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

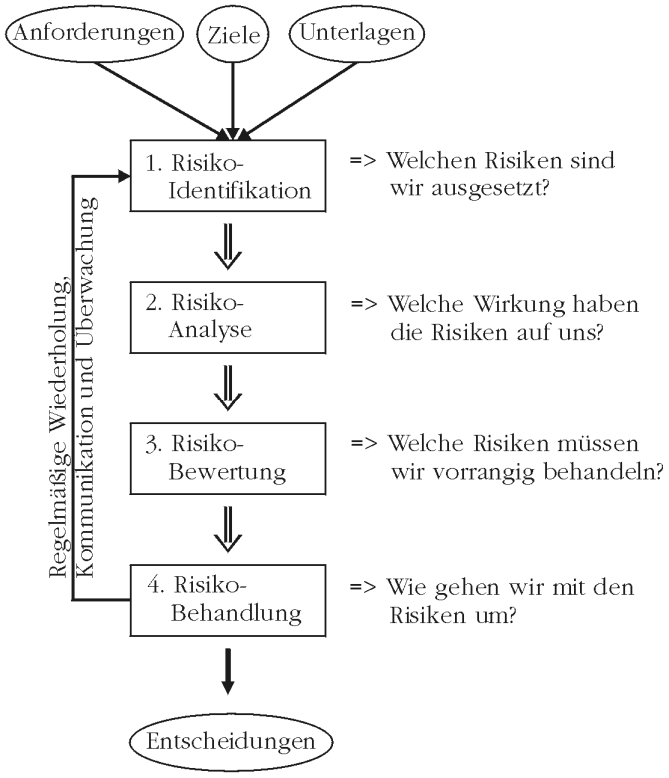
Vorlesung im Sommersemester 2009
an der Universität Ulm
von Bernhard C. Witt

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
✓	Schwerpunktthema zur Vertiefung		Konzeption von IT-Sicherheit

Risiko-Management:
- Übersicht
- Risiko-Identifikation
- Risiko-Analyse
- Risiko-Bewertung
- Risiko-Behandlung

Risiko-Management



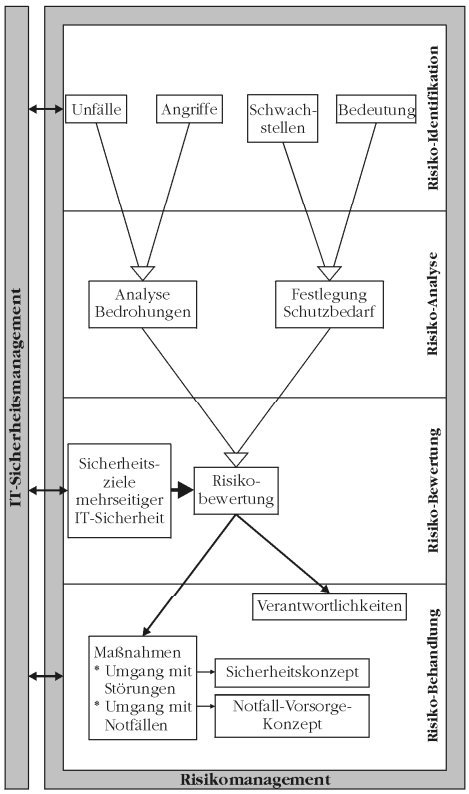
IT-Risiken

Definition 16: Risiko

Nach Häufigkeit und Auswirkung bewertete Abweichung eines zielorientierten Systems.

- System wird mit Zielsetzung verbunden (Prüfbarkeit!)
- Zielabweichung kann auch positiv erfolgen
  → Chancen
- Faktoren: **Häufigkeit * Auswirkung**
  abhängig von Vermögenswerten (assets), Bedrohungen (threats) und Verwundbarkeiten (vulnerabilities)

Zusammenspiel mit IT-Sicherheit



Typische Kriterien zur Einordnung identifizierter Risiken

Bewertungskriterien	2000	2002	2004	2006	2008
Verstöße gegen Gesetze/Verträge	1,15	1,47	1,40	1,46	1,44
Imageverlust	1,23	1,51	1,35	1,36	1,42
Manipulation an Informationen	1,20	1,36	1,26	1,28	1,38
Verzögerung von Arbeitsabläufen	1,23	1,35	1,21	1,31	1,29
Haftungsansprüche Dritter	0,95	1,11	1,27	1,28	1,22
indirekte finanzielle Verluste	0,98	0,98	1,14	1,12	1,16
Verstöße gegen interne Regelungen	0,70	0,85	0,72	0,89	0,94
direkte finanzielle HW-Schaden	0,81	0,97	0,75	0,95	0,88

