Grundlagen des Datenschutzes und der IT-Sicherheit (10)

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

Grob-Gliederung zur Vorlesung

Topics zum Datenschutz:

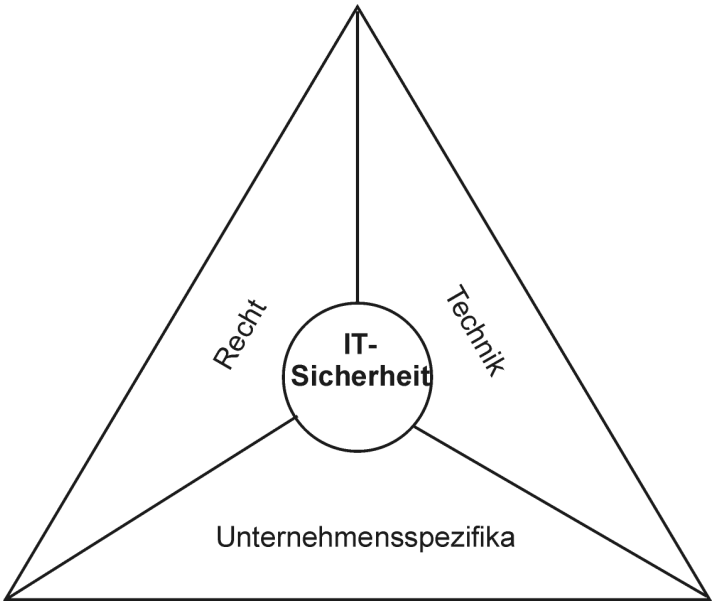
- Geschichte des Datenschutzes
- Datenschutzrechtliche Prinzipien
- Vertiefung in ausgewählten Bereichen
- Verwandte Gebiete zum Datenschutz

Topics zur IT-Sicherheit:

→ Einflussfaktoren zur IT-Sicherheit

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

Einflussfaktoren der IT-Sicherheit



Einflussfaktor Recht (1)

Sorgfaltspflicht:

- KonTraG (§ 91 II AktG, § 43 I GmbHG) → Überwachungssystem zur Erkennung fortbestands-gefährdender Entwicklungen
- Haftungsrecht (§ 276 BGB, § 100 UrhG)
- Betriebs- und Geschäftsgeheimnisse (§ 17 UWG)
- Buchführungspflichten (§§ 238 I & 257 HGB, §§ 145-147 AO)
- Schutz vor Angriffen (§§ 202a, 268, 269, 270, 303b & 305a StGB)

Einflussfaktor Recht (2)

Datenschutz:

- grundlegend: §§ 3a, 4, 9 (samt Anlage), 28 und 31 BDSG
- Haftungsrecht (§§ 7, 43 & 44 BDSG)

Fernmeldegeheimnis:

- §§ 88, 100, 107 & 109 TKG
- § 4 TDDSG
- §§ 206 & 303a StGB

Einflussfaktor Recht (3)

