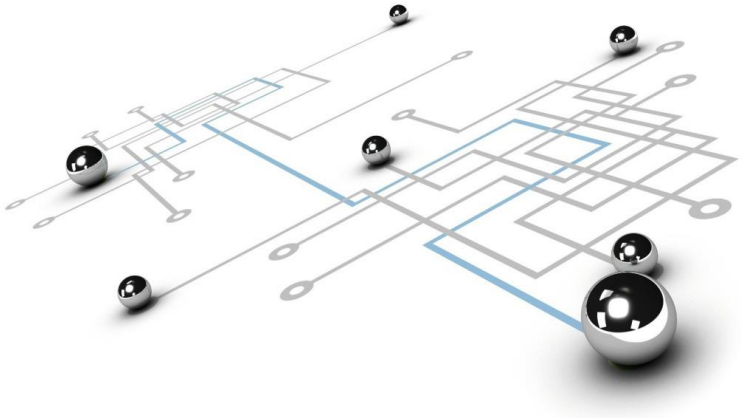
ZTG Zentrum für Telematik und Telemedizin GmbH

Vorgehen bei IT-Sicherheit in der Telemedizin

GMDS Jahrestagung
30.08.2016, München

ZTG Zentrum für Telematik und Telemedizin GmbH
Dipl.-Inform. Med. Eric Wichterich, Dipl.-Soz.Wiss. Lars Treinat

Partner des GESUNDHEITSCAMPUS NORDRHEIN-WESTFALEN



TELEMEDIZIN?

DATENSCHUTZ UND IT-SICHERHEIT?

Begriff Telemedizin

Aus: Hjelm, N. M. & Julius, H. W. (2005): Centenary of tele-eletrocardiography and telephonocardiography. In: *Journal of Telemedicine and Telecare* (11), S. 336–338.

Was meint Telemedizin?

Die WHO definiert Telemedizin allgemein als "The delivery of healthcare services, where distance is a critical factor, by all healthcare professionals using information and communication technologies for the exchange of valid information for **diagnosis, treatment and prevention** of disease and injuries, research and evaluation, and for the continuing education of healthcare providers, all in the interests of advancing the health of individuals and their communities”

Unter Telemedizin lassen sich jene medizinische Behandlungen, Diagnosen und Präventionen zusammenfassen, welche eine **räumliche Distanz** unter Behandelnden oder unter Patienten und Behandelnden durch technische Hilfsmittel **überwinden**.

Was bedeutet Telemedizin?

Telemedizin ist ein Teilbereich der Telematik im Gesundheitswesen.

Veranschaulichende Beispiele zur Abgrenzung von Telematik- von Telemedizinanwendungen:

1. Ärztliche Beratung eines Patienten mittel Videokonferenz (Telemedizin)
2. Senden von EKG-Daten über ein Mobilfunknetz vom Patienten zum Arzt zu diagnostischen Zwecken (Telemedizin)
3. Nutzung der elektronischen Gesundheitskarte zum Einlesen der Patientenstammdaten (Telematik)
4. Elektronisches Übermitteln von Abrechnungsdaten an die KV (Telematik)

Telemedizin braucht Technik! Wieso?

