T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2014
Berlin, 03.–04.11.2014

Entwicklung von sicheren Anwendungen in großen Organisationen

Herausforderungen und Lösungsansätze

Jörn Eichler
Fraunhofer-Institut für
Angewandte und Integrierte Sicherheit

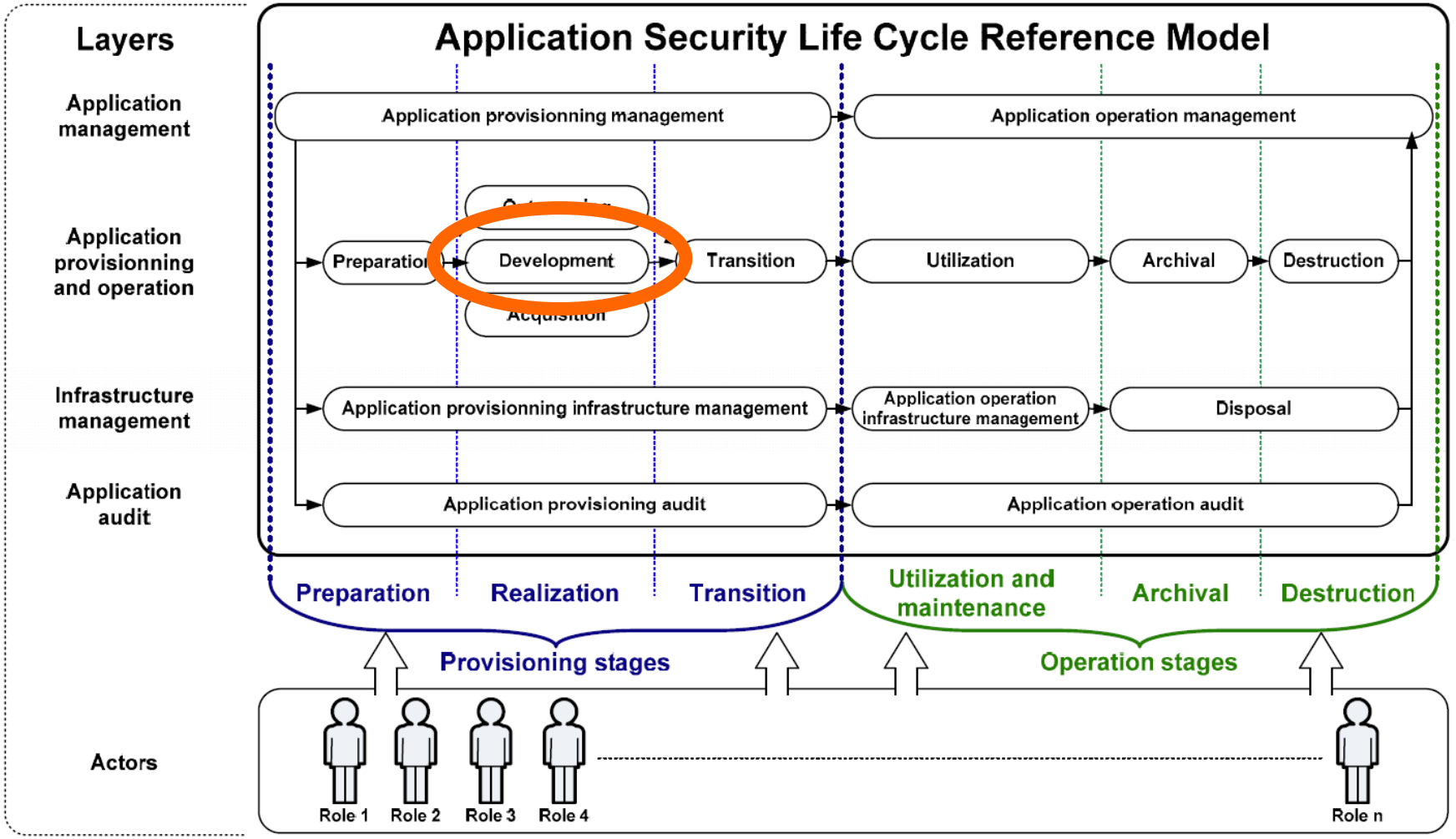
Fraunhofer
AISEC

Motivation

- Immer mehr Firmen entwickeln Software, z.B. Siemens:
  - 17.500 Softwareentwickler
  - 60 % des Umsatzes hängt von Software ab
- Entwicklung sicherer Software ist schwierig, z.B.:
  - < 40 % der Unternehmen hat *keinen* Sicherheitsvorfall aufgrund von Schwachstellen in der Anwendungsschicht in Jahresfrist
  - < 20 % der Beteiligten sehen alle Sicherheitsanforderungen für ihre Anwendungen als erfüllt an
- Macht die Unternehmensgröße einen Unterschied?

