

Grundlagen des Datenschutzes und der IT-Sicherheit (13)

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

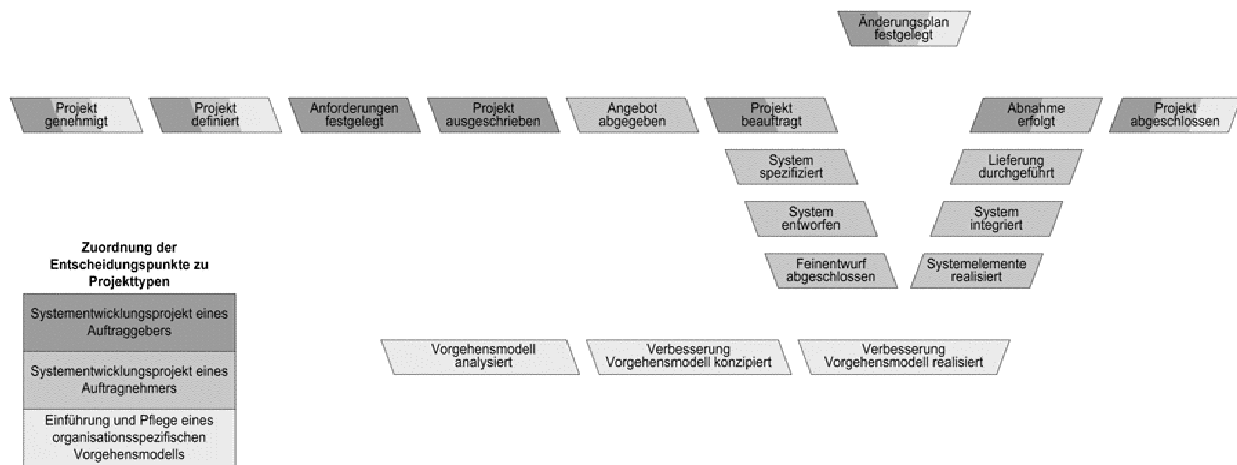
Übersicht zur Konzeption von IT-Sicherheit

- Erstellung sicherer IT-Systeme
- Gestaltung der IT-Infrastruktur
- Datenschutzfreundliche Techniken

Erstellung sicherer IT-Systeme

- **Software-Erstellung** gemäß standardisierter Vorgehensweisen
 - V-Modell XT
 - Software-Qualität nach DIN 9126
 - formaler Nachweis zur Korrektheit
- **Konstruktionsprinzipien**
 - allgemeine Prinzipien
 - Prinzipien für Sicherheitsprozesse

Überblick zum V-Modell XT



Hinweise zum V-Modell XT (1)

- für jedes systemsicherheitskritisch eingestuftes Systemelement ist eine **Sicherheitsanalyse** durchzuführen
- Verfahrens- bzw. Betriebssicherheit sowie Zuverlässigkeit, Fehlertoleranz und Korrektheit als Maßstäbe für **Safety**
- Gewährleistung von Verfügbarkeit, Integrität, Vertraulichkeit und Verbindlichkeit (= beweisbare zugesicherte Eigenschaften) beim Einsatz der IT als Maßstäbe für **Security**

Hinweise zum V-Modell XT (2)

- Systemsicherheitsanalyse mittels
 - **Blackbox-Test** durch Auftraggeber
→ Stellen sich erwartete Ergebnisse ein?
 - **Whitebox-Test** durch Auftragnehmer
→ Werden alle Konstruktionselemente durchlaufen?
- jeder Konstruktionsphase (Anforderungsfestlegung, Spezifikation, Entwurf, Implementation) ist eine Kontrollphase zugeordnet, in der **Verifikation** (System wurde nach den „Regeln der Kunst“ erstellt & weist vordefinierte Eigenschaften auf → Vollständigkeit, Widerspruchsfreiheit, Durchführbarkeit, Testbarkeit) & **Validierung** (System entspricht den vom Nutzer gewünschten Kriterien → Adäquatheit, Benutzbarkeit, Funktionsverhalten im Fehlerfalle)