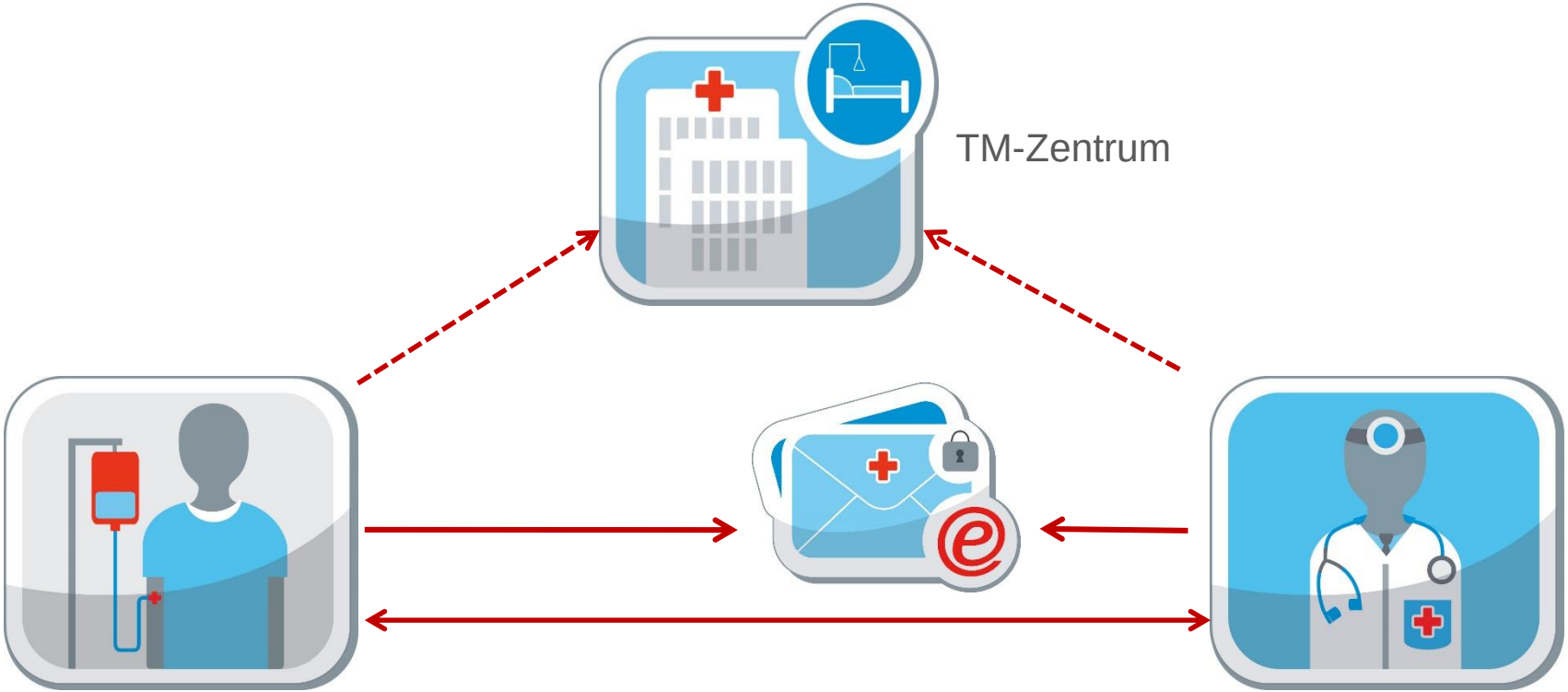
Je nach Krankheitsbild müssen unterschiedliche medizinisch erforderliche Gesundheitsdaten ermittelt und übertragen werden: **IT-Infrastruktur nötig**!

Gesundheitsdaten wie z. B. Vitalparameter, Bildaufnahmen, etc.:

1. Gewicht
2. EKG (Herzfrequenz und Herzrhythmus)
3. Blutdruck
4. Blutzuckerspiegel
5. Atemfrequenz
6. Sauerstoffsättigung
7. Röntgenbilder
8. … usw. …

Typische Kommunikationsszenarien in der Telemedizin

Szenario Home-Monitoring

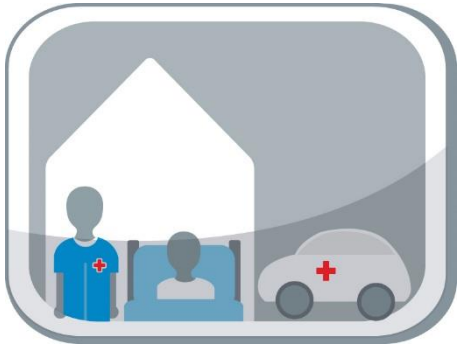


Patientin/Patient misst zu Hause z.B. Vitalparameter, macht Fotos etc.

