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

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

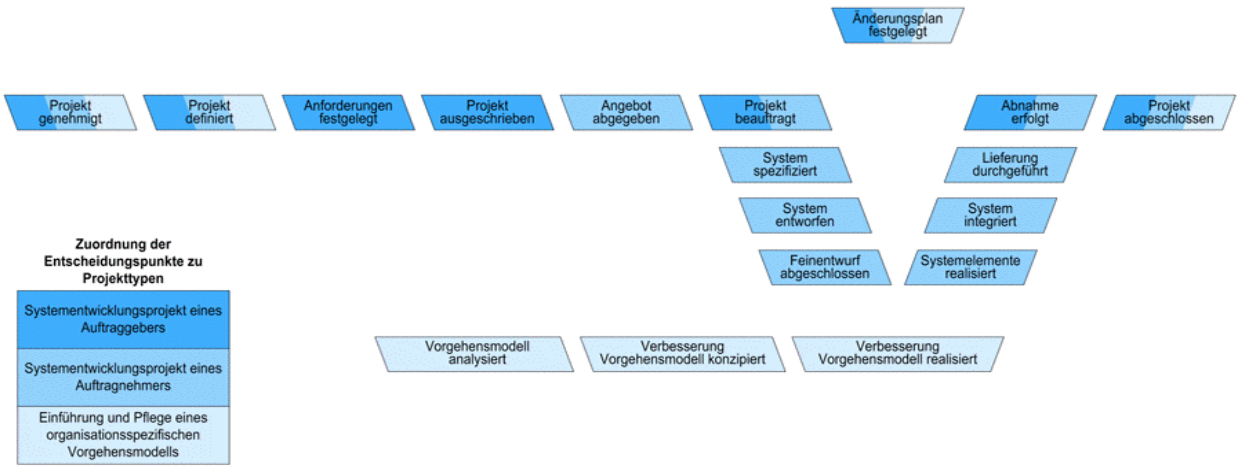
Konzeption von IT-Sicherheit:

- Erstellung sicherer IT-Systeme
- Gestaltung der IT-Infrastruktur
  - ° Architektur der IT-Infrastruktur
  - ° IT-Sicherheit im laufenden Betrieb
- Netzwerksicherheit

Erstellung sicherer IT-Systeme

- **Software-Erstellung**
  → V-Modell XT
- **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)

Konstruktion sicherer IT-Systeme (1)

Allgemeine Prinzipien (nach Saltzer und Schroeder, 1975):

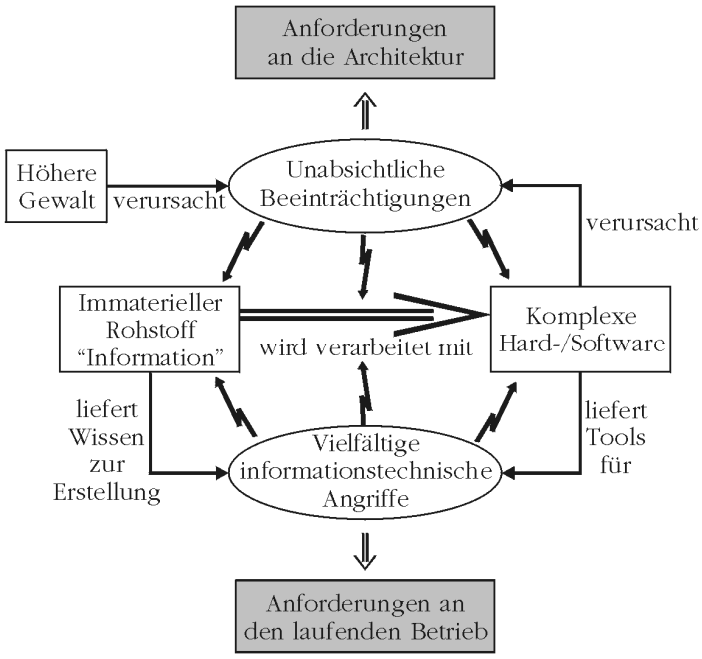
- **Prinzip einfacher Sicherheitsmechanismen**: wirksame, aber möglichst einfache Konstruktion
- **Erlaubnisprinzip**: Zugriff muss ausdrücklich erlaubt werden
- **Prinzip vollständiger Rechteprüfung**: Rechteprüfung bei allen Aktionen
- **Prinzip des offenen Entwurfs**: angewandte Verfahren und Mechanismen 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 Benuterzakzeptanz**: einfache Anwendbarkeit

Konstruktion sicherer IT-Systeme (2)

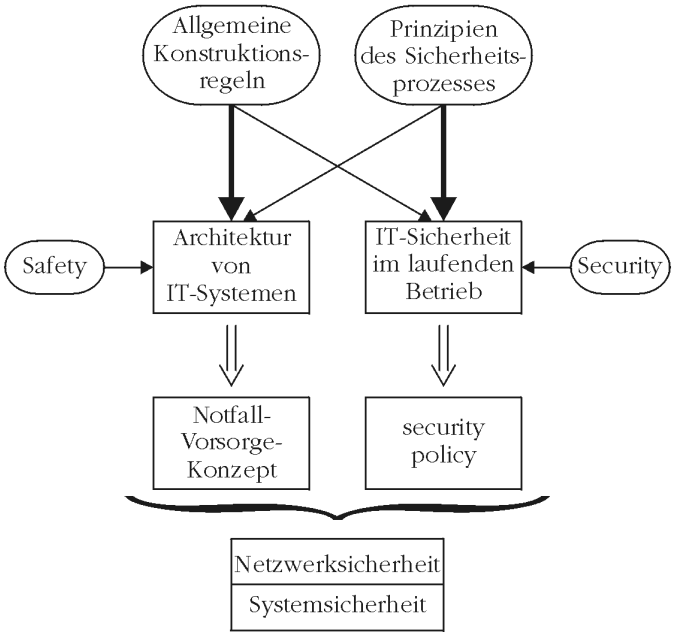
Prinzipien für Sicherheitsprozesse (nach Schneier, 2000):

- **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 Konstruk-tionsprin-zipien (1)



Umsetzung der Konstruk-tionsprin-zipien (2)



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