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

Vorlesung im Sommersemester 2012

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
✓	Kundendatenschutz	➔	Konzeption von IT-Sicherheit

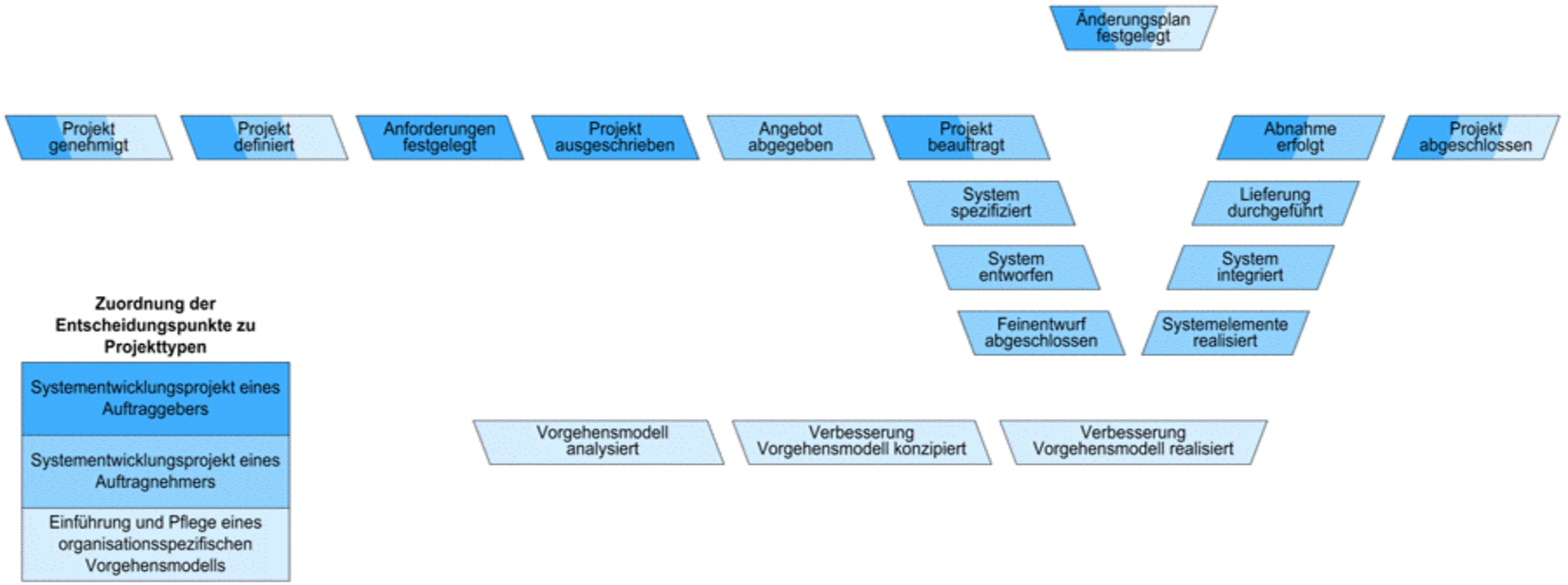
Konzeption von IT-Sicherheit:

- Erstellung sicherer IT-Systeme
- Umsetzung von IT-Sicherheit
  - ° Architektur der IT-Infrastruktur
    → Notfallvorsorgekonzept
  - ° IT-Sicherheit im laufenden Betrieb
    → Sicherheitskonzept

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**, 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):