Quellen: Siemens, Forrester (2012)

Entwicklung sicherer Software



Quelle; ISO 27034

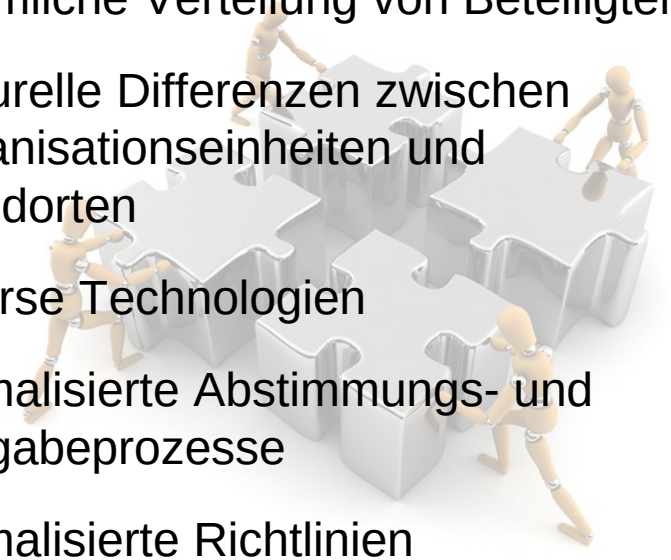
Size Matters …

Kleine Unternehmen

- Mehrere Rollen werden in Personalunion geführt
- Anzahl der Beteiligten ist überschaubar
- Arbeiten an einem Ort
- Kulturelle Homogenität der Beteiligten
- Überschaubare Technologien
- Informelle Prozesse
- Informelle Richtlinien

Große Unternehmen

- Rollen sind in Organisationseinheiten institutionalisiert
- Zahlreiche Beteiligte: personell & organisational
- Räumliche Verteilung von Beteiligten
- Kulturelle Differenzen zwischen Organisationseinheiten und Standorten
- Diverse Technologien
- Formalisierte Abstimmungs- und Freigabeprozesse
- Formalisierte Richtlinien



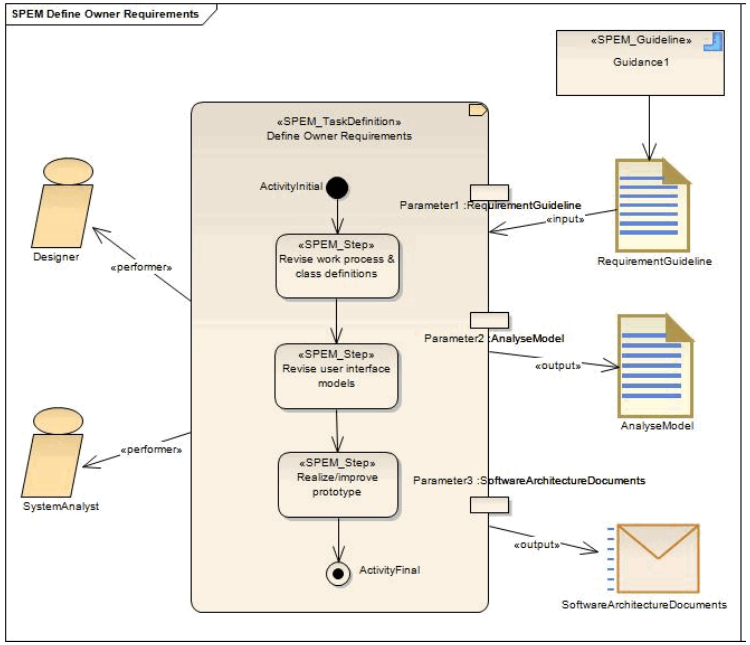
Etablierung von Prozessen

- Instanziierung eines Entwicklungsprozesses
  - Basis sind Vorgehensmodelle, z.B.: V-Modell XT, SCRUM, RUP
  - Konform mit bestehenden Standards, z.B. ISO 12207
- Integration von Aktivitäten, Rollen und Artefakten des Security Engineering
- Etablierung von Schnittstellen
  - ISMS gemäß ISO 27001, …
- Bewertung des Entwicklungsprozesses mithilfe von Reifegradmodellen
  - OpenSAMM, ISO 21827 (SSE-CMM), CMMI Security by Design, …

