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

Vorlesung im Sommersemester 2023

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
✓	Schwerpunkt: Aktuelles	➔	Konzeption von IT-Sicherheit

Konzeption von IT-Sicherheit:

- Informationssicherheitsmanagement *(→ Übung)*
- Sicherheitsvorfallmanagement *(→ Übung)*
- Erstellung sicherer IT-Systeme
  - ° V-Modell XT
  - ° Konstruktionsprinzipien
- Interessensausgleich *(→ Übung)*

Sicherheitsereignisse

- Verlust ausgegebener Zutrittsmittel
- Unzutreffende Klassifizierung des Schutzbedarfs von Informationen
- Detektion unbefugter Zugangs- (Einbruch) oder Zugriffsversuche
- Kenntnis über eine bestehende Schwachstelle bzw. Sicherheitslücke
- Kenntnis über das Vorliegen einer nicht entfernten Malware
- Kenntnis über abrufbare Zugangs- bzw. Zugriffscredentials (z.B. infolge eines unwirksamen Zugangsschutzes von Passwortsafes)
- Kenntnis über ungeschützt abrufbare vertrauliche Daten (z.B. infolge der Migration oder des Transfers von Daten auf einem gesharten Laufwerk)
- Kenntnis über nicht benötigte Schnittstellen zwischen Systemen und Komponenten oder auch für Unbefugte erreichbaren Ports
- Kenntnis über eingesetzte, veraltete Kryptoverfahren
- Kenntnis über eingegangene Versuche von Phishing, Social Engineering oder gezielten Angriffen (spear phishing bzw. targetted attacks)
- Kenntnis über ungewöhnliches Systemverhalten (technisches Versagen oder aufgrund unerwartet angezeigter Systemmeldungen)
- Kenntnis über unerwartet abgelegte Dateien in Speicherbereichen, auf denen Nutzer üblicherweise keine Daten ablegen

Sicherheitsvorfälle

- Ausfall eines IT-Systems, einer Anwendung oder einer IT-Komponente
  → **Verletzung der Verfügbarkeit**
- Störung der Funktionsweise eines IT-Systems, einer Anwendung oder einer IT-Komponente
  → **Verletzung der Verfügbarkeit und/oder Integrität**
- Kenntnis über den Eintritt eines unbefugten Datenabflusses (z.B. E-Mail Datentransfer aber auch Verlust von Papierunterlagen)
  → **Verletzung der Vertraulichkeit**
- Kenntnis über unerwartete Aktionen durch Nutzer oder Systemen gemäß vorliegenden Eventlogs
  → **Verletzung der Vertraulichkeit, Verfügbarkeit und/oder Integrität**
- Kenntnis über Nichteinhaltung vorgeschriebener Arbeitsanweisungen hinsichtlich des Umgangs mit Informationen
  → **Verletzung der Compliance**

Unterschied:

Ein **Sicherheitsvorfall** liegt nur dann vor, wenn ein **Sicherheitsziel verletzt** wurde

Bei **Sicherheitsereignis** nur entsprechende **Verletzung möglich**

Sicherheitsvorfallmanagement

Phasen des Sicherheitsvorfallmanagement nach ISO/IEC 27035-1:

- **Plan and Prepare**
  - Richtlinie zum Umgang mit Informationssicherheitsvorfällen
  - Einsatz eines CSIRT
  - Awareness (Training und Unterweisungen; Berücksichtigung von Vorfallserfahrungen)
- **Detection and Reporting**
  - Aufzeichnung anormaler, verdächtiger oder maliziöser Aktivitäten
  - Informationssammlung über Sicherheitsereignisse (Vorfälle, bekannt gewordene Sicherheitslücken, Infos zur aktuellen Gefährdungslage)
  - Bericht relevanter Sicherheitsereignisse (incl. Erstmeldung meldepflichtiger Vorfälle)
- **Assessment and Decision**
  - Analyse der relevanten Sicherheitsereignisse
  - Entscheidung über Umgang mit Sicherheitsereignissen
- **Responses**
  - Welche relevanten Sicherheitsereignisse werden beherrscht?
  - Wiederherstellung der Arbeitsfähigkeit nach Behebung des Vorfalls
  - Ggf. Krisenkommunikation und Erfüllung vollständiger Meldepflichten
- **Lessons learnt**
  - Verbesserung Informationssicherheit, IT-Risikoanalyse & Vorfallmanagement

Hilfreiche Quellen

- Vulnerability Management:
  https://www.cvedetails.com/
  https://www.heise.de/
- Secure Coding Guidelines:
  https://owasp.org/www-project-proactive-controls/
  https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices
- Maßnahmenplanung:
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