Merkmale von Software-Qualität

- | | |
|---|---|
| <ul style="list-style-type: none">• Funktionalität:<ul style="list-style-type: none">- Angemessenheit- Richtigkeit- Interoperabilität- Ordnungsmäßigkeit- Sicherheit• Zuverlässigkeit:<ul style="list-style-type: none">- Reife- Fehlertoleranz- Wiederherstellbarkeit• Benutzbarkeit:<ul style="list-style-type: none">- Verständlichkeit- Erlernbarkeit- Bedienbarkeit | <ul style="list-style-type: none">• Effizienz:<ul style="list-style-type: none">- Zeitverhalten- Verbrauchsverhalten• Änderbarkeit:<ul style="list-style-type: none">- Analysierbarkeit- Modifizierbarkeit- Stabilität- Prüfbarkeit• Übertragbarkeit:<ul style="list-style-type: none">- Anpassbarkeit- Installierbarkeit- Konformität- Austauschbarkeit <p>nach DIN 9126</p> |
|---|---|

formaler Korrektheitsnachweis

Nachweis verlässlicher IT-System-Erstellung mittels:

- partielle Korrektheit
= Ergebnis automatisch richtig, wenn ein Algorithmus überhaupt ein Ergebnis liefert → Integrität
- totale Korrektheit
= Algorithmus liefert stets ein richtiges Ergebnis
→ Integrität & Verfügbarkeit, da richtige Ergebnisse zum vorbestimmten Zeitpunkt vorliegen müssen
- Erfüllung der Spezifikation
= Übereinstimmung bei Syntax & Semantik
→ weitere Sicherheitskriterien via Semantik

Konstruktion sicherer IT-Systeme (1)

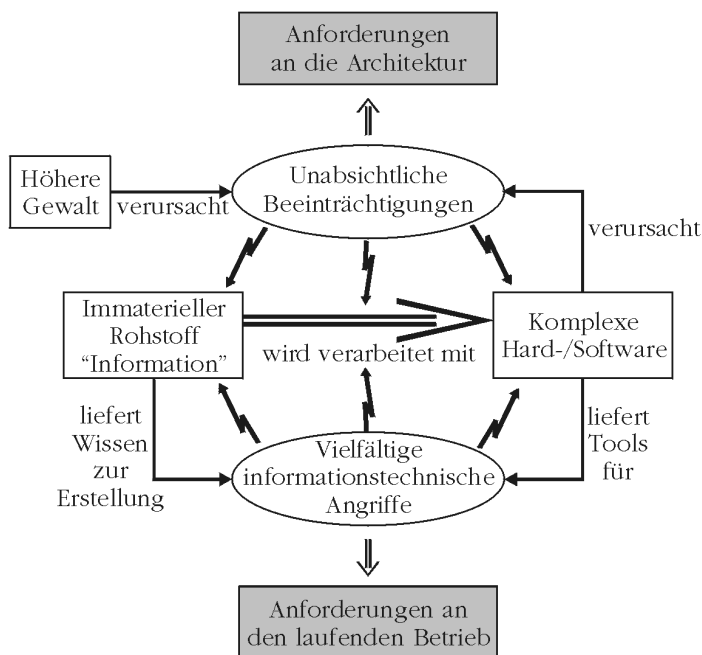
Allgemeine Prinzipien (nach Saltzer und Schroeder, 1975):

- **Prinzip einfacher Sicherheitsmechanismen:** wirksame, aber möglichst einfache Konstruktion
- **Erlaubnisprinzip:** Zugriff muss ausdrücklich erlaubt werden
- **Prinzip vollständiger Rechteprüfung:** Rechteprüfung bei allen Aktionen
- **Prinzip des offenen Entwurfs:** angewandte Verfahren und Mechanismen sind offenzulegen → Kerckhoffs' Prinzip
- **Prinzip der differenzierten Rechtevergabe:** keine Rechte aufgrund nur einer einzigen Bedingung
- **Prinzip minimaler Rechte:** Vergabe nur der Rechte, die zur Aufgabenstellung unbedingt benötigt werden
- **Prinzip durchgreifender Zugriffskontrollen:** Vermeidung verdeckter Kanäle
- **Prinzip der Benutzerakzeptanz:** einfache Anwendbarkeit

