Fachhochschule
Dortmund
University of Applied Sciences and Arts

Informationssicherheit – SoSe 2023
Informationssicherheit im Gesundheitswesen

Prof. Dr. Holger Schmidt
holger.schmidt004[at]fh-dortmund.de

Fachhochschule Dortmund
Fachbereich Informatik
Professur für IT-Sicherheit, Informatik

Themen & Lernziele

Themen

- Besonderheiten und Herausforderungen im Kontext Gesundheitswesen
- Bedrohungen und Schwachstellen in Arztpraxen, Krankenhäusern und bzgl. Medizinprodukten
- DS-GVO, Recht, Standards (insb. KRITIS, MDR, IEC 82304-1, IEC 62304)
- IT-Grundschutz, BSI-Standards 200-1 und 200-2

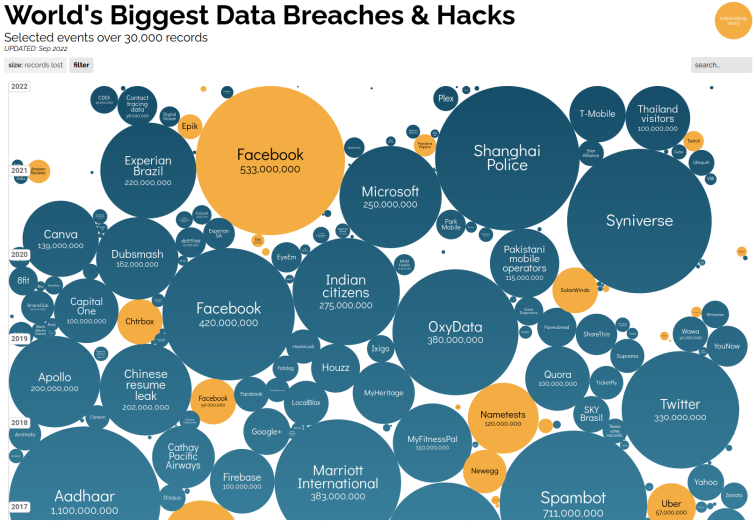
Lernziele

Die Studierenden sind in der Lage,

- Herausforderungen im Kontext Gesundheitswesen zu erklären.
- Besonderheiten bzgl. Bedrohungen, Schwachstellen, DS-GVO und nationalem Recht zu erklären.
- Medizinprodukte und Nicht-Medizinprodukte zu differenzieren.
- IT-Grundschutz und die BSI-Methodik prinzipiell umzusetzen.

Motivation

Bekanntgewordene erfolgreiche Angriffe



Quelle: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/, aufgerufen am 28. Juni 2023

ECRI Top 10 Health Technology Hazards

- 2022er Version[1]: „Cybersecurity Attacks Can Disrupt Healthcare Delivery, Impacting Patient Safety“ ist auf Rang 1.
- 2023er Version[2]: „Failure to Manage Cybersecurity Risks Associated with Cloud-Based Clinical Systems Can Result in Care Disruptions“ ist auf Rang 5.
- ECRI Institute ist gemeinnützige Organisation und widmet sich Safety im Gesundheitswesen

[1] https://assets.ecri.org/PDF/White-Papers-and-Reports/ECRI_Top10Hazards_2022_ExecutiveBrief.pdf, aufgerufen am 28. Juni 2023

[2] https://assets.ecri.org/PDF/ECRI_2023_Top_10_Hazards_Executive_Brief.pdf, aufgerufen am 28. Juni 2023

Beispiel: Ransomware

- **Schadprogramm (Malware)** verschlüsselt Daten, Betreiber erpressen Opfer bzgl. Entschlüsselung
- Ausprägungen[3]
  - Ransomware betrieben durch cyber-kriminelle Gruppen, z. B. Royal[4]
  - Ransomware-as-a-Service, z. B. Blackcat[5]
- **Faktor Mensch** als Schwachstelle (**Phishing**)

[3] https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf, aufgerufen am 28. Juni 2023

[4] https://www.hhs.gov/sites/default/files/royal-ransomware-analyst-note.pdf, aufgerufen am 28. Juni 2023

