Seminar 7: IT-Sicherheit – notwendige Voraussetzung für Datenschutz

- Christoph Isele
- Cerner, Lead Regulatory Affairs Strategist

- *Fachtagung Datenschutz im Gesundheitswesen 6./7. Mai 2021*

Agenda …

- Digitalisierung und Vernetzung
- Datenschutz - TOMs
- IT Sicherheit - gesetzliche Regelungen
- IT Sicherheitskonzept
- Aktuelle Entwicklung bei Medizingeräten

- Christoph Isele

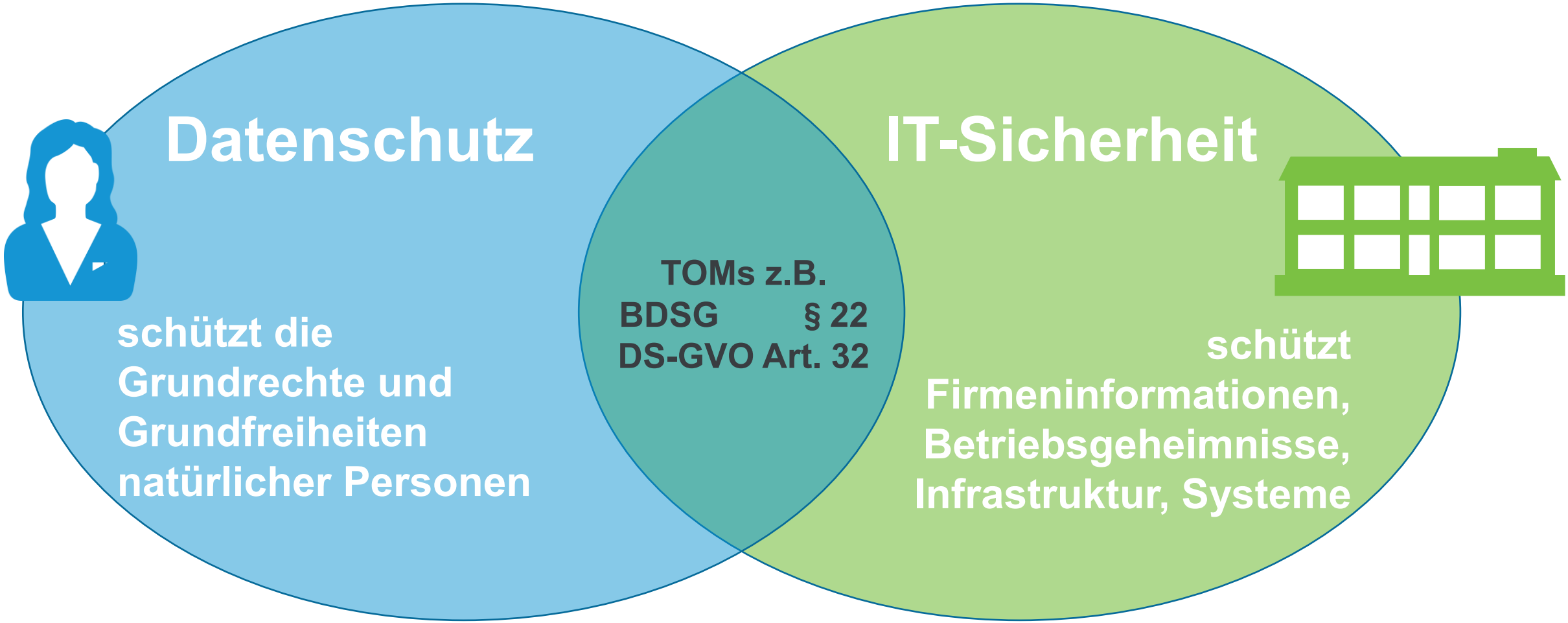
  bvitg Leiter AG Datenschutz und IT Sicherheit

  Cerner European IP

  Lead Regulatory Affairs Strategist

- Christoph.isele@cerner.com
- +49 173 2385940

Datenschutz vs. IT-Sicherheit



Datenschutz und IT Sicherheit sind Querschnittsaufgaben

Geschäftsinteresse / Verfahren

Eingesetzte Technik

Mitarbeiter / Schulung

Verzeichnis der Verarbeitungstätigkeiten (Auszug)

Dieses Verzeichnis enthält sämtliche folgenden Angaben:

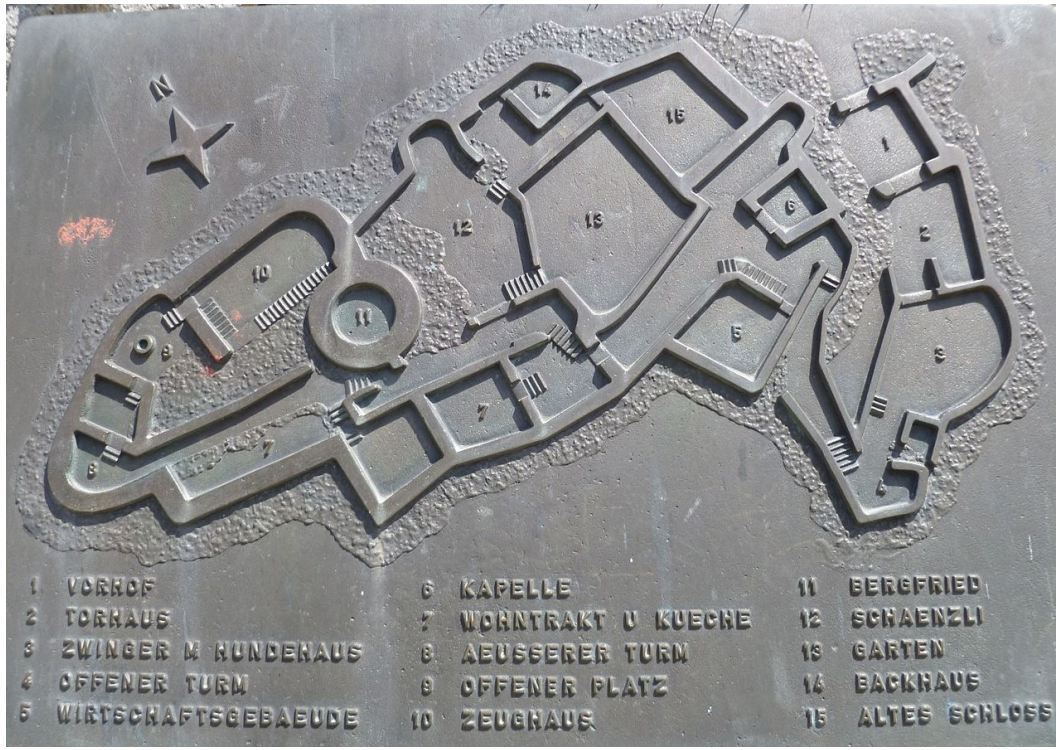
- a) den Namen und die Kontaktdaten des Verantwortlichen …
- b) die Zwecke der Verarbeitung;
- c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- d) die Kategorien von Empfängern, … ;
- e) gegebenenfalls Übermittlungen von personenbezogenen Daten ….
- f) wenn möglich, die vorgesehenen Fristen für die Löschung …
- g) wenn möglich, eine allgemeine Beschreibung der TOMs …