Prozesse versus Techniken

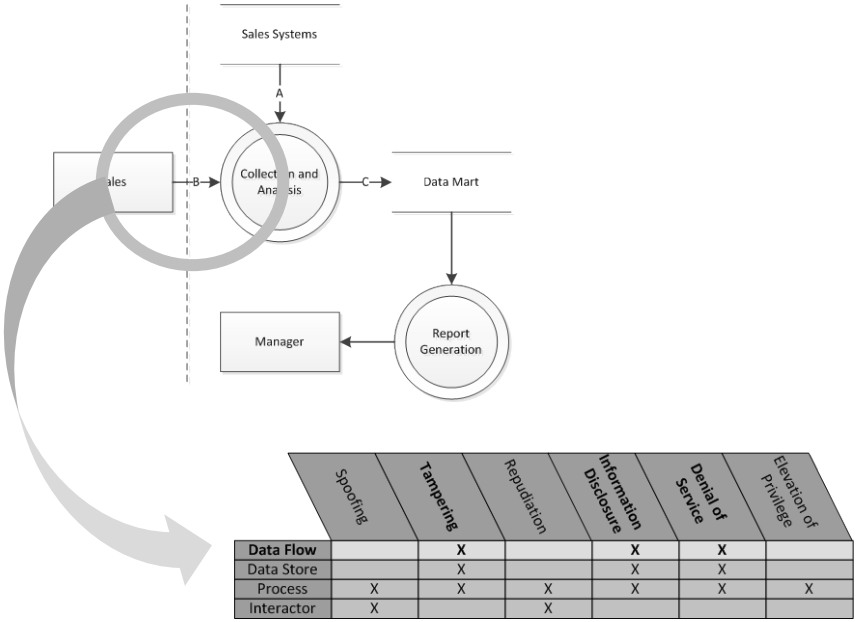
Prozess (-modell)

- *Wer* tut *was wann*, *womit* und *wofür*?
- Logische (und zeitliche) Verknüpfung von *Aktivitäten*, *Rollen* und *Artefakten*



Technik (oft auch: Methode)

