Grundlagen des Datenschutzes und der IT-Sicherheit (12)

Vorlesung im Sommersemester 2007
an der Universität Ulm
von Bernhard C. Witt

Grob-Gliederung zur Vorlesung

Topics zum Datenschutz:
- Geschichte des Datenschutzes
- Datenschutzrechtliche Prinzipien
- Vertiefung in ausgewählten Bereichen
- Verwandte Gebiete zum Datenschutz

Topics zur IT-Sicherheit:
- Einflussfaktoren zur IT-Sicherheit

→ **Mehrseitige IT-Sicherheit**
- Risiko-Management
- Konzeption von IT-Sicherheit

Sicherung der Integrität

- → Ein Nachweis von Integrität erfolgt z.B. mittels Authentifizierungs-mechanismen
- → Ebenso im Einsatz vor allem zur Vermeidung ungewollter Manipulationen: fehlerkorrigierender Code & verschiedene Fehlermeldeverfahren
- → Die Zuverlässigkeit von IT-Komponenten kann durch entsprechende Zertifikate (Common Criteria) nachgewiesen werden
- → Protokollierungen erforderlich für Datenqualität
- → Revisionssicherheit z.B. durch Abspeichern auf nur einmal beschreibbaren Datenträgern

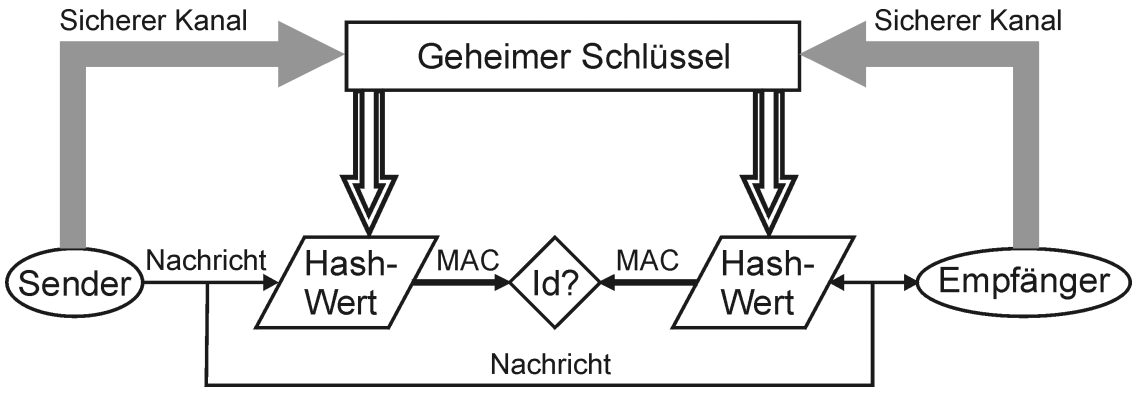
Hinweis:

Authentisierung = Nachweis einer Identität

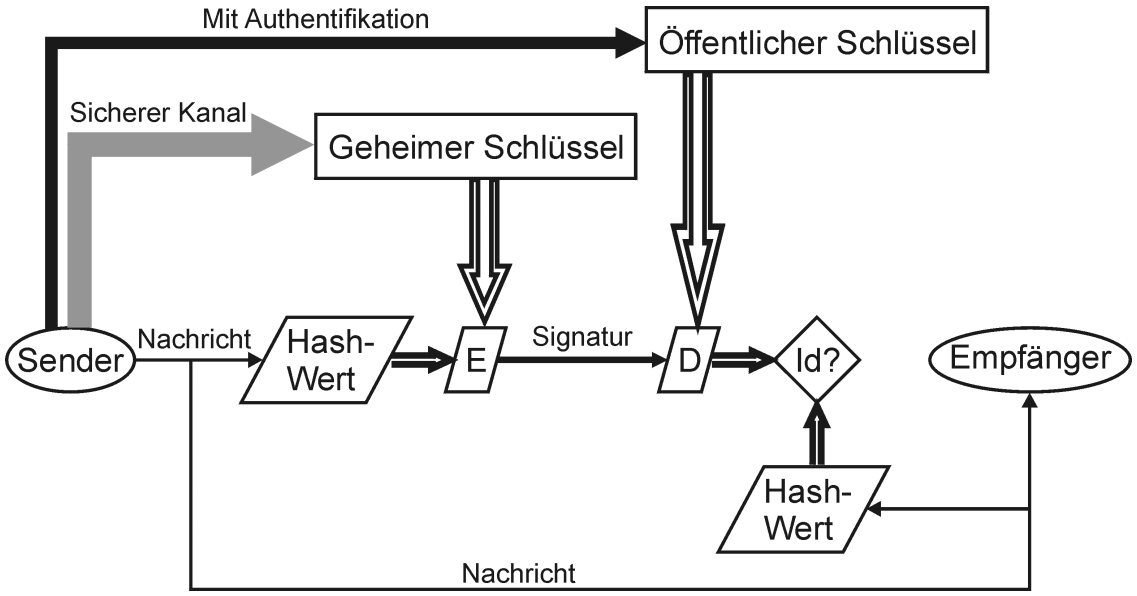
Authentifizierung = Überprüfung einer Identität