Digitalisierung und Vernetzung

Vernetzung - rechnergestützte strukturierte Kommunikation

- Medizinische Geräte
- Abteilungssysteme
- Telematik Infrastruktur
- PDSG, KHZG, GPVG, …
- Terminplanung
- Patientenportale
- Meldepflichten
- Übermittlung diagnostische Bilder
- Onkologisch Fallbesprechung
- …

IT-Sicherheit Anfang 21tes Jahrhundert



- Perimeter Schutz
- Wenige kontrollierbare Zugänge
- Isolierbare Schutzbereich im Kernbereich

- Netzwerk, Firewall
- Server: Systeme, Härtung
- Proprietäre System
- Endgeräte: Malware Schutz

IT Landschaft 2021 - Herausforderungen

- „Kein Gerät ohne IP Anschluss“
- Mobilität: WLAN statt Kabel
- Lösungen brauchen regelmäßige / permanente Verbindung nach Außen
- Fernwartung VPN Tunnel
- Web Architektur
- Mitarbeiter Awareness

Die „Gegenseite“ hat sich professionalisiert

- Viren, Würmer und Trojaner
- Gezielte Angriffe aus Rache gibt es immer noch

- Mehrstufige Angriffe
- Halbautomatische Angriffe
- Phishing
- Social engineering
- Angreifer könnte auch in einem anderen Kontinent sitzen

Rechtliche Grundlagen
Datenschutz - technische Maßnahmen

Grundlagen - Gesetze

- VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES (DSGVO)
- BDSG
- Landeskrankenhausgesetze
- Sozialgesetzbücher
- …

z.B. Digital Green Certificate

DSGVO: Kapitel I - Allgemeine Bestimmungen

Artikel 5: Grundsätze für die Verarbeitung personenbezogener Daten

- Schutzziele
  - Integrität
  - Vertraulichkeit

  - technisch organisatorische Maßnahmen

DSGVO: Kapitel IV - Verantwortlicher und Auftragsverarbeiter

- Insbesondere Artikel 32 Sicherheit der Verarbeitung
- Präventiv Schutzmaßnahmen;

- Artikel 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde aber auch Informationspflicht wenn eine Verletzung des Schutzes erfolgte

- Auch Artikel 35 Datenschutz-Folgenabschätzung

BDSG §22

- Greift die Zulässigkeit der Verarbeitung von Gesundheitsdaten aus Art 9 (h) DSGVO auf und
- Ergänzt durch Absatz (2) u.a. die Forderung nach
  - 1. technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt,
  - 2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,

BDSG §22

- 8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
- 9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Landeskrankenhaus Gesetze

- Viele enthalten mehr oder weniger pauschal die Verpflichtung technisch organisatorische Maßnahmen zu treffen

- Beispiel Rheinland-Pfalz
- Der Krankenhausträger hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich und angemessen sind, um die Beachtung der in den Absätzen 1 bis 7 enthaltenen Bestimmungen zu gewährleisten.

Zusammenfassung

- Es gibt die Verpflichtung technisch organisatorische Maßnahmen zu treffen
- Es gibt aber keine konkreten Maßnahmen, die umzusetzen sind
- Idealerweise trotzdem aufschreiben und regelmäßig überprüfen

In der DSGVO explizit erwähnte Technische Maßnahmen
PbyD: Privacy Enhancing Technology

DS-GVO Artikel 32

… , diese Maßnahmen schließen unter anderem Folgendes ein:

- a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Pseudonymisierung (Definition DS-GVO Art. 4)

- „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

- Dieser Pseudonymisierungsbegriff geht von einer getrennten Speicherung identifizierender Daten und “Nutzdaten” aus, ein anderer Name in der Akte wäre ein Alias.

Pseudonymisierung

- Auch bei einer Pseudonymisierung der Daten muss immer die Rechtmäßigkeit der Verarbeitung gewährleistet sein. Insbesondere muss bei der Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 ein Erlaubnistatbestand zur Pseudonymisierung vorhanden sein.
- Pseudonyme Daten gelten nur dann als pseudonym, wenn der die Daten Verarbeitende keine Möglichkeit hat, die Zuordnungsvorschrift zwischen Pseudonym und Personenkennung zu erhalten und eine „De-Pseudonymisierung“ mittels dieser Liste vornehmen kann.
- Pseudonymisierte Daten sind nicht mit anonymisierten Daten gleichzusetzen. D.h., dass für pseudonymisierte Daten alle Anforderungen der DSGVO gelten. Pseudonymisierung verringert lediglich die Verknüpfbarkeit eines Datenbestands mit der wahren Identität einer betroffenen Person.

De- Identifikationsmöglichkeiten

- Primäre oder direkte Identifikationsmerkmale
  - Ein oder mehrere Attribute, die eine eindeutige Zuordnung erlauben
  - Bild, biometrische Merkmale
  - Primäre Identifikationsmerkmale sind bei der Pseudonymisierung abzutrennen
- Sekundäre Identifikationsmerkmale
  - Attribute können durch zusätzliche Informationen zu Identifizierung herangezogen werden (typische Beispiele aus der Anonymisierung)
  - Sekundäre Identifikationsmerkmale können durch Techniken aus der Anonymisierung so verändert werden, dass ein Rückschluss auf die Indentität des Betroffenen kaum mehr möglich ist. Damit sinkt aber die Aussagekraft der Daten.

