Grundlagen des Datenschutzes und der IT-Sicherheit (Teil 2c)

Vorlesung im Sommersemester 2024

an der Universität Ulm

von Bernhard C. Witt

2. Grundlagen der IT-Sicherheit

Grundlagen des Datenschutzes		Grundlagen der IT-Sicherheit	
✓	Geschichte des Datenschutzes	✓	Anforderungen zur IT-Sicherheit
✓	Datenschutzrechtliche Prinzipien	✓	Mehrseitige IT-Sicherheit
✓	Technischer Datenschutz	➔	Risiko-Management
✓	Schwerpunkt: Aktuelles		Konzeption von IT-Sicherheit

Risiko-Management:

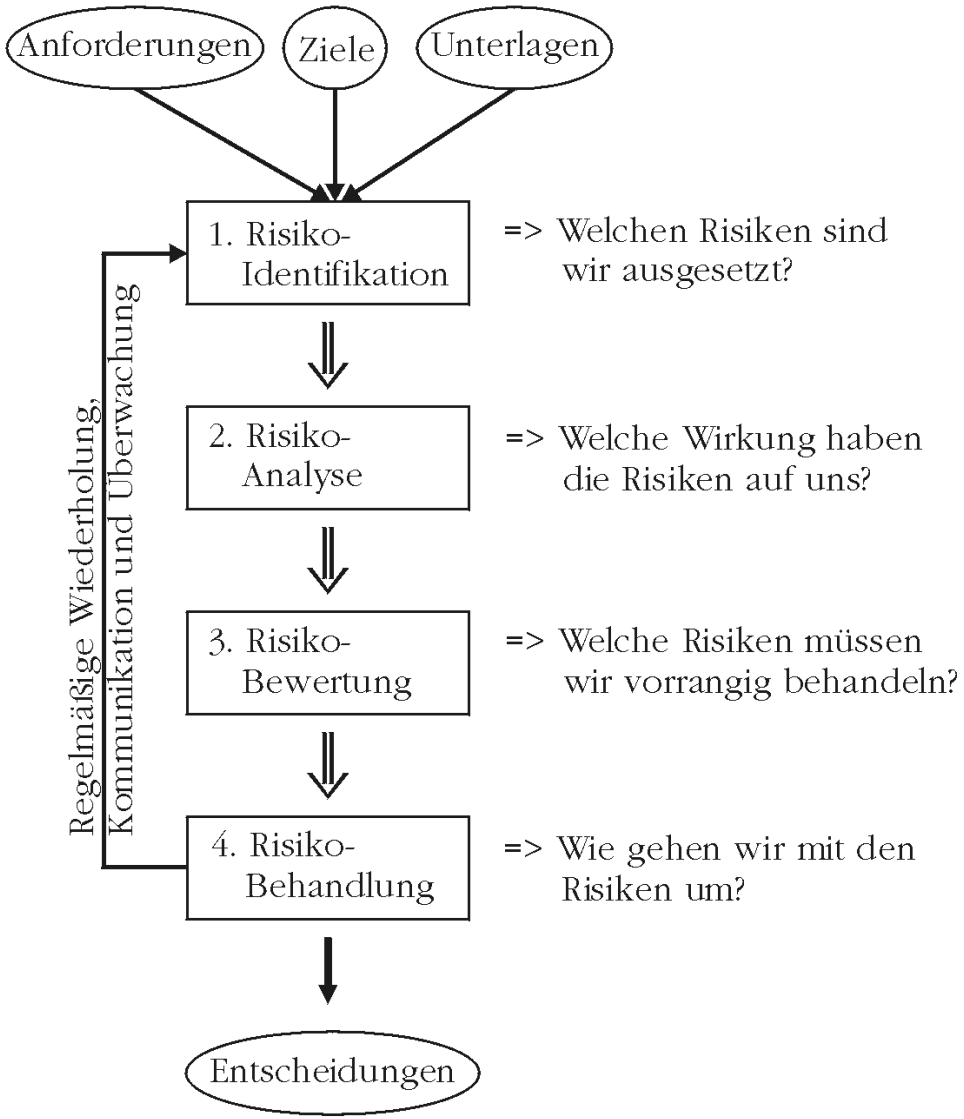
- Übersicht
  - Definition, Prozess, Standards
- Risiko-Identifikation
  - Aktuelle Gefährdungsszenarien
- Risiko-Analyse
- Risiko-Bewertung
- Risiko-Behandlung
  - Besonderheiten KRITIS

IT-Risiken

Definition 17: Risiko

Nach Häufigkeit und Auswirkung bewertete Abweichung eines zielorientierten Systems.

- **ISO/IEC 27000**: effect of uncertainty on objectives
- System wird mit Zielsetzung verbunden (Prüfbarkeit!)
- Positive Zielabweichung → Chancen
- Negative Zielabweichung → Gefährdung
- Risiko nur, wenn Zielerreichung unsicher ist!
- Faktoren: **Häufigkeit * Auswirkung**
  abhängig von Vermögenswerten (assets), Bedrohungen (threats) und Verwundbarkeiten (vulnerabilities)
- Risiken sind kontextabhängig!



