UNIVERSITÄT LEIPZIG

Institut für Medizinische Informatik, Statistik und Epidemiologie (IMISE)

Erfahrungen bei der Erstellung und Umsetzung von Sicherheitskonzepten in medizinischen Forschungsverbünden

Ronald Speer[1] ,Wolfgang Dolak[2]

[1]Koordinierungszentrum für Klinische Studien, Universität Leipzig

[2]Institut für Medizinische Informatik, Statistik und Epidemiologie, Universität Leipzig

07.11.2006

imise. KKSL KOORDINIERUNGSZENTRUM FÜR KLINISCHE STUDIEN LEIPZIG Kompetenznetz Maligne Lymphome

Forschungsverbünde

- Kompetenznetze in der Medizin
  www.kompetenznetze-medizin.de
- Koordinierungszentren für klinische Studien
  www.kks-netzwerk.de
- Verbundprojekte (DFG, Krebshilfe)

- übergreifende Telematikplattform TMF e.V.
  www.tmf-ev.de

gefördert vom Bundesministerium für Bildung und Forschung

gefördert vom Bundesministerium für Bildung und Forschung

gefördert vom Bundesministerium für Bildung und Forschung

Telematikplattform für Medizinische Forschungsnetze e. V.

TMF

Situation in den Verbünden

- ähnliche Strukturen
- kaum Erfahrungen im Bereich IT-Sicherheit
- begrenzte Ressourcen (Personal & Finanzen)
- fehlende IT-Qualitätssicherungsprozesse
- „Dienstleister“ (KKS)
- Einsatz komplexer IT-Prozesse

