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

Vorlesung im Sommersemester 2013

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
✓	Kundendatenschutz		Konzeption von IT-Sicherheit

Risiko-Management:

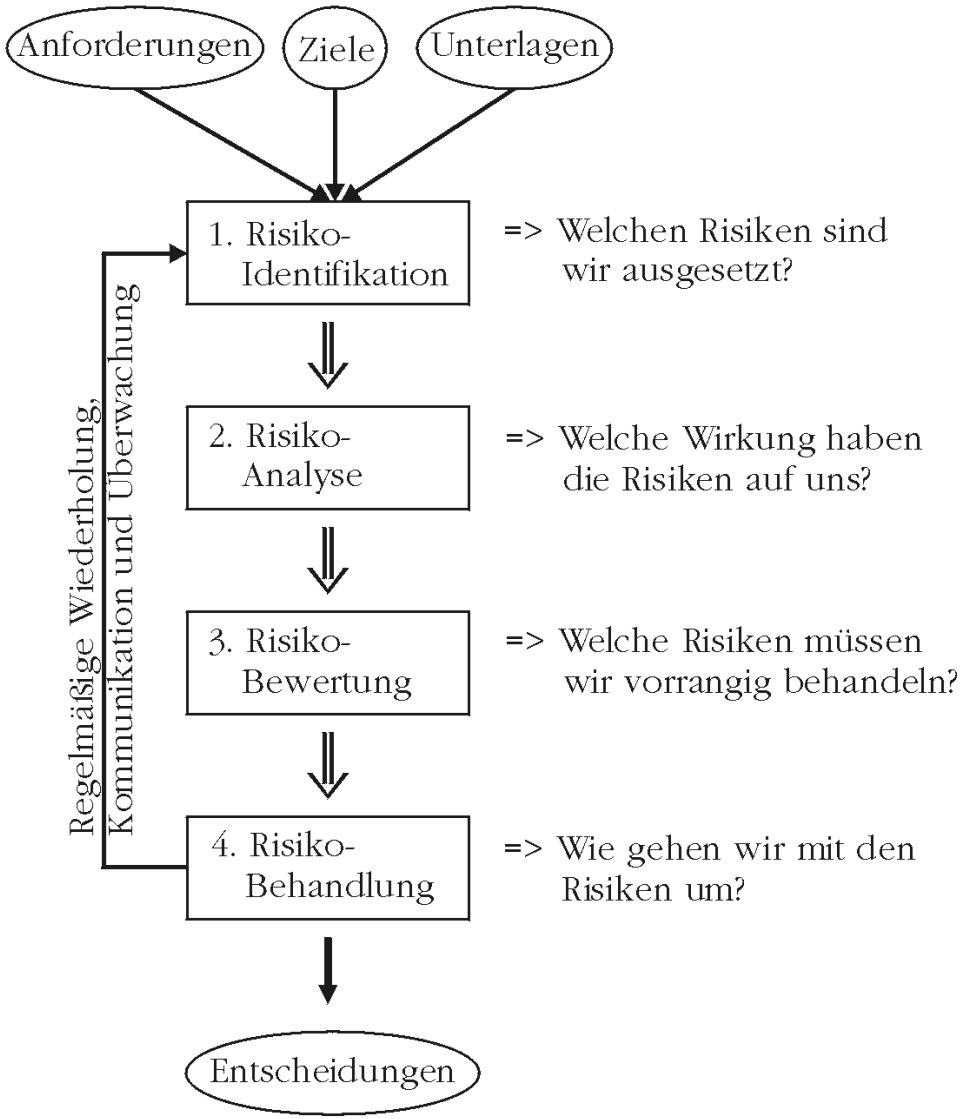
- Übersicht
- Risiko-Identifikation
- Risiko-Analyse
- Risiko-Bewertung
- Risiko-Behandlung

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
- 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
- Bestimmung der Verwundbarkeiten