Daten werden an behandelnde Ärztin/Arzt gesendet

Ärztin/Arzt beobachtet Datenverlauf, nimmt ggf. Kontakt zu Patientin/ Patienten auf

Szenario
Arztentlastende Versorgung mit Telemedizin

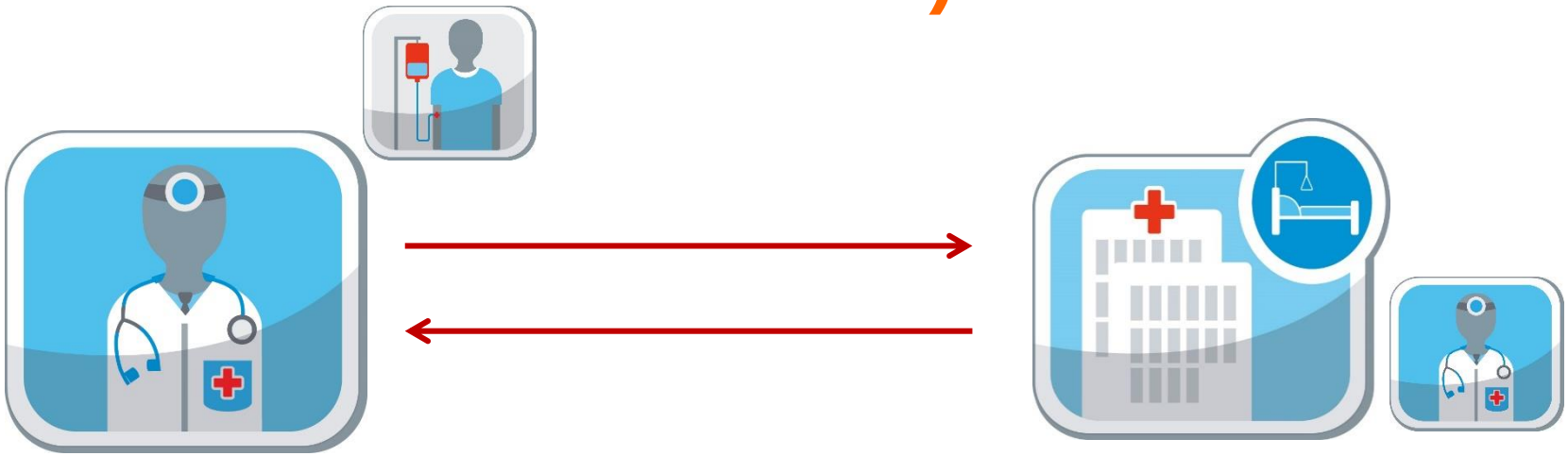


Arzthelfer/in besucht Patient/in zu Hause und nimmt mittels Telemedizin Kommunikation zu Ärztin/Arzt auf

Daten werden an behandelnde Ärztin/Arzt gesendet, ggf. Konferenzschaltung

Ärztin/Arzt sieht Daten ein und berät Arzthelfer/in

Szenario
Konferenzschaltung mittels Telemedizin (telemedizinisches Konsil)



Ärztin/Arzt untersucht Patientin/Patienten vor Ort und nimmt Kommunikation zu Expertin/Experten auf

z. B. Konferenzschaltung (Audiovideo), Teleradiologie (Senden CT-Bilder)

Expertin/Experte interpretiert Daten und berät Ärztin/Arzt über notwendige Schritte

Exkurs:

Teleradiologie nach RÖV

... ist die Untersuchung eines Menschen mit Röntgenstrahlung unter der Verantwortung eines Teleradiologen, der sich nicht am Ort der technischen Durchführung befindet und der mit Hilfe elektronischer Datenübertragung und Telekommunikation, insbesondere zur rechtfertigenden Indikation und Befundung, unmittelbar mit den Personen am Ort der technischen Durchführung in Verbindung steht.

Von Bill Rhodes from Asheville - mid-shaft humeral compound comminuted fx lat, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=5784840

Röntgenverordnung in der Fassung der Bekanntmachung vom 30. April 2003 (BGBl. I S. 604), die zuletzt durch Artikel 6 der Verordnung vom 11. Dezember 2014 (BGBl. I S. 2010) geändert worden ist

Exkurs:

Teleradiologie nach RÖV

Die RÖV beschränkt Teleradiologie grundsätzlich auf...

- ... den Nacht-,
- … Feiertags-
- ... und Wochenenddienst.

Es ist möglich, die Teleradiologie darüber hinaus zuzulassen, wenn ein entsprechendes Bedürfnis im Hinblick auf die gesundheitliche Versorgung der Patientinnen und Patienten besteht.

