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

Vorlesung im Sommersemester 2008

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

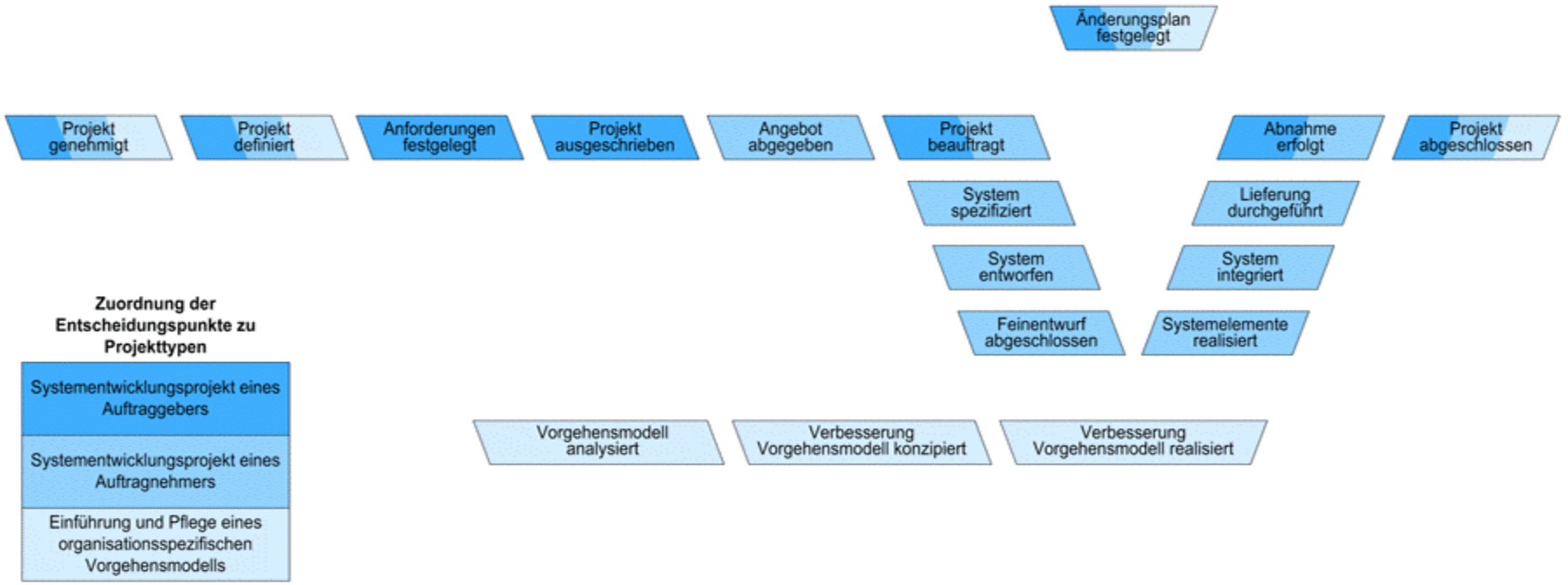
Konzeption von IT-Sicherheit:

- Erstellung sicherer IT-Systeme
- Gestaltung der IT-Infrastruktur
  - Berücksichtigung gängiger Standards
  - Architektur der IT-Infrastruktur
  - IT-Sicherheit im laufenden Betrieb

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

- **Funktionalität**:
  - Angemessenheit
  - Richtigkeit
  - Interoperabilität
  - Ordnungsmäßigkeit
  - Sicherheit
- **Zuverlässigkeit**:
  - Reife
  - Fehlertoleranz
  - Wiederherstellbarkeit
- **Benutzbarkeit**:
  - Verständlichkeit
  - Erlernbarkeit
  - Bedienbarkeit
- **Effizienz**:
  - Zeitverhalten
  - Verbrauchsverhalten
- **Änderbarkeit**:
  - Analysierbarkeit
  - Modifizierbarkeit
  - Stabilität
  - Prüfbarkeit
- **Übertragbarkeit**:
  - Anpassbarkeit
  - Installierbarkeit
  - Konformität
  - Austauschbarkeit

nach DIN 9126

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):