➧ Vertragliche und Rechtliche Forderungen

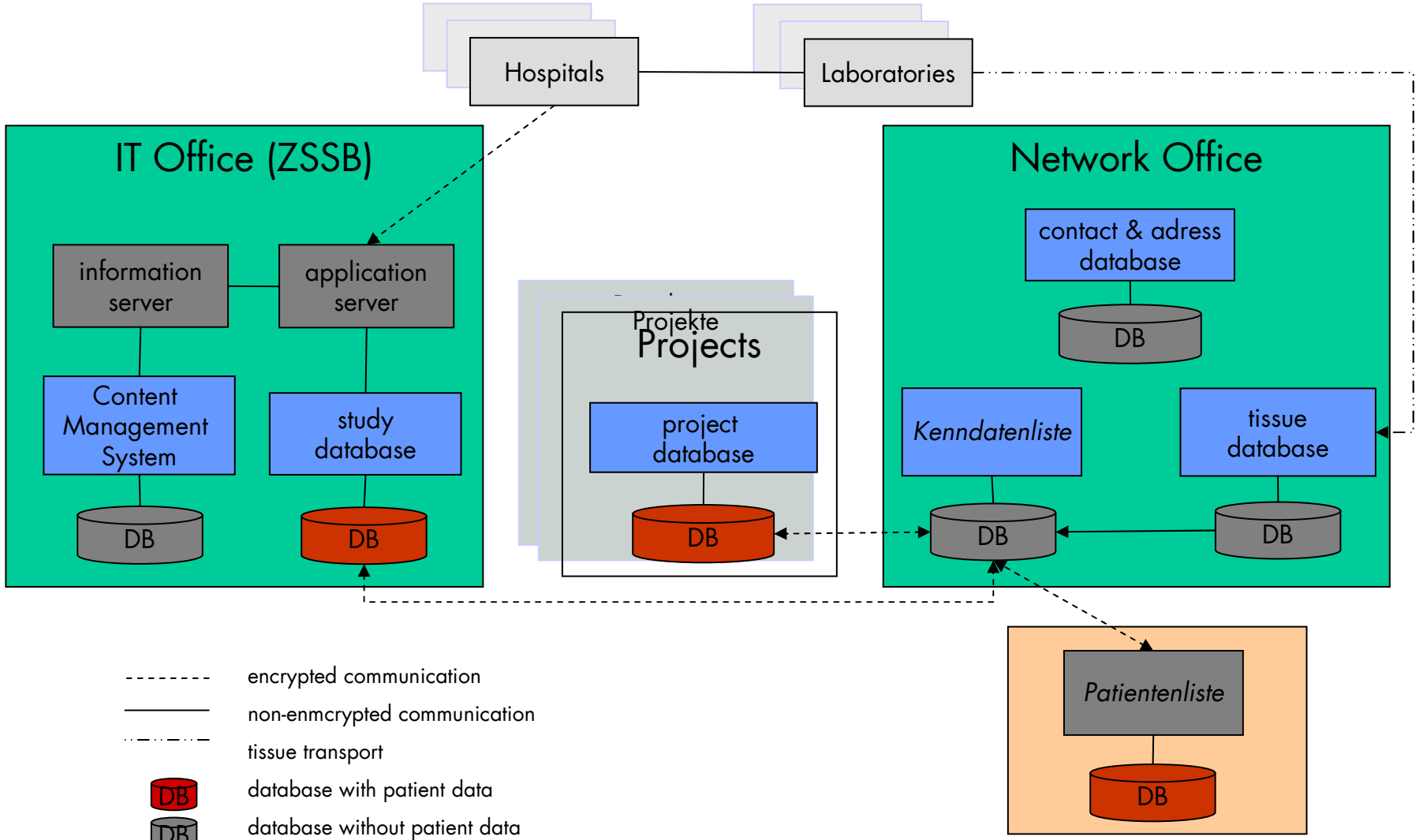
IT-Verbund IMISE/KKSL

- Bereitstellung von Diensten
  - Patientenliste, Kenndatenliste, CMS, Studiendatenbanken, Materialdatenbanken, etc.
- verschiedene Forschungsverbünde
  - KN Lymphome, KN Herzinsuffizienz, KN Sepsis
- Application Service Providing
  - KKS Halle

IT-Struktur der FV
(Beispiel KN Herzinsuffizienz)

UNIVERSITÄT LEIPZIG

Institut für Medizinische Informatik, Statistik und Epidemiologie (IMISE)