Von Bill Rhodes from Asheville - mid-shaft humeral compound comminuted fx lat, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=5784840

Szenario Portalklinikkonzept

Ärztin/Arzt untersucht Patientin/Patienten vor Ort in Klinik ohne Fachabteilung und nimmt Kommunikation zu Expertin/Experten auf

z. B. Konferenzschaltung (Audiovideo), Teleradiologie (Senden CT-Bilder)

Expertin/Experte in Fachklinik interpretiert Daten und berät über notwendige Schritte bzw. Verlegung

Typische Fragen hinsichtlich Telemedizin-Szenarien

Wer kommuniziert?	z.B. Sichere Handhabung der Geräte (Safety & Security)
Zu welchem Zweck kommuniziert sie/er?	z.B. Verfügbarkeit, Validität, ärztl. Haftung bei Nutzung der Daten für Therapien
Mit wem kommuniziert sie/er?	z.B. Authentizität
Wo kommuniziert sie/er?	z.B. Ort der Untersuchung → Schweigepflicht? Vertraulichkeit gegeben?
Womit kommuniziert sie/er?	z.B. Funk? Internet? Sichere Kommunikationsnetze?

Abgrenzung
Datenschutz und IT-Sicherheit

Datenschutz

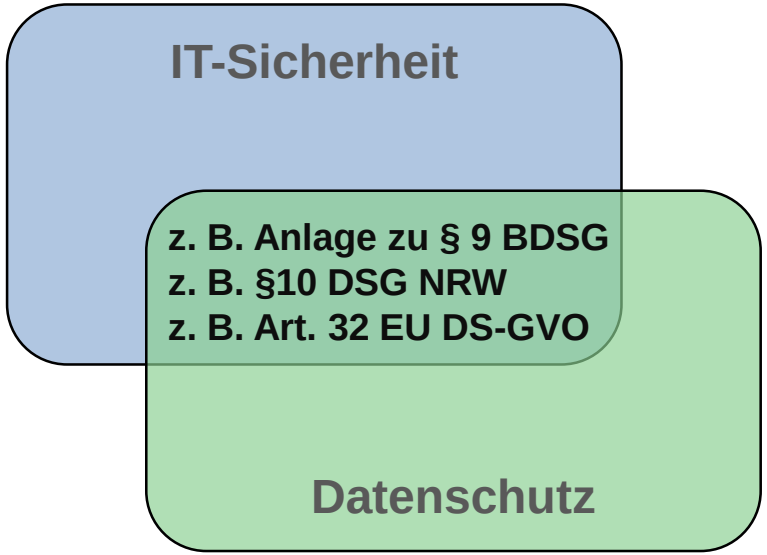
Schutz der Rechte der Betroffenen (Personen)

IT-Sicherheit

Schutz im Interesse der Betreiber der DV

IT-Sicherheit

Verantwortung des Unternehmens, Schutz im eigenen Sinne und Interesse.



Obwohl Datenschutz überwiegend technikneutral argumentiert, gibt es teilweise direkte Aussagen in Datenschutzgesetzen zur IT-Sicherheit.

Unabhängig von Datenschutzgesetzen gibt es zahlreiche haftungsrelevante rechtliche Regelungen, hier nur auszugsweise:

	Ursprung		
	D	USA	Global
Gesetzliche Regelungen			
KonTraG	☒		
GmbHG	☒		
HGB	☒		
Abgabenordnung	☒		
BDSG	☒		
Sarbanes-Oxley-Act			
Richtlinien			
G			
Ba			☒

	Ursprung		
	D	USA	Global
Standards			
Buchführung			
GoB und GoBS	☒		
Wirtschaftsprüfung			
IDW RS FAIT			
		☒	
IDW PS 331	☒		
BSI-Grundschutz	☒		
ISO 17799	☒		
Qualität			
ISO 9001:2000			☒

	Ursprung		
	D	USA	Global
Referenzmodelle			
COSO			☒
			☒

Frage: Welche Gesetze gelten für mich?