Risiko-Management

Risikoidentifikation:

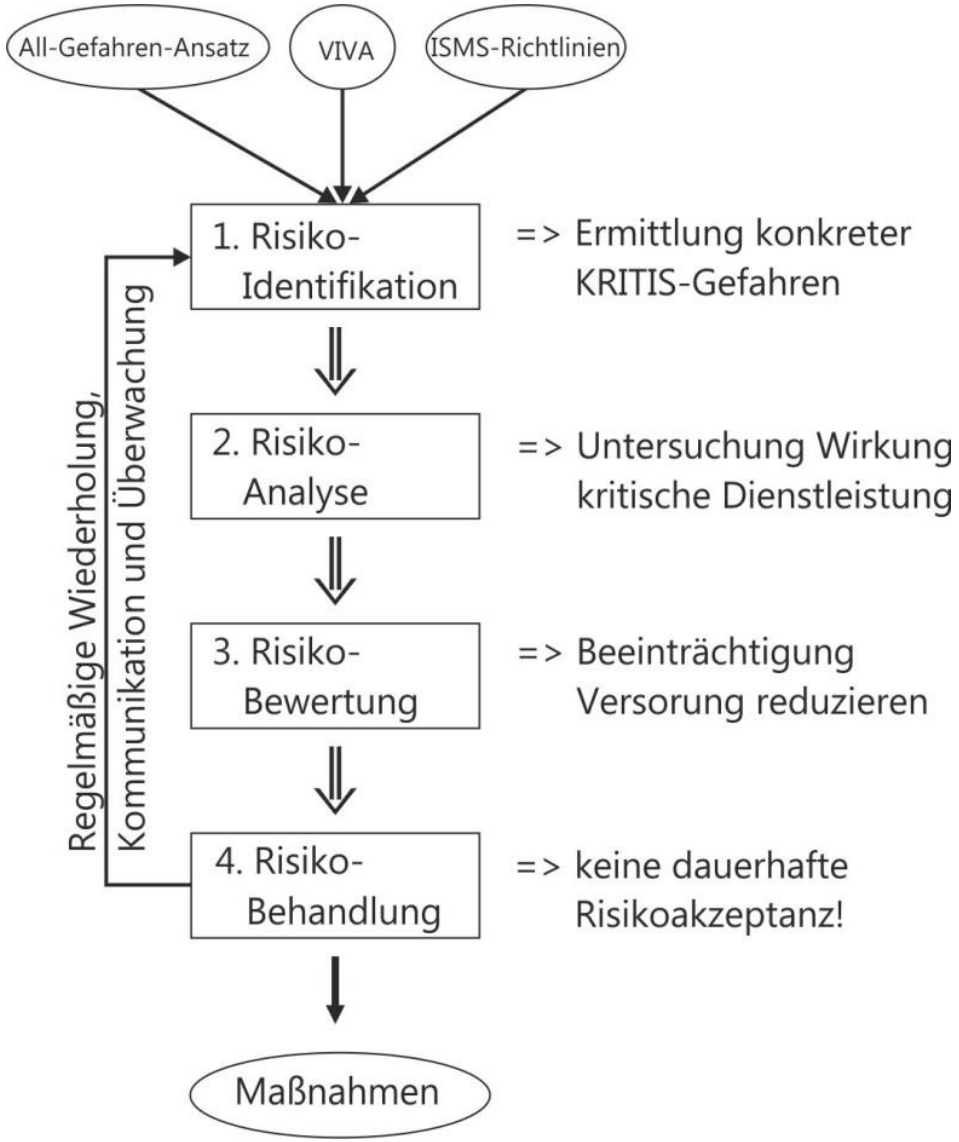
- Bestimmung relevanter Assets (Prozesse, IT-Systeme, Personen, Daten)
- Bestimmung der Bedrohungen / Chancen
- Bestimmung der Verwundbarkeiten / Stärken

Risikoanalyse:

- Ermittlung Eintrittswahrscheinlichkeiten
- Ermittlung potenzieller Schadens- / Chancenauswirkungen

Risikobewertung:

- Priorisierung zu festgestellten Risiken



KRITIS-Risiken

Risikoidentifikation:

- Maßgebliche IT-Systeme, IT-Komponenten & Prozesse zur Erbringung der kritischen Dienstleistung
- Bedrohungen + Schwachstellen nach All-Gefahren-Ansatz

Risikoanalyse:

- Ermittlung Eintrittswahrscheinlichkeiten
- Ermittlung Beeinträchtigung für Versorgung der Bevölkerung

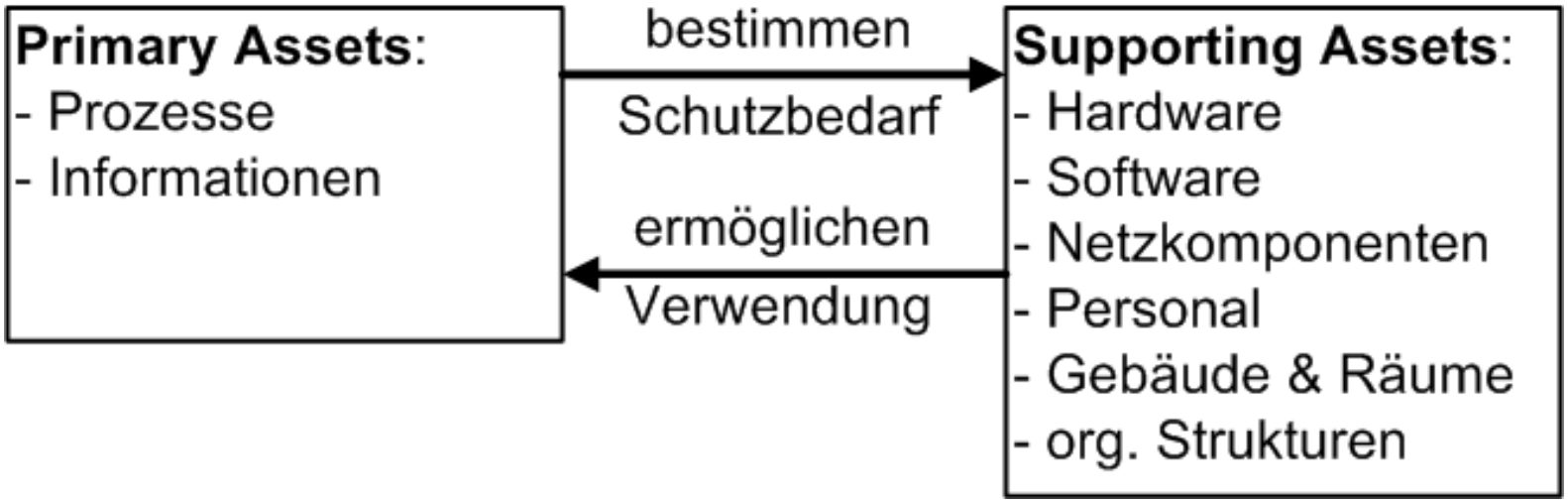
Risikobewertung:

- Versorgungssicherheit darf nicht dauerhaft beeinträchtigt sein

IT Risk Assessment Standards

- Risk Management – Guidelines (**ISO 31000:2018**)
  → generelles Vorgehen für Risikomanagement
- Risk Management – Risk Assessment Techniques (**IEC 31010:2019**)
  → Sammlung verschiedener Methoden
  → Bewertung zur Eignung je Einsatzfeld
- Information security, cybersecurity and privacy protection – Guidance on managing information security risks (**ISO/IEC 27005:2022**)
  → Adaption Risikomanagement für Informationssicherheit
  → Eingebettet in Management der Informationssicherheit
  → kompatibel mit ISO/IEC 27001:2022 & ISO/IEC 27002:2022
  → Reproduzierbarkeit der Ergebnisse
  → Maßnahmen zur Behandlung von Risiken können präventiv, erkennend oder korrigierend wirken

Zusammenhang von Primary Assets & Supporting Assets



Risiko-Identifikation

1. Ermittlung der zu schützenden Vermögenswerte (**Assets**):
   ° **Primary Assets**: Prozesse & Informationen
   ° **Supporting Assets**: Hardware, Software, Netzwerkkomponenten, Personal, Gebäude, Räume & organisatorische Strukturen
2. Ermittlung der zu berücksichtigenden Anforderungen (rechtlich, technische Abhängigkeiten, Wertschöpfung) des Schutzbedarfs der Assets mittels einer **Business Impact Analysis** (BIA)
   → welche Folgen hätte ein Ausfall der betrachteten Assets auf die Geschäftstätigkeit? (z.B. auf Reputation, Finanzen, Compliance, Personenschaden)
3. Feststellung der Bewertung der Assets, z.B. anhand einer **CIA-Analyse**, d.h. der maximalen Bedeutung des Assets hinsichtlich der Sicherheitsziele Vertraulichkeit (C), Integrität (I) und Verfügbarkeit (A) → siehe Übung
4. Ermittlung der **Bedrohungen** (Threats), denen die (kritischen) Assets (z.B. hinsichtlich CIA) ausgesetzt sind
5. Ermittlung der **Verwundbarkeiten** (Vulnerabilities) der Assets, über die die Bedrohungen (z.B. hinsichtlich CIA) ihre Wirkung entfalten können
6. Ermittlung der **Wahrscheinlichkeit**, mit der eine ermittelte Bedrohung festgestellte Verwundbarkeiten ausnutzen kann

Aktuelle Gefährdungsszenarien

Neue Angriffsvektoren auf die Cybersicherheit:

- **Ransomware** (bei Erfolg der Angreifer i.d.R. sehr hoher Wiederherstellungs-aufwand nötig, so dass gefordertes Kryptogeld eher bezahlt wird)
- **Supply Chain Angriffe** (entweder Sabotage benötigter Supply Chain Services, um gravierende Störungen beim eigentlichen Ziel auszulösen, oder Missbrauch der Supply Chain als „Transporteur“ verdeckter Angriffe)
- Bekannte **Schwachstellen** massenhaft genutzter Systeme / Endgeräte oder gezielte Ausnutzung von Zero-Day-Exploits vom Schwarzmarkt
- Ausnutzung besonderer Begleitumstände, z.B. Informationsbedarf bzw. Hilfsbe-reitschaft bei weltweiten Krisen (Pandemie, Kriege), für **Social Engineering**…

Weitere Details abrufbar unter

- BSI-Lagebericht: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html
- ENISA Threat Landscape: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

Weitere Methoden zur Risiko-Identifikation

- Brainstorming
- Strukturierte Interviews
- Delphi Methode / Szenarientechnik
- Checklisten

Methoden der Risiko-Analyse

- Fehlerbaum-Analyse (Details in Übung)
- Angriffsbaum-Analyse (Details in Übung)
- Fehlermöglichkeits- und -einfluss-Analyse (Überblick)

Risikoanalyse: Fehlerbaum-Analyse

- Top-Down-Methode [**Fault Tree Analysis**, IEC 61025]
  → ausgehend vom **Fehlerereignis** werden deduktiv die **ursächlichen** Ereignisse (Kasten) gesucht, die für das Top-Ereignis verantwortlich sind
  → logische Verknüpfung (UND, ODER) der jeweiligen Ereignisse zugunsten einer **Baumstruktur**
  → Blätter sind **Basis-Ereignisse**, die unabhängig von anderen Ereignissen eintreten (Kreis) bzw. Ereignisse mit ungeklärter Ursache (Raute) darstellen
- Ermittlung minimaler Gruppen von Basisereignissen, die das Topereignis eintreten lassen (**Minimal Cut Sets**)
- liegt die Ursache für einen Fehler in einem einzigen Basis-Ereignis (kann und wird i.d.R. in mehreren Zweigen vertreten sein) → **Single-Point-of-Failure**!