Autorisierung = Gewährung von Zutritts-/Zugangs-/Zugriffsrechten

Symmetrische Authentifikation: Message Authentication Code



Asymmetrische Authentifikation: Digitale Signatur



Vergleich der Authentifikationen

Symmetrisch:

- Gängige Verfahren: SecurID, GSM-Authentikation
- Ziel: Sicherung d. **Integrität**
- Key-Recovery sinnvoll: Hinterlegung des Entschlüsselungsschlüssels zur Vorbeugung gegen Schlüsselverlust

Asymmetrisch:

- Gängige Verfahren: RSA, ElGamal, DSS, DSA
- Ziel: Sicherung d. **Integrität** & **Zurechenbarkeit**
- erfüllt Anforderungen zur fortgeschrittenen Signatur nach SigG, sofern geheimer Schlüssel unter alleiniger Kontrolle des Schlüsselinhabers (qualifizierte Signatur, wenn zertifiziert und mit sicherer Einheit erzeugt)

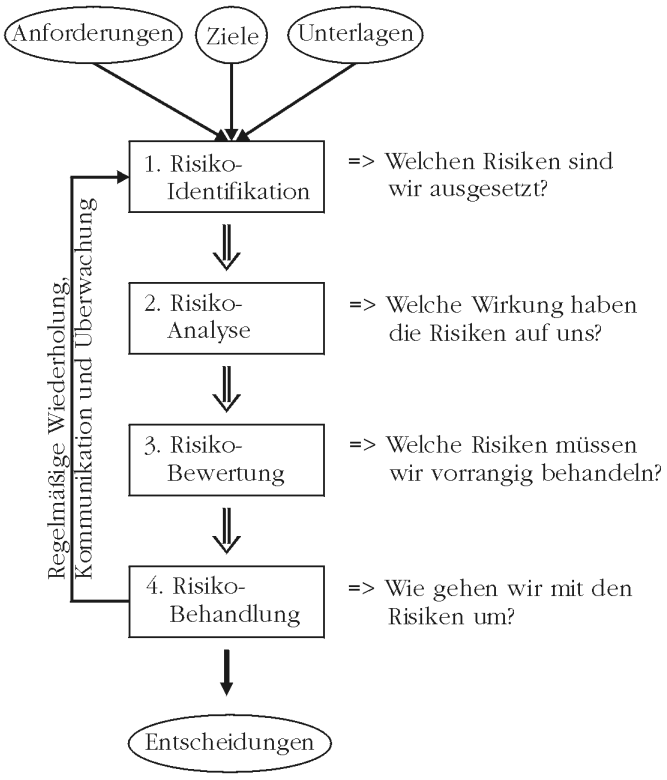
Grob-Gliederung zur Vorlesung

Topics zum Datenschutz:
- Geschichte des Datenschutzes
- Datenschutzrechtliche Prinzipien
- Vertiefung in ausgewählten Bereichen
- Verwandte Gebiete zum Datenschutz

Topics zur IT-Sicherheit:
- Einflussfaktoren zur IT-Sicherheit
- Mehrseitige IT-Sicherheit

→ **Risiko-Management**
- Konzeption von IT-Sicherheit

Risiko-Management



IT-Risiken

Definition 13: Risiko

Nach Häufigkeit und Auswirkung bewertete Abweichung eines zielorientierten Systems.