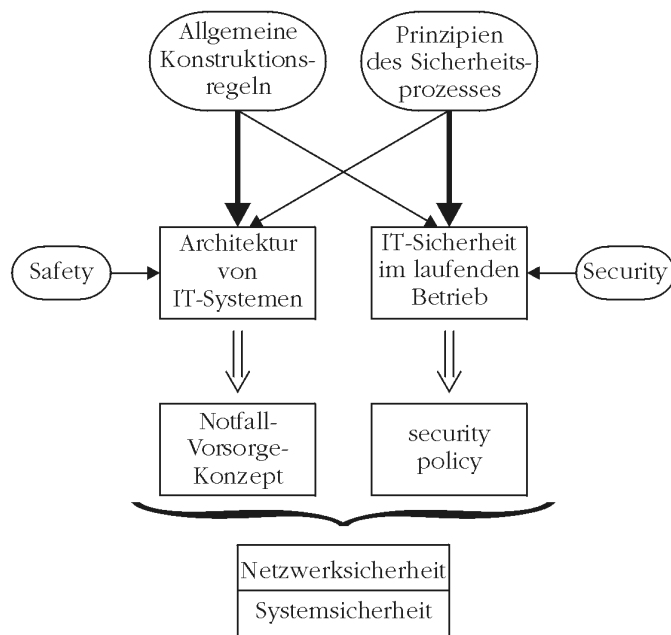
Konstruktion sicherer IT-Systeme (2)

Prinzipien für Sicherheitsprozesse (nach Schneier, 2000):

- **Risiko durch Aufteilung verringern:** nur benötigtes Privileg vergeben
- **das schwächste Glied sichern:** Angriffsbaum betrachten
- **Choke-Points verwenden:** Benutzer durch engen Kanal zwingen
- **gestaffelte Abwehr:** hintereinander geschaltete Barrieren aufbauen
- **Folgeschäden begrenzen:** Rückkehr zum sicheren Normalzustand bei Systemausfällen
- **Überraschungseffekt nutzen:** innere Einstellungen des IT-Systems verdeckt halten
- **Einfachheit:** lieber wenige, dafür effektive Schutzmechanismen
- **Einbeziehung der Benutzer:** Insider so weit & oft wie möglich beteiligen
- **Gewährleistung:** Produktverhalten gemäß Zusicherung
- **Alles in Frage stellen:** Nicht mal sich selbst vertrauen



Umsetzung der Konstruktionsprinzipien (1)

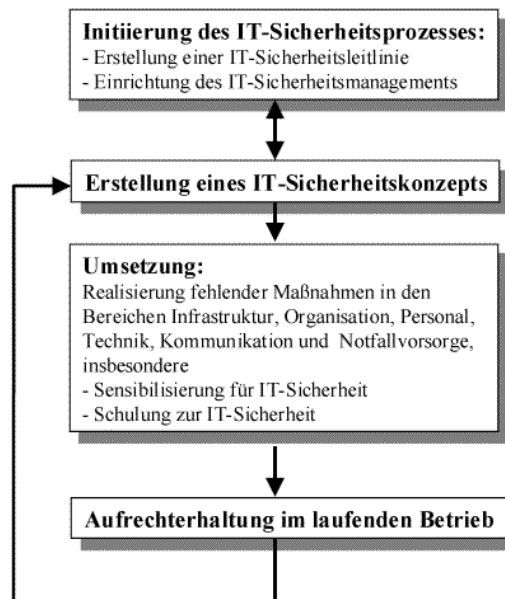


Umsetzung der Konstruktionsprinzipien (2)

