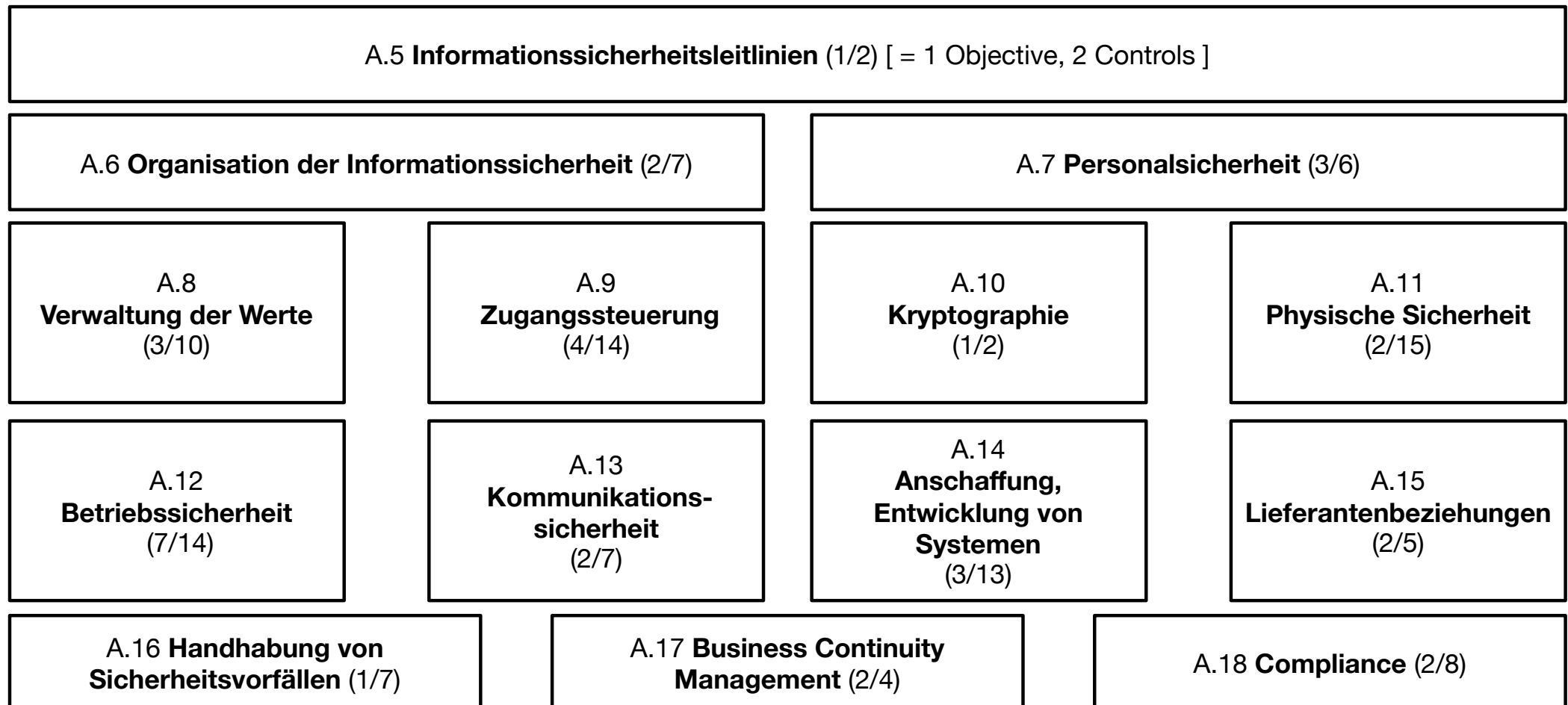


Kerninhalte/Struktur von DIN ISO/IEC 27001



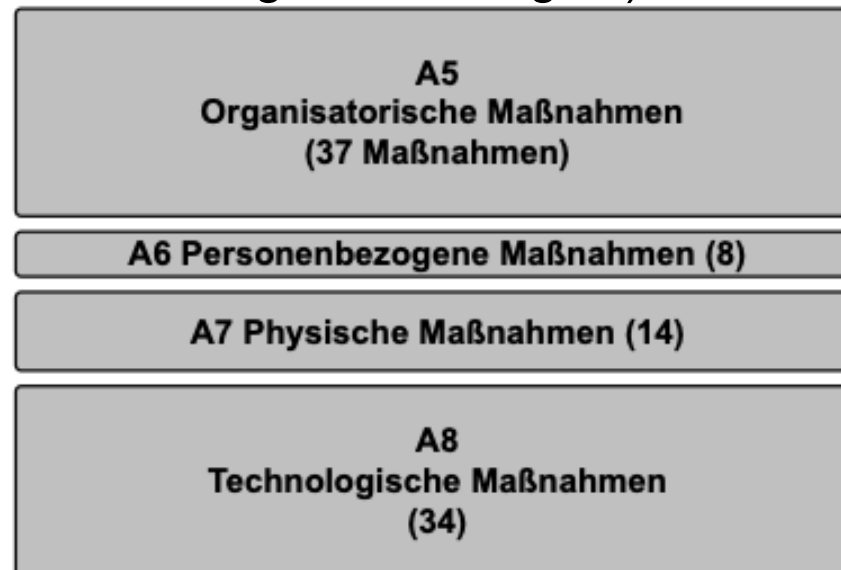
- Begriffsdefinitionen (Verweis auf DIN ISO/IEC 27000)
- PDCA-basierter Prozess zum Konzipieren, Implementieren, Überwachen und Verbessern eines ISMS
- Mindestanforderungen u.a. an Risikomanagement, Dokumentation und Aufgabenverteilung
- Normativer Anhang A enthält:
 - Definition von Maßnahmen (controls)
 - Gruppierung in vier Kategorien
- Aktuell bei der DIN in Überarbeitung, engl. Fassung 2022, deutsche 2024 aktualisiert,
- Umfang:
 - DIN ISO/IEC 27001:2024 - 31 Seiten
 - DIN ISO/IEC 27002:2024 - 209 Seiten - 2015: 103 S.

Maßnahmenziele und Maßnahmen - alte Version (2015)



ISO/IEC 27001:2024 Anhang A - Maßnahmen

- Anhang A wurde ziemlich stark umgebaut
 - Maßnahmenziele sind nicht mehr angegeben; „nur“ noch Controls
 - Umgruppierung und Zusammenfassung alter Controls
 - 93 Maßnahmen in :2024; 112 in :2015
 - Gruppierung auf vier Gruppen anstatt 14 vorher
 - 10 neue Controls (z.B. Clouddienste, Überwachung physischer Sicherheit, Konfig-Mgmt., Webfilterung, sichere Programmierung,...)



A.5 Organisatorische Maßnahmen

5.12	Klassifizierung von Informationen	Maßnahme Informationen müssen entsprechend den Informationssicherheitserfordernissen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen der interessierten Parteien klassifiziert werden.
------	-----------------------------------	---

- Im LRZ drei Stufen
 - Öffentlich
 - Intern
 - Vertraulich (hier ist anzugeben, wer die Berechtigten sind)

A.6 Personenbezogene Maßnahmen

6.7	Remote-Arbeit	Maßnahme Es müssen Sicherheitsmaßnahmen ergriffen werden, wenn Mitarbeiter aus der Ferne arbeiten, um Informationen zu schützen, die außerhalb der Räumlichkeiten des Unternehmens abgerufen, verarbeitet oder gespeichert werden.
-----	---------------	--

- Richtlinie zum Umgang mit mobilen Geräten und Arbeit außerhalb des LRZ
 - Datensparsamkeit und Verschlüsselung
 - Schutz vor unberechtigttem Zugriff und Diebstahl
 - Netzzugänge und sichere Verbindungen ins LRZ
 - Nutzung von Programmen auf dienstlichen Geräten
 - Nutzung freigegebener Programme auf privaten Geräten