Risikoanalyse: Angriffsbaum-Analyse

- Top-Down-Methode [**Attack Tree Analysis**, nach Schneier]
  → ausgehend vom zu untersuchenden **Angriffsziel** (= erfolgreiche Bedrohung eines Assets) werden die zum Ergebnis **möglicherweise** führenden Schritte (unter Ausnutzung potentieller Verwundbarkeiten) näher untersucht
  → logische Verknüpfung (UND, ODER) der jeweiligen Wege zugunsten einer **Baumstruktur**
  → Blätter sind die **Basisbedrohungen** unter Ausnutzung entsprechender Verwundbarkeiten, attributiert um den erforderlichen Aufwand für den Angreifer
- Ermittlung aufwandsgünstiger **Vorgehensweisen** aus Angreifersicht, um entsprechende Gegenmaßnahmen ermitteln zu können (wahrscheinliche Angriffswege werden optisch hervorgehoben)

Risikoanalyse: FMEA

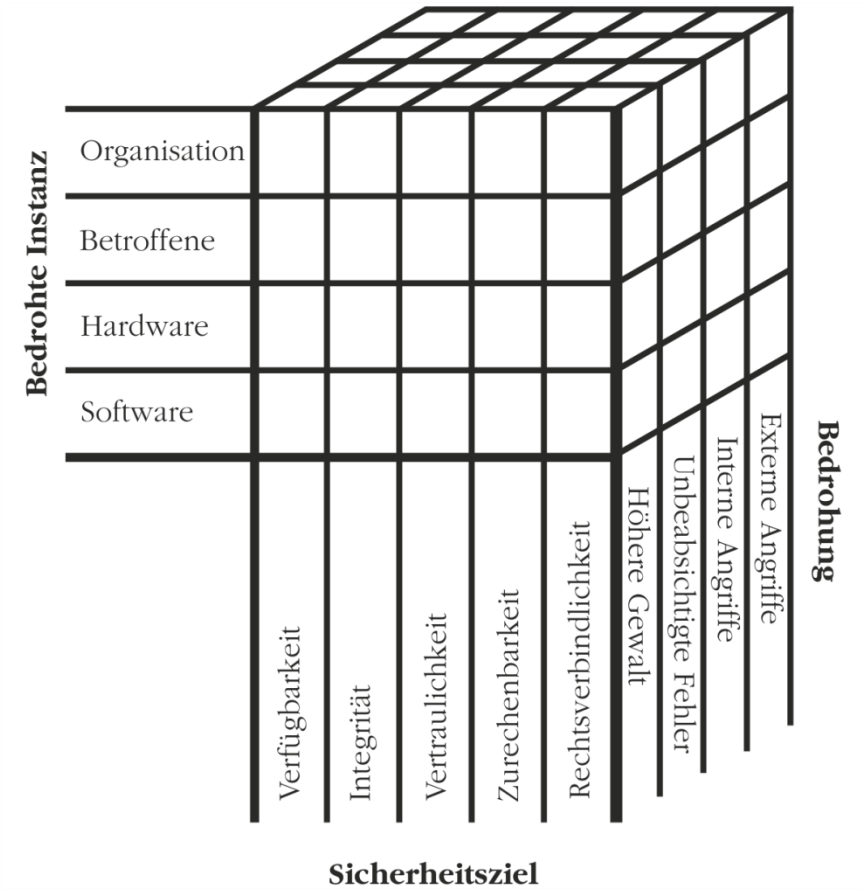
Fehlermöglichkeits- und -einflußanalyse (FMEA)
[Failure Mode and Effect Analysis, IEC 60812]

→ Beurteilung der Bedeutung potentieller Fehler (Skala: 1 .. 10)

Entdeckungswahrscheinlichkeit aber mit (10 – W) angegeben
→ je schwerer Fehler zu entdecken ist, desto höher das Risiko
(allerdings ist die Entdeckungswahrscheinlichkeit oft nur schwer zu bestimmen → Honeynets & Honeypots);
Bedeutung = Schaden

→ Bottom-Up-Methode zur Schwachstellen-Analyse

Ergebnis Risikoanalyse: Risikokubus



Methoden der Risikobewertung

- Risikotabelle / Risikomatrix [Consequence/Probability Matrix] (Details in Übung)
- Risikoportfolio / Risk Map (Details in Übung)
- SWOT-Analyse & Balanced Scorecard (Überblick)

Risikomatrix (Risikotabelle)