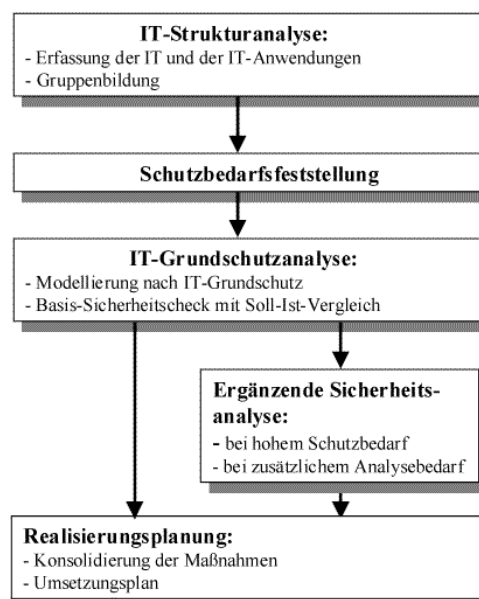
Gestaltung der IT-Infrastruktur

- Berücksichtigung gängiger Standards
 - IT-Grundschatz-Kataloge des BSI
 - Informationssicherheitsmanagement nach ISO/IEC 17799 & 27001
 - ITIL
- Konzeption von IT-Sicherheit
 - Architektur von IT-Systemen
 - laufender Betrieb von IT-Systemen

Vorgehensmodell nach Grundschutz



Sicherheitskonzept des BSI



Informationssicherheit

Definition 14: Informationssicherheit

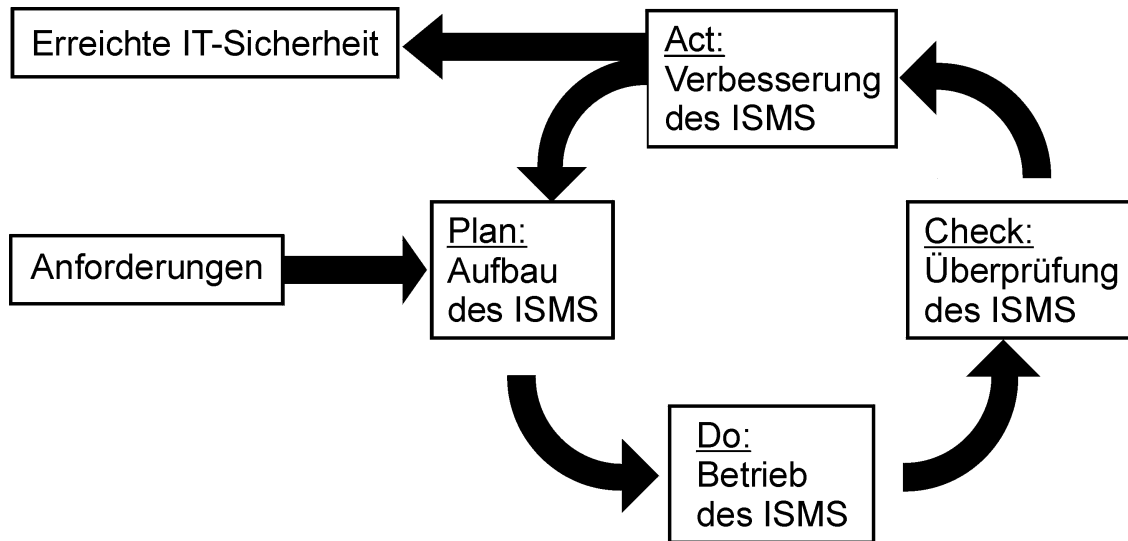
Schutz der Verfügbarkeit, Integrität und Vertraulichkeit
(und ggf. weiterer Eigenschaften) von Informationen
(nach ISO/IEC 17799)

- Gewährleistung von Schutzzielen
- betrifft alle Informationen eines Unternehmens
- Information ist ein hoher Vermögenswert
- Verknüpfung mit IT-Risiko-Management
- Informationssicherheit ist Aufgabe des Managements