Compliance in IT-Outsourcing- Projekten
LEITFADEN
zur Umsetzung rechtlicher Rahmenbedingungen

BITKOM

Entnommen aus: Bitkom „Compliance in IT-Outsourcing-Projekten“, 2006, S. 24
https://www.bitkom.org/Publikationen/2006/Leitfaden/Leitfaden-Compliance-in-IT-Outsourcing-Projekten/BITKOM-Leitfaden-Compliance-in-IT-Outsourcing-Projekten-290806.pdf

An Maßnahmen orientierte Sicht

BDSG § 9 und Anlage zu § 9 Abs.1

„Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

(Eher veraltende Sicht:)

Anforderungen anhand technischer und organisatorischer Maßnahmen an Datenverarbeitungssystemen gemäß Anlage zu § 9 Satz 1 BDSG

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Weitergabekontrolle
5. Eingabekontrolle
6. Auftragskontrolle
7. Verfügbarkeitskontrolle
8. Trennungsgebot

An Daten orientierte Schutzziele

vgl. etwa §10 DSG NRW

1. Vertraulichkeit
2. Authentizität/Zurechenbarkeit
3. Integrität
4. Revisionsfähigkeit
5. Rechtssicherheit
6. Nicht-Abstreitbarkeit von Übermittlungen
7. Nutzungsfestlegungen
8. Validität
9. Verfügbarkeit

(s.a. „Datenschutz und Telemedizin - Anforderungen an Medizinnetze -"; Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 2002)

Art. 32 EU DS-GVO
„Sicherheit der Datenverarbeitung“

1) Unter Berücksichtigung des Stands der Technik (…) treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten

2) Bei der Beurteilung des **angemessenen Schutzniveaus** sind insbesondere die Risiken zu berücksichtigen (…)

3) Die **Einhaltung** genehmigter Verhaltensregeln gemäß Artikel 40 (…)

4) Der Verantwortliche und der Auftragsverarbeiter (…) sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese **nur auf Anweisung** des Verantwortlichen verarbeiten

Einschub: Semantisches Modell der IT-Sicherheit

Sichten	Ziele	Funktionen	Mechanismen
Security	Vertraulichkeit	Authentifizierung	Zutrittskontrolle
Verlässlichkeit/ Sicherheit des Systems	Integrität	Rechtevergabe	Zugangskontrolle
	Verfügbarkeit	Rechtekontrolle	Zugriffskontrolle
	Zurechenbarkeit	Protokollierung	Dig. Signaturen
		Fehler-kompensation	
Safety/ Dependability	Rechtsverbindlichkeit	Überwachung	Verschlüsselung
Beherrschbarkeit/ Sicherheit der Betroffenen	Revisions-fähigkeit	usw.	Gewaltenteilung usw.

(geringfügig angepasst nach Rüdiger Dierstein, 82234 Oberpfaffenhofen)

BSI Grundschutz-Standards für das methodische Vorgehen

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
- BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
- BSI-Standard 100-4: Notfallmanagement

s. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

Praktische Hinweise zu ISMS-Tools

vom BSI zum 31.12.2014 eingestellt

Auflistung des BSI zu alternativen Tools:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/GSTOOL/AndereTools/hersteller.html

Abb. CSC: http://assets1.csc.com/de/images/190_gstool_studie.jpg

CSC-Studie: GSTOOL Quo Vadis?

http://www.csc.com/de/insights/133725-csc_cybersecurity_studie_gstool_quo_vadis

IT-Grundschutz: Vorgehen

Quelle

Bundesamt für Sicherheit in der Informationstechnik

www.bsi.bund.de

IT-SICHERHEITSKONZEPTION

1. Definition des Geltungsbereichs/des IT-Verbundes
2. Strukturanalyse
3. Schutzbedarfsfeststellung
4. Modellierung
5. Basis-Sicherheitscheck
6. Ergänzende Sicherheitsanalyse/Risikoanalyse

Hinweise/Fragen

- Welcher Teil der IT-Infrastruktur wird in IT-Sicherheitskonzeption einbezogen (z.B. Organisationseinheit im Unternehmen oder abgrenzbare Prozesse)?
- → sog. „IT-Verbund“

Übernommen und angepasst aus www.bsi.bund.de: BSI-Standard 100-2 Version 2.0 und IT-Grundschutz-Profile – Anwendungsbeispiel für eine kleine Institution

IT-SICHERHEITSKONZEPTION

1. Definition des Geltungsbereichs/des IT-Verbundes
2. Strukturanalyse
3. Schutzbedarfsfeststellung
4. Modellierung
5. Basis-Sicherheitscheck
6. Ergänzende Sicherheitsanalyse/Risikoanalyse

Hinweise/Fragen

- Analyse des Zusammenspiels der Geschäftsprozesse/Anwendungen und IT
- Welche relevanten Informationen und IT-Systeme gibt es im IT-Verbund?
- Auf welchen IT-Systemen laufen die relevanten Prozesse ab?