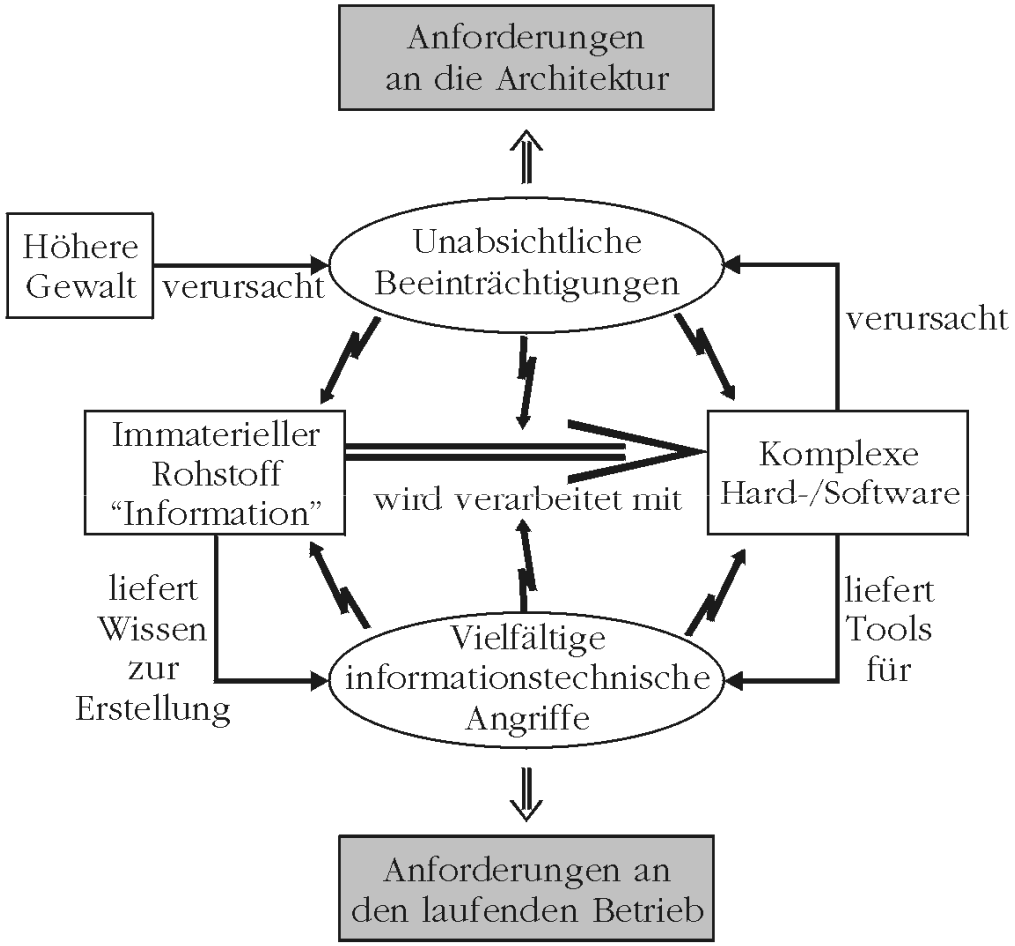
- **Prinzip einfacher Sicherheitsmechanismen**: wirksame, aber möglichst einfache Konstruktion
- **Erlaubnisprinzip**: Zugriff muss ausdrücklich erlaubt werden
- **Prinzip vollständiger Rechteprüfung**: Rechteprüfung bei allen Aktionen
- **Prinzip des offenen Entwurfs**: angewandte Verfahren und Mechanismen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

Konstruktion sicherer IT-Systeme (2)