Bestandteile Informationssicherheit

- Informations-Sicherheits-Politik (security policy)
- Organisation der Informationssicherheit
- Verantwortlichkeit für die und Klassifizierung der Vermögenswerte
- Sicherheit im Rahmen des Personalwesens
- Physische und umgebungsbezogene Sicherheit → Schutzzonen
- Netzwerksicherheit & Datensicherung
- Steuerung von Zutritt, Zugang & Zugriff
- Sicherung der Betriebsbereitschaft & Umgang mit Verwundbarkeiten
- Management von Störfällen & Angriffen
- Gewährleistung eines kontinuierlichen Geschäftsbetriebs
- Erfüllung der Verpflichtungen (aus rechtlichen und organisatorischen Anforderungen, z.B. zum Datenschutz)

Vorgehensmodell nach ISO/IEC 27001



Prozess-Sichtweise nach ITIL (1)

- **ITIL** = IT Infrastructure Library (best-practice-Referenzmodell für IT-Service-Prozesse)
- Prozesse für die Unterstützung & den Betrieb von IT-Diensten:
 - **Incident Management** → Behebung von Störungen
 - **Problem Management** → Ermittlung der Störungs-Ursachen
 - **Configuration Management** → Bereitstellung der IT-Infrastruktur
 - **Change Management** → reibungslose Änderung der IT-Infrastruktur
 - **Release Management** → Steuerung der Implementierung neuer Hard-/Software

Prozess-Sichtweise nach ITIL (2)

- Prozesse zur Planung & Lieferung von IT-Diensten:
 - Service Level Management → Vereinbarung sinnvoller Anforderungen (Service Level Agreements)
 - Financial Management → Kosten-/Nutzenbetrachtung
 - Capacity Management → Optimierung des Ressourcen-Einsatzes
 - Availability Management → Sicherstellung vereinbarter Verfügbarkeiten
 - Business Continuity Management → Abwehr von Katastrophen/Notfällen
- Für Zertifizierung nach ISO/IEC 20000 außerdem kontinuierlicher Verbesserungsprozess erforderlich

Konzeption von IT-Systemen (1)

Konzeption der Architektur von IT-Systemen:

- Aufteilung in Sicherheitszonen (→ Rechenzentrum als closed shop)
 - Rechtevergabe nach need-to-know-Prinzip
 - Verschlüsselung des Datentransports
 - Härtung der IT-Systeme (→ keine sicherheitskritischen oder überflüssigen Dienste)
 - Einrichtung einer Firewall bzw. einer DMZ
 - Einrichtung von Virtual Network Computing (VNC)
 - Beachten der Single-Points-of-Failure
- ➔ **Hilfsmittel:** Notfall-Vorsorge-Konzept

Konzeption von IT-Sicherheit (2)

Sicherheit im laufenden Betrieb von IT-Systemen:

- Sensibilisierung und Schulung der Mitarbeiter
 - Authentisierung bei Zugang und Zugriff anhand Wissen/Besitz/Merkmal
 - Schutz vor Viren, Würmer, Trojanische Pferde etc.
 - Protokollierung (→ Überwachung der Technik & Datenströme; z.B. Netzwerkmonitoring, Intrusion Detection Systems)
 - Änderung von Produktivsystemen erst nach Erfolg bei Testsystemen
 - Dokumentation von Änderungen an Systemeinstellungen
 - regelmäßige Kontrollen (z.B. durch Penetrationstests)
 - Einrichtung eines Vulnerability Managements
- **Hilfsmittel:** Sicherheitsleitlinie (security policy)

Sicherheitsarchitektur des ISO/OSI-Referenzmodells

- Sicherheitsdienste (nach ISO 7498-2):
 - Authentifizierung
 - Zugriffskontrolle
 - Gewährleistung der Vertraulichkeit
 - Gewährleistung der Integrität
 - Nachweis der Verursachung
- richtet sich nicht gegen Ausnutzung der Protokollfunktionalitäten (requests for comments)

Management der Netzwerksicherheit (1)