Anonymisierung bei Gesundheitsdaten

- Viele Attribute sind spezifisch, eine Kombination kann oft quasi identifizierend sein
- Bei der Anonymisierung geht Information verloren, in der Medizin hat man oft nicht so viele Fälle die den Verlust ausgleichen
- Mustererkennung schreitet rasch voran, die Grenze für die „nicht-Auffindbarkeit“ verschiebt sich laufend

Literatur

gmds AG DIG

https://www.gesundheitsdatenschutz.org/html/pseudonymisierung_anonymisierung.php

Fachtagung DiG 2020: Vortrag Herr Eiermann

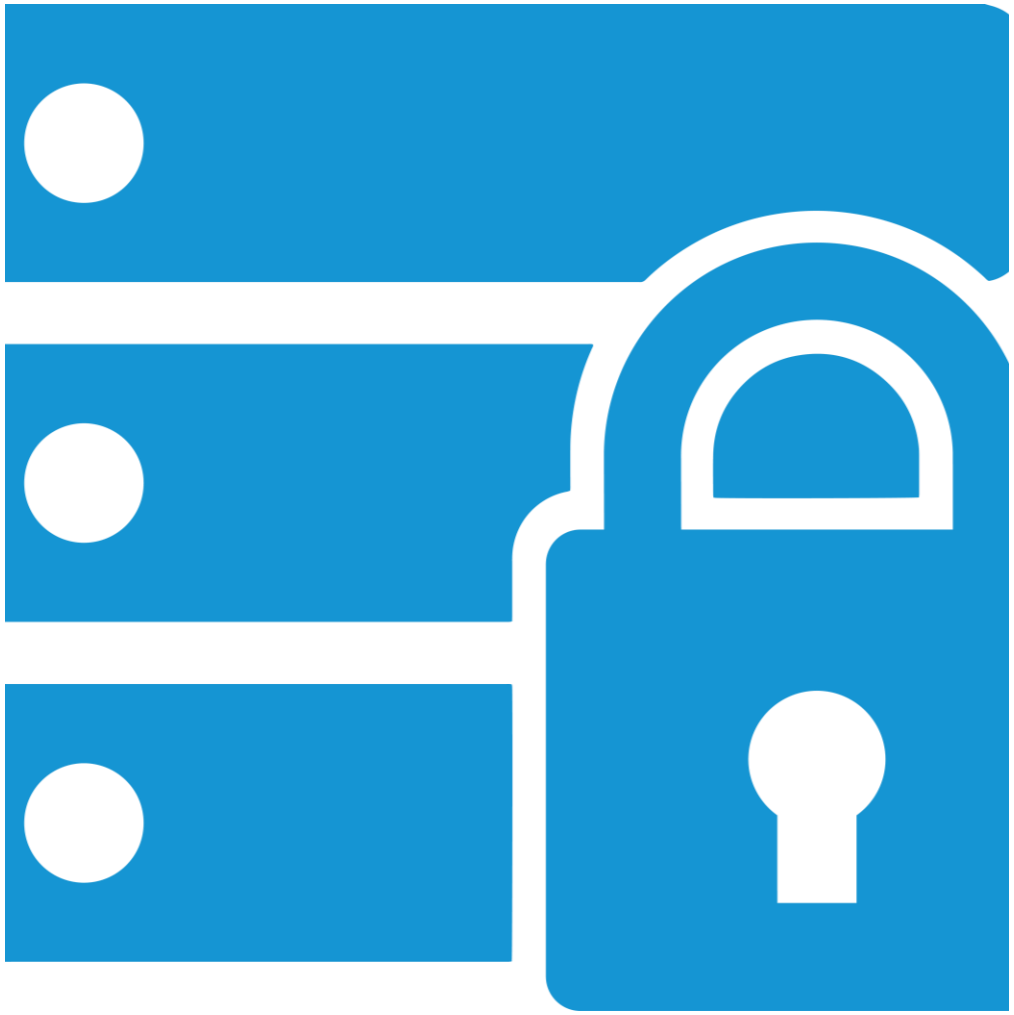
https://www.fachtagung-gesundheitsdatenschutz.de/download/2020/04a3_Datenschutz_Wegbegleiter_Gesundheitsversorgung.pdf

bitkom Leitfaden: Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens

https://www.bitkom.org/Bitkom/Publikationen/Anonymisierung-und-Pseudonymisierung-von-Daten-fuer-Projekte-des-maschinellen-Lernens

IT-Sicherheit: z.B. Pseudonymisierung bei Protokollen

Verschlüsselung



- In der DSGVO nicht weiter definiert
- Soll verhindern, dass Dritte Informationen interpretieren können, wenn sich nicht verhindern lässt, dass diese auf die Daten zugreifen können, z.B. verschlüsselte Nachrichten in einem Mail System

Transport Verschlüsselung (encryption in motion)

- Programm-Programm Kommunikation zwischen Clients und Server
  - Web interface: https
  - Fat Clients: teilweise proprietäre Protokolle
- Programm-Programm Kommunikation zwischen Servern
  - https (?) und proprietäte Protokolle
  - Manchmal wird aber aus Performance Überlegungen darauf verzichtet
- Beispiel: Transport Verschlüsselung bei Kommunikationsanwendung
  - Sichere Messenger Dienste mit Ende-zu-Ende Verschlüsselung bei eingeschränkter Funktion
  - Verschlüsselung von Inhalten, nur für den bekannten Adressaten lesbar (Schlüsselaustausch erforderlich, s/mime); eher bei oft genutzten Partnern
  - Mailclient: üblicherweise nur Verschlüsselung zwischen Client/Server des Providers,

Speicher Verschlüsselung (encryption in rest)

- Festplatten Verschlüsselung
- DB Verschlüsselung
- Ablage von verschlüsselten Dateien, XML Strukturen
- Ablage von verschlüsselten Datenbankfeldern (Herausforderung Länge der zu speichernden Information)

- Festplatten und DB Verschlüsselung helfen vor allem bei Angriffen von außen, weil “berechtigte” Benutzer die Daten entschlüsselt bekommen.
- Kryptographie Konzept erstellen, je nach Angriffsszenarien kann eine Verschlüsselung helfen.
- Schlüsselmanagement wenn möglich in der Hand des Krankenhauses

Krypto-Konzept: Kann ich die Daten verschlüsseln?

- Transparente Verschlüsselung gegen Angriffe von außen
- Bei Diebstahl verschlüsselter Datenträger - Meldung als Datenpanne?
  Wird unterschiedlich entschieden
- Arztindividuelle Verschlüsselung von sensiblen Informationen?
  Eher schwierig, weil dann auch Sonderfälle wie Nichtverfügbarkeit, Ausscheiden des Arztes abgebildet werden müssen.
- Vertretungsregelung?
  Ein Schutz der Daten durch Verschlüsselung sollte auch immer ein Notfallkonzept enthalten.

