

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

Vorlesung im Sommersemester 2017  
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
✓	Mitarbeiterdatenschutz	→	Konzeption von IT-Sicherheit

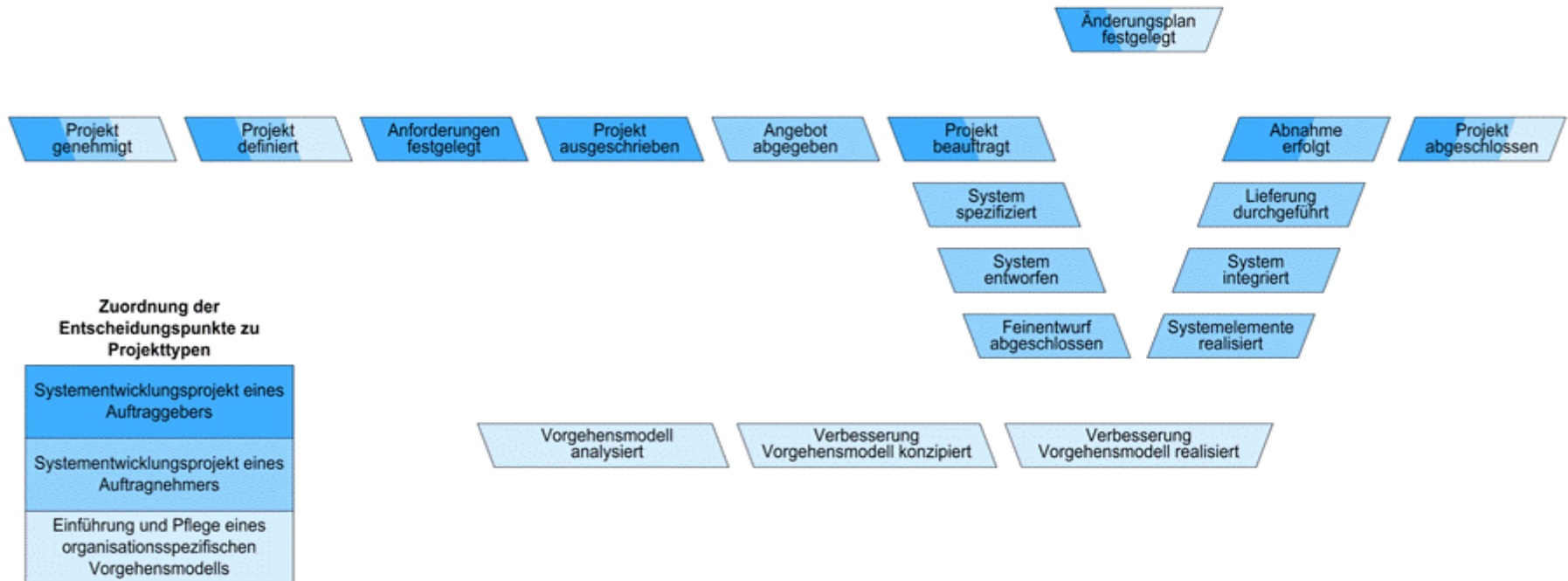
## Konzeption von IT-Sicherheit:

- Erstellung sicherer IT-Systeme
  - V-Modell XT
  - Konstruktionsprinzipien
- Umsetzung von IT-Sicherheit
  - Architektur der IT-Infrastruktur
    - Notfallvorsorgekonzept
    - Notfallplan
  - IT-Sicherheit im laufenden Betrieb
    - Sicherheitskonzept

# Erstellung sicherer IT-Systeme

- **Software-Erstellung**
  - V-Modell XT
- **Konstruktionsprinzipien**
  - allgemeine Prinzipien
  - Prinzipien für Sicherheitsprozesse
- **Konzeption von Informationssicherheit**
  - Sicherheitskonzept [Übung]
  - Notfallvorsorgekonzept & Notfallplan [Übung]

# 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**, unter Beachtung von:
  - **Verifikation**: System wurde zu jedem Zeitpunkt nach den „Regeln der Kunst“ erstellt & weist vordefinierte Eigenschaften auf
    - Vollständigkeit, Widerspruchsfreiheit, Durchführbarkeit, Testbarkeit
  - **Validierung**: System entspricht den vom Nutzer gewünschten Kriterien & den geltenden Anforderungen
    - 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 Benutzerakzeptanz:** einfache Anwendbarkeit