A.7 Physische Maßnahmen

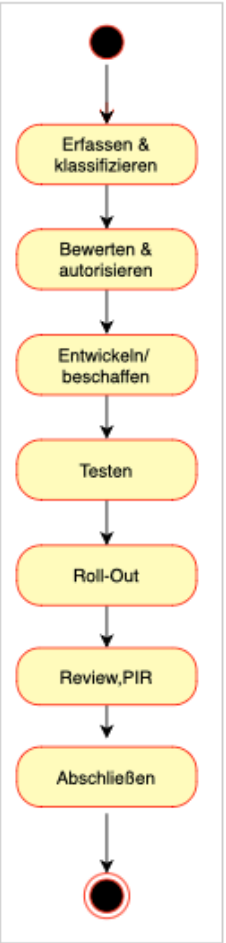
7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	Maßnahme Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, müssen überprüft werden, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.
------	--	--

- Richtlinie zur Weitergabe und Entsorgung von Datenträgern
 - Papier -> Shredder (Sicherheitsstufe 4 nach DIN 66399)
 - Datenträger, Wechseldatenträger -> verschrotten (mind. O-3, E-3 bzw. H-3, ISO/IEC 21964)
 - Weiterverwendung -> Irreversibel überschreiben (7-35 mal überschreiben)
- Entsorgung Datenschutz- und Informationssicherheitskonform
 - z.B. zertifizierte Entsorgungsdienstleister
- Entsorgung von Geräten
 - Zurücksetzen (Config) und alle lokalen Passwörter löschen