Gesetzliche Verpflichtung zu IT-Sicherheit

In Europa …

- enisa - europäische Behörde
- VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. April 2019
- Kritische Infrastruktur: Sektor Health
  - https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health
  - Cloud Security for Healthcare Services (Report)
  - Security and Resilience in eHealth Infrastructures and Services
  - Procurement Guidelines for Cybersecurity in Hospitals

In Europa …

- RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
  - Umsetzung in nationales Recht
    - in D: IT Sicherheitsgesetz
    - IT-SiG 2.0 verabschiedet 04/2021
  - NIS Version 2.0 wird erarbeitet

Im Gesundheitswesen …

Symbolbild

- Krankenhäuser sollten ein ISMS aufbauen,
  - KRITIS Häuser müssen entsprechende Zertifikate regelmäßig einreichen
  - §75c SGB V … nach Stand der Technik angemessene organisatorische und technische Vorkehrungen … treffen
- Niedergelassener Bereich KBV
  - Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT Sicherheit
- Telematik Infrastruktur

Beispiel Branchenspezifischer Sicherheitsstandard


DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus

Gesamtdokument

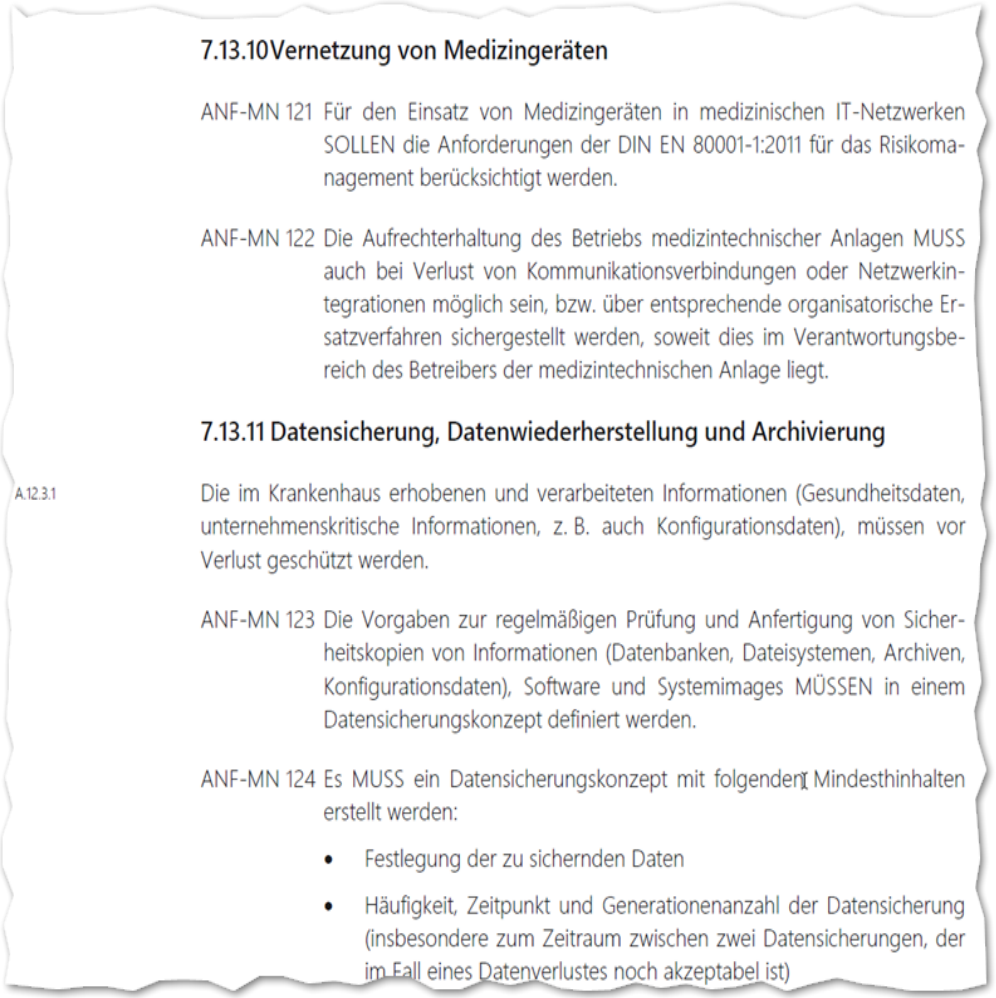
22.10.2019

Gemäß Feststellungsbescheid vom 22.10.2019 zur Gewährleistung der Anforderungen nach § 8a Absatz 1 BSIG geeignet.

TLP-Klassifikation: WHITE
Kategorie: öffentlich
Version: 1.1

- Risikomanagement (Nähe zur ISO/IEC 2700x)
- Identifikation der kritischen Dienstleistung
  - Kernprozesse
  - Kritische Anwendungssysteme
- Anforderungen und Maßnahmenempfehlungen zur Umsetzung
- 168 Anforderungen, 88 Seiten
- MUSS, SOLL, KANN Anforderungen

Inhalt des B3S Gesundheitsversorgung



7.13.10 Vernetzung von Medizingeräten

ANF-MN 121 Für den Einsatz von Medizingeräten in medizinischen IT-Netzwerken SOLLEN die Anforderungen der DIN EN 80001-1:2011 für das Risikomanagement berücksichtigt werden.

ANF-MN 122 Die Aufrechterhaltung des Betriebs medizintechnischer Anlagen MUSS auch bei Verlust von Kommunikationsverbindungen oder Netzwerkintegrationen möglich sein, bzw. über entsprechende organisatorische Ersatzverfahren sichergestellt werden, soweit dies im Verantwortungsbereich des Betreibers der medizintechnischen Anlage liegt.

7.13.11 Datensicherung, Datenwiederherstellung und Archivierung

A.12.3.1 Die im Krankenhaus erhobenen und verarbeiteten Informationen (Gesundheitsdaten, unternehmenskritische Informationen, z. B. auch Konfigurationsdaten), müssen vor Verlust geschützt werden.

ANF-MN 123 Die Vorgaben zur regelmäßigen Prüfung und Anfertigung von Sicherheitskopien von Informationen (Datenbanken, Dateisystemen, Archiven, Konfigurationsdaten), Software und Systemimages MÜSSEN in einem Datensicherungskonzept definiert werden.