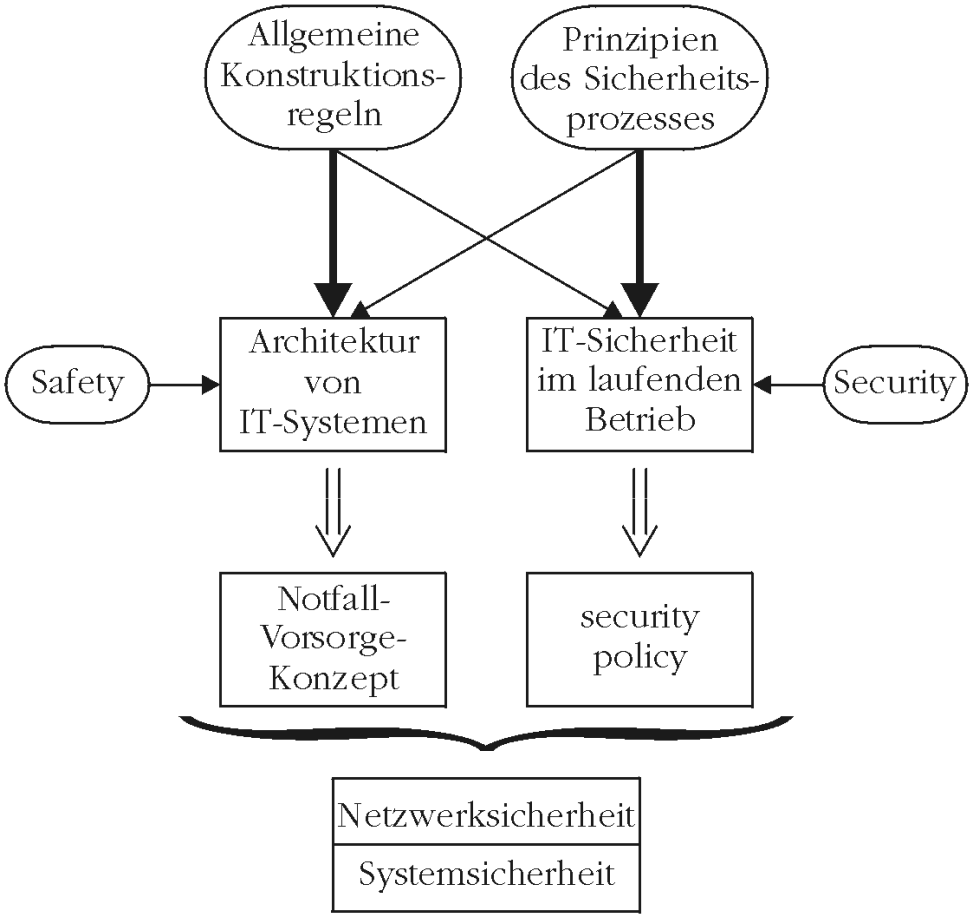
Prinzipien für Sicherheitsprozesse (nach Schneier, 2000):

- **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)



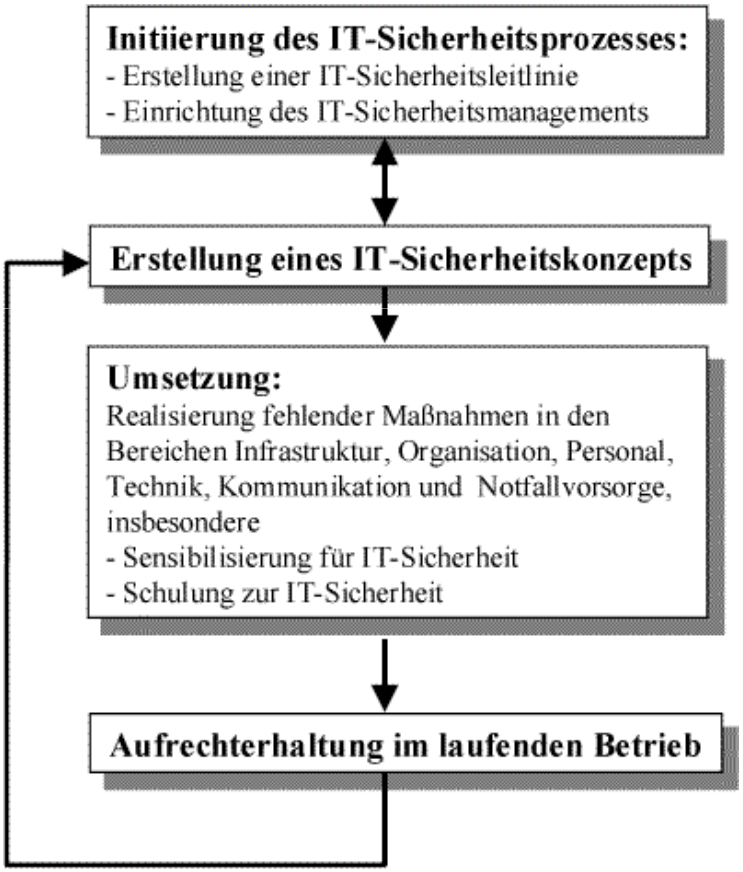
Umsetzung der Konstruk-tionsprin-zipien (2)