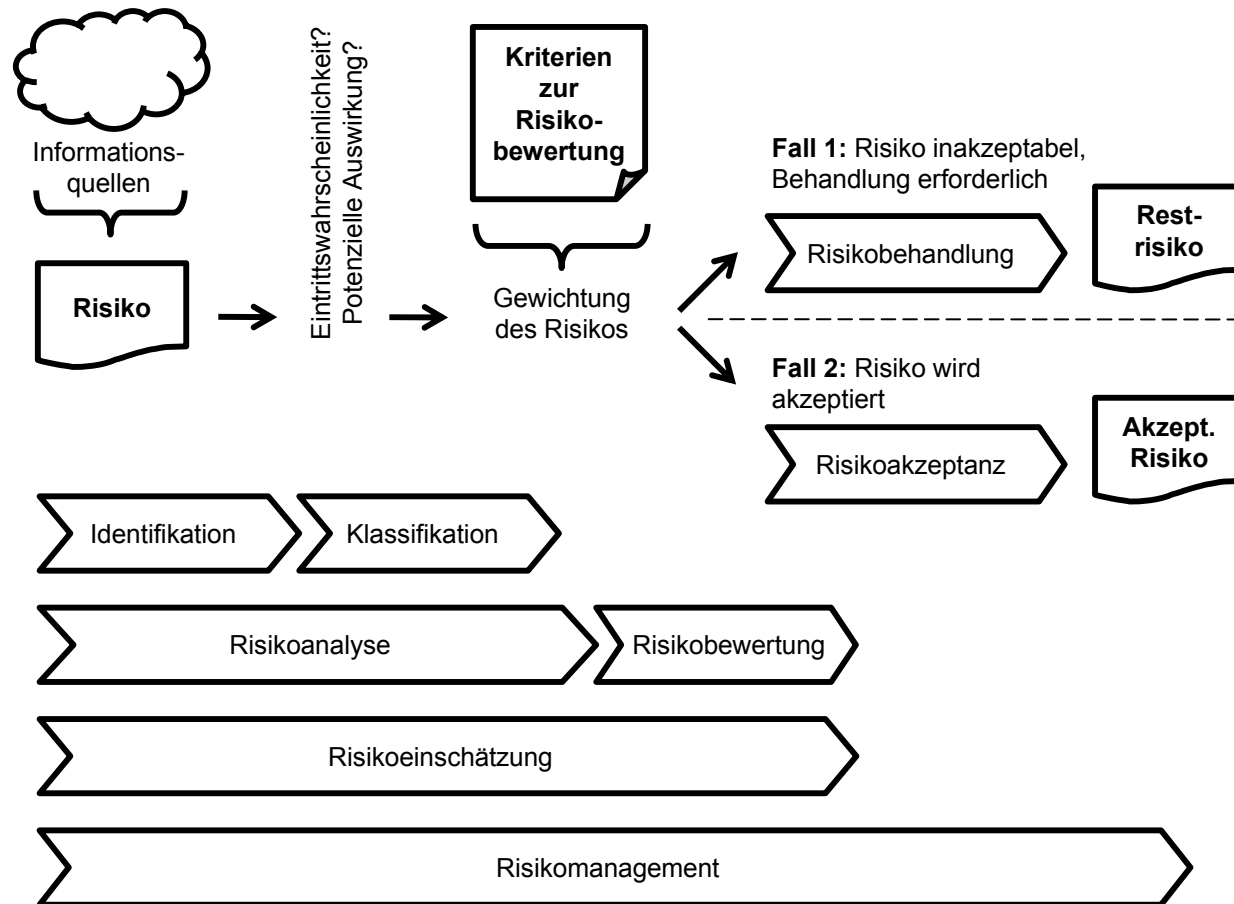
A.8 Technische Maßnahmen

8.32	Änderungssteuerung	Maßnahme Änderungen an Informationsverarbeitungseinrichtungen und Informationssystemen müssen Gegenstand von Änderungsmanagementverfahren sein.
------	--------------------	---

- Rückgriff auf ISO/IEC 20000 - Servicemanagementsystem
 - Change-Management Prozess und -Richtlinie

S Suppliers / eingehende Schnittstellen	I Input	P Prozess	O Output	C Customers / ausgehende Schnittstellen
ISRM Incident- Service Request Management	Request for Change (RfC)	 <pre> graph TD Start(()) --> Erfassen(Erfassen & klassifizieren) Erfassen --> Bewerten(Bewerten & autorisieren) Bewerten --> Entwickeln(Entwickeln/ beschaffen) Entwickeln --> Testen(Testen) Testen --> RollOut(Roll-Out) RollOut --> Review(Review, PIR) Review --> Abschließen(Abschließen) Abschließen --> End((())) </pre>	Informationen bzgl. Erfolg von Changes	ISRM Incident- Service Request Management
SPM Service Portfolio Management	Informationen zu geänderten Service Bedarfen (RfC)		Informationen bzgl. Erfolg von Changes	SPM Service Portfolio Management
RDM Release und Deployment Management	Informationen aus dem umgesetzten Release für das PIR		freigegebenes RfC zur Umsetzung des Release	RDM Release und Deployment
PM Problem Management	RfC		Informationen bzgl. Erfolg von Changes	PM Problem Management
CAPM , SACM Capacity/Availability/Continuity Management	RfC		Informationen bzgl. Erfolg von Changes	CAPM , SACM Capacity/Availability/Continuity Management
CONFM Configuration Management	Status von Komponenten vor Umsetzung des Changes		Änderungen am Status von Komponenten bzw. neuer Status nach Ausrollen des Change.	CONFM Configuration Management
SUPPM Supplier Management	RfC		Änderungen an Verträgen	SUPPM Supplier Management



Grundlagen des Risikomanagements



LRZ:

seit August 2019
zertifiziert nach:

- ISO 27001
- ISO 20000



ZERTIFIKAT

Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

ISO/IEC 27001:2015

DEKRA Certification GmbH bescheinigt hiermit, dass die Organisation





Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften

Zertifizierter Bereich:
Informationswerte und informationsverarbeitende Einrichtungen für die Erbringung aller IT-Services für Kunden des LRZ sowie die dazugehörige Rechenzentrums- und Kommunikationsinfrastruktur

Zertifizierter Standort:
Boltzmannstraße 1, 85748 Garching bei München, Deutschland

ein Informationssicherheitsmanagementsystem entsprechend der oben genannten Norm sowie der Anwendbarkeitserklärung vom 28.06.2019 eingeführt hat und aufrechterhält. Der Nachweis wurde mit Auditbericht-Nr. A19031463 erbracht.