- System wird mit Zielsetzung verbunden (Prüfbarkeit!)
- Zielabweichung kann auch positiv erfolgen
  → Chancen
- maßgebliche Einflussfaktoren:
  Häufigkeit * Auswirkung

→ nötig: Analyseinstrumentarien & Management

Hinweise zum Risiko-Management (1)

- **Risiko-Identifikation**

→ siehe 5. Übung!

  ° abhängig von den zu schützenden Werten (assets)
  ° Berücksichtigung von Bedrohungen (threats) & Schwachstellen (vulnerabilities)

- **Risiko-Analyse**

→ siehe 6. Übung!

  ° Fehlerbaum-Analyse
  ° Angriffsbaum-Analyse
  ° Fehlermöglichkeits- und -einflussanalyse (FMEA)

Typische Kriterien zur Einordnung identifizierter Risiken

Bewertungskriterien	2000	2002	2004	2006
Verstöße gegen Gesetze/Verträge	1,15	1,47	1,4	1,46
Imageverlust	1,23	1,51	1,35	1,36
Verzögerung von Arbeitsabläufen	1,23	1,35	1,21	1,31
Haftungsansprüche Dritter	0,95	1,11	1,27	1,28
Manipulation an Informationen	1,2	1,36	1,26	1,28
indirekte finanzielle Verluste	0,98	0,98	1,14	1,12
direkte finanzielle HW-Schaden	0,81	0,97	0,75	0,95
Verstöße gegen interne Regelungen	0,7	0,85	0,72	0,89

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

Gründe für fehlende IT-Sicherheit

Hinderungsgründe	1998	2000	2002	2004	2006
Geld	40%	31%	46%	62%	55%
Bewusstsein bei Mitarbeitern	55%	60%	65%	51%	52%
Bewusstsein Top-Managment	50%	51%	50%	45%	45%
Bewusstsein mittl. Managem.	45%	38%	61%	42%	37%
verfügb. kompetente Mitarb.	34%	38%	37%	33%	32%
Durchsetzungsmöglichkeit	30%	29%	38%	28%	31%
strategische Grundlagen	28%	38%	34%	31%	29%
Kontrollen auf Einhaltung	27%	26%	34%	29%	27%
unvorbereitete Anwendungen	-----	-----	22%	17%	25%
Nichtumsetzen vorh. Konzepte	12%	14%	20%	18%	22%
realisierbare (Teil-)Konzepte	19%	15%	21%	16%	19%
geeig. Methoden & Werkzeuge	20%	21%	18%	18%	16%
geeignete Produkte	10%	14%	12%	17%	13%
praxisorient. Sicherheitsberater	9%	11%	10%	8%	8%

Quelle: <kes>-Sicherheitsstudien

Risikoanalyse: FMEA

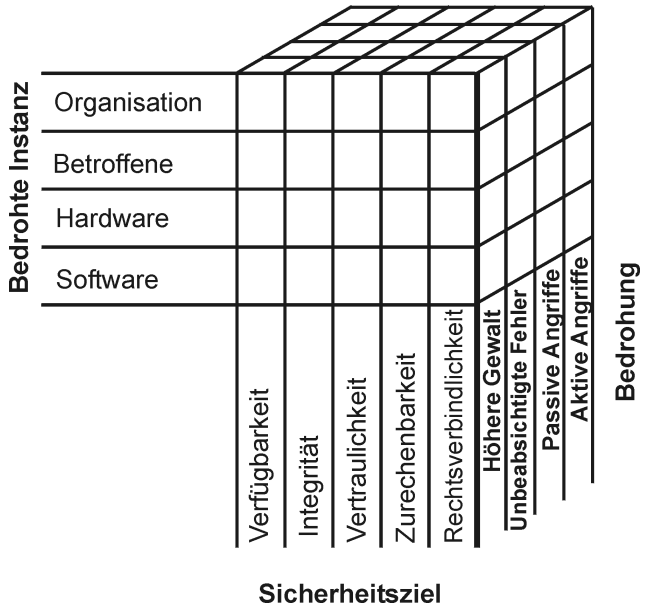
Fehlermöglichkeits- und -einflußanalyse (FMEA)
[Failure Mode and Effect Analysis]

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

Entdeckungswahrscheinlichkeit mit (10 – W) angegeben; Bedeutung = Schaden

→ Bottom-Up-Methode zur Schwachstellen-Analyse

Ergebnis Risikoanalyse: Risikokubus



Hinweise zum Risiko-Management (2)

- **Gängige Methoden zur Risiko-Bewertung**:

→ siehe 7. Übung!