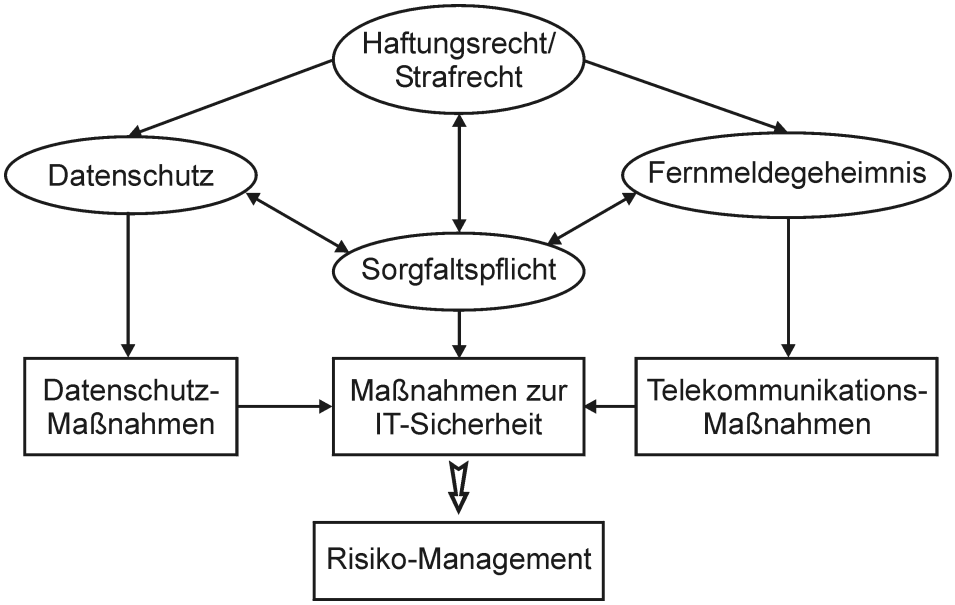
sowie spezialrechtliche Vorgaben:

- insbes. für Banken, Gesundheitswesen, Sozialwesen, Arbeitsrecht und international tätige Unternehmen (z.B. Sarbanes-Oxley-Act)

und vertragsrechtliche Verpflichtungen:

- New Basel Capital Accord (Basel II)
  → Verbilligung der Fremdkapitalfinanzierung für Unternehmen mit gutem Rating
  → Berücksichtigung operationaler Risiken & Nachweis der Verlässlichkeit und Stabilität des DV-Systems

Übersicht Sicherheitsrecht



Einflussfaktor Technik

1. Bedeutung von Informationen & IuK-Technik (VL 18.04.2007)

- Informationen als „Rohstoff“
- Fortentwicklung der Informationstechnik

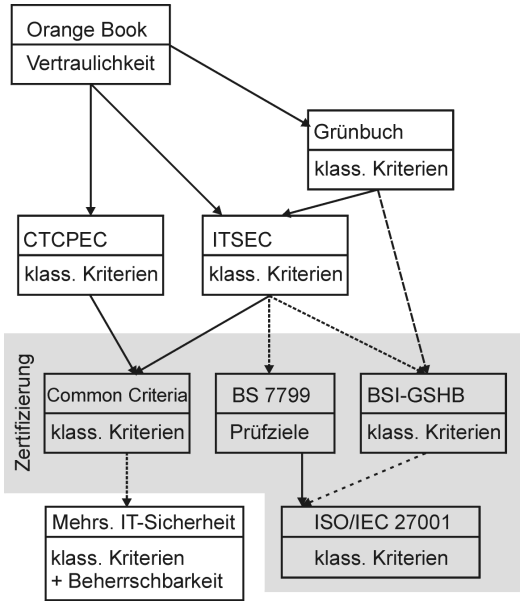
2. Kenndaten aus den <kes>-Sicherheitsstudien:

- Verhältnis von eingesetzter IT pro Mitarbeiter anwachsend:
  1990: 0,06 → 1996: 0,23 → 2002: 0,63 → 2006: 0,72
  Telearbeit stark anwachsend:
  2004: 0,01 → 2006: 0,07

3. Standardisierungen:

- internationale Normen & best-practice-Standards

Entwicklung relevanter Standards



Hinweise zu den Standards (1)

„Orange Book“ (1983):

- Trusted Computer System Evaluation Criteria

„Grünbuch“ (1989):