Zertifikats Registrier-Nr.:	DS-0819022	Zertifikat gültig vom:	08.08.2019
Gültigkeit vorheriges Zertifikat:	-	Zertifikat gültig bis:	07.08.2022



Dr. Gerhard Nagel
DEKRA Certification GmbH, Berlin, 08.08.2019

DEKRA Certification GmbH * Handwerksstraße 15 * D-70565 Stuttgart * www.dekra-certification.de

Seite 1 von 1

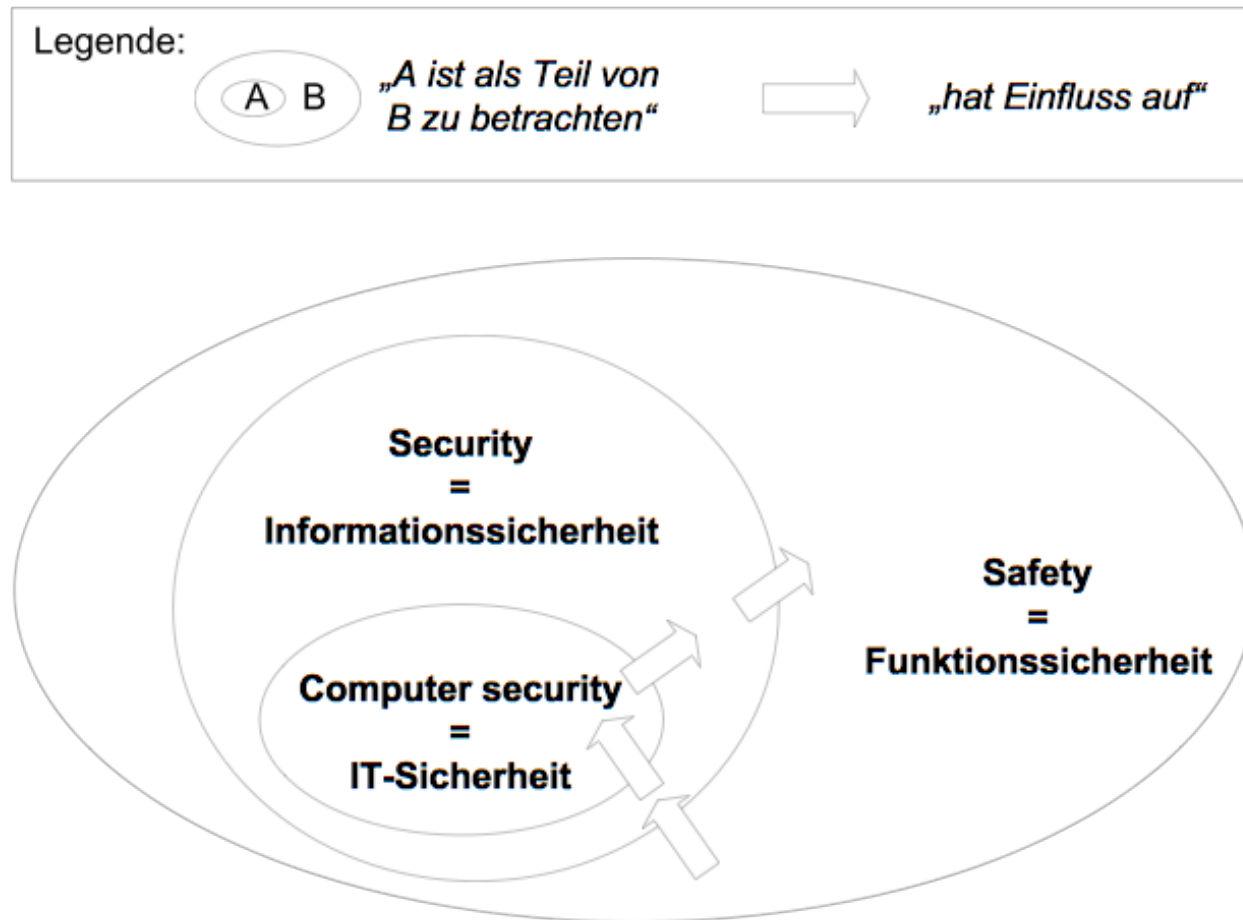


1. Ziele der Informationssicherheit
2. Systematik zur Einordnung von Sicherheitsmaßnahmen
3. Technik & Organisation - ISO/IEC 27000
4. Abgrenzung: Security vs. Safety