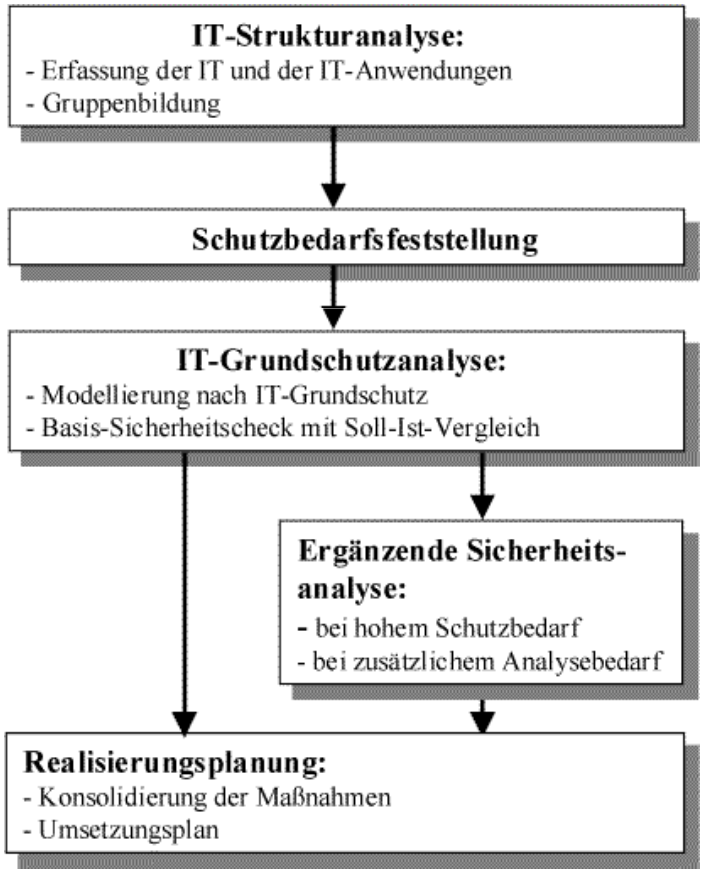
Gestaltung der IT-Infrastruktur

- Berücksichtigung gängiger Standards
  - IT-Grundschutz-Kataloge des BSI
  - Informationssicherheitsmanagement nach ISO/IEC 27002 & 27001
  - Business Continuity Management nach BS 25999
  - ITIL v2
- Architektur der IT-Infrastruktur
- IT-Sicherheit im laufenden Betrieb

Vorgehensmodell nach Grundschutz



Sicherheitskonzept des BSI



Informationssicherheit

Definition 16: Informationssicherheit

Schutz der Verfügbarkeit, Integrität und Vertraulichkeit (und ggf. weiterer Eigenschaften) von Informationen *(nach ISO/IEC 27002)*