- Kriterien für die Bewertung der Sicherheit von Systemen der IT

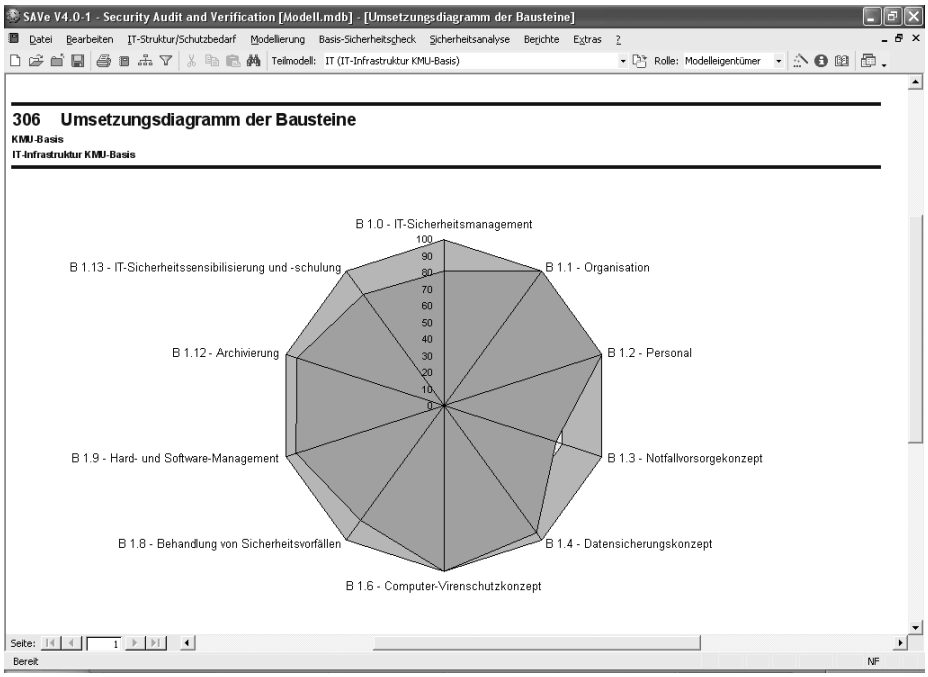
„ITSEC“ (1990):

- Information Technology Security Evaluation Criteria

„Grundschutz“ (1995):

- bis 2005 „IT-Grundschutzhandbuch“, seither „IT-Grundschutz-Kataloge“
- prüft nur Maßnahmen, die einen niedrigen bis mittleren Schaden abwenden (Grundschutz)

Umsetzung der Pflichtbausteine



Hinweise zu den Standards (2)

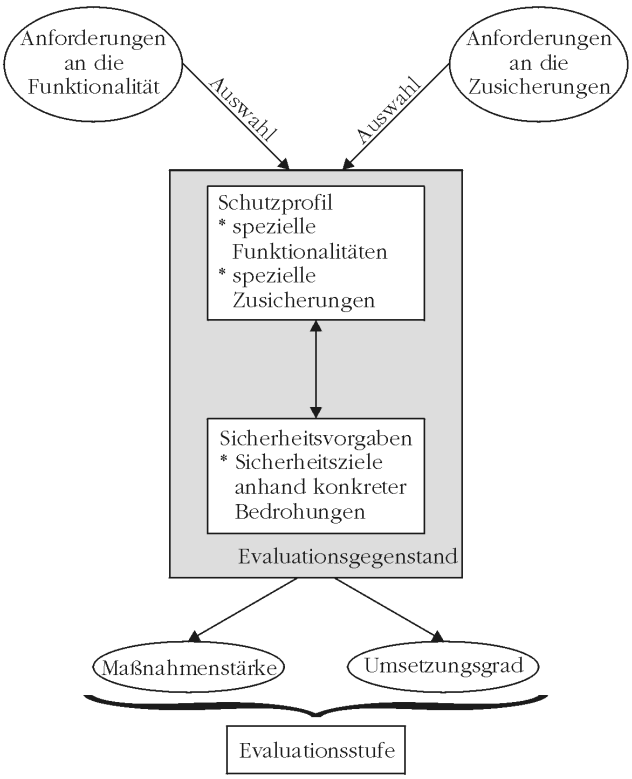
„Common Criteria“ (1996):