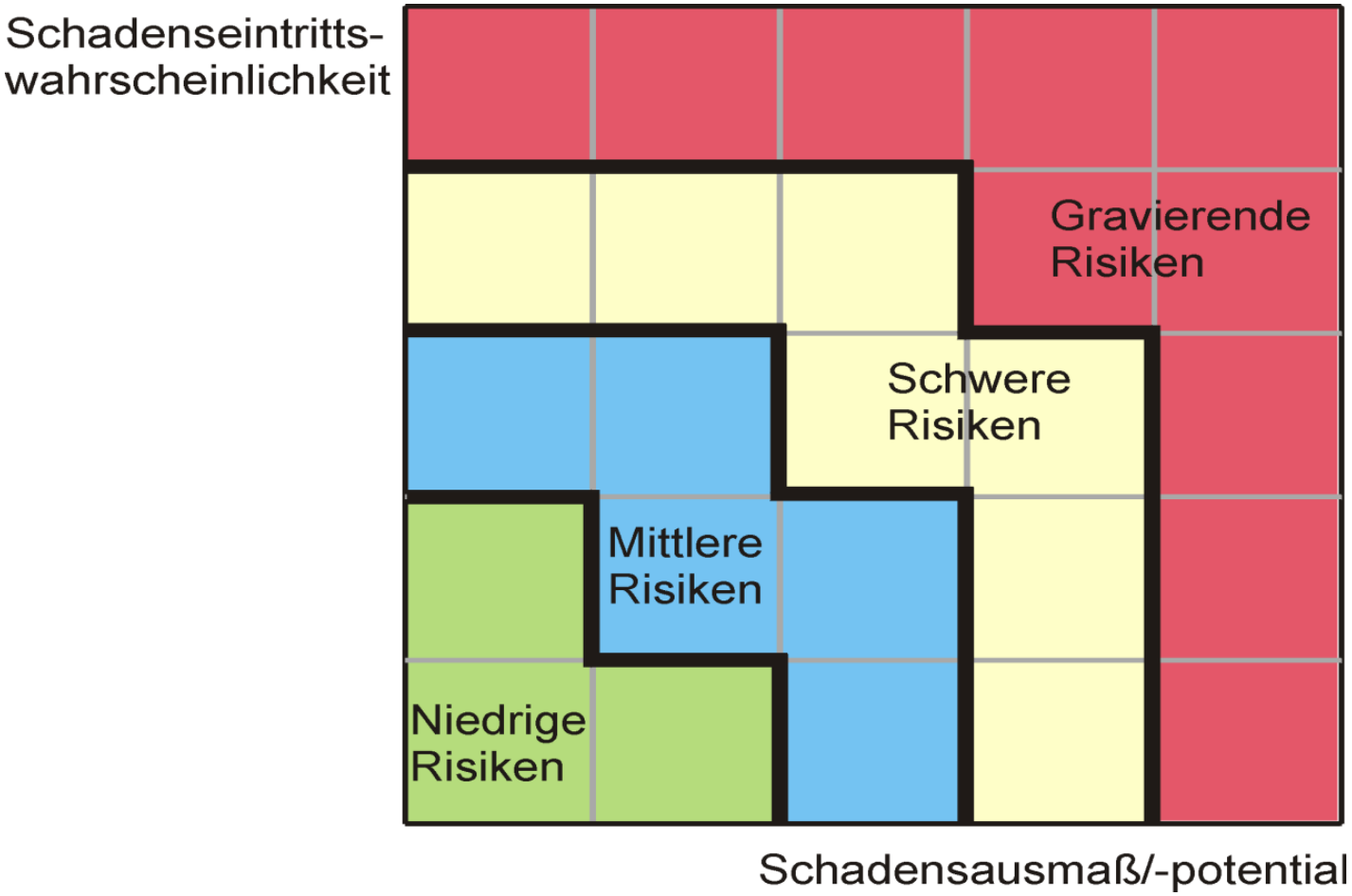
Risiko-Rang	Risiko-Kategorie	Auswirkung	Eintrittswahrscheinlichkeit	Risikofaktor	
1.	Text 1	A_1	W_1	A_1*W_1	**erfordert Maßnahmen**
2.	Text 2	A_2	W_2	A_2*W_2	
...	...	...	...	...	
n	Text n	A_n	W_n	A_n*W_n	**akzeptierbar**
...	...	...	...	...	

Beispiel: CIA-Analyse

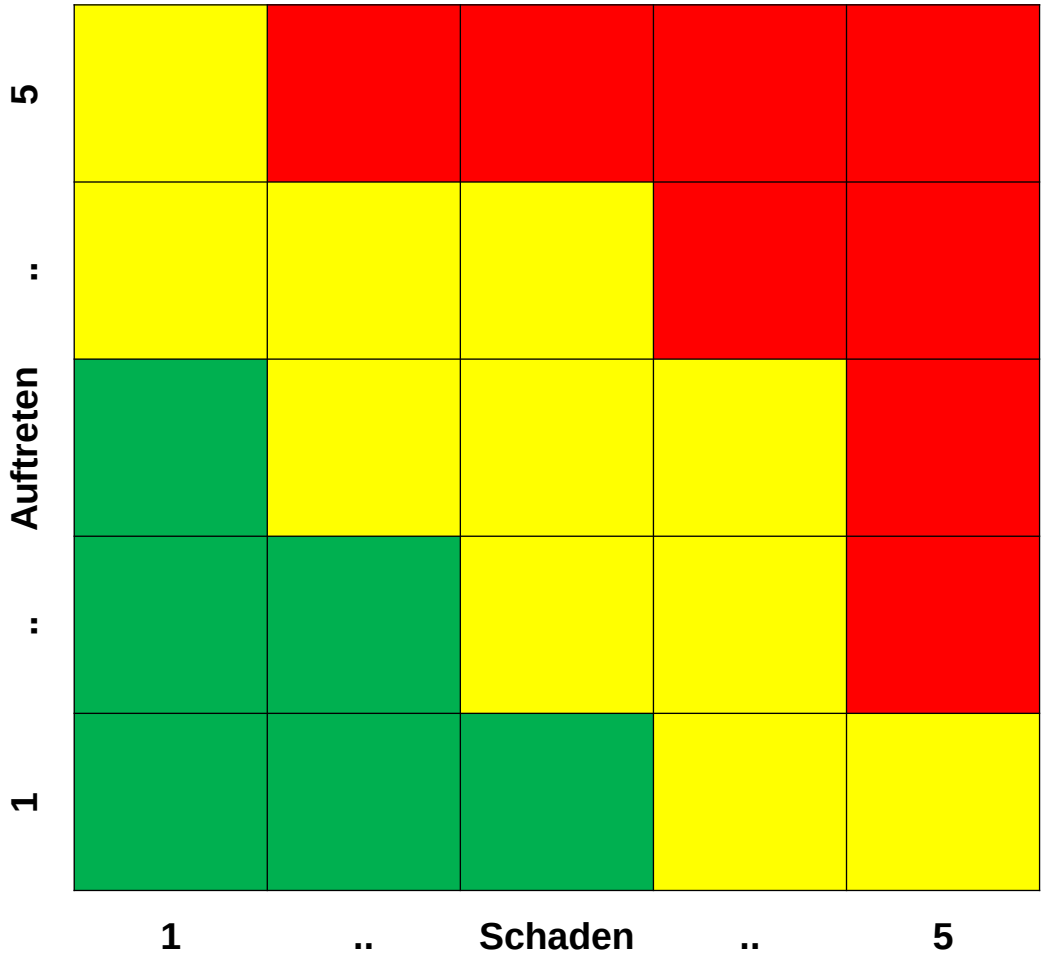
Bedrohung	Verwundbarkeit	Auftreten	Schaden		
			C	I	A
Datenverlust	fehlende Clusterung	3	1	1	3
Datenverlust	Ermüdung Backupmedien	2	1	4	4
unbefugter Zugriff	fehlende Schutzzonen	3	5	1	5
unbefugter Zugriff	schlechte Passwörter	4	4	3	2
unbefugter Zugriff	fehlende Systemhärtung	3	4	4	4
unbefugter Zugriff	fehlende Timeoutfunktion	2	3	3	3
unbefugter Zugriff	Missbrauch Adminrechte	1	2	5	5
Vireninfektion	fehlende Schutzzonen	3	3	4	4
Vireninfektion	schlechter Virenscanner	2	3	3	3
DoS-Attacke	fehlende Schutzzonen	4	1	1	5
DoS-Attacke	fehlende Timeoutfunktion	2	1	1	4