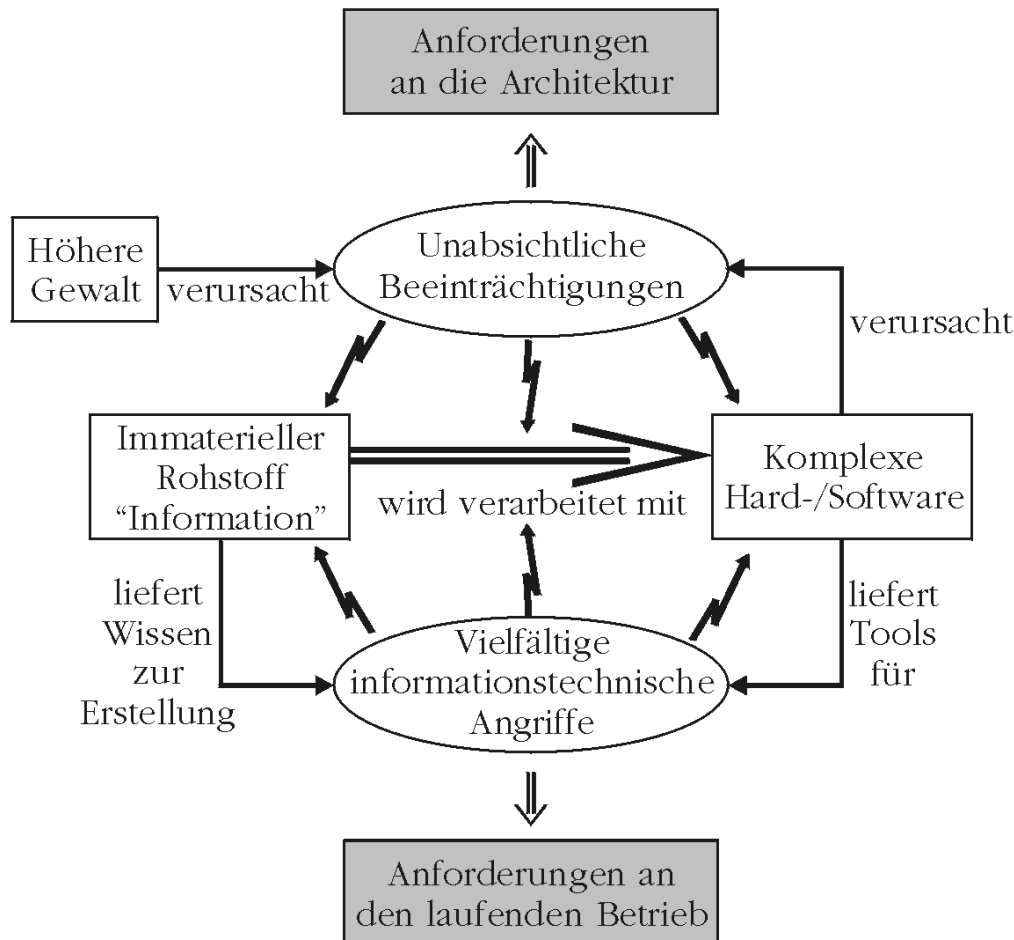
# Konstruktion sicherer IT-Systeme (2)