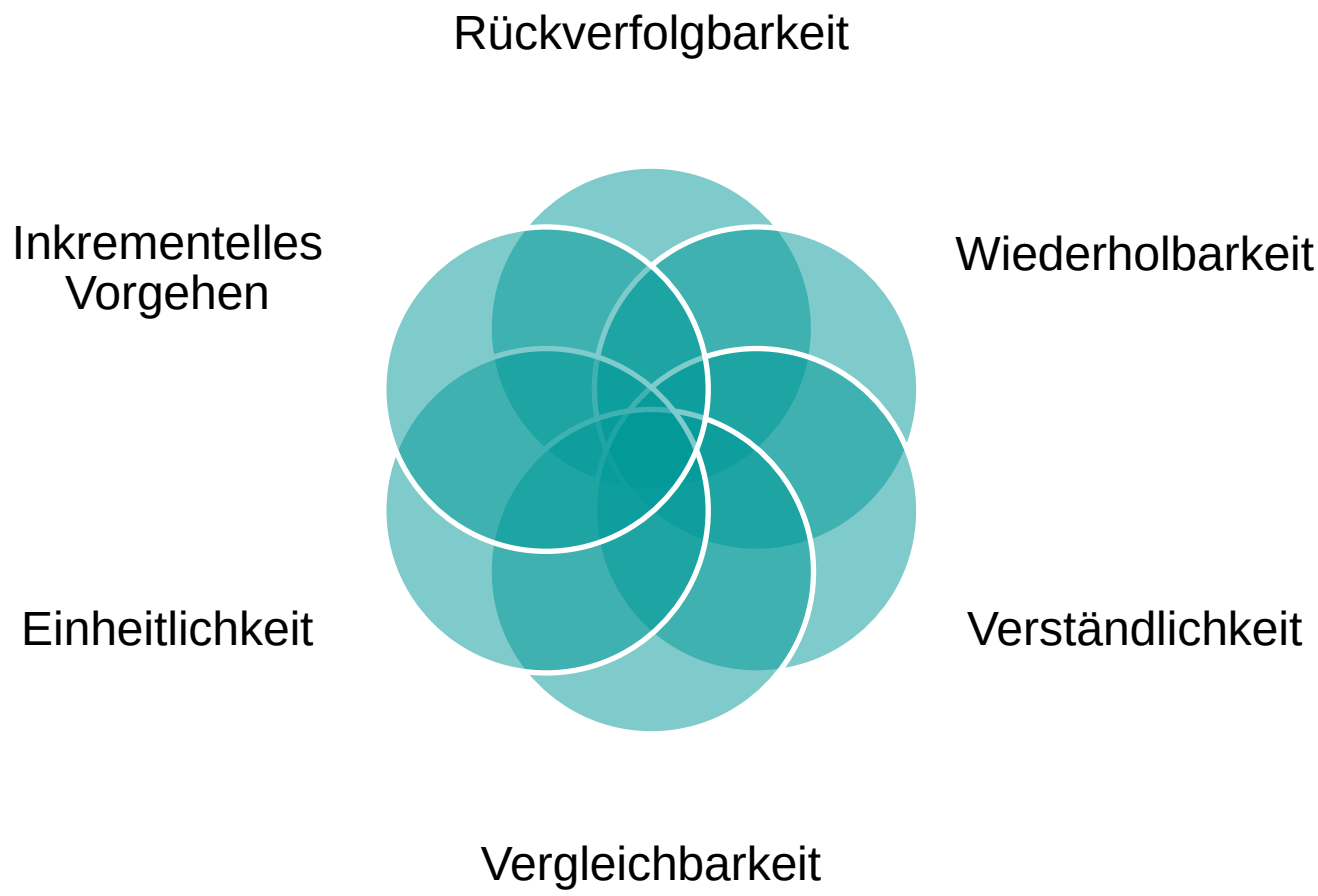
- *Wie* wird etwas getan?
- Fachliche und handwerkliche Fähigkeiten und Kenntnisse



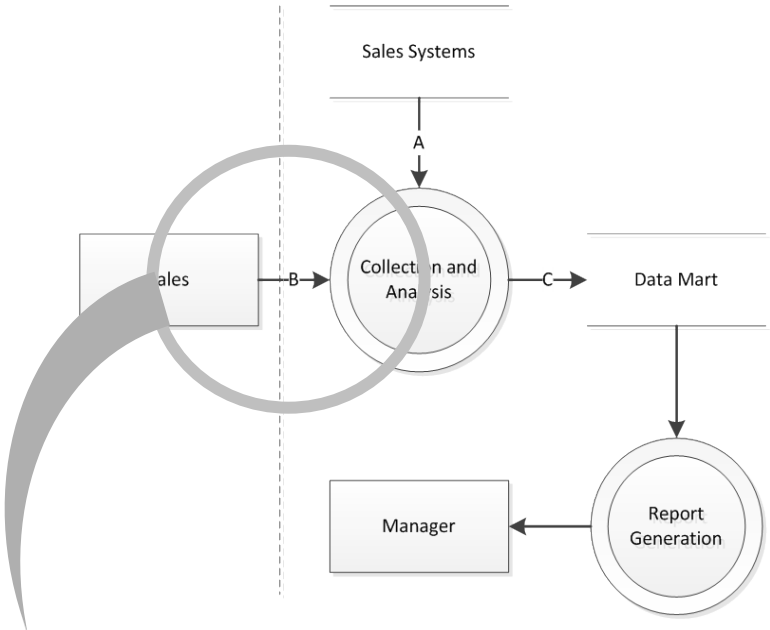
	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Data Flow		X		X	X	
Data Store		X		X	X	
Process	X	X	X	X	X	X
Interactor	X		X			