C = Confidentiality; I = Integrity; A = Availability; Werteskala von 1 (very low) bis 5 (very high)

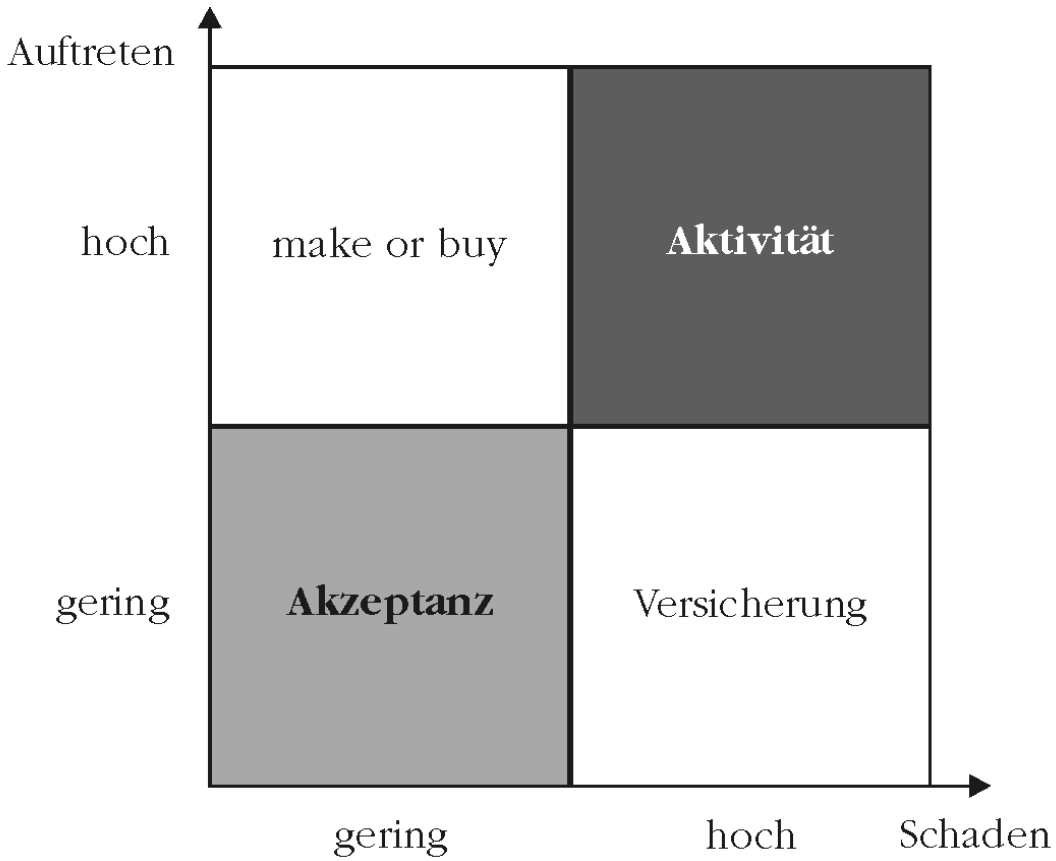
Portfolio-Analyse (1)



Portfolio-Analyse (2)



Variante Risk-Map



Weitere Methoden zur Risikobewertung

SWOT-Analyse:

- Gegenüberstellung von
  - Stärken (**s**trengths)
  - Schwächen (**w**eaknesses)

  und
  - Chancen (**o**pportunities)
  - Gefahren (**t**hreats)
- Strategien:
  - Ausbau: Stärken & Chancen
  - Aufholen: Schwächen & Chancen
  - Absicherung: Stärken & Gefahren
  - Abbau: Schwächen & Gefahren