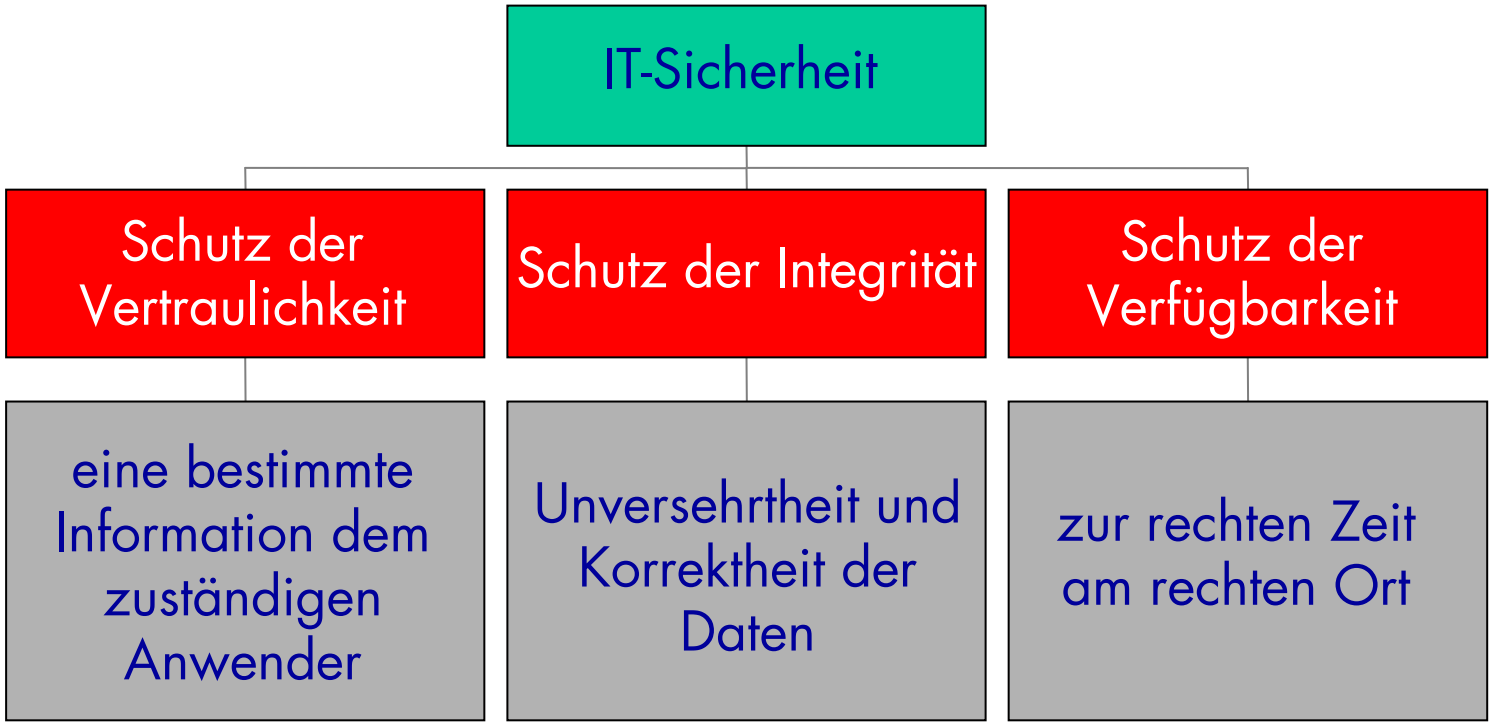
Motivation

- Erstellung Sicherheitskonzept notwendig:
  - Akzeptanz bei externen Partnern
  - Arbeitsgrundlage für eigene Aufgaben
  - IT-Qualitätssicherung
  - Sponsor-Audits
  - Begutachtung und Reviews
  - Validierung der Systeme und Verfahren
  - …

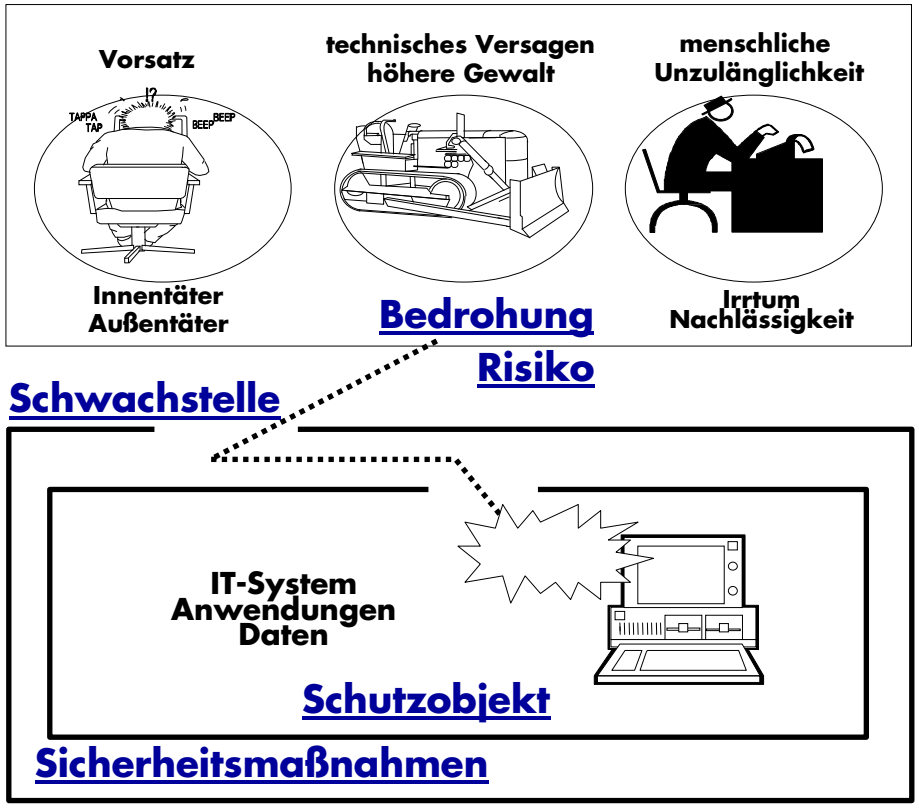
Fragen

- Wie sind die gesetzlichen Anforderungen ?
- Wie ist das Vorgehen bei der Erstellung ?
- Wer sind die Ansprechpartner ?
- Wer prüft/zertifiziert das Sicherheitskonzept ?
- Gibt es Vorarbeiten oder Muster für ein derartiges Sicherheitskonzept ?
- Was bedeutet IT-Sicherheit ?