- Common Criteria for Information Technology Security Evaluation
- = ISO/IEC 15408
- verwendete Schutzprofile werden nach ISO/IEC 15446 erstellt

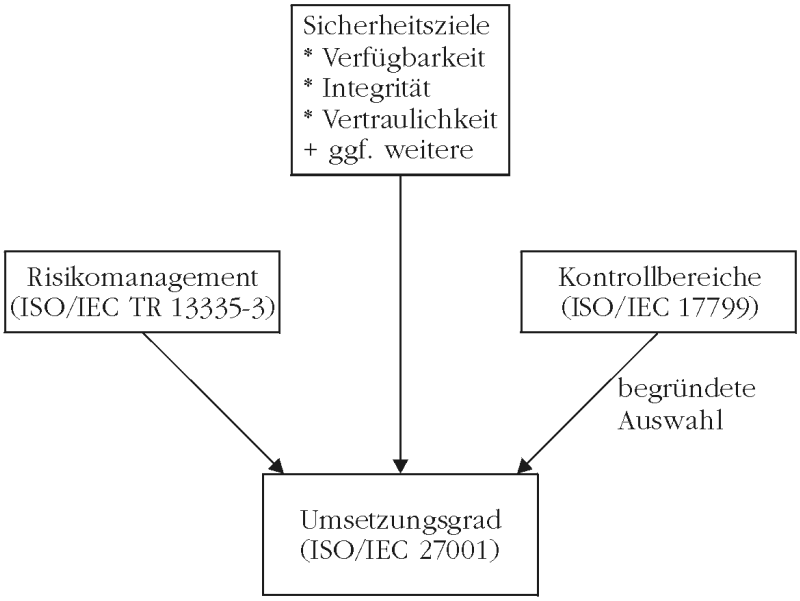
„BS 7799“ (1995):

- Information Security Management System
- British Standard 7799
- seit 2000 (für BS 7799-1): ISO/IEC 17799
- seit 2005 (für BS 7799-2): ISO/IEC 27001 (zertifizierbarer Teil)

Struktur der Common Criteria



Struktur zum Information Security Management



Weitere Standards

- **FIPS 140-1/2** (1994)
  = ISO/IEC 19790
- **ITIL** (1995)
  Information Technology Infrastructure Library
  → prozess-, service- & kunden-orientierte IT-Organisation
  → zertifizierbar via ISO/IEC 20000
- **CobiT** (1996)
  Control Objectives for Information and related Technology
  → IT-Governance
- **ISO TR 13335** (1996)
  → Technische Reports zum IT-Sicherheitsmanagement
  → seit 2004 (für ISO TR 13335-1 & 13335-2): ISO/IEC 13335-1

Einflussfaktor Unternehmensspezifika (1)

Branchenzugehörigkeit & Marktstellung

- branchenspezifische Anforderungen (insb. für Banken, Versicherungen, Pharmaunternehmen, Automobilindustrie → Nachweis guter Praxis)
- marktbeherrschende Stellung
- internationale Ausrichtung (vor allem hinsichtlich SOX)
- Vorteile durch bzw. Forderung nach Zertifizierungen
- Abwehr von Wirtschaftsspionage
  (KPMG-Studie: Verletzung Betriebs- und Geschäftsgeheimnis von 20 % (2003) auf 31 % (2006) gestiegen!)

Einflussfaktor Unternehmensspezifika (2)

Innerbetriebliche Organisation

- Stellenwert der IT-Administration
- Bestellung eines Datenschutzbeauftragtens
- Einsetzung eines IT-Sicherheitsbeauftragtens (CIO, CISO etc.)
- Aktivität der internen Revision
- Bewusstsein hinsichtlich der IT-Sicherheit
- Erfahrung aus Sicherheitsvorfällen
- Zufriedenheit der Mitarbeiter