- Grundlage: ISO/IEC 18028-1
- Sicherheitsniveau abhängig von Schutzwürdigkeit & Stellung der Zugriffsberechtigten
- berücksichtigt die Verfügbarkeit, Integrität, Vertraulichkeit und Ausfallsicherheit der (Übertragungs-) Daten sowie die Authentizität, Zurechenbarkeit und Nichtabstreitbarkeit der Kommunikationspartner

Management der Netzwerksicherheit (2)

Maßnahmen:

- Erstellung eines aktuellen Netzwerkplans
- Einrichtung technischer Schutzzonen mittels Firewalls
- Erkennen & Blockieren verdächtigen Netzwerktraffics
- Einsatz eines aktuellen Antivirenschutzes
- dem Schutzgrad angemessen hohe Passwortgüte
- Härtung der Rechner durch Abschaltung unnötiger Dienste
- Gewährleistung technischer Redundanz
- Einsatz von Verschlüsselungstechniken bei der Datenübertragung
- Benutzung der Network Address Translation

Perimeterschutz mittels Firewalls

- Firewall = System aus Hard- und Software zur Separation eines Netzes von anderen Netzen
- nur autorisierter Datenverkehr soll Firewall (bei eingestellten Ports & IP-Adressen sowie einer definierten Durchlassrichtung) passieren dürfen (Achtung: Firewall kann umgangen werden!)
- Einsatz mehrerer Netzwerkkarten geboten
- Unterschied physischer Verbindungen & logischen Datenflusses
- Es gibt verschiedene Architekturen:
 - Paketfilter (Filterung von IP-Paketen); z.B. Screening Router
 - Application Level Gateways (auf Proxy-Server = Bastian Host); z.B. Dual Homed Host
 - Mischformen (Screened Host/Subnet)
- Demilitarisierte Zone (DMZ) als Pufferzone

Sicherheitsstrategien zur Gestaltung von Firewalls

nach Zwicky, Cooper & Chapman (2000):

- least privilege → Anwendung need-to-know-Prinzip
- defense in depth → Aufbau einer gestaffelten Abwehr
- choke point → Etablierung eines engen Kanals
- weakest link → Absicherung des schwächsten Glieds
- fail-safe stance → Anwendung des Erlaubnisprinzips
- universal participation → Beteiligung von Insidern
- diversity of defense → Verwendung von Komponenten unterschiedlicher Händler & Aufteilung der Administration
- simplicity → Anwendung des Prinzips der Einfachheit
- security through obscurity → Ausnutzung von Überraschungseffekten durch Reduzierung aktiver Mitteilungen

Maßnahmen physischer Sicherheit

ergriffene Maßnahmen	1998	2000	2002	2004	2006
Unterbrechungsfr. Stromvers.	76%	79%	97%	91%	90%
Klimatisierung	74%	74%	94%	83%	85%
Brandmeldesysteme	71%	71%	83%	83%	81%
Datensicherungsschränke	75%	78%	80%	85%	80%
Sicherheitstüren	62%	65%	76%	76%	68%
Einbruchmeldesysteme	52%	51%	70%	72%	67%
Löschanlagen	47%	48%	50%	57%	54%
Glasflächendurchbruchschutz	48%	43%	56%	55%	52%
Bewachung	40%	44%	46%	49%	47%
Video-Überwachung	23%	25%	28%	39%	38%
Schutz gg. komprom. Abstrahl.	11%	10%	13%	13%	13%

Quelle: <kes>-Sicherheitsstudien

Sicherung der Authentisierung

- Sicherung der Benutzeridentifikation anhand
 - Wissen → z.B. Password
 - Besitz → z.B. Chipkarte (= Prozessorkarte)
 - Merkmal → z.B. Unterschrift/Biometrie
 - nur Feststellung, ob Benutzer berechtigt ist, nicht ob dessen Identität korrekt ist!
- Zugangs-/Zugriffskontrolle mittels Rechteprüfung