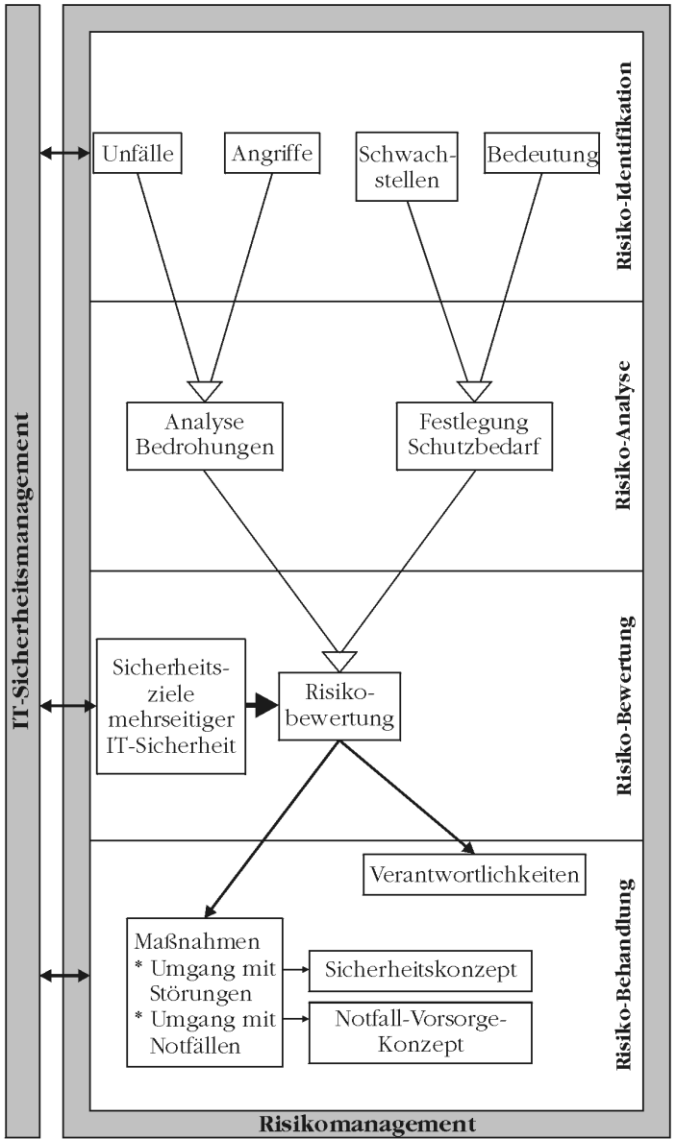
Risikoanalyse:

- Ermittlung Eintrittswahrscheinlichkeiten
- Ermittlung potenzieller Schadensauswirkungen

Risikobewertung:

- Priorisierung zu festgestellten Risiken

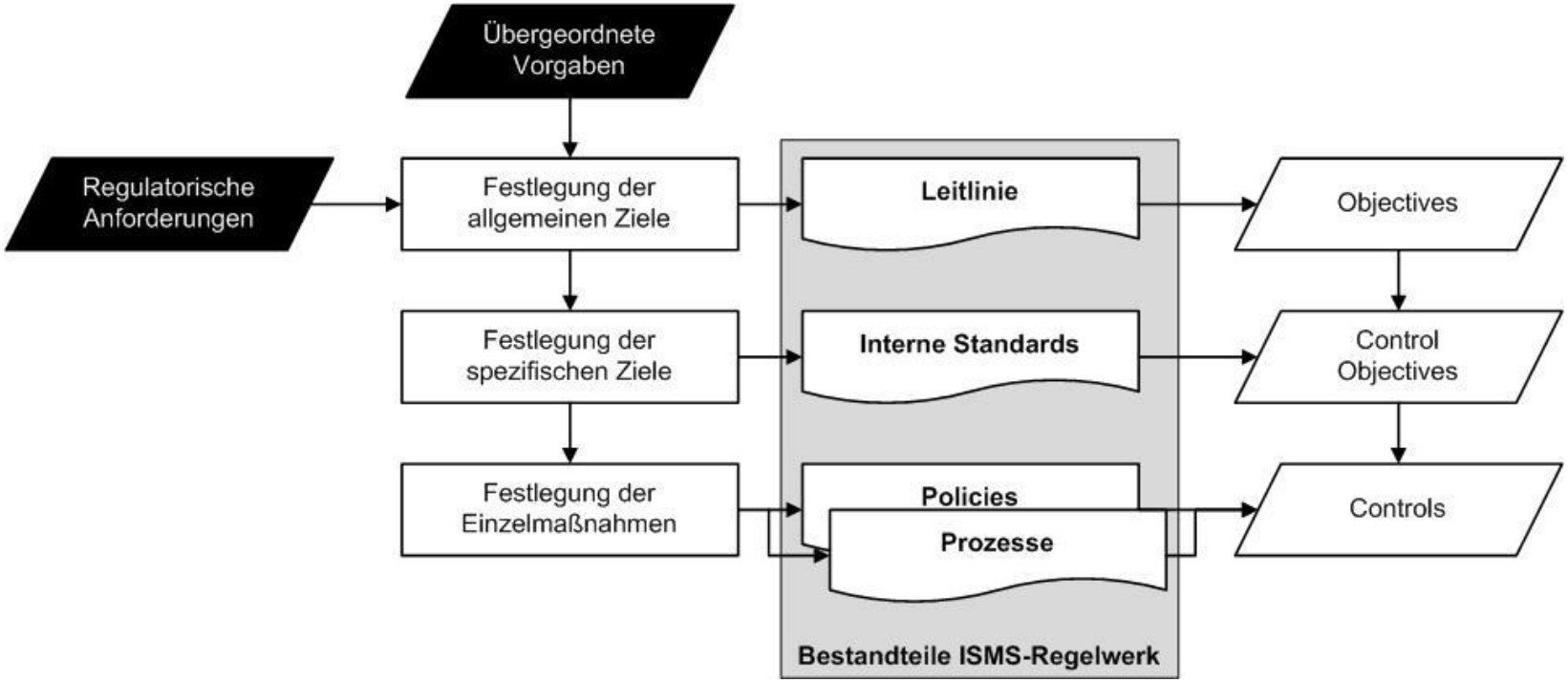
Zusammenspiel mit IT-Sicherheit



IT Risk Assessment Standards

- Risk Management – Principles & Guidelines (**ISO 31000:2009**)
  → generelles Vorgehen für Risikomanagement
- Risk Management – Risk Assessment Techniques (**IEC/ISO 31010:2009**)
  → Sammlung verschiedener Methoden
  → Bewertung zur Eignung je Einsatzfeld
- IT Security Techniques – Information Security Risk Management (**ISO/IEC 27005:2011**)
  → Adaption Risikomanagement für Informationssicherheit
  → Eingebettet in Management der Informationssicherheit
  → kompatibel mit ISO/IEC 27001:2005 & ISO/IEC 27002:2005
  → typische Anwendung in der Praxis (Annex E):
    1. High-Level Risk Assessment → wo genauer analysieren?
    2. Detailed Risk Assessment → zielgenaue Detailanalyse

Controls abgeleitet aus Ziele des ISMS zum Umgang mit Risiken



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)
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