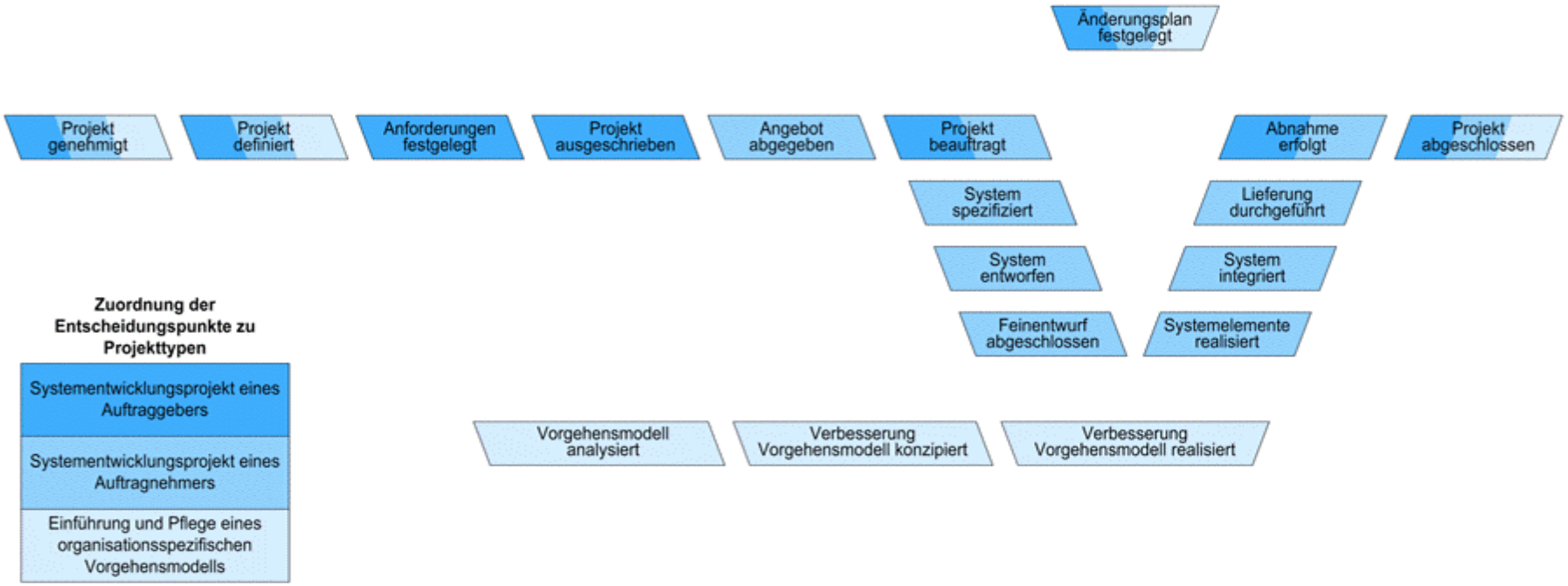
Erstellung sicherer IT-Systeme

- **Software-Erstellung**
  → V-Modell XT
  → Sichere Softwareentwicklung *(→ Übung)*

- **Konstruktionsprinzipien**
  → allgemeine Prinzipien
  → Prinzipien für Sicherheitsprozesse

- **Systemsicherheit**
  → Serversicherheit & Clientsicherheit *(→ 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)

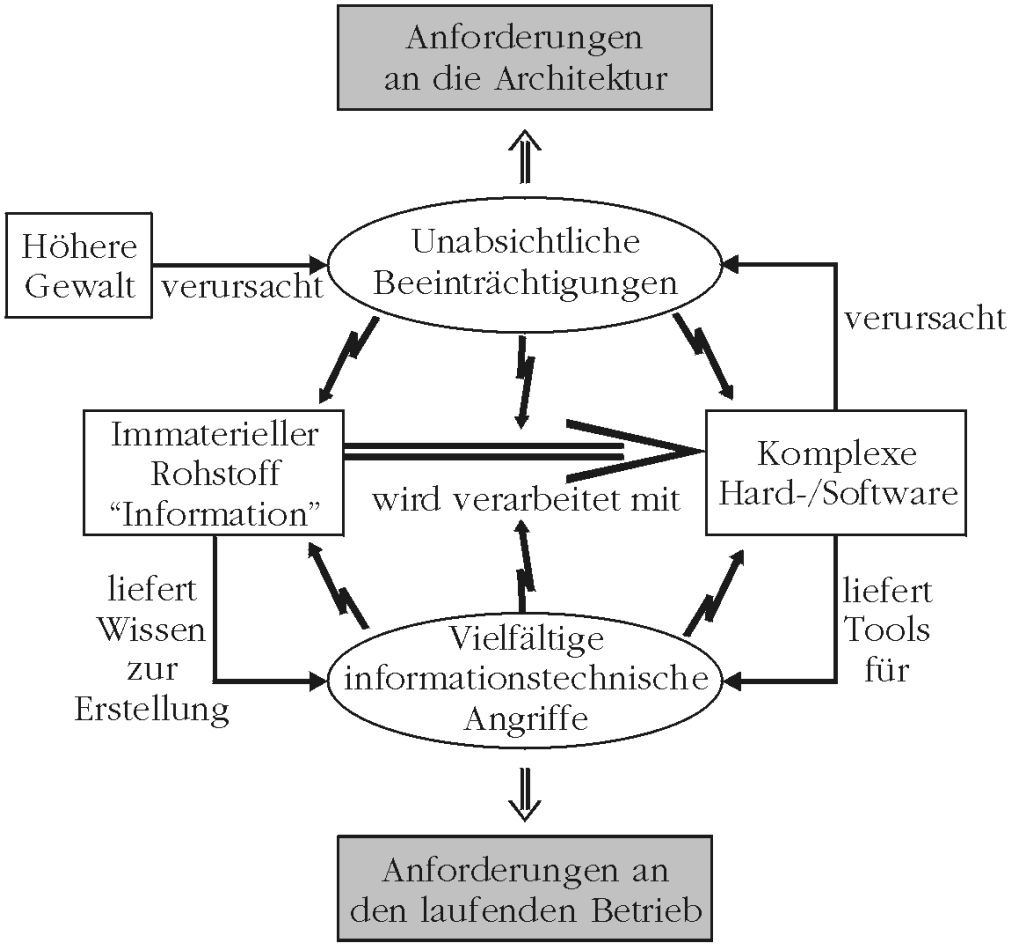
Allgemeine Prinzipien (nach Saltzer und Schroeder, 1975):

- **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 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