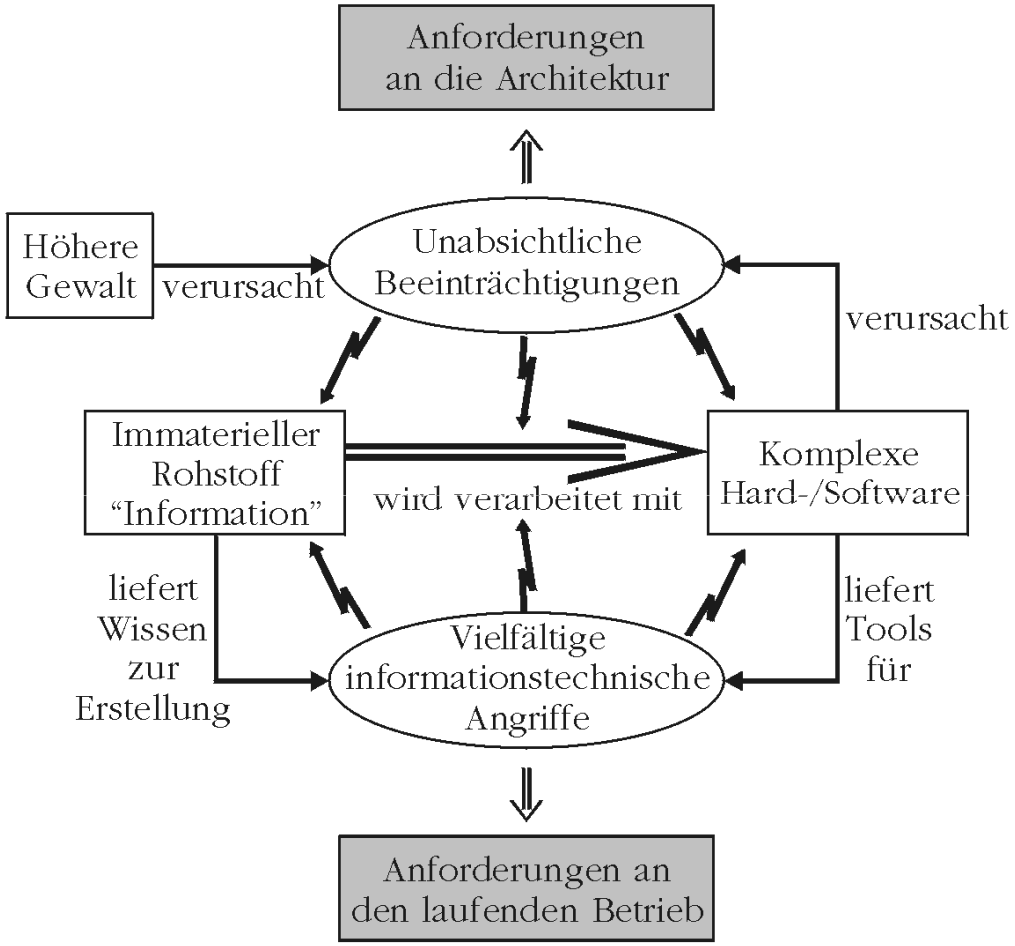
- **Prinzip einfacher Sicherheitsmechanismen**: wirksame, aber möglichst einfache Konstruktion
- **Erlaubnisprinzip**: Zugriff muss ausdrücklich erlaubt werden
- **Prinzip vollständiger Rechteprüfung**: Rechteprüfung bei allen Aktionen
- **Prinzip des offenen Entwurfs**: angewandte Verfahren und Mechanismen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

Konstruktion sicherer IT-Systeme (2)

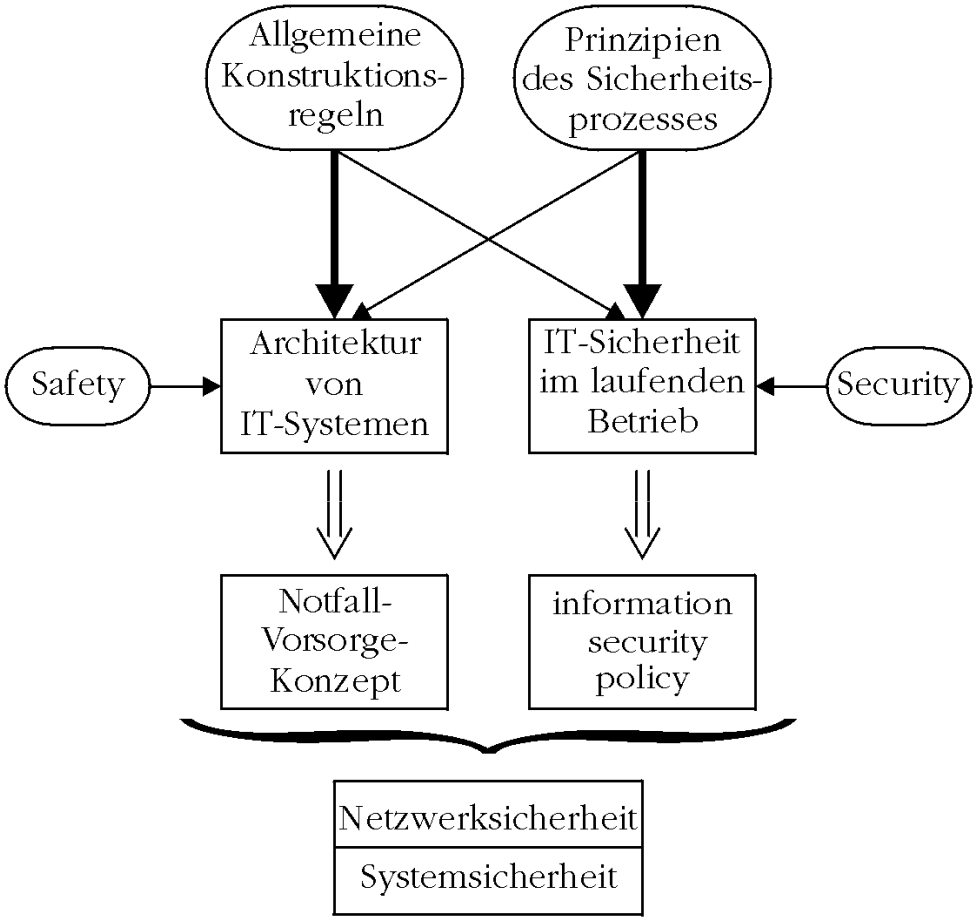
Prinzipien für Sicherheitsprozesse (nach Schneier, 2000):