Security vs. Safety

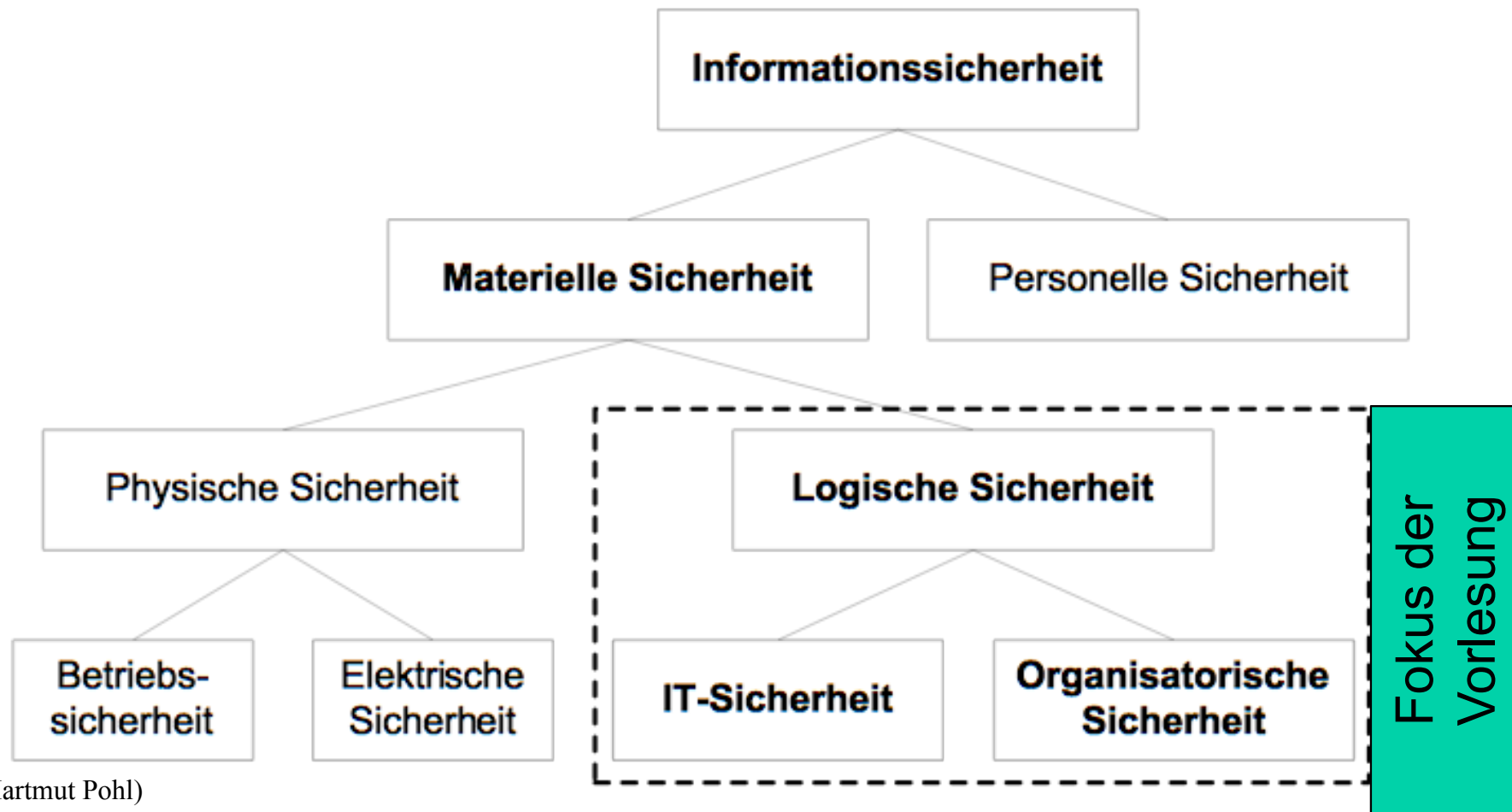
- Beide Begriffe werden oft mit „Sicherheit“ übersetzt
- Typische Themen der Safety („Funktionssicherheit“)
 - Betriebssicherheit für sicherheitskritische Programme, z.B. Steuerung und Überwachung von Flugzeugen, Kraftwerken und Produktionsanlagen
 - Ausfallsicherheit (Reliability)
 - Gesundheitsrelevante 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

Safety vs. Security (1/2)



(nach Hartmut Pohl)

Safety vs. Security (2/2)



(nach Hartmut Pohl)