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

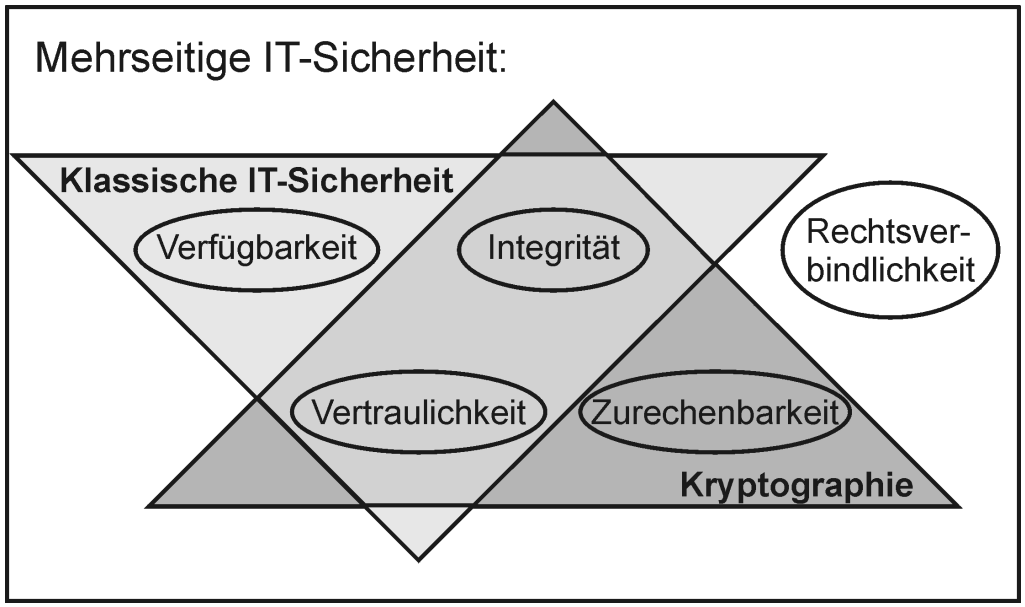
→ **Mehrseitige IT-Sicherheit**

- Risiko-Management
- Konzeption von IT-Sicherheit

Mehrseitige IT-Sicherheit (1)

- 1997: „Duale“ bzw. „Mehrseitige“ IT-Sicherheit entwickelt vom Ladenburger Kolleg „Sicherheit in der Kommunikationstechnik“
- Erweiterung der klassischen Sicherheitsziele, die der Verlässlichkeit der IT-Systeme dienen, um Komponenten zur Beherrschbarkeit der IT-Systeme (→ Integration der Betroffenensicht) → komplementäre Sicht
- **Verlässlichkeit** = keine unzulässige Beeinträchtigung der IT-Systeme, Daten bzw. Funktionen/Prozessen im Bestand, ihrer Nutzung oder ihrer Verfügbarkeit
- **Beherrschbarkeit** = keine unzulässige Beeinträchtigung von Rechten oder schutzwürdigen Belangen der Betroffenen durch Vorhandensein oder Nutzung von IT-Systemen

Mehrseitige IT-Sicherheit (2)



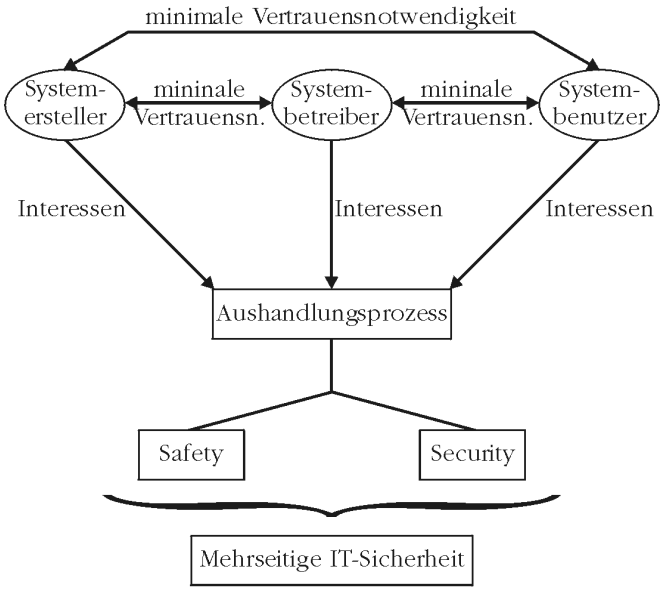
Mehrseitige IT-Sicherheit (3)