Grundwerte der IT-Sicherheit



Bedrohungen für die IT-Sicherheit



aus „Folien zum IT-Grundschutz ", Bundesamt für Sicherheit in der Informationstechnik, Bonn

IT-Sicherheitsprozess

Auswahl der Methode

Anwendungsbereich	Anforderungen
Sicherheitskonzept Sicherheitshandbuch Revision	Standardisierung Unabhängigkeit Zertifizierbarkeit Umsetzbarkeit Anpassbarkeit Aktualisierung Wirtschaftlichkeit

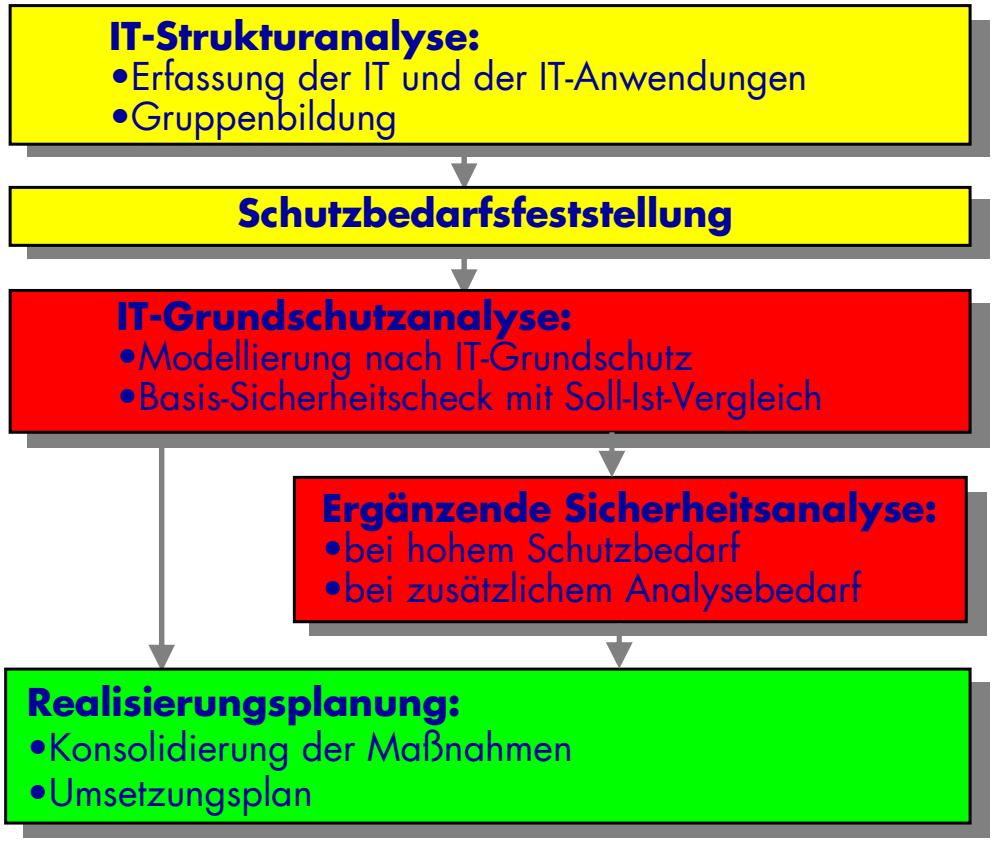
„CoP, COBIT, Marion, IT-Grundschutzhandbuch – vier Methoden im Vergleich", Information Systems Audit and Control Association ISACA