Balanced Score Card (BSC):

- Kennzahlensystem zur strategischen Unternehmensplanung
- Ausbalancierung vorgegebener Werte von Perspektiven:
  - finanzielle Perspektiven
  - Kundenperspektive
  - interne Prozessperspektive
  - Lernen- und Wachstumsperspektive
- Untersuchung erfolgt anhand
  - Ziele
  - Kennzahlen
  - Vorgehen
  - Maßnahmen

Risikobewertung: Qualitativ vs. Quantitativ

Gründe für die Wahl einer qualitativen Risikobewertung:

- Sowohl die Höhe des Schadens wie auch die Höhe der Eintrittswahrscheinlichkeit lassen sich besser qualitativ abschätzen (aufgrund mangelnder historischer Vergleichswerte, vor allem über Angriffswahrscheinlichkeiten)
- Häufig hängt der Eintritt eines Schadensfalls von etlichen Bedingungen ab (Ausnutzung von Schwachstellenketten), die sich mit bedingten Wahrscheinlichkeiten nur unzureichend berechnen lassen
- Schnellere Methodik für Entscheidung über nötige Maßnahmen

Gründe für die Wahl einer quantitativen Risikobewertung:

- Außerhalb des IT-Risikomanagements sind quantitative Risikobewertungen vorherrschend, womit sich Ergebnisse besser mit anderen Risiken kumulieren lassen
- Im Bereich der Gefährdungen durch höhere Gewalt (→ Safety) liegen aus der Versicherungsmathematik umfassende Vergleichswerte vor (da Gründe für Versicherungsfall)
- Wenn sich Risiken quantitativ sinnvoll berechnen lassen, greifen die etablierten Methoden aus der Versicherungsmathematik

Risikobewertung: Unterschied zum Datenschutz

Typische Risiko-Matrix zu Datenschutzrisiken:

Risikobasierte Abschätzung zum Datenschutz	Schwere des potenziellen Schadens		
Eintrittswahrscheinlichkeit	niedrig	normal	hoch
hoch			**Handeln**
normal		**Prüfen**	
niedrig	**Akzeptieren**		

Keine Akzeptanz von Risiken, die sicher zu Datenschutzverstößen führen!

Typische Risiko-Matrix zu IT-Risiken:

Risikobasierte Abschätzung zur Informationssicherheit	Schwere des potenziellen Schadens		
Eintrittswahrscheinlichkeit	niedrig	normal	hoch
hoch			**Handeln**
normal		**Prüfen**	
niedrig	**Akzeptieren**		

Mehr Spielraum bei der Akzeptanz von Risiken (außer KRITIS), da umfangreicher in Betrachtung (alle Geheimnisse!)

Risikobehandlung (1)

Möglichkeiten der Risikobehandlung:

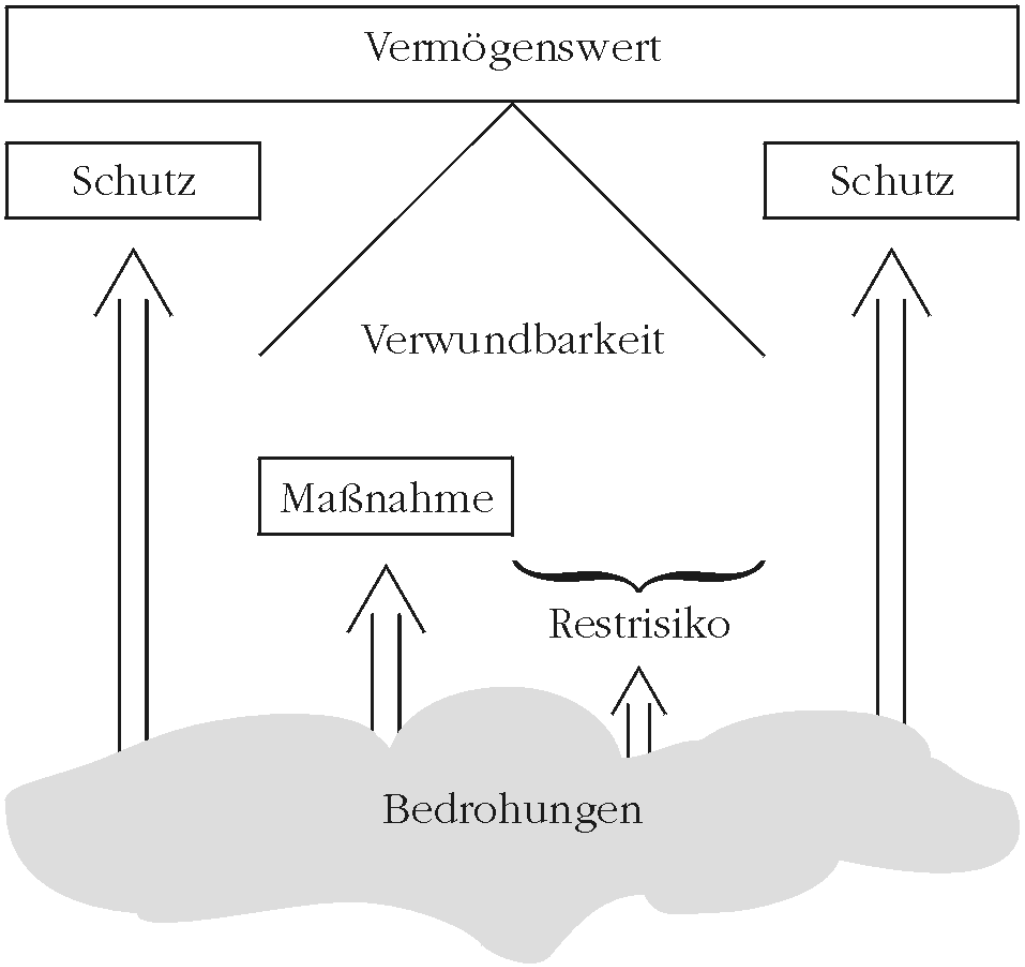
- **Risiko modifizieren** (Risk Modification)
  → Senkung der Eintrittswahrscheinlichkeit durch Maßnahmen
  → Senkung der Auswirkung durch Maßnahmen
  → Ziel: akzeptables Rest-Risiko nach Maßnahmen
- **Risiko beibehalten** (Risk Retention)
  → ausdrückliche & bewusste Akzeptanz des Risikos anhand klar definierter Risikoakzeptanzkriterien
- **Risiko vermeiden** (Risk Avoidance)
  → komplette Abwehr des Risikos, z.B. Unterlassen der das Risiko auslösenden Aktivitäten (→ kein Einsatz des Systems)
- **Risiko teilen** (Risk Sharing)
  → Aufteilung des Risikos auf verschiedene Einrichtungen, z.B. durch Outsourcing an Spezialisten oder durch Versichern
  → daraus resultierendes Risiko separat bewerten