ANF-MN 124 Es MUSS ein Datensicherungskonzept mit folgenden Mindesthinhalten erstellt werden:

- Festlegung der zu sichernden Daten
- Häufigkeit, Zeitpunkt und Generationenanzahl der Datensicherung (insbesondere zum Zeitraum zwischen zwei Datensicherungen, der im Fall eines Datenverlustes noch akzeptabel ist)

- Informationssicherheitsmanagementsystem (ISMS)
- Organisation der Informationssicherheit
- Meldepflichten nach § 8b Absatz 4 BSI-Gesetz
- Betriebliches Kontinuitätsmanagement
- Asset Management
- Robuste/resiliente Architektur
- Physische Sicherheit
- Personelle und organisatorische Sicherheit
- Vorfallerkennung und Behandlung
- Überprüfungen im laufenden Betrieb
- Externe Informationsversorgung und Unterstützung
- Lieferanten, Dienstleister und Dritte
- Technische Informationssicherheit

Schutzziele des B3S Gesundheitsversorgung

- VERFÜGBARKEIT von Dienstleistungen, Funktionen eines Informationssystems, IT-Systems, IT-Netzinfrastruktur oder auch von Informationen ist dann gegeben, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.
- INTEGRITÄT bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.
- VERTRAULICHKEIT stellt den Schutz vor unbefugter Preisgabe von Informationen sicher. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in zulässiger Weise zugänglich sein.
- AUTHENTIZITÄT der Informationen ist sichergestellt, wenn sie von der angegebenen Quelle erstellt wurden.
- PATIENTENSICHERHEIT als die Freiheit von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen. Dies schließt auch die Vermeidung einer nachhaltigen psychischen Belastung ein.
- BEHANDLUNGSEFFEKTIVITÄT stellt die wirksame Behandlung des Patienten unter Benutzung von Informationen und wirksamen Therapiemaßnahmen, ggf. auf Basis eines Informationsaustausches zwischen unterschiedlichen verantwortlichen Organisationseinheiten, sicher.

Beispiel Vertragsärztlicher Bereich

KBV KASSENÄRZTLICHE BUNDESVEREINIGUNG

RICHTLINIE NACH § 75B SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

- Die Richtlinie adressiert die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme in der vertragsärztlichen – psychotherapeutischen Praxis.
- Die Richtlinie legt technischen Anforderungen fest und beschreibt das Mindestmaß der zu ergreifenden Maßnahmen, um die Anforderungen der IT-Sicherheit zu gewährleisten.
- Mit der Umsetzung der Anforderungen werden die Risiken der IT-Sicherheit minimiert.
- Bei der Umsetzung können Risiken auch an Dritte, wie IT-Dienstleister oder Versicherungen, übertragen oder durch den Verantwortlichen akzeptiert werden.

Inhalt

ANLAGE 2

Zusätzliche Anforderungen für mittlere Praxen

	Zielobjekt	Anforderung	Erläuterung	Geltung ab
	Software: Rechner-Programme, mobile Apps und Internet-Anwendungen			
1.	Mobile Anwendungen (Apps)	Minimierung und Kontrolle von App-Berechtigungen	Minimierung der App-Berechtigungen.	01.04.2021
2.	Internet-Anwendungen	Zugriffskontrolle bei Webanwendungen	Sicherstellung von Berechtigungen.	01.01.2022
	Hardware: Endgeräte und IT-Systeme			
3.	Endgeräte	Nutzung von TLS	Benutzer sollten darauf achten, dass zur Verschlüsselung von Webseiten TLS verwendet wird.	01.01.2022
4.	Endgeräte	Restriktive Rechtevergabe	Restriktive Rechtevergabe.	01.01.2022
5.	Endgeräte mit dem Betriebssystem Windows	Sichere zentrale Authentisierung in Windows-Netzen	In reinen Windows-Netzen SOLLTE zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden.	01.07.2022
6.	Smartphone und Tablet	Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten	Es sollte eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten erstellt werden.	01.07.2022

- Drei Klassen von Praxen
  - Praxen
  - Mittlere Praxen
  - Großpraxen
- Anforderungen bezogen auf
  - Rechner-Programme, mobile Apps und Internet Anwendungen
  - Hardware Endgeräte
  - Medizinische Großgeräte
  - Dezentrale Komponenten der Telematikinfrastruktur

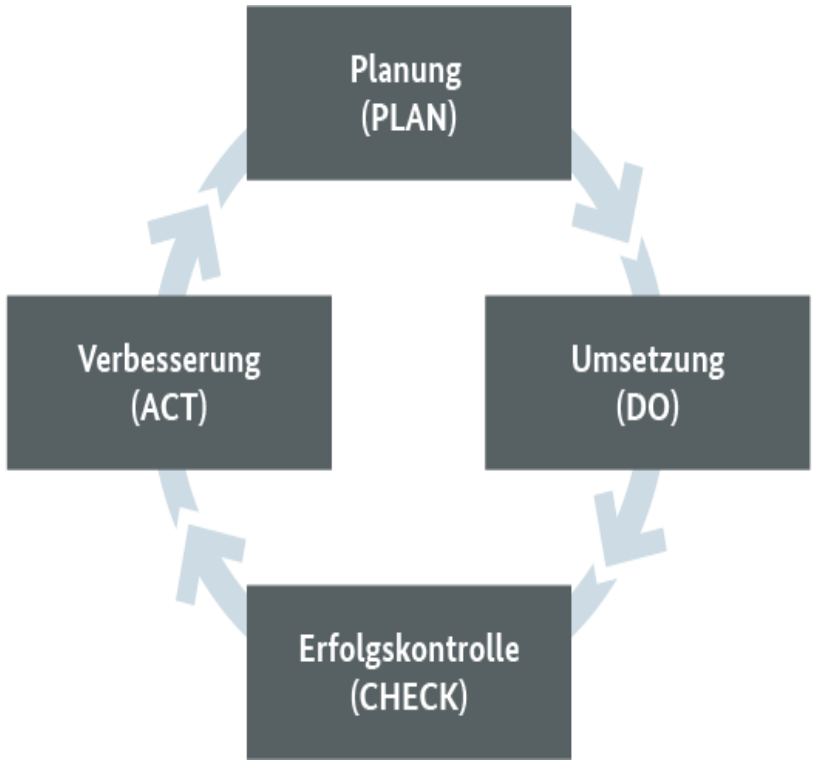
KBV KASSENÄRZTLICHE BUNDESVEREINIGUNG

RICHTLINIE ZUR ZERTIFIZIERUNG NACH § 75B ABSATZ 5 SGB V

[KBV_ISAP_RL_ZERT_P75B_SGBV]

- Ergänzend setzt die KBV auf die Zertifizierung von Dienstleistern
- Typischerweise Mitarbeiter von Hauptlieferanten
- Herausforderung Komplexität der Praxis

Kommentar: Management System



- Bei kleinen „standardisierbaren“ Einrichtungen externer Dienstleister, wenn man mit dessen Konzept leben kann

- Eigener KnowHow Aufbau
  - Methode (Wissen)
  - Analyse der eingesetzten Technik
  - Beschreibung Geschäftsprozesse
  - Beschreibung Rechte
  - …

Kommentar: Meldewesen - Austauschforen - CERT

- Meldewesen ist ein wichtiger Teil der Sicherheitsinfrastruktur (IT SiG § 8b)
- Computer Emergency Response Team (CERT)

IT Sicherheitskonzept

Material

Leitfaden für die Erstellung eines IT-Sicherheitskonzeptes

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.