Vergleich der Methoden

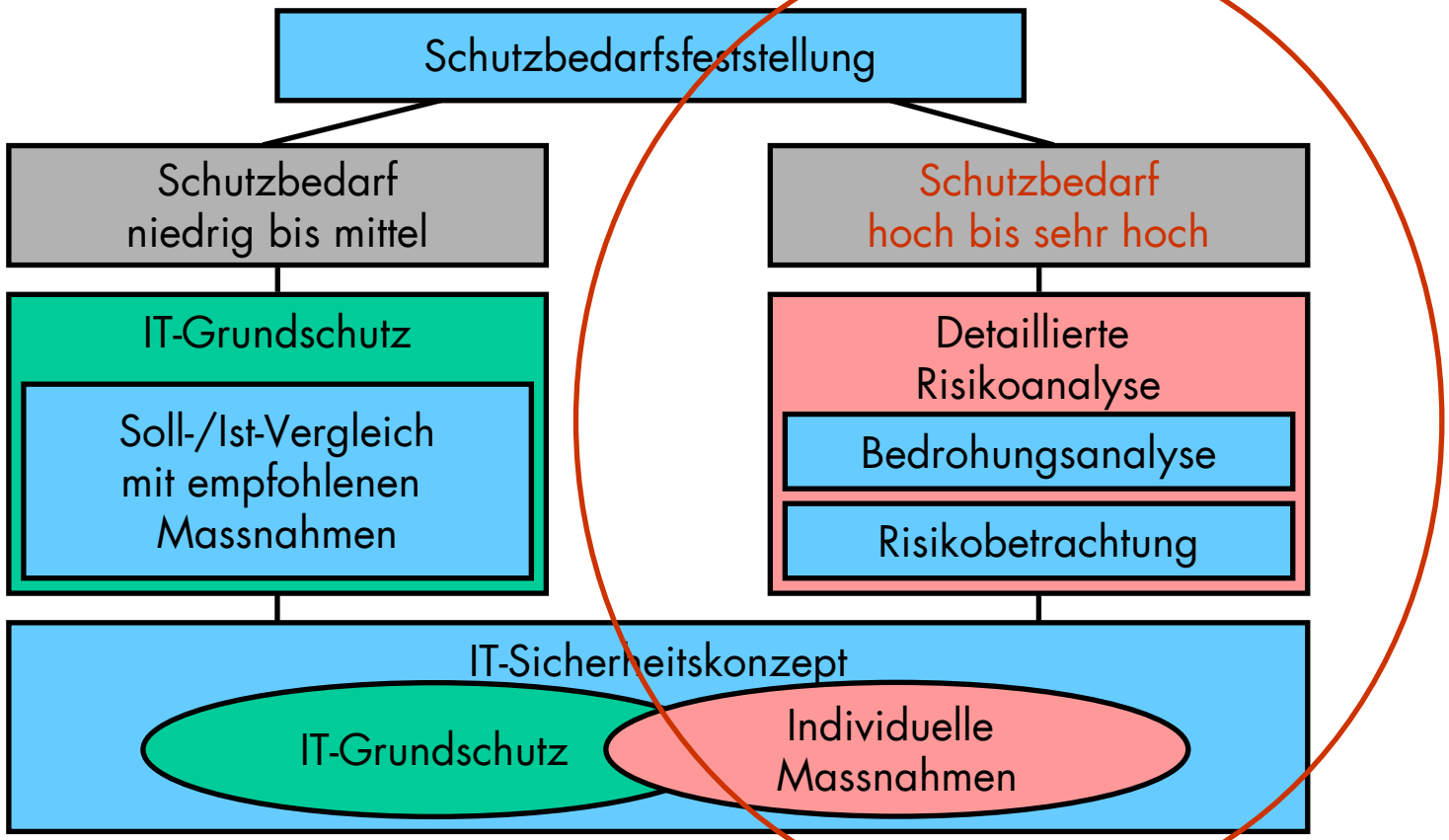
System-bezogen		IT-GSHB	ISO 9000 ISO 13335 ISO 17799 CobiT
	Task Force Sicheres Internet	DS-Produktaudit	
Produkt-bezogen	FIPS 140 ITSEC/CC		
	Technisch		Nicht technisch