Definition 7: Mehrseitige IT-Sicherheit

Schutz von Hardware, Software und Daten vor Gefährdungen der Verfügbarkeit, Integrität, Vertraulichkeit, Zurechenbarkeit und Rechtsverbindlichkeit

- Mehrseitige IT-Sicherheit erfordert die Einbeziehung der Schutzinteressen aller Beteiligten:
  - → Formulierung der spezifischen Sicherheitsinteressen
  - → Erkennen der zu lösenden Schutzkonflikte
  - → Aushandlung zur Auflösung dieser Konflikte
  - → Durchsetzung eigener Sicherheitsinteressen (Kompromiss)
- **Grundsatz**: Sicherheit mit minimalen Annahmen über andere (d.h.: möglichst wenig Vertrauen in andere setzen müssen)

Mehrseitige IT-Sicherheit (4)



Ziele mehrseitiger IT-Sicherheit (1)

Definition 8: Verfügbarkeit (availability)
Gewährleistung, dass das IT-System (für befugte Nutzer) zugänglich und funktionsfähig ist

- → Prozessausführung in vorgesehener Weise zum geplanten Zeitpunkt im vorgegebenen Zeitrahmen
- → Sicherung vor Ausfällen und ungewolltem Verlust
- → betrifft auch die Vollständigkeit des Datenbestands (Nutzdaten, Passwortdaten, Konfigurationsdaten & Protokolldaten)

Ziele mehrseitiger IT-Sicherheit (2)

Definition 9: Integrität (integrity)
Gewährleistung, dass die Daten des IT-Systems nur durch befugte Nutzer verändert werden

- → Vorliegen korrekter (= originalgetreuer und unverfälschter) und aktueller Daten
- → Feststellbarkeit von Manipulationen (Datenqualität)
- → zielt auf die Vollständigkeit des Datenbestandes ab
- → Anforderungen an disaster recovery

Ziele mehrseitiger IT-Sicherheit (3)

Definition 10: Vertraulichkeit (confidentiality)
Gewährleistung, dass die Daten des IT-Systems nur durch befugte Nutzer interpretiert werden

- → kein unbefugter Informationsgewinn
- → Daten für Unbefugte nicht zugänglich (auch nicht über verdeckte Kanäle)
- → ergänzt durch Anonymität/Pseudonymität, Unbeobachtbarkeit & Verdecktheit aus Kommunikationstechnik

Ziele mehrseitiger IT-Sicherheit (4)

Definition 11: Zurechenbarkeit (accountability)
Gewährleistung, dass jederzeit festgestellt werden kann, welcher Nutzer einen Prozess ausgelöst hat

- → Verantwortlichkeit & Authentizität (Glaubwürdigkeit)
- → Diese Daten kommen vom betreffenden Kommunikations-partner
- → Die betreffenden Daten kommen von diesem Kommunikations-partner
- → Kern des Rechtemanagements

Ziele mehrseitiger IT-Sicherheit (5)

Definition 12: Rechtsverbindlichkeit (legal liability)
Gewährleistung, dass Daten und Vorgänge gegenüber Dritten jederzeit rechtskräftig nachgewiesen werden können

→ Transparenz (Nachvollziehbarkeit)

→ Reversibilität & Verhinderung falschen Abstreitens

→ Nachweis zugesicherter Eigenschaften (assurance)

→ Voraussetzung für Auditierbarkeit

→ Ausgleich für fehlenden klassischen Augenscheinbeweis