Arbeitsgruppe „Datenschutz und IT Sicherheit“

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)

Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

ZTG Zentrum für Telematik und Telemedizin GmbH (ZTG)

- Arbeitshilfe zu finden bei der gmds Arbeitsgruppe
- Leitfaden zur Erstellung eines IT-Sicherheitskonzeptes

Ein Leitfaden zur Erstellung eines IT Sicherheitskonzepts

- Ein Betreiber einer Kritischen Infrastruktur, ein Krankenhaus nach §75c SGB V eine Arztpraxis nach §75b müssen konkrete Vorgaben erfüllen.

- Der Leitfaden zeigt exemplarisch die Kernelemente eines IT Sicherheitskonzeptes und richtet sich an Projekte, Register und andere nicht regulierte Verarbeiter von Gesundheitsdaten

Konzept des Leitfadens

- Exemplarisches Inhaltverzeichnis
- Erläuterung was in den Kapiteln behandelt werden sollte
- Ein paar Beispiele
- Verweis auf Literatur

(Muster-)Inhaltverzeichnis eines IT Sicherheitskonzeptes

1. Zusammenfassung / Management Summary
2. Einleitung mit Darstellung der Ziele des IT-Sicherheitskonzeptes
3. Begriffsbestimmungen
4. Überblick Organisation
5. Überblick Zuständigkeiten
6. Darstellung der Rahmenbedingungen
7. Beschreibung der Systemarchitektur

(Muster-)Inhaltverzeichnis eines IT Sicherheitskonzeptes

8. Darlegung des Schutzbedarfs
9. Berücksichtigte Vorgaben
10. Anforderungen
11. Maßnahmen
12. Darlegung der Restrisiken
13. Kontrolle und Fortschreibung des IT-Sicherheitskonzeptes
14. Mitgeltende Unterlagen

Beispiel ISO/IEC Normenfamilie 2700x

DEUTSCHE NORM März 2015

DIN ISO/IEC 27001

DIN

ICS 35.040

Ersatz für
DIN ISO/IEC 27001:2008-09

Informationstechnik –
IT-Sicherheitsverfahren –
Informationssicherheits-Managementsysteme – Anforderungen
(ISO/IEC 27001:2013 + Cor. 1:2014)

Information technology –
Security techniques –
Information security management systems – Requirements (ISO/IEC 27001:2013 + Cor. 1:2014)

Technologies de l'information –
Techniques de sécurité –
Systèmes de gestion de sécurité de l'information – Exigences (ISO/CEI 27001:2013 + Cor. 1:2014)

- ISO/IEC 27001 (Informationssicherheits-Managementsysteme – Anforderungen)
- ISO/IEC 27002 (Leitfaden für das Informationssicherheits-Management)
- ISO/IEC 27003 (Informationssicherheitsmanagementsystem-Einführungsleitlinie)
- ISO/IEC 27004 (Informationssicherheits-Management - Überwachung, Messung, Analyse und Evaluation)
- ISO/IEC 27005 (Informationssicherheits-Risikomanagement)
- …

DEUTSCHE NORM März 2015

DIN ISO/IEC 27001

DIN

ICS 35.040

Ersatz für
DIN ISO/IEC 27001:2008-09

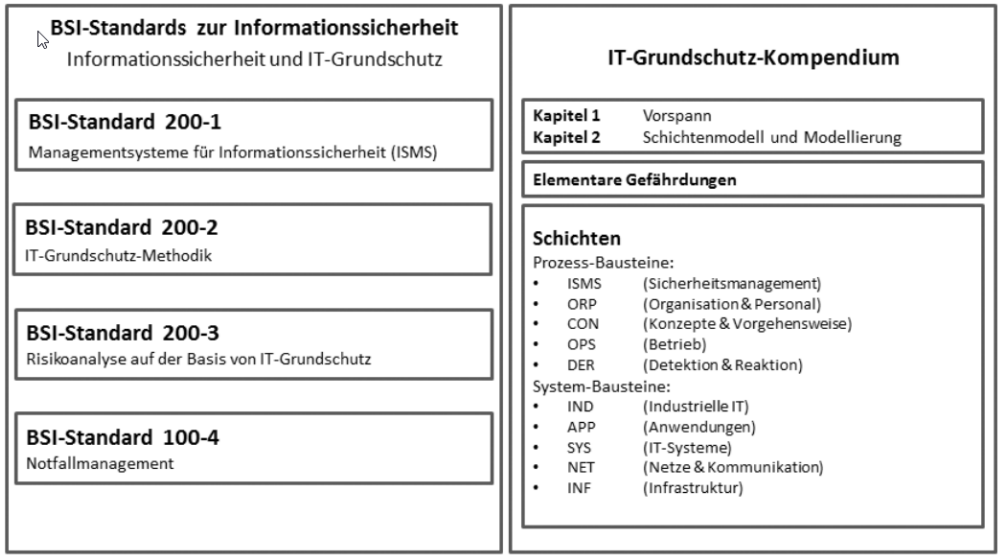
Informationstechnik –
IT-Sicherheitsverfahren –
Informationssicherheits-Managementsysteme – Anforderungen
(ISO/IEC 27001:2013 + Cor. 1:2014)

Information technology –
Security techniques –
Information security management systems – Requirements (ISO/IEC 27001:2013 + Cor. 1:2014)

Technologies de l'information –
Techniques de sécurité –
Systèmes de gestion de sécurité de l'information – Exigences (ISO/CEI 27001:2013 + Cor. 1:2014)

- Norm muss man kaufen
- Es gibt Schulungen zum Einstieg
- Großes Angebot an Beratungsdienstleistung
- Es gibt verschiedene Werkzeuge
- Manchmal empfiehlt sich eine Kombination aus Berater und Werkzeug

Beispiel: IT Grundschutz mit BSI Standards



- Die Grundschutz Methodik 200-2 ist kompatibel zur ISO 27000
- Das Grundschutzkompendium bietet prozess- und systemorientierte Bausteine mit Anforderungen
- Der Baustein CON.2 enthält den Datenschutz
- Ergänzend gibt es den Katalog der elementaren Gefährdungen
- … Werkzeuge …