**Prinzipien für Sicherheitsprozesse** (nach Schneier, 2000):

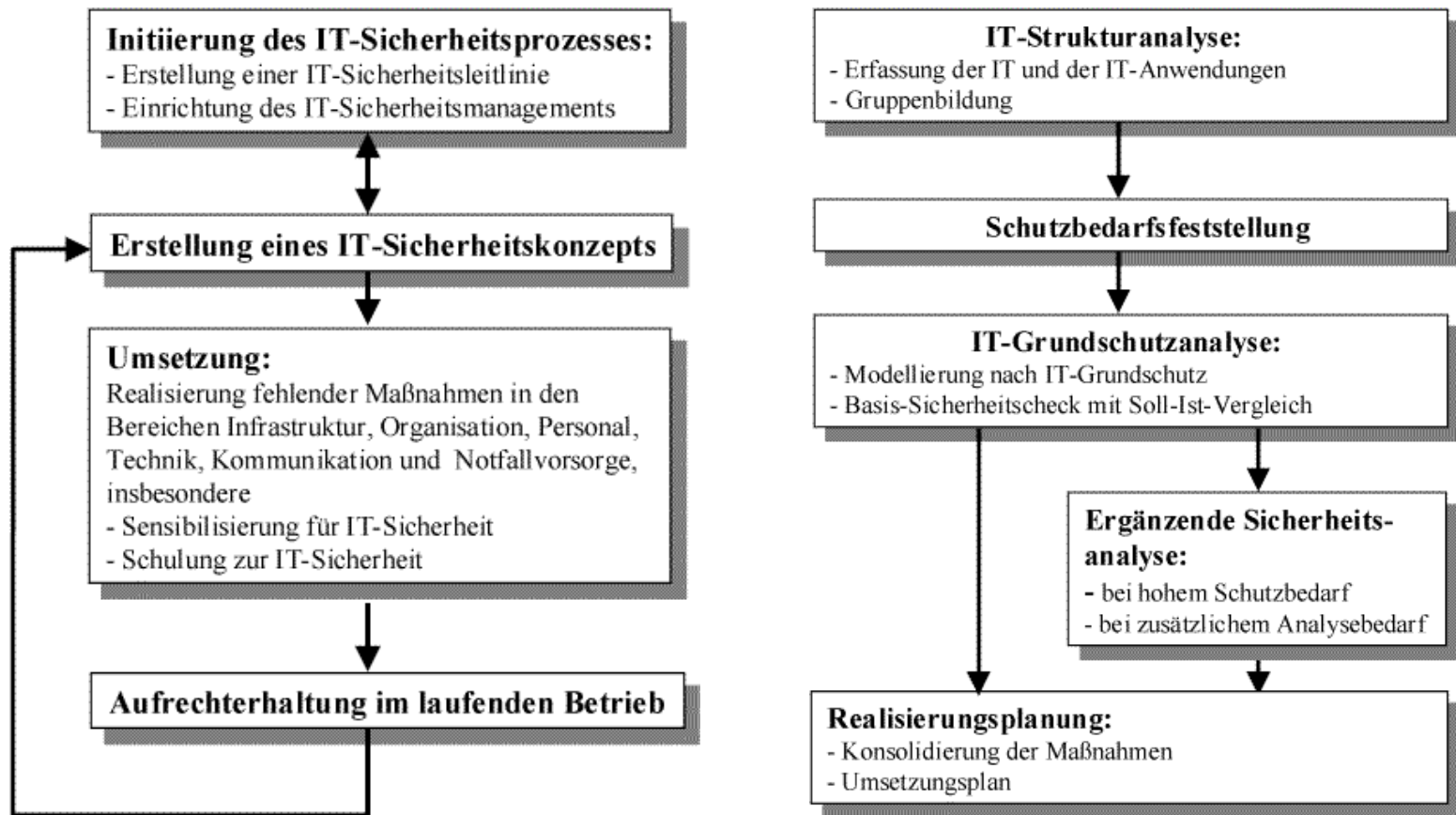
- **Risiko durch Aufteilung verringern:** nur benötigtes Privileg vergeben
- **das schwächste Glied sichern:** Angriffsbaum betrachten
- **Choke-Points verwenden:** Benutzer durch engen Kanal zwingen
- **gestaffelte Abwehr:** hintereinander geschaltete Barrieren aufbauen
- **Folgeschäden begrenzen:** 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 Konstruk- tionsprin- zipien



# Vorgehensmodell gemäß IT-Grundschutzkataloge



# Authentifizierung

- Sicherung der Benutzeridentifikation (gemäß Authentifizierung) anhand
  - Wissen → z.B. Password
  - Besitz → z.B. Chipkarte (= Prozessorkarte)
  - Merkmal → z.B. Unterschrift/Biometrie
  - Zwei-Faktor-Authentifizierung (anhand zweier der drei aufgeführten Mechanismen)
- nur Feststellung, ob Benutzer berechtigt ist, nicht ob dessen (vorgegebene) Identität tatsächlich korrekt ist!  
→ Zugangs-/Zugriffskontrolle mittels Rechteprüfung

# Rechtevergabe

## 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!  
→ Role-Based Access Control; RBAC)
- beachtenswert: spezifischere Regeln vor allgemeineren Regeln!