[5] https://www.heise.de/news/Skrupellos-Cybergang-Alphv-veroeffentlicht-Patientenbilder-nach-Einbruch-7536239.html, aufgerufen am 28. Juni 2023

Herausforderungen

- **Menschenleben in Gefahr**, indirekt durch Informationssicherheitsbedrohungen
- **Branchenspezifische Regularien** sind einzuhalten
- Verarbeitung von **Gesundheitsdaten** gem. Art. 9 DS-GVO nur unter besonderen Bedingungen erlaubt
- Kein nativ digitales Ökosystem
- **Digitalisierung** schreitet voran
- Besondere Systemumgebung, z. B. Personal, zu wenig im Fokus

Digitalisierungsprojekte (Auswahl) im Gesundheitswesen[6]

- Elektronische Gesundheitskarte (eGK) seit 2015
- Elektronische Patientenakte (ePA) seit 2021
- Elektronisches Rezept (E-Rezept) voraussichtlich ab 2023
- Digitale Gesundheitsanwendungen (DiGA) seit 2022
- Digitale Pflegeanwendungen (DiPA) seit 2020

[6] https://www.bundesgesundheitsministerium.de/themen/digitalisierung/digitalisierung-im-gesundheitswesen.html, aufgerufen am 28. Juni 2023

Bedrohungen und Schwachstellen

Dieser Abschnitt basiert auf Darms et al., 2019, Kapitel 5, 6, 8. Aufgrund der Präsentation als Folien und Notizen sind die Texte der Quelle typischerweise paraphrasiert.

Systembeschreibung (Auswahl)

- Räumlichkeiten (z. B. Wartezimmer, Behandlungs-/Patientenzimmer, Home Office)
- Standard-IT (z. B. PC, Tablet, USB-Stick)
- Vernetzung (z. B. LAN, WLAN)
- Medizinprodukte (z. B. Narkosesystem, auch Software)
- Personal (z. B. Arzt*Ärztin, medizinische*r Fachangestellte*r), Patienten, weitere Personen (z. B. Reinigungspersonal)

Arztpraxen

Besonderheiten zu klein für eigenes IT-Personal

Daten **Gesundheitsdaten** (Anamnese, Diagnose, Rezept)

Weitere **personenbezogene Daten**: AU, Rechnung, Fax, E-Mail, Arztbrief

Räumlichkeiten Empfang, Wartezimmer, Behandlungszimmer, Labor, Technikraum, Lager

Bedrohungen z. B. Diebstahl, Malware, Brand, Wasserschaden

Schwachstellen z. B. LAN-Anschlüsse, USB-Anschlüsse, ungesperrter PC, offene Räume, mangelnde Security Awareness

Krankenhäuser

Besonderheiten Aufgrund Größe anonymer Zugang, lohnendes Ziel

Daten wie bei Arztpraxen, und zusätzlich
Forschungsdaten

Räumlichkeiten wie bei Arztpraxen, und zusätzlich
Operationsräume, Telechirurgieräume, Patientenzimmer

Bedrohungen z. B. Manipulation von Medizinprodukten

DS-GVO

Gesundheitsdaten

- Bereits bekannt: **Gesundheitsdaten** sind personenbezogene Daten gem. Art. 4 DS-GVO
- Personenbezogene Daten bzgl. **körperlicher oder geistiger Gesundheit einer natürlichen Person**; einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.
- Gesundheitsdaten gem. Art. 9 DS-GVO **besondere Kategorie** personenbezogener Daten, z. B. dadurch erhöhte Geldbußen gem. Art. 83 DS-GVO

Verarbeitung von Gesundheitsdaten

- **Eigenständige Verarbeitungsgrundlage**
- Verarbeitung von Gesundheitsdaten gem. Art. 9 Abs. 1 DS-GVO **verboten**
- Ausnahmen gem. Art. 9 Abs. 2 DS-GVO
  - (a) **Einwilligung** für definierte Zwecke
  - (h) **Zwecke** der Gesundheitsvorsorge, Arbeitsmedizin, Beurteilung der Arbeitsfähigkeit des Beschäftigten, medizinische Diagnostik, Behandlung im Gesundheits- oder Sozialbereich, Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich, Vertrag mit Angehörigem eines Gesundheitsberufs
  - (i) aus **Gründen des öffentlichen Interesses** im Bereich der öffentlichen Gesundheit erforderlich