Zusammenfassung

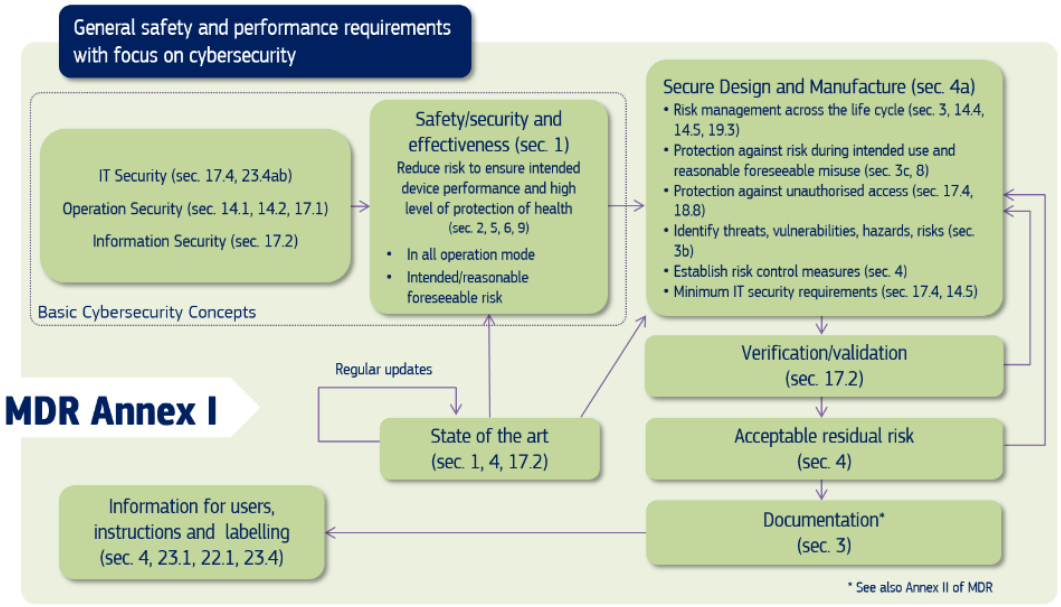
- IT Sicherheit beginnt mit einem Managementsystem
- Dabei entstehen Konzepte, Richtlinien, …
- Mitarbeiter müssen geschult werden
- Richtlinien und Einhaltung müssen regelmäßig überprüft werden
- Transparenz und Dokumentation für Nachfragen von außen

Vernetzte Medizinprodukte

IT Sicherheit und Medizinprodukt

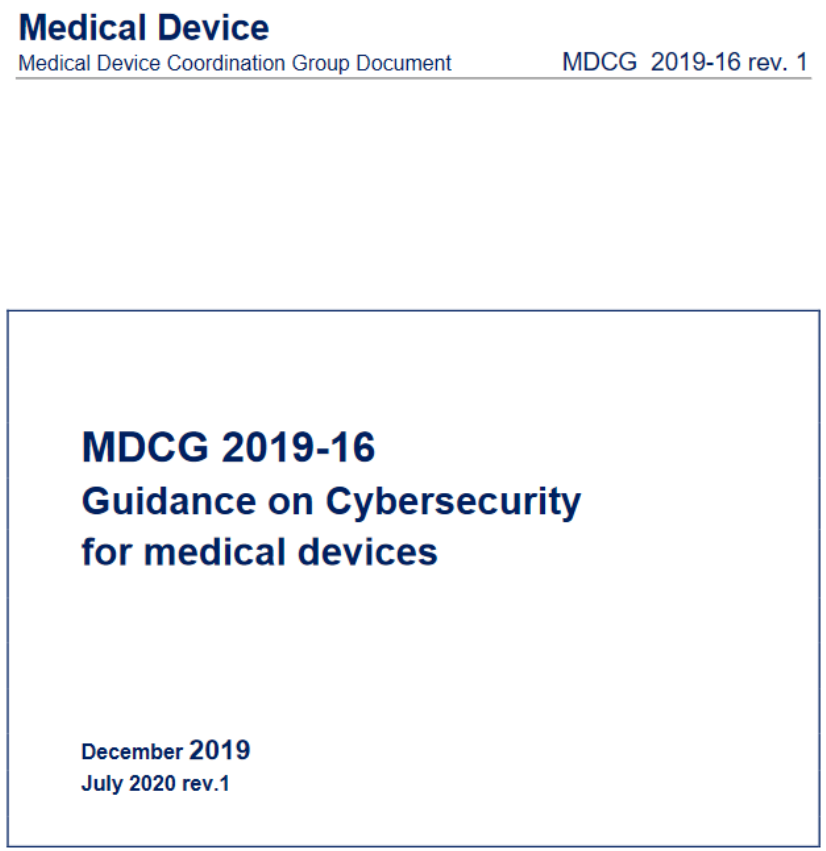
- Hersteller erklärt, dass er die Anforderungen einhält (Konformitätserklärung)

MDR: Software als Medizinprodukt



- MDR Anhang I
  GRUNDLEGENDE SICHERHEITS- UND LEISTUNGSANFORDERUNGEN
  - 17. Programmierbare Elektroniksysteme — Produkte, zu deren Bestandteilen programmierbare Elektroniksysteme gehören, und Produkte in Form einer Software
    - Fordert dass die Hersteller beim Entwurf Mindestanforderungen an IT-Sicherheit festlegen bzw. berücksichtigen
  - 23. Kennzeichnung und Gebrauchsanweisung
    - In die Gebrauchsanweisung soll auch der Hinweis aufgenommen werden, dass schwerwiegende Vorfälle im Zusammenhang mit der IT-Sicherheit an den Hersteller zu melden sind.

Medical Device Coordination Group



- MDCG 2019-16 Guidance on Cybersecurity for medical devices
  - Sicheres Desgin
  - Sicherheit bei der Implementierung
  - Verifizieren und validieren
  - Updates managen
  - Sicherheitsrichtlinien /Anweisung
  - Überwachung nach dem Inverkehrbringen
  - Vigilanz / Meldewesen

https://ec.europa.eu/health/sites/default/files/md_sector/docs/md_cybersecurity_en.pdf

Digitale Gesundheitsanwendungen

- Geregelt in Digitale-Gesundheitsanwendungen-Verordnung (DiGAV)
  - §4 Anforderungen an Datenschutz und Datensicherheit
  - Datentransfer in Drittstaaten
- Sind Medizinprodukte
- BSI unterstützt die Hersteller mit der Technischen Richtlinie BSI TR 03161