- **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)



Notfall-Vorsorge-Konzept

Ein Notfallvorsorgekonzept beschreibt, wie das Eintreten eines Notfalls vorzugsweise verhindert werden kann/soll → **präventiver Schutz**

Inhalt Notfallvorsorgekonzept **gemäß BSI-Standard 100-4** (Kapitel 5.5):

- ° Verantwortlichkeiten, Geltungsbereich, Inhaltsangabe
- ° Abgrenzungen, Ziele, Zuständigkeiten, Ablauforganisation
- ° Notfallszenarien, Wiederanlauf-Anforderungen, Priorisierungen
- ° Alarmierungsverfahren, Beschreibung vorbeugender Maßnahmen
- ° Einbinden des Notfallmanagements in Unternehmenskultur
- ° Aufrechterhaltung & Kontrolle

Bestandteile eines Notfall(vorsorge)konzepts zudem **nach M 6.114**:

- Übersicht zu Verfügbarkeitsanforderungen (maximal tolerierbare Ausfallzeiten, Wiederanlaufparameter, Prioritäten für Wiederanlauf)
- Vorgehen zur Durchführung einer Business Impact Analyse (BIA) & einer Risikoanalyse
- Auflistung der Maßnahmen zur Risikobehandlung

Notfallplan

Ein Notfallplan beschreibt, was bei Eintritt eines Notfalls zu tun ist!

→ **reaktiver Schutz**

→ **Bestandteile** eines Notfallplans:

- Zielsetzung des Notfallplans und ggf. geltende Abgrenzungen (Scope)
- Festlegung der Verantwortlichkeiten (wer macht was?)
- Aufstellung des Alarmierungsplans (wer ist wann anzurufen?)
- Ablaufpläne für entsprechende Notfallszenarien (im Sinne von Checklisten)
- Dokumentationen zur eingesetzten IT-Infrastruktur und den Maßnahmen zur Notfall-Vorsorge (→ Verweis auf Notfall-Vorsorge-Konzept)
- Bereitstellung aller wesentlichen Unterlagen und Nachweise (z.B. zu durchgeführten Notfall-Übungen)