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

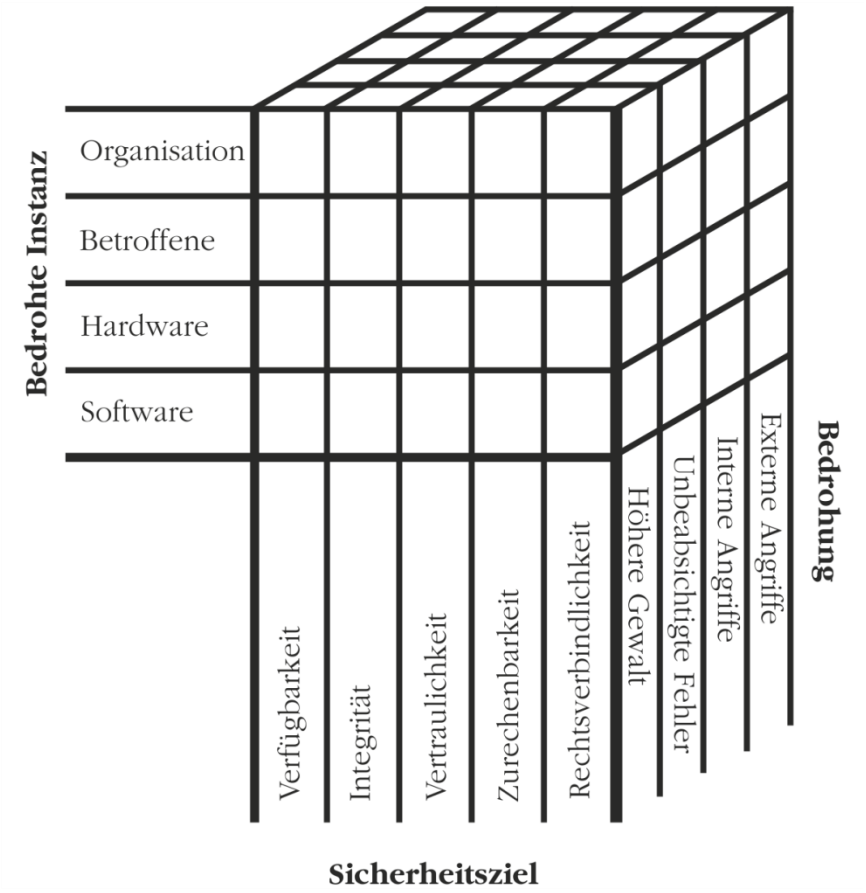
Fehlermöglichkeits- und -einflußanalyse (FMEA)
[Failure Mode and Effect Analysis, IEC 60812]

→ 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)

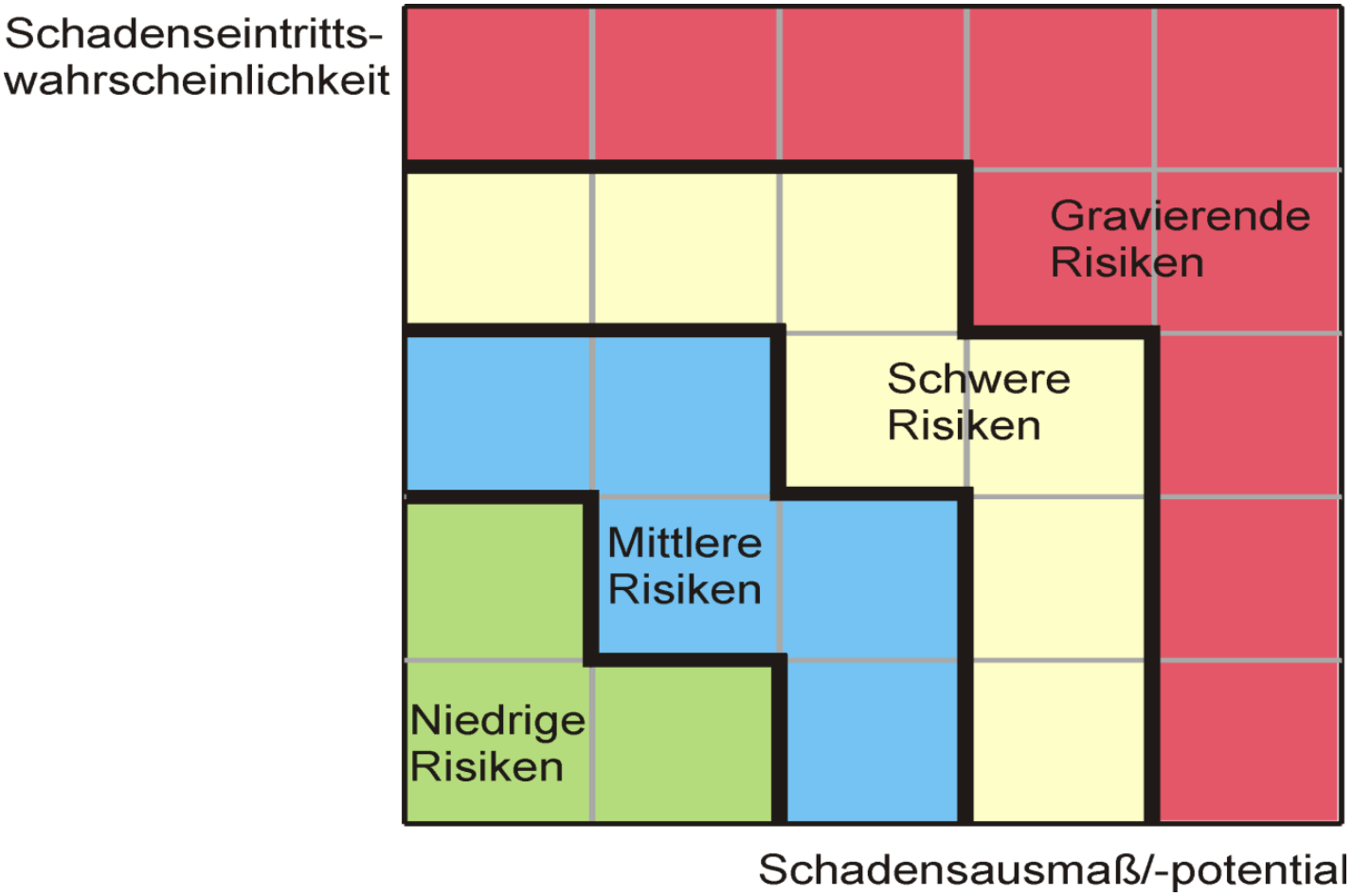
Risiko-Rang	Risiko-Kategorie	Auswirkung	Eintrittswahrscheinlichkeit	Risikofaktor	
1.	Text 1	A_1	W_1	A_1*W_1	**erfordert Maßnahmen**
2.	Text 2	A_2	W_2	A_2*W_2	
...	...	...	...	...	
n	Text n	A_n	W_n	A_n*W_n	**akzeptierbar**
...	...	...	...	...	