aus „IT-Sicherheitskriterien im Vergleich“, INITI@TIVE D21, Berlin 2001

Vorgehen IT-Grundschutz

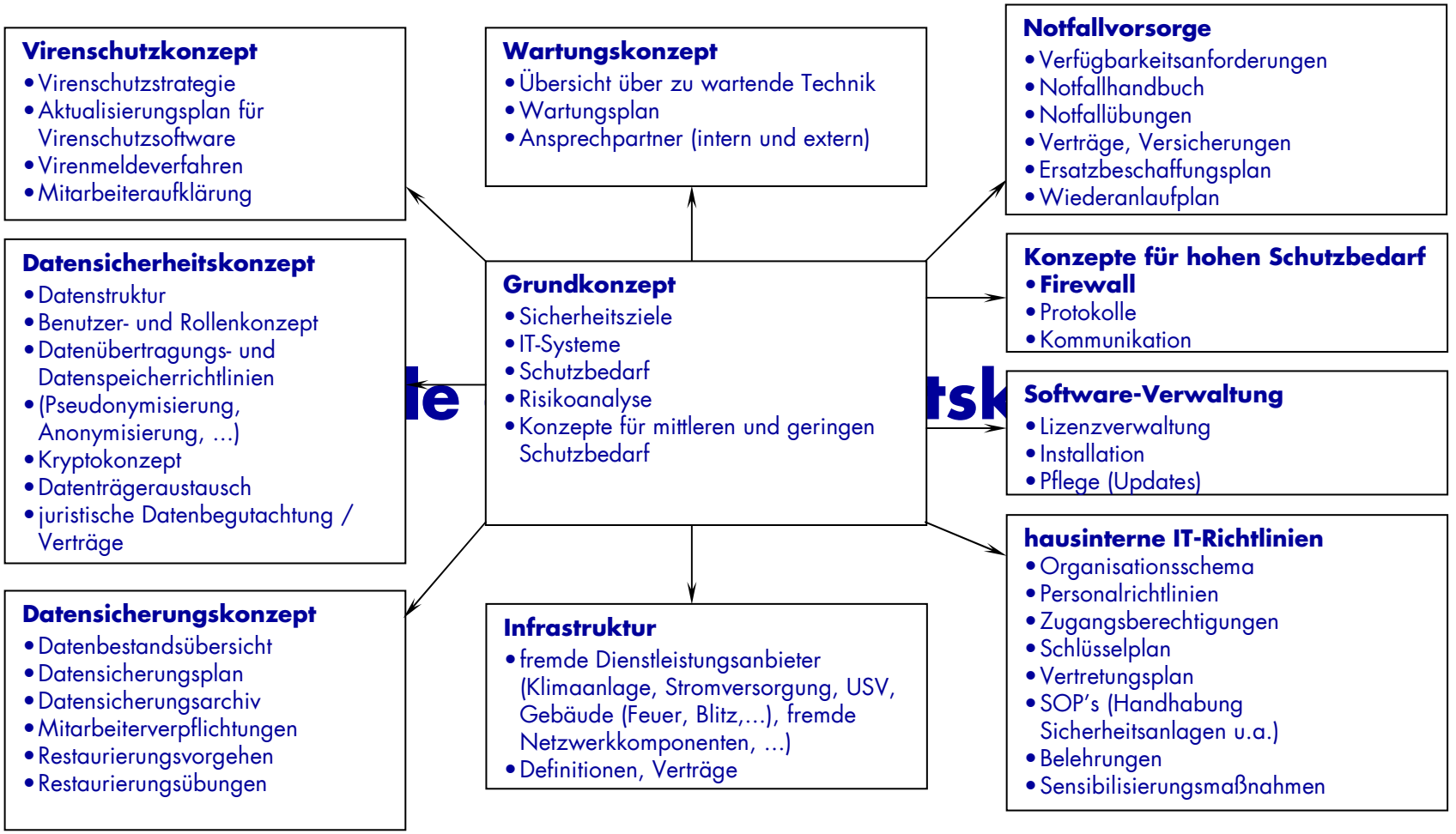


Schutzbedarfsfeststellung



Ergänzende Sicherheitsanalyse

- Schutzbedarfskategorie „hoch“ oder „sehr hoch“ liegt in mindestens einem der drei Grundwerte vor:
  - Risikoanalyse
    - relevante Bedrohungen ermitteln
    - Eintrittswahrscheinlichkeiten schätzen
  - Penetrationstest
    - Verhalten eines Angreifers simulieren
    - Blackbox- und Whitebox-Ansatz unterscheiden
  - Differenz-Sicherheitsanalyse
    - höherwertige Maßnahmen identifizieren
    - Schutzklassenmodelle