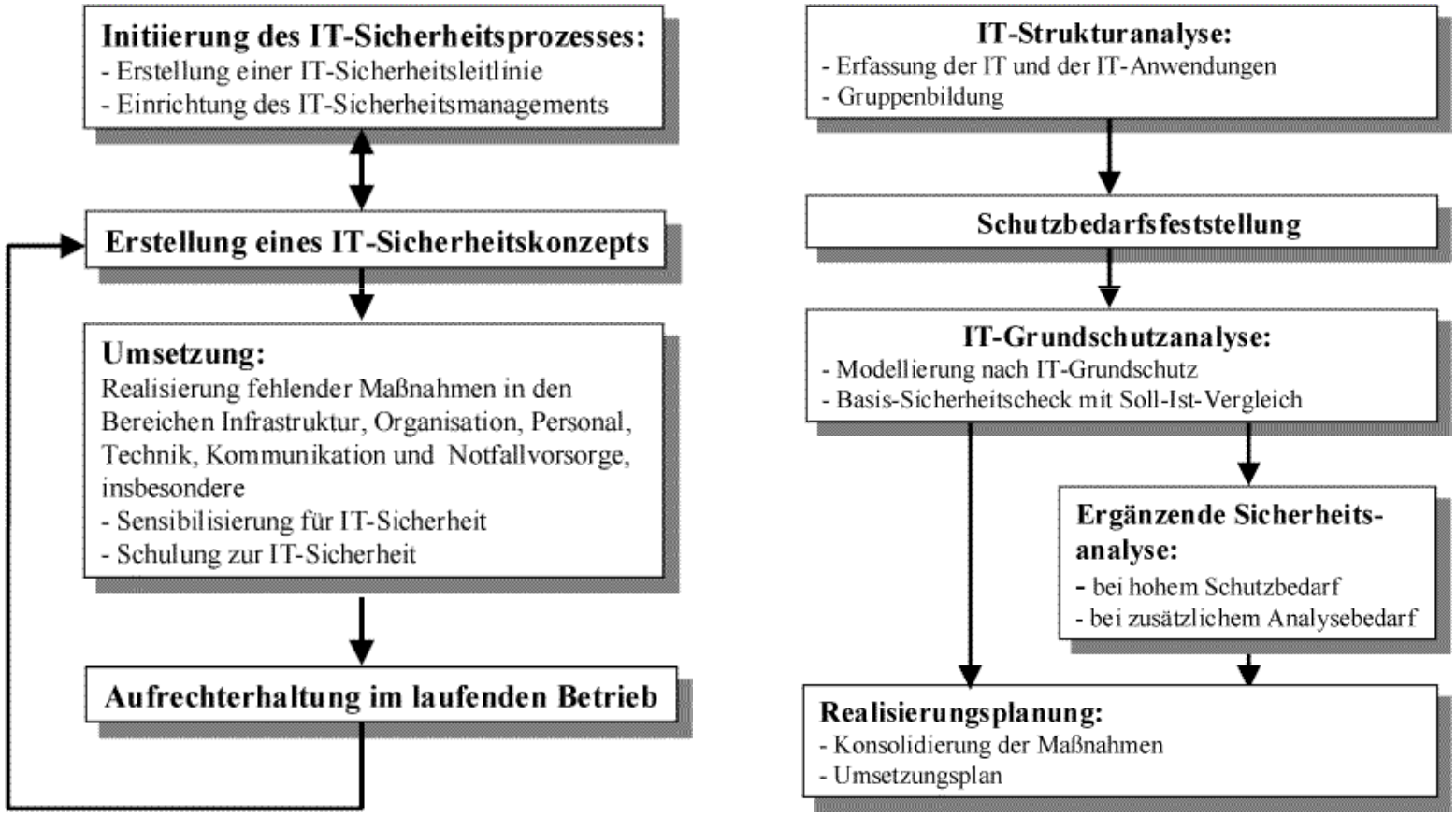
Sicherheitskonzept

Abwehr von Schwachstellen durch folgende Controls:

- 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 System)
- Änderung von Produktivsystemen erst nach Erfolg bei Test-systemen, inkl. Verwendung von Testdaten statt Echtdaten
- Dokumentation von Änderungen an Systemeinstellungen
- regelmäßige Kontrollen (z.B. durch Penetrationstests)
- Einrichtung eines Vulnerability Managements

→ **Hilfsmittel**: Sicherheitsleitlinie (information security policy)

Vorgehensmodell gemäß IT-Grundschutzkataloge



PDCA-Vorgehen bei der Erstellung des IT-Sicherheitskonzepts (1)

PLAN:

- Festlegung der **Zielsetzung und** der Abgrenzung des Sicherheitskonzepts (**Scope**)
- Festlegung der zugrunde liegenden Vorgehensweisen und Methodiken (insb. welche **Methoden** beim **Risk Assessment** angewandt werden sollen)
- Ermittlung der zu schützenden Vermögenswerte (**Assets**)
- Bestimmung der **Kritikalität** (und Wertigkeit) der Assets
- **Durchführung des Risk Assessments**, um das aktuelle Risiko der Assets bestimmen zu können
- Festlegung der **Gegenmaßnahmen und Prüfsteine**, um das festgestellte Risiko auf ein akzeptables Restrisiko reduzieren zu können