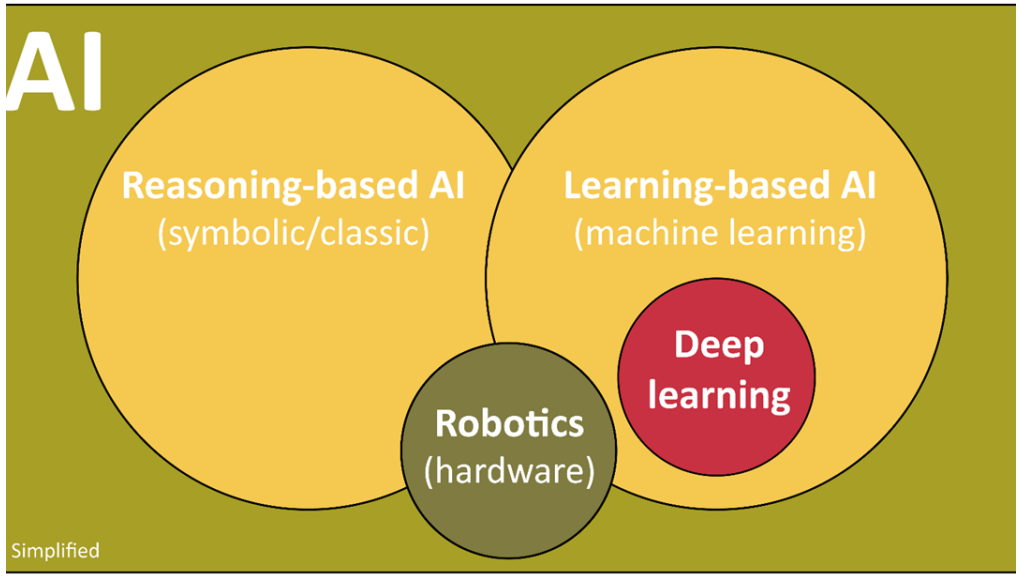
BSI Projekt ManiMed

- In der Regel weisen die Medizinprodukte eine hohe Sicherheit aus.
- Patchmanagement, hohe Variabilität, Mechanismen, Bereitstellung
- Authentifizierung und Zugriffskontrolle
- Proprietäre, teilweise nicht wirklich sichere Implementierungen bei den Kommunikationsprotokollen
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/ManiMed_Abschlussbericht.pdf?__blob=publicationFile&v=1

ACS - Expertenkreis CyberMed

- Allianz für Cybersicherheit - unterstützt von BSI
- Thema IT-Sicherheit von Medizinprodukten
- Leitfaden zur Nutzung des Manufacturer Disclosure Statement for Medical Device Security (MDS2)
  - MDS2 herausgegeben von NEMA
  - Für Zulassung bei der FDA

Künstliche Intelligenz im Medizinprodukt



- MDCG New technologies
  - Artificial Intelligence under MDR/IVDR framework
- COCIR: ARTIFICIAL INTELLIGENCE IN EU MEDICAL DEVICE LEGISLATION 09/ 2020 ()
  - https://www.cocir.org/fileadmin/Position_Papers_2020/COCIR_Analysis_on_AI_in_medical_Device_Legislation_-_Sept._2020_-_Final_2.pdf

Werbeblock

gmds AG „Datenschutz und IT-Sicherheit im Gesundheitswesen“

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

GMDS Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

Datenschutzhinweise Cookie-Hinweise Impressum Kontakt Sitemap

Home | Veranstaltungen | DS-GVO | Interpretation DS-GVO | Praxishilfen | Literatur | Nationale Umsetzung | GMDS AG DIG | Links | Hilfe

Leitfaden zur Erstellung eines IT-Sicherheitskonzeptes

Information hat sich im Rahmen des ökonomischen Strukturwandels in fast allen Industrienationen zum vierten Produktionsfaktor neben Arbeit, Kapital und Boden entwickelt. Die Wertschöpfung verlagert sich in vielen Unternehmen von der Produktion hin zur Dienstleistung. Im Dienstleistungssektor Gesundheitswesen entscheiden die Informationen zu einem Patienten über dessen Wohlergehen: bei der Patientenbehandlung ist deshalb insbesondere die Gewährleistung von Verfügbarkeit und von Integrität der notwendigen Informationen essenziell.
Da die IT als Infrastruktur eine immer wichtigere Rolle bei der Gesundheitsversorgung einnimmt und die meisten Geschäftsprozesse mit IT abgebildet werden, handelt derjenige, der eine Verarbeitung personenbezogener Gesundheitsdaten ohne ein entsprechendes IT-Sicherheitskonzept vornimmt, zumindest fahrlässig, wenn nicht sogar grob fahrlässig. Dieses kann im Ernstfall nicht unerhebliche Haftungskonsequenzen nach sich ziehen.
Doch auch wenn man ein IT-Sicherheitskonzept als grundlegende Voraussetzung zum konstruktiven Ansatz zur Gewährleistung von „IT-Sicherheit“ ansieht, ist oftmals nicht klar, was in ein solches Konzept eigentlich alles hineingehört bzw. wie man ein solches sinnvollerweise, auf die eigene Institution zugeschnitten, entwickelt. Ferner ist oft nicht bekannt, wie bzw. nach welchen Kriterien die wesentlichen technischen und organisatorischen Maßnahmen gruppiert bzw. beschrieben werden sollen. Der von den Verbänden

- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)
  „Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“
- ZTG Zentrum für Telematik und Telemedizin GmbH (ZTG)

erstellte „Leitfaden zur Erstellung eines IT-Sicherheitskonzeptes“ (Stand: 2017-09-29) ist deshalb so konzipiert, dass er bezogen auf die Anforderungen des Gesundheitswesens, praxisorientiert bei der Erstellung eines IT-Sicherheitskonzepts eine entsprechende Hilfestellung geben soll. Wie die Verfasser sich den Aufbau und Struktur eines IT-Sicherheitskonzeptes vorstellen, wird genauer im Abschnitt „Teil 1: Aufbau und Struktur eines IT-Sicherheitskonzeptes“ beschrieben. Dementsprechend sieht der grundsätzliche Aufbau eines diesem Leitfaden folgenden IT-Sicherheitskonzeptes wie folgt aus:

Kapitel 1 Zusammenfassung/Management Summary
Kapitel 2 Einleitung mit Darstellung der Ziele des IT-Sicherheitskonzeptes
Kapitel 3 Begriffsbestimmungen
Kapitel 4 Administrativa
Kapitel 5 Überblick bzgl. Zuständigkeiten, usw.
Kapitel 6 Darstellung der Rahmenbedingungen
Kapitel 7 Beschreibung der Systemarchitektur
Kapitel 8 Darlegung des Schutzbedarfs
Kapitel 9 Anzuwendende Vorgaben
Kapitel 10 Anforderungen
Kapitel 11 Implementierungsvorgaben
Kapitel 12 Darlegung der Restrisiken
Kapitel 13 Beschreibung der Kontrolle und Fortschreibung des IT-Sicherheitskonzeptes
Kapitel 14 Mitgeltende Unterlagen.

Im Abschnitt „Teil 2: Umsetzungshinweise“ werden weiterführende Informationen angeboten, z. B. Beschreibung von Akteuren, Begriffsbestimmungen und weiterführende Literatur.

https://www.gesundheitsdatenschutz.org/html/itsicherheitskonzept.php

Vielen Dank für Ihre Aufmerksamkeit

Christoph Isele

christoph.isele@cerner.com