Bundesdatenschutzgesetz

Bundesdatenschutzgesetz (BDSG) §22[7] ergänzt und verschärft gem. Art. 9 Abs. 4 DS-GVO durch

- **angepassten Ausnahmenkatalog** in (1), z. B. Differenzierung öffentliche bzw. nichtöffentliche verarbeitende Stellen
- **Forderung konkreter organisatorischer und technischer Maßnahmen** in (2), z. B. Security Awareness, Pseudonymisierung, Verschlüsselung

[7] https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2097.pdf, aufgerufen am 28. Juni 2023

KRITIS

KRITIS-Strategie

- Nationale Strategie zum **Schutz kritischer Infrastrukturen**[8]
- **Kritische Infrastruktur**: Organisation / Einrichtung mit wichtiger Bedeutung für das staatliche Gemeinwesen; Ausfall / Beeinträchtigung führt zu nachhaltigem Versorgungsengpass, erheblicher Störung der öffentlichen Sicherheit, o. ä.
- **Gesundheitswesen** ist kritische Infrastruktur (sozioökonomische Dienstleistungsinfrastruktur)
- Ziele: **Prävention, Reaktion, Nachhaltigkeit**

[8] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html;jsessionid=2678D599A63F0018F375BBB8745658ED.2_cid350, aufgerufen am 28. Juni 2023

KRITIS-Umsetzung

- Durch BSI-Gesetz §2 Absatz 10 reguliert[9]
- **EU Agency for Cybersecurity (ENISA)** mit ähnlichem Ansatz spezifisch für Gesundheitswesen und Informationssicherheit[10]
- Maßnahmen: u. a. **konkrete Handlungsempfehlungen**, z. B. BSI IT-Grundschutz[11] und **Standards**, z. B. BSI Standards 200-1/2/3/4[12]

[9] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html, aufgerufen am 28. Juni 2023

[10] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health, aufgerufen am 28. Juni 2023

[11] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html, aufgerufen am 28. Juni 2023

[12] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html, aufgerufen am 28. Juni 2023

MDR

Medizinprodukte

- Die Europäische **Medizinprodukte-Verordnung (MDR)**[13] ist ab dem 26. Mai 2021 europaweit geltendes Recht.
- Nach Artikel 2 (1) MDR entscheidet **Zweckbindung** des Herstellers über Qualifizierung als Medizinprodukt
- Diagnose, Therapie oder Überwachung von Krankheiten und Verletzungen in Zweckbindung ausschlaggebend

[13] https://eur-lex.europa.eu/eli/reg/2017/745/oj, aufgerufen am 28. Juni 2023

Risikoklassen I

MDR definiert vier **Risikoklassen** und 22 Regeln für Einteilung von Medizinprodukten

- **Klasse I – geringes Risiko** nicht steril sind oder ohne Messfunktion haben (z. B. Pflaster); keine unabhängige Zertifizierung notwendig; weiter unterteilt:
  - **Is** in sterilem Zustand auf den Markt gebracht (z. B. Schutzausrüstung)
  - **Im** mit Messfunktion (z. B. Thermometer)
  - **Ir** wiederaufbereitet oder wiederverwendet (z. B. Chirurgische Instrumente)

Risikoklassen II

- **Klasse IIa – mittleres Risiko** typischerweise mit externer Energiequelle, für Diagnose oder Überwachung, kurzfristig invasiv über natürliche Körperöffnungen (z. B. Hörgeräte)
- **Klasse IIb – mittleres Risiko** längerfristig und chirurgisch invasiv (z. B. Infusionspumpen)
- **Klasse III – hohes Risiko** unmittelbare Wirkung auf Kreislauf- oder Nervensystem (z. B. Herzschrittmacher)

DiGA

Digitale Gesundheitsanwendungen (DiGA)

DiGA sind **Medizinprodukte niedriger bis mittlerer Risikoklasse (I bis IIa)**.