Risikobehandlung (2)

Vorbereitung zur Risikobehandlung:

- zur Schwachstellenanalyse von IT-Systemen werden u.a. Penetrationstests und Security-Scans durchgeführt
  → gezieltes Schließen von Schwachstellen
- Planung und Überwachung des Risikomanagements bei IT-Systemen durch IT-Sicherheitsbeauftragten
- zur Prävention bzw. Behandlung von Sicherheitsvorfällen:
  → Einrichtung eines Sicherheitsteams („Computer Security Incident Response Team“ = CSIRT) zur Unterstützung des IT-Sicherheitsbeauftragten (s.a. RFC 2350, abrufbar unter https://datatracker.ietf.org/doc/html/rfc2350)
- Ausarbeitung eines Sicherheitsmodells (= abstrakte Beschreibung der nach der zugrundeliegenden Sicherheitsleitlinie für wesentlich gehaltenen Aspekte der IT-Sicherheit)

Risikobehandlung (3)



Risikowahrnehmung

- Unabhängig von der ausgewählten Methode zur Risikobewertung unterliegt die Entscheidung über die Risikobehandlung verschiedenen **subjektiven Faktoren**:
  - ° Für einen hohen potenziellen Nutzen werden höhere Risiken in Kauf genommen
  - ° Gefährdungen, die vermeintlich besser kontrollierbar sind, werden typischerweise unterschätzt
  - ° Bekannte Risiken gelten als beherrschbarer als unbekannte Risiken
  - ° Sind von einem Risiko mehr Personen/Institutionen betroffen, wird dieses Risiko höher gewichtet
- Gefährdungen der Security werden systematisch als gravierender eingeschätzt als Gefährdungen der Safety
- Advanced Persistant Threats (APT) entziehen sich der „klassischen“ Risikobewertung, da dabei vom Angreifer der Aufwand zielgenauer Angriffe (targetted attacks) aufgrund der umfangreichen „Handarbeit“ und der Zielsetzung, möglichst lange nicht entdeckt zu werden, bewusst in Kauf genommen wird

Besonderheiten im Rahmen des IT-Sicherheitsgesetzes

- Bei der **Sicherheit kritischer Infrastrukturen** liegt das Augenmerk auf die **Vermeidung von Störungen** (der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit), die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind
  → Schwerpunkt liegt auf Gewährleistung der Verfügbarkeit
  → Verfügbarkeitsstörungen müssen identifiziert werden
  → maßgebliche Störungen der Funktionsfähigkeit sind zu vermeiden
  → Risikomanagement berücksichtigt vor allem Gefährdungen der Verfügbarkeit (unter Berücksichtigung von Abhängigkeiten)
  → Risiken, die die Funktionsfähigkeit von kritischen Infrastrukturen maßgeblich stören, sind nicht akzeptierbar und auch nicht aufteilbar!
  → Risikobehandlung reduziert auf:
    ° Risikovermeidung (→ keine Störung)
    ° Risikomodifizierung (→ Reduzierung, bis Störung nicht mehr maßgeblich ist)

Besonderheiten im Rahmen der EU-NIS2-Richtlinie

- Jede Beeinträchtigung der Verfügbarkeit, Authentizität, Integrität bzw. Vertraulichkeit stellt einen Sicherheitsvorfall dar, der vorzugsweise zu vermeiden und ansonsten auf ein akzeptables Maß zu reduzieren ist
  → **Beherrschbarkeit von Risiken** durch operativ wirksame Maßnahmen
- Jede (relevante) Gefahr derartiger Sicherheitsvorfälle ist zu ermitteln
- Bei der **Bewertung von Risiken** ist entscheidend, wie exponiert die Einrichtung ist (Größe & Kritikalität) und welche gesellschaftliche & wirtschaftliche Auswirkung mit dem Sicherheitsvorfall verbunden wäre
- **Gefahrenübergreifender Ansatz** = Einbeziehung physisches Umfeld, Schutz vor Systemfehler, menschlichen Fehlern, böswilligen Handlungen oder natürlichen Phänomen, Sicherheit des Personals, angemessene Zugangskontrolle und Folgen aus der Lieferkette unter Berücksichtigung spezifischer Schwachstellen, etablierter Cybersicherheitspraxis und der Sicherheit zugehöriger Entwicklungsprozesse
- Dokumentation von Schwachstellen in europäischer Schwachstellendatenbank