→ Gewährleistung von Schutzzielen

→ betrifft alle Informationen eines Unternehmens

→ Information ist ein hoher Vermögenswert

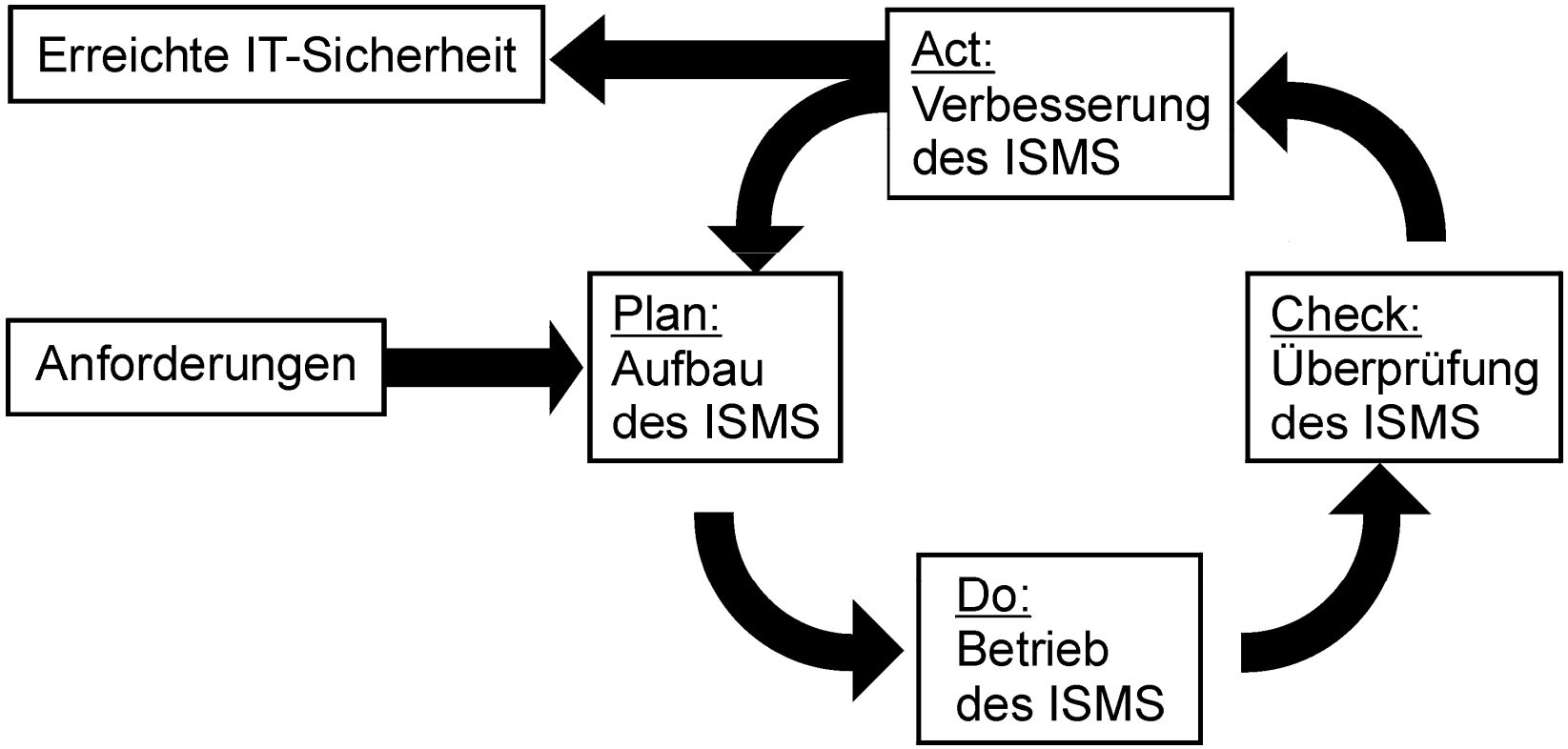
→ Verknüpfung mit IT-Risiko-Management

→ Informationssicherheit ist Aufgabe des Managements

Bestandteile Informationssicherheit

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

Vorgehensmodell nach ISO/IEC 27001



Hinweise zum PDCA-Modell

- Basiert auf sog. **Deming Cycle** (Qualitätsverbesserungszyklus nach W. Edwards Deming)
- In der **PLAN**-Phase werden die Vorgaben und Anforderungen bestimmt (inkl. Zielsetzung!) und die Übereinstimmung der vorgefundenen Einstellungen hinsichtlich dieser Rahmen überprüft (1. Risk Assessment)
- In der **DO**-Phase werden entsprechende technische und organisatorische Maßnahmen ergriffen, um die Vorgaben und Anforderungen zielgerichtet umzusetzen, und dabei insbesondere entsprechende Konfigurationen vorgenommen
- In der **CHECK**-Phase wird überprüft, inwiefern die getroffenen Maßnahmen dazu geeignet sind, die vorgegebenen Ziele zu erreichen (2. Risk Assessment – über Wirksamkeit der Controls)
- In der **ACT**-Phase werden im Sinne einer kontinuierlichen Verbesserung Konsequenzen aus der Überprüfung gezogen, der bestehende Status Quo neu bewertet und die Grundlage für den nächsten Durchlauf gelegt

Business Continuity Management

- Grundlage: **BS 25999** (Teil 1: 2006; Teil 2: 2007)
- **Gewährleistung der Geschäftskontinuität** mithilfe
  - **Business Impact Analysis** (BIA) → Identifikation kritischer und für den Fortbestand bedrohlicher Prozesse der gesamten Wertschöpfungskette (inkl. Stakeholder!) → Priorisierung für Wiederanlauf
    Maximum Tolerable Period of Disruption (MTPD) = maximal tolerierbare Ausfallzeit (für jeden Prozess und jede Ressource!)
    Recovery Time Objective (RTO) = Dauer f. Wiederanlauf kritischer IT
    Recovery Point Objective (RPO) = maximal zulässiger Datenverlust
  - **Business Continuity Plan** → Dokumentation der Vorgehensweisen beim Eintreten eines bedrohlichen Notfalls (= Notfallkonzept)
    *Hinweis: **Notfall** = außergewöhnliche Abweichung vom Normalbetrieb (→ zu unterscheiden von Störfällen, die im Rahmen des laufenden Betriebs beherrschbar sind, und Katastrophen, die sich großflächig auswirken und i.d.R. staatlich reglementiert werden)*
  - Durchführung von **Notfallübungen** anhand stimmiger Szenarien