→ Grundlagen für Planung und Entwurf des Sicherheitskonzepts

PDCA-Vorgehen bei der Erstellung des IT-Sicherheitskonzepts (2)

DO:

- **Erstellung des** (vorläufigen) **Sicherheitskonzepts** und Einbettung spezifischer Sicherheitskonzepte (z.B. zur Telearbeit) in übergreifende (einrichtungsweit geltende) Sicherheitskonzepte
- **Umsetzung der geplanten Gegenmaßnahmen** (Basismaßnahmen, die Asset-übergreifend gelten, sowie Asset-spezifischer Maßnahmen)
- **Umsetzung der vorgesehenen Prüfsteine**, so dass insbesondere auch das gemessen werden kann, was gemessen werden soll
- **Einstellung der** relevanten **Konfigurationen** bei der IT-Infrastruktur
- **Erstellung erforderlicher Handbücher/Dokumentationen**
- **Durchführung von Schulungsmaßnahmen** und Sensibilisierung der Mitarbeiter hinsichtlich der Schutzziele

→ Umsetzung der Vorgaben aus der Planungsphase

PDCA-Vorgehen bei der Erstellung des IT-Sicherheitskonzepts (3)

CHECK:

- **Auswertung** der aufgetretenen **Sicherheitsvorfälle** (Störfälle und Notfälle) **und** der vorgenommenen Veränderungen im Rahmen des **Change-Managements**
- **Überprüfung**, ob (im Rahmen der Policies) festgelegte **Prüfsteine wirkungsvoll** einen Anstieg des Risikos vermieden haben
- **Überprüfung**, ob der umgesetzte **Maßnahmenplan geeignet** war, die vorab ermittelten und tatsächlich eingetretenen Risiken im geplanten Umfang zu reduzieren
- **Berichterstattung** über den **aktuellen Stand** hinsichtlich der IT Governance, des Risikomanagements und der Compliance zu allen relevanten Regelungen (Gesetze, vertragliche Vereinbarungen wie SLAs, geltende Standards, interne Richtlinien & Policies & Anweisungen)

→ Überwachung im Sinne einer Erfolgskontrolle

PDCA-Vorgehen bei der Erstellung des IT-Sicherheitskonzepts (4)

ACT:

- Feststellung über den **Grad erreichter IT-Sicherheit**
- **Anpassung der Maßnahmenpläne, Policies und Prüfsteine** aufgrund der Erkenntnisse aus der Überprüfungsphase
- Bestimmung **ergänzender Kontrollmaßnahmen** (z.B. in Form von Computer-Aided Audit Tools)
- Festlegung der ggf. modifizierten bzw. **ergänzten** Anforderungen hinsichtlich der **Compliance** (z.B. durch Korrektur einer bestehenden Policy oder durch Erlass einer weiteren Handlungsanweisung)
- **Anpassung des bestehenden Sicherheitskonzepts**, sofern erforderlich

→ Optimierung des Sicherheitsprozesses und Konsolidierung des Sicherheitskonzepts

Zur Zugriffskontrolle: 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!

Authentifizierung

- Sicherung der Benutzeridentifikation (gemäß Authentisierung) 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

Zur Zugriffskontrolle: Password („Wissen“)

- 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. ¼ 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 Zugriffskontrolle: Chipkarte („Besitz“)

- 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 Zugriffskontrolle: Biometrie („Merkmal“)

= Erfassung und (Ver-)Messung von Lebewesen und ihren Eigenschaften

- Unterscheidung in:
  - physiologische Merkmalsverfahren (Fingerabdruckverfahren, Iris-/Retinaerkennungsverfahren, Gesichtserkennungsverfahren)
  - verhaltensabhängige Merkmalsverfahren (Sprachmuster- / Schriftdynamikerkennungsverfahren, Tipprhythmusverfahren)
- Speicherung eines Referenzmusters und Abgleich hiermit (Probleme: falsche Akzeptanz → „false acceptance rate“, falsche Ablehung → „false rejection rate“; Genauigkeit unterschiedlich und größtenteils diametral zur gesellschaftlichen Akzeptanz → lediglich Fingerabdruck in beiden Kategorien gut)