Quelle: SPARX

Techniken und Methoden in großen Unternehmen



Ein Beispiel: Bedrohungsanalyse mit STRIDE

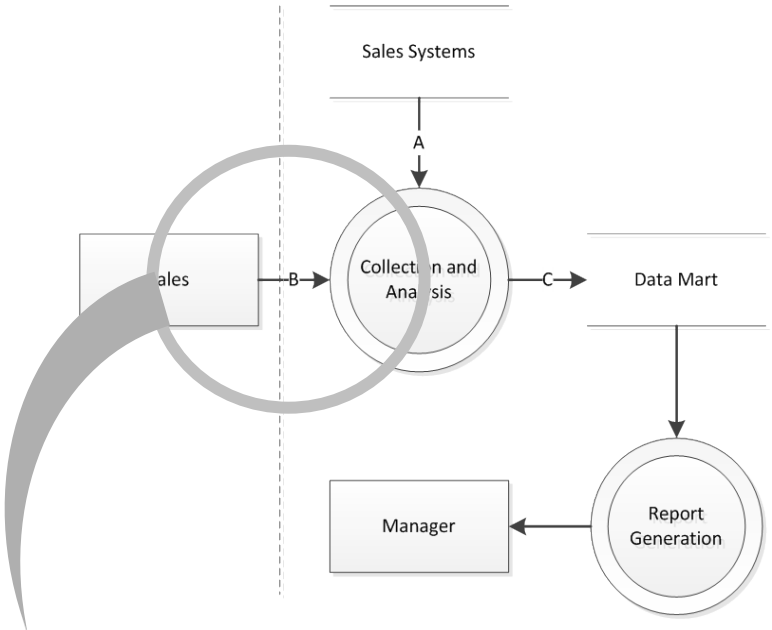


Vorgehen

- Systembeschreibung als DFD erstellen
- Vertrauensgrenzen einführen
- Bedrohungsklassen prüfen
- Bedrohungen zusammenfassen
- Bedrohungen bewerten

	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Data Flow		X		X	X	
Data Store		X		X	X	
Process	X	X	X	X	X	X
Interactor	X		X			

Skaliert STRIDE in großen Unternehmen?