Beispiel: CIA-Analyse

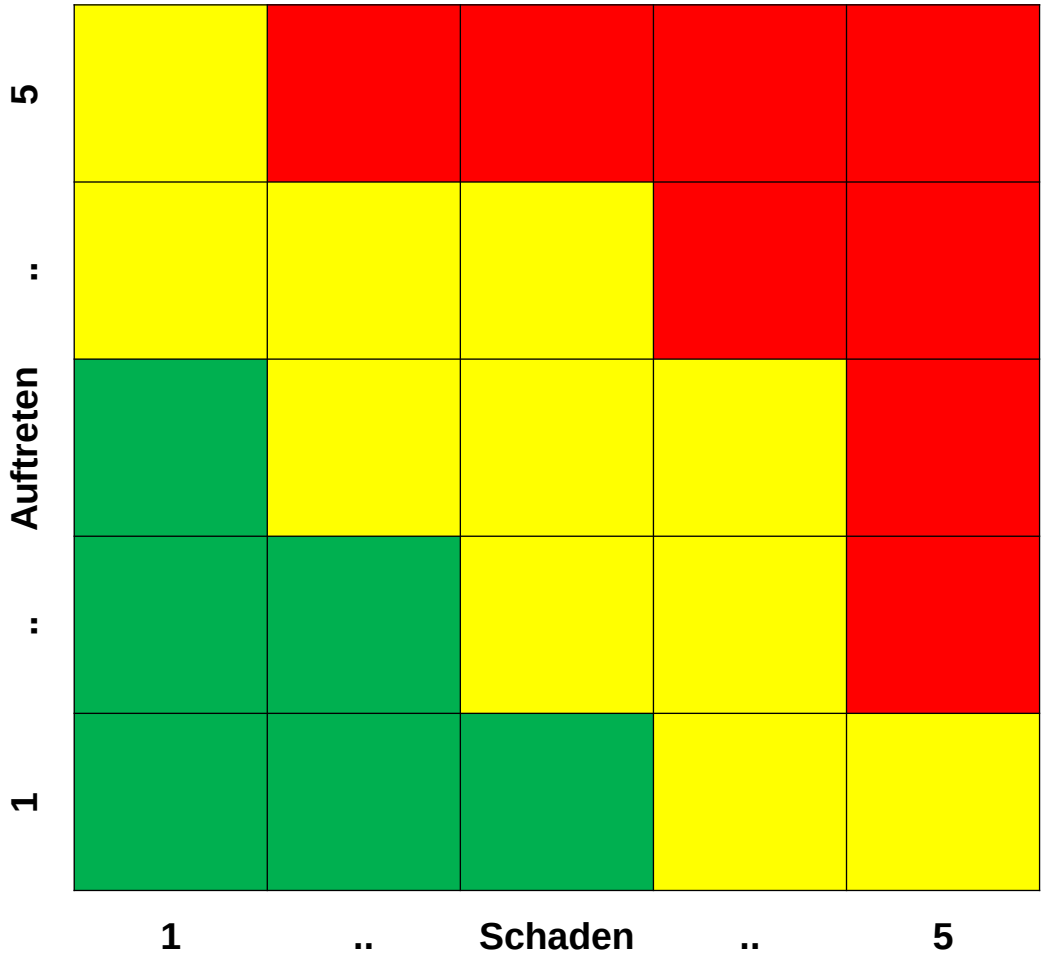
Bedrohung	Verwundbarkeit	Auftreten	Schaden		
			C	I	A
Datenverlust	fehlende Clusterung	3	1	1	3
Datenverlust	Ermüdung Backupmedien	2	1	4	4
unbefugter Zugriff	fehlende Schutzzonen	3	5	1	5
unbefugter Zugriff	schlechte Passwörter	4	4	3	2
unbefugter Zugriff	fehlende Systemhärtung	3	4	4	4
unbefugter Zugriff	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)