Übernommen und angepasst aus www.bsi.bund.de: BSI-Standard 100-2 Version 2.0 und IT-Grundschutz-Profile – Anwendungsbeispiel für eine kleine Institution

IT-SICHERHEITSKONZEPTION

1. Definition des Geltungsbereichs/des IT-Verbundes
2. Strukturanalyse
3. Schutzbedarfsfeststellung
4. Modellierung
5. Basis-Sicherheitscheck
6. Ergänzende Sicherheitsanalyse/Risikoanalyse

Hinweise/Fragen

- Welchen Schutzbedarf haben die einzelnen IT-Systeme im IT-Verbund? → Ergeben sich aus DS-Anforderungen und unternehmenskritischen Erwägungen
- Kategorien: normal, hoch, sehr hoch
- Zur Einordnung sind die Beispiele in BSI 100-2, S. 49ff. sehr zu empfehlen.

Verfahren				
		Schutzaspekt	Schutzbedarf	Begründung
Verfahren 1		Vertraulichkeit	normal, hoch, sehr hoch	Text
		Integrität	normal, hoch, sehr hoch	Text
		Verfügbarkeit	normal, hoch, sehr hoch	Text

Übernommen und angepasst aus www.bsi.bund.de: BSI-Standard 100-2 Version 2.0 und IT-Grundschutz-Profile – Anwendungsbeispiel für eine kleine Institution

IT-SICHERHEITSKONZEPTION

1. Definition des Geltungsbereichs/des IT-Verbundes
2. Strukturanalyse
3. Schutzbedarfsfeststellung
4. Modellierung
5. Basis-Sicherheitscheck
6. Ergänzende Sicherheitsanalyse/Risikoanalyse

Hinweise/Fragen

- Mit Hilfe des BSI-Grundschutz-Katalogs werden die zutreffenden Bausteine für den IT-Verbund und seine Bestandteile identifiziert
  - Mögliche Gefährdungen
  - Empfohlene Maßnahmen

Übernommen und angepasst aus www.bsi.bund.de: BSI-Standard 100-2 Version 2.0 und IT-Grundschutz-Profile – Anwendungsbeispiel für eine kleine Institution

IT-SICHERHEITSKONZEPTION

1. Definition des Geltungsbereichs/des IT-Verbundes
2. Strukturanalyse
3. Schutzbedarfsfeststellung
4. Modellierung
5. Basis-Sicherheitscheck
6. Ergänzende Sicherheitsanalyse/Risikoanalyse

Hinweise/Fragen

- Es folgt ein Abgleich der vorgenommenen Modellierung mit dem IST-Zustand: Sind die vom BSI empfohlenen Maßnahmen getroffen worden?
- Verbleiben Maßnahmen?
- Bzw. Neukonzeption entlang der empfohlenen Maßnahmen.

Übernommen und angepasst aus www.bsi.bund.de: BSI-Standard 100-2 Version 2.0 und IT-Grundschutz-Profile – Anwendungsbeispiel für eine kleine Institution

IT-SICHERHEITSKONZEPTION

1. Definition des Geltungsbereichs/des IT-Verbundes
2. Strukturanalyse
3. Schutzbedarfsfeststellung
4. Modellierung
5. Basis-Sicherheitscheck
6. Ergänzende Sicherheitsanalyse/Risikoanalyse