- Krankheiten erkennen, überwachen, behandeln oder lindern
- Verletzungen oder Behinderungen erkennen, behandeln, lindern oder kompensieren
- Digitale Technologie bestimmt wesentlich Hauptfunktion und medizinischen Zweck

Standards

Übersicht

- Zuständigkeit des BSI[14] via KRITIS
- Gesetzliche Anforderungen aus MDR
- Standards (Umsetzung)
  - IEC 62304 Medical device software - Software life cycle processes
  - IEC 82304-1 Health Software - Part 1: General requirements for product safety

[14] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/E-Health/e-health_node.html, aufgerufen am 28. Juni 2023

Medizingeräte-, Medizinprodukte- und Health Software: Definitionen und Beispiele

Fachhochschule Dortmund
University of Applied Sciences and Arts

Medizingeräte-Software embedded Software eines auch aus Hardware bestehenden Medizinproduktes, z. B. embedded Software eines Defibrillators

Medizinprodukte-Software nur aus Software bestehendes Medizinprodukt, z. B. Programme, Webseiten und Apps zur Diagnose, Therapie und Überwachung von Krankheiten und Verletzungen - auch indirekt, z. B. Krankenhaus-Informationssystem (KIS)

Health Software wie obige Software-Typen, und zusätzlich solche die keine Medizinprodukte gem. MDR sind, z. B. Husteblume App[15]

[15] https://www.tk.de/techniker/magazin/digitale-gesundheit/apps/husteblume-allergie-app-2025388, aufgerufen am 28. Juni 2023

Medizingeräte-, Medizinprodukte- und Health Software: Standards

Fachhochschule Dortmund
University of Applied Sciences and Arts

	Embedded Software	Standalone Software
Medizinprodukt gem. MDR	IEC 62304	IEC 62304, IEC 82304-1
kein Medizinprodukt		IEC 82304-1

Umsetzung

IT-Grundschutz

- IT-Grundschutz-Kompendium mit
  Gefährdungskatalog[16] z. B. G 0.42 Social Engineering
  Bausteinen[17] z. B. CON.3 Datensicherungskonzept und
  INF.8 Häuslicher Arbeitsplatz
- Anforderungen je nach Schutzbedarf, z. B. Basis- oder Standard-Anforderungen
- Profile als Vorlagen[18], z. B. für Hochschulen

[16] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Elementare-Gefaehrdungen/elementare-gefaehrdungen_node.html, aufgerufen am 28. Juni 2023

[17] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html, aufgerufen am 28. Juni 2023

[18] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Profile/Profile/itgrundschutzProfile_Profile_node.html, aufgerufen am 28. Juni 2023

BSI-Standards 200-1 und 200-2

Methodik basierend auf

- BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)[19]
- BSI-Standard 200-2: IT-Grundschutz-Methodik[20]
- **Zertifizierung nach ISO/IEC 27001** (auf Basis von IT-Grundschutz)

[19] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html, aufgerufen am 28. Juni 2023

[20] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html, aufgerufen am 28. Juni 2023