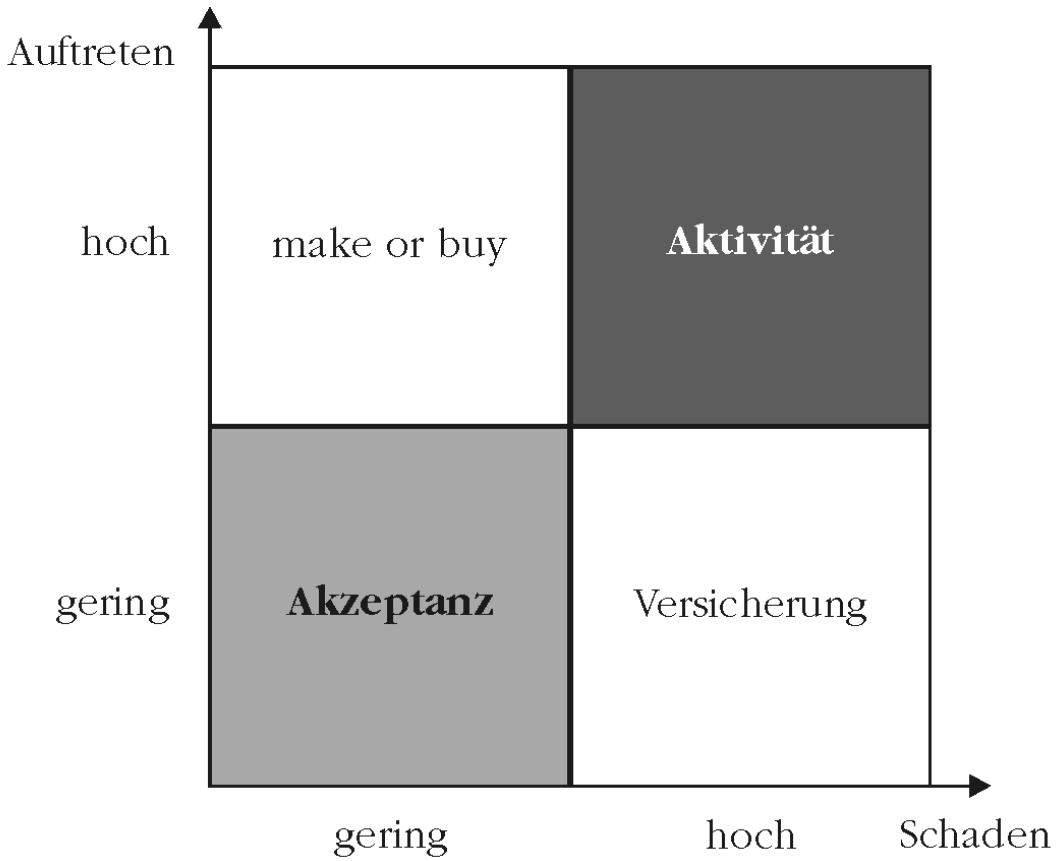
Portfolio-Analyse (1)