Quelle: <kes>-Sicherheitsstudien (Angaben: [0 .. 2])

Gründe für fehlende IT-Sicherheit

Hinderungsgründe	1998	2000	2002	2004	2006	2008
Geld	40%	31%	46%	62%	55%	43%
Bewusstsein bei Mitarbeitern	55%	60%	65%	51%	52%	69%
Bewusstsein Top-Managment	50%	51%	50%	45%	45%	55%
Bewusstsein mittleres Management	45%	38%	61%	42%	37%	45%
verfügbare kompetente Mitarbeiter	34%	38%	37%	33%	32%	43%
Durchsetzungsmöglichkeit	30%	29%	38%	28%	31%	38%
strategische Grundlagen	28%	38%	34%	31%	29%	36%
Kontrollen auf Einhaltung	27%	26%	34%	29%	27%	41%
unvorbereitete Anwendungen	-----	-----	22%	17%	25%	27%
Nichtumsetzen vorhandener Konzepte	12%	14%	20%	18%	22%	27%
realisierbare (Teil-)Konzepte	19%	15%	21%	16%	19%	25%
geeignete Methoden & Werkzeuge	20%	21%	18%	18%	16%	16%
geeignete Produkte	10%	14%	12%	17%	13%	16%
praxisorientierte Sicherheitsberater	9%	11%	10%	8%	8%	14%

Quelle: <kes>-Sicherheitsstudien

Risiko-Identifikation

1. Ermittlung der zu schützenden Vermögenswerte (**Assets**): Prozesse, IT-Systeme, Personen, Daten
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…)
3. Feststellung der Bewertung der Assets, z.B. anhand einer **CIA-Analyse**, d.h. der maximalen Bedeutung des Assets hinsichtlich der Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit
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

Methoden der Risiko-Analyse

- Fehlerbaum-Analyse
- Angriffsbaum-Analyse
- Fehlermöglichkeits- und -einfluss-Analyse

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)

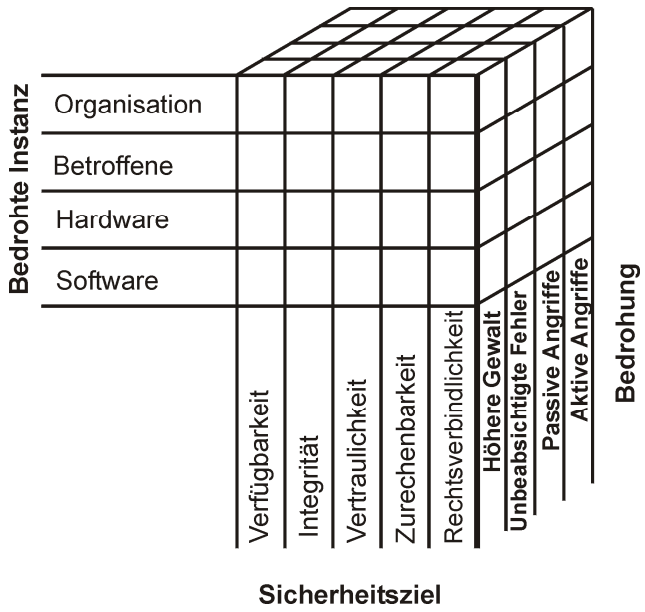
Risikoanalyse: FMEA

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

→ Beurteilung der Bedeutung potentieller Fehler (Skala: 1 .. 10)
Entdeckungswahrscheinlichkeit mit (10 – W) angegeben (allerdings oft nur schwer zu bestimmen → Honeynets & Honeypots); Bedeutung = Schaden

→ Bottom-Up-Methode zur Schwachstellen-Analyse

Ergebnis Risikoanalyse: Risikokubus



Methoden der Risikobewertung

- Risikotabelle / Risikomatrix
- Risikoportfolio / Risk Map
- SWOT-Analyse & Balanced Scorecard

Risikomatrix (Risikotabelle)