Zum Password

- BIOS-/Boot-Password kann durch Jumper-Umsetzung, Ausbau der Festplatte oder mittels Software-Unterstützung umgangen werden
- Bildschirmschoner-Password kann durch Neustart (über trusted path) oder Original-Software im CD-ROM-Laufwerk umgangen werden
- jedes Password ist mit Brute Force (= Ausprobieren) knackbar: bei 26 Groß- und 26 Kleinbuchstaben, sowie 10 Zahlen (= 62 Zeichen) dauert Brute Force bei 6 Stellen ca. $\frac{1}{4}$ h (bei 1,4 GHz), erst ab 7. Stelle werden ein paar wenige Tage benötigt
- bei Verwendung sprechender Wörter ist das Password durch Dictionary Attack binnen weniger Sekunden geknackt
- Achtung: Ausspähen von Daten strafbar! (§ 202a StGB)

Zur Chipkarte

- Unterscheidung zwischen kontaktloser Karte (z.B. Uni-Chipkarte) und Kontaktkarte (z.B. Krankenversicherungskarte)
- Kennzeichen aller Chipkarten: Vorhandensein eines Prozessor-Chips (→ Speicher- und Verarbeitungsmedium im Sinne von § 6c BDSG)
- leichte Angreifbarkeit:
 - Durchdringung der Schutzschichten durch Abschleifen / Anätzen
 - Manipulierbarkeit gespeicherter Bits durch Beschuss mit elektromagnetischer Strahlung (z.B. Blitzlicht)
 - Messbarkeit des Energieverbrauchs („power analysis“) oder der benötigten Rechenzeit („timing attacks“)
- Schlüssel oder PIN auf EEPROM (nicht-flüchtiger Speicher), Verschlüsselung üblicherweise symmetrisch

Zur Biometrie

- = Erfassung und (Ver-)Messung von Lebewesen und ihren Eigenschaften
- Unterscheidung in:
 - physiologische Merkmalsverfahren (Fingerabdruckverfahren, Iris-/Retinaerkennungungsverfahren, Gesichtserkennungsverfahren)
 - verhaltensabhängige Merkmalsverfahren (Sprachmuster- / Schriftdynamikerkennungungsverfahren, Tipprhythmusverfahren)
- Speicherung eines Referenzmusters und Abgleich hiermit (Probleme: falsche Akzeptanz → „false acceptance rate“, falsche Ablehnung → „false rejection rate“; Genauigkeit unterschiedlich und größtenteils diametral zur gesellschaftlichen Akzeptanz → lediglich Fingerabdruck in beiden Kategorien gut)

Zugriffskontrolle

Matrizen:

- Subjekt (Benutzer & Prozesse) = Zeilen
- Objekt (Dateien & Datenträger) = Spalten
- Zugriffsart (lesen, schreiben, ausführen, löschen) = Zellen
- Access Control List: wer darf auf gegebenes Objekt zugreifen
- Capability List: auf welche Objekte darf ein gegebener Benutzer zugreifen
- Grundsatz: need-to-know (nur benötigte Rechte einräumen)
- Pflege erfordert z.T. hohen Aufwand (darum: Benutzerrollen!)
- beachtenswert: spezifischere Regeln vor allgemeineren Regeln!

Beispiele zur Sicherheitsleitlinie (security policy)

Inhalte

(aus <kes> 5/2000, S. 55ff):

- Leitaussagen
- IT-Sicherheitspolitik (allgemein + für IT-Systeme & IT-Anwendungen)
- IT-Sicherheitsmanagement (Aufgabendefinition bis Projekt-Handbuch)
- Regelwerke der IT-Sicherheit (nach Verantwortlichkeiten)
- Anhänge mit Dienstanweisungen und Richtlinien

Anforderungen

(aus DuD 2/2002, S. 104ff):

- Stellenwert der Sicherheit (Priorisierungen)
- Sicherheitsziele/-strategie
- Sicherheitsprozess (Umsetzung im Unternehmen)
- Umfassender Anspruch (auch Produktsicherheit etc.)
- Relevanz (für alle Mitarbeiter)
- Ansprechpartner (Kontakt innerhalb des Unternehmens)
- Umfang (kurz, dafür Verweis auf umfangreichen Anhang)
- Formaler Rahmen (Integration in übliches Lay-Out)