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):

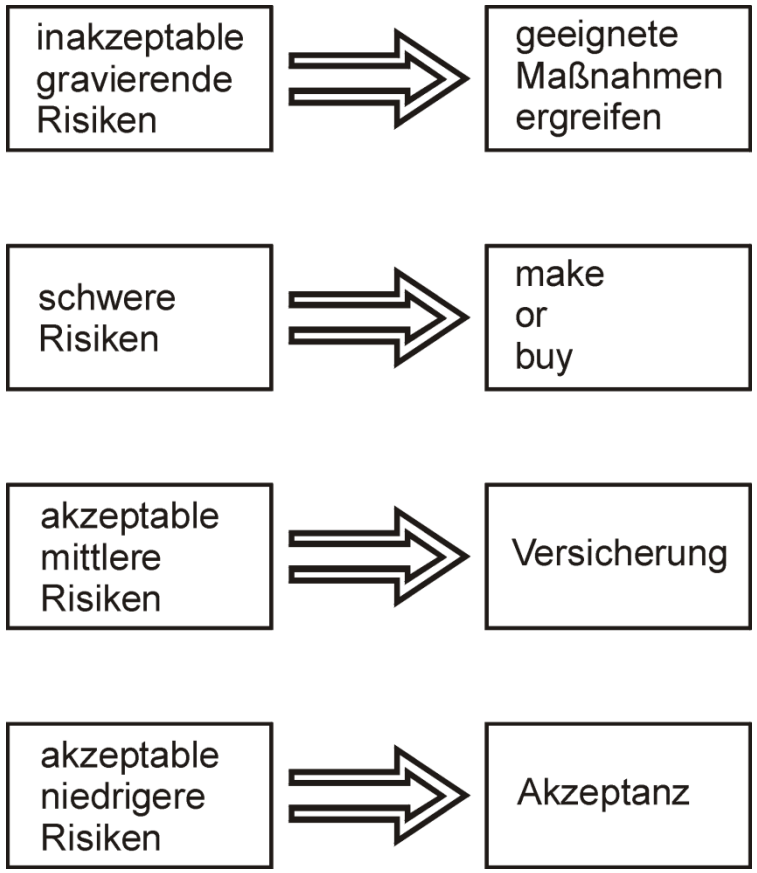
- Kennzahlensystem zur strategischen Unternehmensplanung
- Ausbalancierung vorgegebener Werte von Perspektiven:
  - finanzielle Perspektiven
  - Kundenperspektive
  - interne Prozessperspektive
  - Lernen- und Wachstumsperspektive
- Untersuchung erfolgt anhand
  - Ziele
  - Kennzahlen
  - Vorgehen
 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

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
- **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)



Risikobehandlung (3)

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 bei IT-Systemen:
  → Einrichtung eines Sicherheitsteams („Computer Emergency Response Team“ = CERT) zur Unterstützung des IT-Sicherheitsbeauftragten
- Ausarbeitung eines Sicherheitsmodells (= abstrakte Beschreibung der nach der zugrundeliegenden Sicherheitsleitlinie für wesentlich gehaltenen Aspekte der IT-Sicherheit)

Risikobehandlung (4)