Erstellung der Sicherheitskonzeption bei der Standard-Absicherung

Fachhochschule Dortmund
University of Applied Sciences and Arts

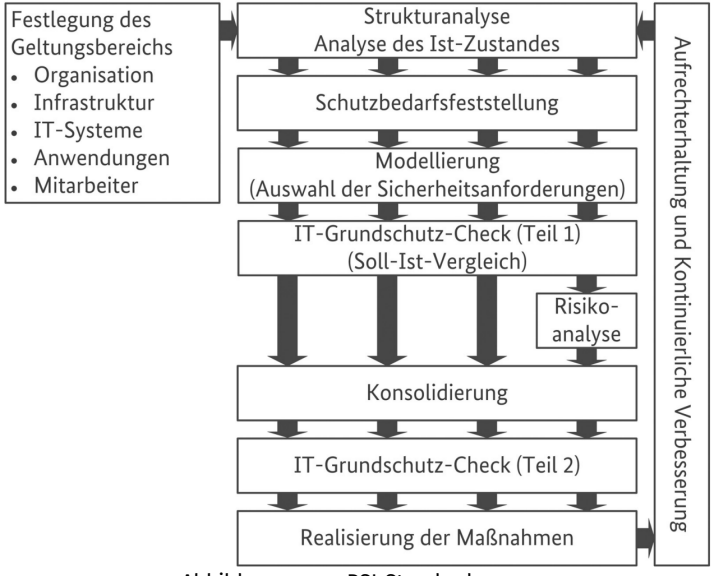


Abbildung 11 aus BSI-Standard 200-2

Schichtenmodell des IT-Grundschutz

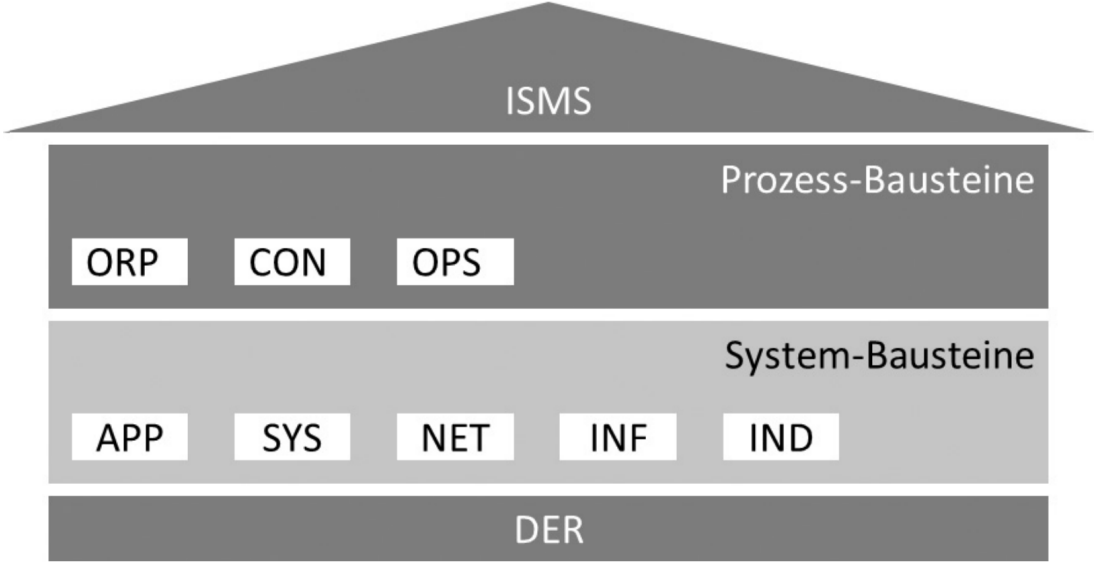


Abbildung 18 aus BSI-Standard 200-2

Zusammenfassung

Zusammenfassung

- Herausforderungen im Kontext Gesundheitswesen erkannt
- Besonderheiten bzgl. Bedrohungen, Schwachstellen, DS-GVO und nationalem Recht erklärt
- Unterschied zwischen Medizinprodukten und Nicht-Medizinprodukten gelernt
- IT-Grundschutz und die BSI-Methodik angewandt

Weiterführende Literatur

Weiterführende Literatur

- *IT-Sicherheit und Datenschutz Im Gesundheitswesen: Leitfaden Für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis* von Darms, Haßfeld und Fedtke (2019)
- *Leitfaden IT-Sicherheit für Medizinprodukte*[21]
- *Basiswissen Medizinische Software*, Kapitel 9 von Johner, Hölzer-Klüpfel und Wittorf (2020)

[21] https://github.com/johner-institut/it-security-guideline/blob/master/Guideline-IT-Security_DE.md, aufgerufen am 28. Juni 2023

Literatur

Darms, M., Haßfeld, S., & Fedtke, S. (2019). *IT-Sicherheit und Datenschutz Im Gesundheitswesen: Leitfaden Für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis*. Springer Vieweg. in Springer Fachmedien Wiesbaden GmbH. (Siehe S. 11, 40).

Johner, C., Hölzer-Klüpfel, M., & Wittorf, S. (2020). *Basiswissen Medizinische Software: Aus- und Weiterbildung zum Certified Professional for Medical Software*. dpunkt.verlag. (Siehe S. 40).