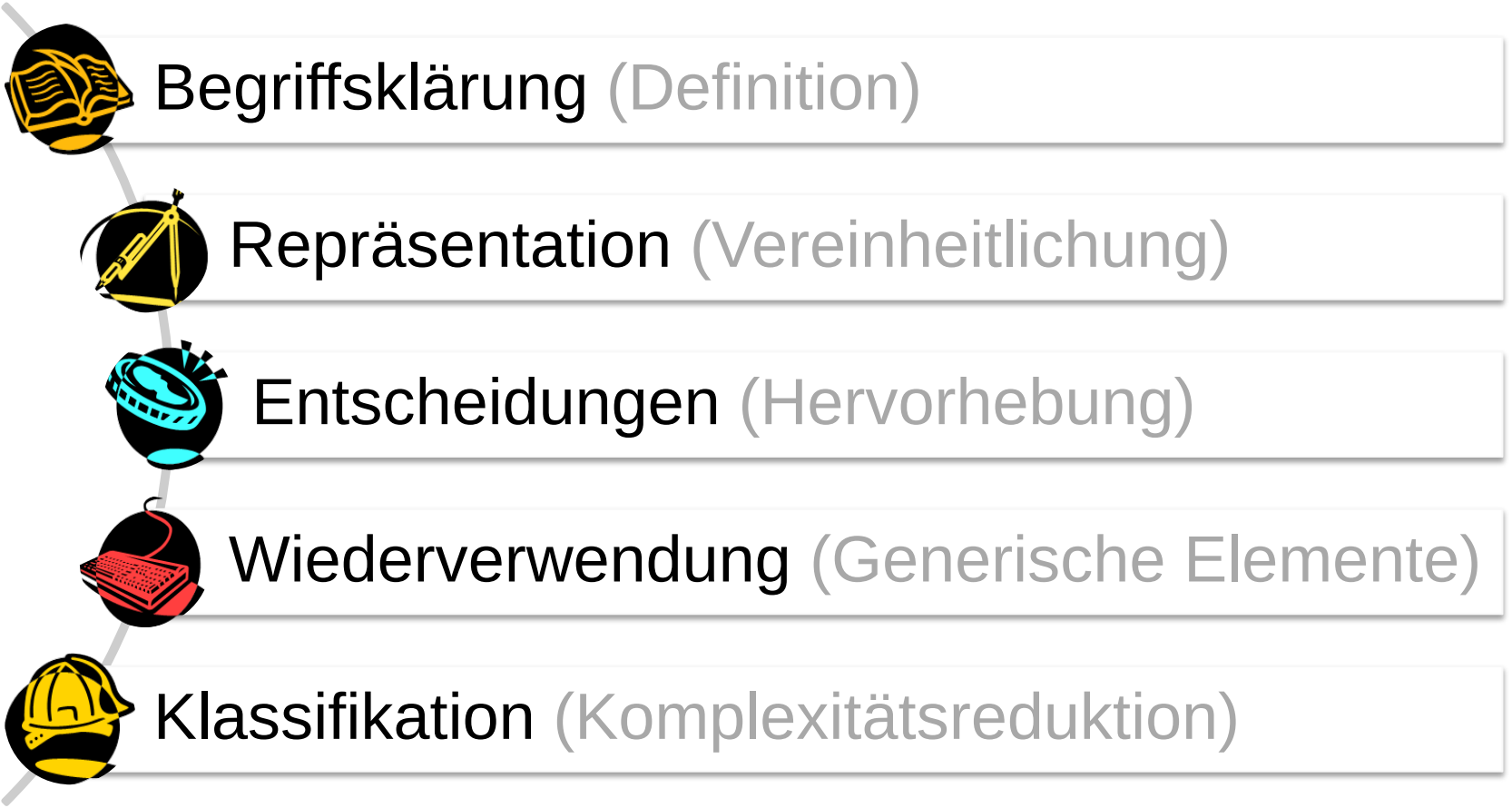


Herausforderungen, z.B.

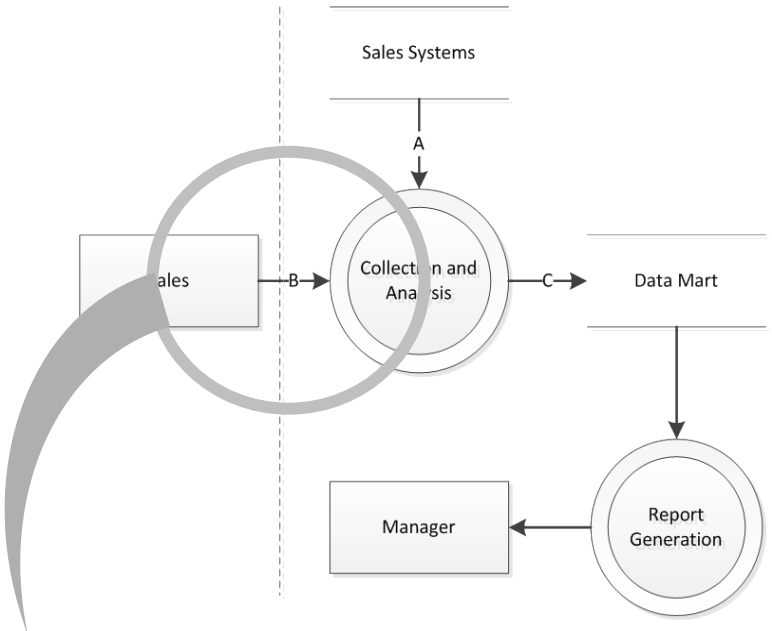
- Welche Elemente und Beschriftungen im DFD?
- Welche Perspektive und Gültigkeitsbereich?
- Welche Bedrohungen sind irrelevant?
- Wie werden Bedrohungen zusammengefasst?

	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Data Flow		X		X	X	
Data Store		X		X	X	
Process	X	X	X	X	X	X
Interactor	X		X			

Methoden und Techniken skalieren



Zum Beispiel: STRIDE skalieren



- Definition Bedrohung, …
- Vorgabe Granularität für DFDs, Richtlinien für Benennung, …
- (Toolgestützte) Dokumentation unberücksichtigter Bedrohungen, …
- Bereitstellung von verfeinerten System- und Bedrohungskatalogen
- Zusammenfassung von Bedrohungen anhand definierter Eigenschaften

	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Data Flow		X		X	X	
Data Store		X		X	X	
Process	X	X	X	X	X	X
Interactor	X		X			

Zusammenfassung

- Unternehmensgröße ist ein Faktor
- Etablierung von Prozessen ist Standard
- Methoden und Techniken dürfen nicht vergessen werden:
  - Begriffsklärung
  - (Vereinheitlichung der) Repräsentation
  - (Hervorhebung von) Entscheidungen
  - Wiederverwendung (generischer Elemente)
  - Klassifikation (zur Komplexitätsreduktion)

Jörn Eichler
joern.eichler@aisec.fraunhofer.de