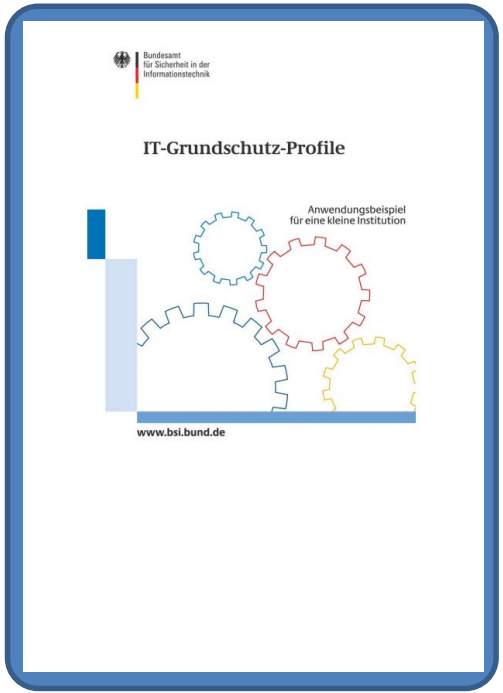
Hinweise/Fragen

- Sollten bei der Schutzbedarf-Ermittlung ein hoher oder sehr hoher Schutzbedarf festgestellt sein, ist eine ergänzende Sicherheitsanalyse durchzuführen und zu dokumentieren.
- **Zusätzliche Arbeitsschritte für die betreffenden Komponenten**
  - Erstellung Gefährdungsübersicht
  - Ermittlung zusätzlicher Gefährdung (eigene spezifische Analyse!)
  - Gefährdungsbewertung
  - Behandlung von Risiken
  - Konsolidierung

Übernommen und angepasst aus www.bsi.bund.de: BSI-Standard 100-2 Version 2.0 und IT-Grundschutz-Profile – Anwendungsbeispiel für eine kleine Institution

Veranschaulichende Beispiele

www.bsi.bund.de



www.bsi.bund.de

www.kbv.de

Vielleicht in baldiger Zukunft?

Telemedizin als Mehrwertanwendung der Telematikinfrastruktur?

Einheitliche PKI mit großer Reichweite hinsichtlich der Teilnehmerinnen und Teilnehmer, z.B.:

- → Einbindung BfDI und BSI
- → Starke Kryptographie (basierend auf elliptischen Kurven)
- → Eindeutige, bestätigte elektronische Identitäten
- → Ende-zu-Ende-Verschlüsselung (sichere Kommunikation)
- → Sichere eSignaturen (nach Bedarf fortgeschritten/qualifiziert): Basis für dauerhafte eArchivierung

FAZIT

Das Vorhandensein **technischer Schutzmaßnahmen**
und **Sicherheitseinrichtungen**
ist keine alleinige Garantie
für IT-Sicherheit!

Notwendig ist auch
ein **verantwortlicher Umgang**
mit Daten und Systemen!

IMMER: Gehirn eingeschaltet lassen!

Beispiel gefällig?

Aktenvernichtung: Aber klar doch! …???

MDR Thüringen berichtet Februar 2016:
(http://www.mdr.de/thueringen/sued-thueringen/patientenakten-konfetti100.html, Zugriff 26.08.2016):

Patientenakten als Faschingskonfetti
In Dermbach im Wartburgkreis wurden während der närrischen Tage Patientenakten als Konfetti verwendet. Patientennummern und Diagnosen waren auf den Papierstreifen zu lesen. Die geschredderten Akten stammen womöglich aus einem medizinischen Versorgungszentrum in Kaltennordheim. Nach MDR THÜRINGEN-Informationen sind unter den Schnipseln auch Dienstpläne des Ärztlichen Notdienstes. Der Datenschutzbeauftragte ermittelt.

Bildrechte: MDR/Ruth Breer

ZTG
Zentrum für Telematik und Telemedizin GmbH

Fragen?

Wir sind für Sie da!

Dipl.-Inform. Med.
Eric Wichterich
e.wichterich@ztg-nrw.de

Dipl.-Soz.Wiss.
Lars Treinat
l.treinat@ztg-nrw.de

ZTG Zentrum für Telematik und Telemedizin GmbH
Universitätsstraße 142
44799 Bochum
Geschäftsführer: Rainer Beckers, M.P.H., M.A.; Lars Treinat, Dipl.-Soz.Wiss.

Abb. © Sebastian Kaulitzki - Fotolia