  ° Risikomatrix in der Form einer Risikotabelle
  ° Risikoportfolio
  ° SWOT-Analyse
  ° Balanced Score Card (BSC)

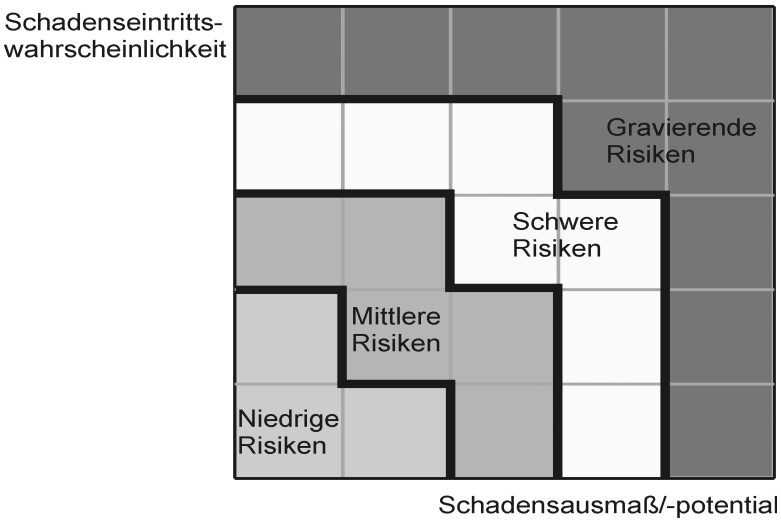
- **Risiko-Behandlung:**

→ Priorisierung anhand Höhe des Risikos gemäß festgelegter Akzeptanzlinie

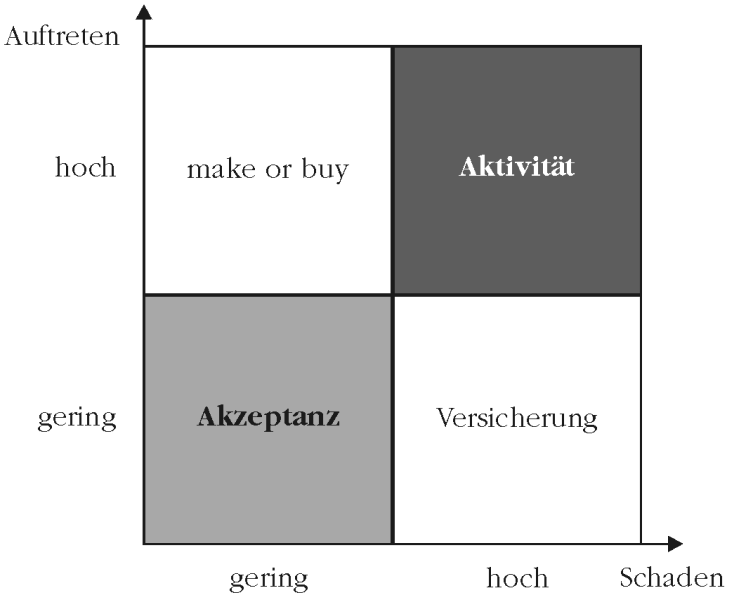
Risikomatrix (Risikotabelle)

Risiko-Rang	Risiko-Kategorie	Auswirkung	Eintrittswahrscheinlichkeit	Risikofaktor	
1.	Text 1	A_1	W_1	A_1*W_1	Maß-nahmen
2.	Text 2	A_2	W_2	A_2*W_2	erfordert
...	...	...	...	...	
n	Text n	A_n	W_n	A_n*W_n	bar
...	...	...	...	...	akzeptier-

Portfolio-Analyse



Variante Risk-Map



Weitere Methoden zur Risikobewertung

SWOT-Analyse:

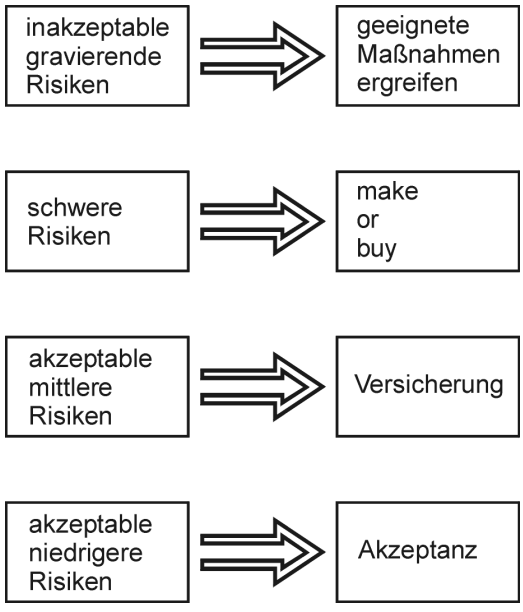
- Gegenüberstellung von
  - ° Stärken (**s**trengths)
  - ° Schwächen (**w**eaknesses)

  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

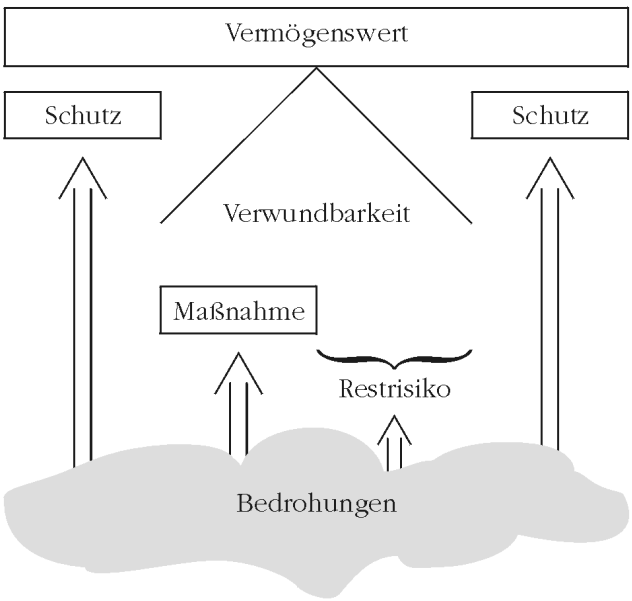
Risikobehandlung (1)



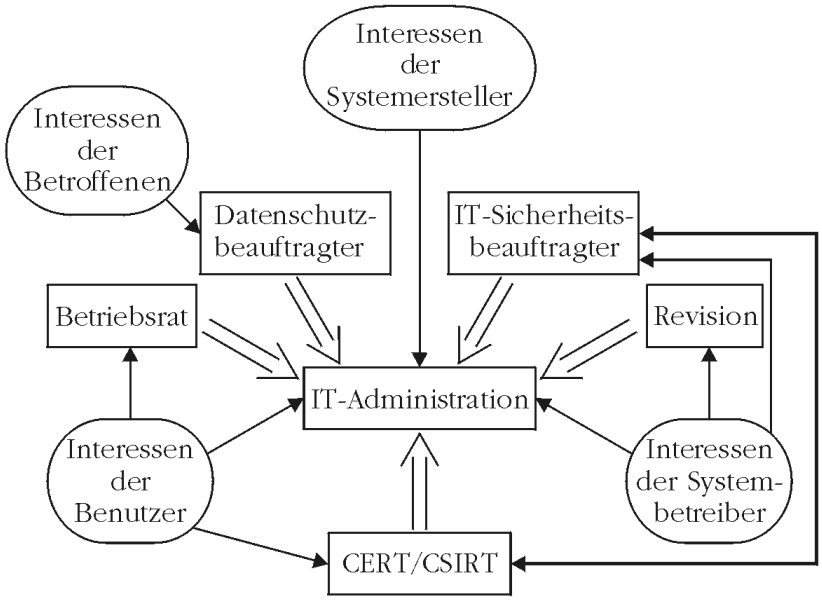
Risikobehandlung (2)

- 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“) zur Unterstützung des IT-Sicherheits-beauftragten
- Ausarbeitung eines Sicherheitsmodells (= abstrakte Beschreibung der nach der zugrundeliegenden Sicherheits-leitlinie für wesentlich gehaltenen Aspekte der IT-Sicherheit)

Risikobehandlung (3)



Akteure zur IT-Sicherheit



Zusammenspiel mit IT-Sicherheit