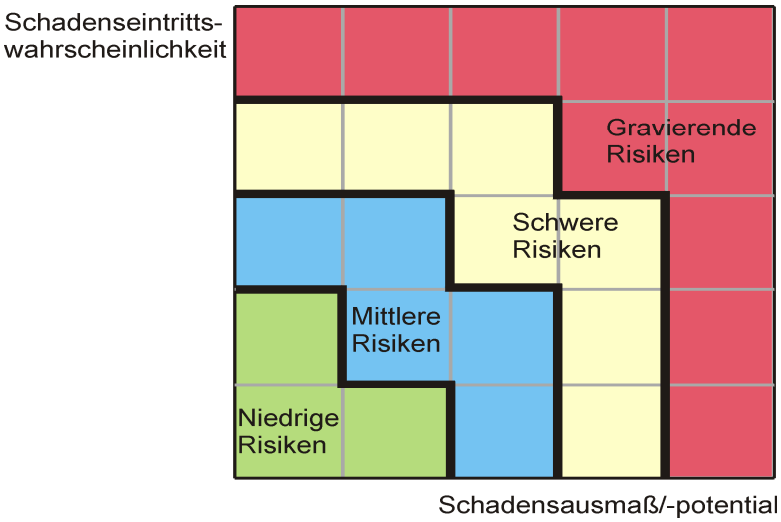
Risiko-Rang	Risiko-Kategorie	Auswirkung	Eintrittswahrscheinlichkeit	Risikofaktor	
1.	Text 1	A_1	W_1	A_1*W_1	erfordert Maßnahmen
2.	Text 2	A_2	W_2	A_2*W_2	
...	...	...	...	...	
n	Text n	A_n	W_n	A_n*W_n	akzeptierbar
...	...	...	...	...	

Beispiel: CIA-Analyse

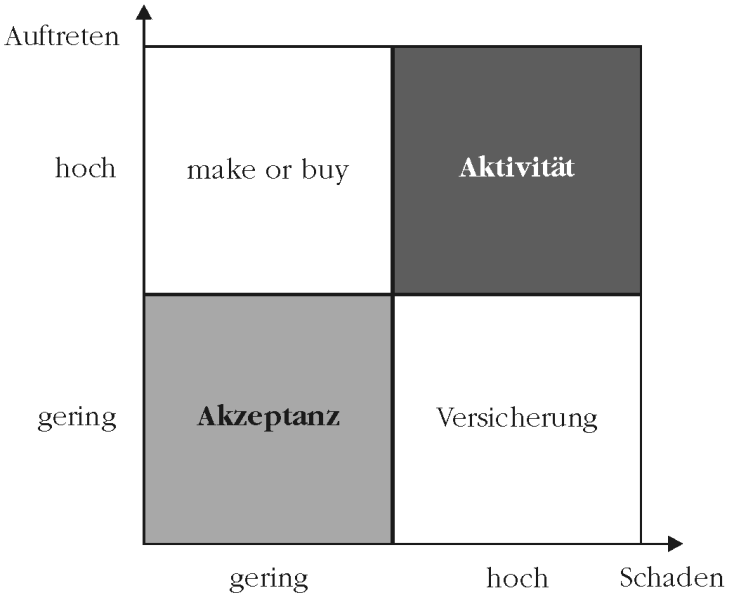
Bedrohung	Verwundbarkeit	Auftreten	Schaden		
			C	I	A
Datenverlust	fehlende Clusterung	3	1	1	3
Datenverlust	Ermüdung Backupmedien	2	1	4	4
unbefugter Zugriff	fehlende Schutzzonen	3	5	1	5
unbefugter Zugriff	schlechte Passwörter	4	4	3	2
unbefugter Zugriff	fehlende Systemhärtung	3	4	4	4
unbefugter Zugriff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



Variante Risk-Map



Weitere Methoden zur Risikobewertung

SWOT-Analyse:

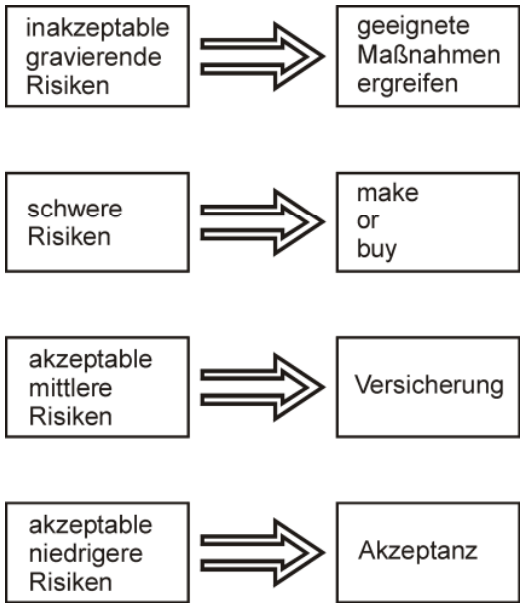
- Gegenüberstellung von
  - ° Stärken (**s**trengths)
  - ° Schwächen (**w**eaknesses)

  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)



Risikobehandlung (2)

- zur Schwachstellenanalyse von IT-Systemen werden u.a. Penetrationstests und Security-Scans durchgeführt
- 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 (3)