Virenschutzkonzept
• Virenschutzstrategie
• Aktualisierungsplan für Virenschutzsoftware
• Virenmeldeverfahren
• Mitarbeiteraufklärung
Wartungskonzept
• Übersicht über zu wartende Technik
• Wartungsplan
• Ansprechpartner (intern und extern)
Notfallvorsorge
• Verfügbarkeitsanforderungen
• Notfallhandbuch
• Notfallübungen
• Verträge, Versicherungen
• Ersatzbeschaffungsplan
• Wiederanlaufplan
Datensicherheitskonzept
• Datenstruktur
• Benutzer- und Rollenkonzept
• Datenübertragungs- und Datenspeicherrichtlinien
• (Pseudonymisierung, Anonymisierung, ...)
• Kryptokonzept
• Datenträgeraustausch
• juristische Datenbegutachtung / Verträge
Grundkonzept
• Sicherheitsziele
• IT-Systeme
• Schutzbedarf
• Risikoanalyse
• Konzepte für mittleren und geringen Schutzbedarf
Konzepte für hohen Schutzbedarf
• Firewall
• Protokolle
• Kommunikation
Software-Verwaltung
• Lizenzverwaltung
• Installation
• Pflege (Updates)
Datensicherungskonzept
• Datenbestandsübersicht
• Datensicherungsplan
• Datensicherungsarchiv
• Mitarbeiterverpflichtungen
• Restaurierungsvorgehen
• Restaurierungsübungen
Infrastruktur
• fremde Dienstleistungsanbieter (Klimaanlage, Stromversorgung, USV, Gebäude (Feuer, Blitz,...), fremde Netzwerkkomponenten, ...)
• Definitionen, Verträge
hausinterne IT-Richtlinien
• Organisationsschema
• Personalrichtlinien
• Zugangsberechtigungen
• Schlüsselplan
• Vertretungsplan
• SOP's (Handhabung Sicherheitsanlagen u.a.)
• Belehrungen
• Sensibilisierungsmaßnahmen

Realisierung im IT-Verbund

- Etablierung eines IT-Sicherheitsmanagements
- Erstellung eines Grundkonzeptes auf Basis des IT-Grundschutzhandbuches
- Erarbeitung weiterer Module
- Umsetzung der Maßnahmen
- Überprüfung der Umsetzung durch Tests
- Zertifizierung des Sicherheitskonzeptes

Vorteile IT-Grundschutz

- arbeitsökonomische Anwendungsweise durch Soll-Ist-Vergleich
- kompakte IT-Sicherheitskonzepte durch Verweis auf Referenzquelle
- praxiserprobte Maßnahmen mit hoher Wirksamkeit
- Erweiterbarkeit und Aktualisierbarkeit
- Überprüfung und Nachweis des Umsetzungsgrades der Maßnahmen

Nachteile IT-Grundschutz

- zu hoher Detaillierungsgrad
- fehlende Maßnahmen für hohen und sehr hohen Schutz bedarf
- hohe Anforderungen an Ressourcen
- Risikoanalyse nicht ausreichend

Fazit

- prinzipiell IT-Grundschutz gut geeignet
- Problem der zusätzlichen Maßnahmen bei hohem Schutzbedarf
- Detaillierungsgrad zu hoch → Kombination mit ISO 27799 ?
- Ressourcenanforderungen problematisch
- hoher Aufwand für Pflege und Aktualisierung
- bei Planung berücksichtigen !

UNIVERSITÄT LEIPZIG

Institut für Medizinische Informatik, Statistik und Epidemiologie (IMISE)

Vielen Dank für die Aufmerksamkeit !

Kontakt
Ronald Speer
ronald.speer@imise.uni-leipzig.de

Vielen Dank an
Wolfgang Dolak, Barbara Heller,
Frank Meineke, Jan Ramsch