Alternative Vorsorgestrategien

Wiederanlauf-Maßnahmen	**1998**	**2000**	**2002**	**2004**	**2006**
Cluster (mit Überkapazitäten)	9%	14%	46%	38%	36%
laufende Systeme („hot“)	16%	17%	40%	34%	31%
Räume m. wicht. HW („warm“)	20%	19%	43%	28%	37%
leere Räume („cold“)	12%	15%	36%	29%	25%
Räume f. Pers. mit Infrastrukt.	-----	9%	25%	17%	18%
Räume f. Pers. oh. Infrastrukt.	-----	7%	13%	9%	9%
konfigurationsidentische Netze	13%	11%	25%	19%	22%
Nutzungsvertrag v. Ressourcen	17%	15%	30%	25%	20%
Nutzungsvertrag v. Containern	5%	6%	7%	8%	12%
Vertrag schnelle HW-Ersatzlief.	25%	31%	44%	41%	37%
Abschluss von Versicherungen	31%	41%	61%	44%	41%

Quelle: <kes>-Sicherheitsstudien

Prozess-Sichtweise nach ITIL (1)

- **ITIL** = IT Infrastructure Library (best-practice-Referenzmodell für IT-Service-Prozesse)

  [Angaben zu ITIL v2]
- 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
  - **Availabilty Management** → Sicherstellung vereinbarter Verfügbarkeiten
  - **Business Continuity Management** → Abwehr von Katastrophen/Notfällen
- Für Zertifizierung nach ISO/IEC 20000 außerdem kontinuierlicher Verbesserungsprozess erforderlich

Konzeption von IT-Sicherheit (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. 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 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-/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)

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!

Umgang mit § 202c StGB

§ 202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft , einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Folgen für die Administration der IT-Sicherheit:

- Die Einstufung als Straftat setzt Vorsatz voraus. Insofern steht die Tätigkeit der IT-Administration mit dem Ziel der Gewährleistung der IT-Sicherheit keineswegs unter Strafe. Allerdings ist es hierzu zweckmäßig, die Methoden der Angreifer und damit insbesondere die Wirkungsweise der sog. „Hackertools“ zu kennen.
- Der IT-Administration kann daher angeraten werden, sich sowohl die „Beschaffung“ als auch den Einsatz von „Hackertools“ durch die Geschäftsleitung genehmigen zu lassen, so dass deren Einsatz nicht unbefugt erfolgt.
- Entsprechende „Hackertools“ sind gegen unbefugten Zugriff zu schützen.
- Über den durchgeführten Einsatz ist ein Protokoll zu erstellen, das ebenfalls gegen unbefugten Zugriff abzusichern ist.

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)

Aufgabe: Prüfungsfragen

→ Formulieren Sie je eine Prüfungsfrage zu den

- Grundlagen des Datenschutzes
- Grundlagen der IT-Sicherheit

  soweit diese in Vorlesung oder Übung behandelt wurden!

→ Erstellen Sie zu einer Frage Ihre Musterlösung!

→ Geben Sie zur Musterlösung die Punktevergabe an!

Zeit: 15 Minuten! (pro Teilaufgabe ca. 5 min)

Ziel: Präsentierbare Lösung!

Literaturhinweise

Im Semesterapparat verfügbar:

- Bernhard C. Witt: IT-Sicherheit kompakt und verständlich; Wiesbaden, Vieweg, 2006
- Claudia Eckert: IT-Sicherheit; München, Oldenbourg, 2006, 4. Auflage [im Semesterapparat noch die 3. Auflage von 2004]

Zum Hintergrund der Vorlesung empfehlenswert:

- Hans-Peter Königs: IT-Risiko-Management mit System; Wiesbaden, Vieweg, 2005
- Bruce Schneier: Secrets & Lies – IT-Sicherheit in einer vernetzten Welt; Heidelberg, dpunkt, 2001
- Günter Müller & Andreas Pfitzmann (Hrsg): Mehrseitige Sicherheit in der Kommunikationstechnik; Bonn, Addison Wesley, 1997
- Zeitschriften: <kes>, hakin9, IEEE security & privacy, IT-SICHERHEIT