vSecure

security as a service

Risikomanagement in der technischen Betriebsführung

VAMED
health. care. vitality.

- Besteht seit 1982
- Sitz in Wien und Berlin
- mehr als 1.000 Gesundheitprojekte weltweit realisiert
- Tätig im Projekt- und Dienstleistungsgeschäft in 98 Ländern auf fünf Kontinenten
- Technische Dienstleistungen für rund 840 Gesundheitseinrichtungen mit rund 227.000 Betten weltweit

René Knab

- IT Security / Risk Manager Medizintechnik
- Leitung Medical IT – Vamed SME

VAMED
health. care. vitality.

Projektgeschäft

PROJEKT-ENTWICKLUNG	BERATUNG	PLANUNG	PROJEKT-MANAGEMENT und ERRICHTUNG

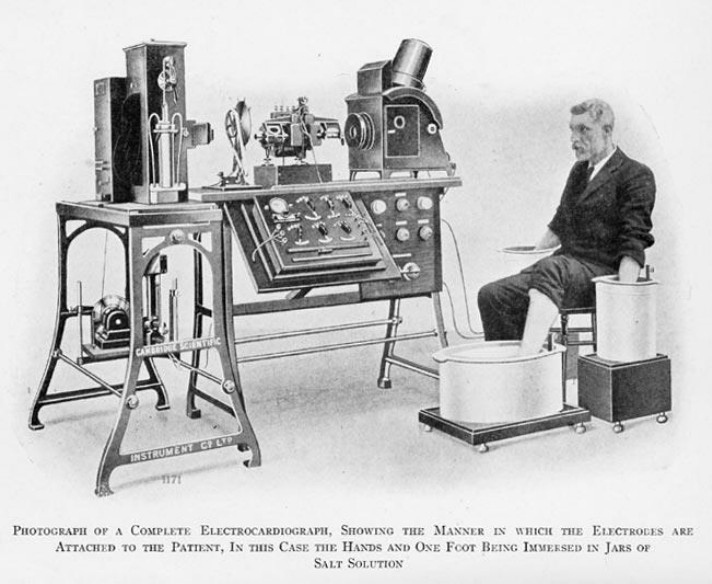
Dienstleistungsgeschäft

HIGH-END DIENSTLEISTUNGEN technisch, kaufm., infrastrukturell	GESAMTBETRIEBS-FÜHRUNG

- **Prävention**
- **Akutmedizin**
- **Rehabilitation**
- **Pflege**

- Projektgeschäft
- Dienstleistungsgeschäft

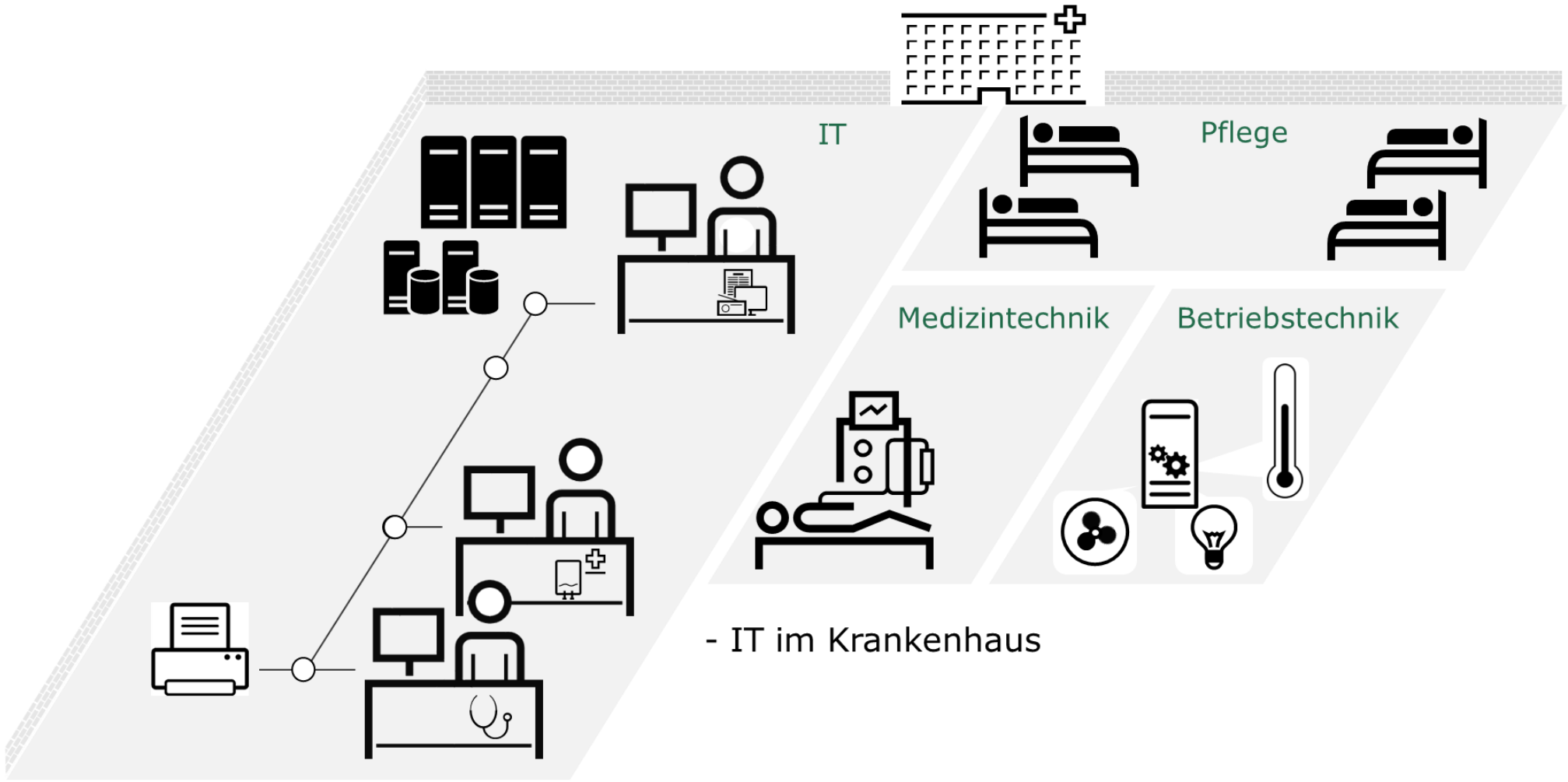
Digitalisierung im Gesundheitswesen



Photograph of a Complete Electrocardiograph, Showing the Manner in which the Electrodes are Attached to the Patient, In this Case the Hands and One Foot Being Immersed in Jars of Salt Solution

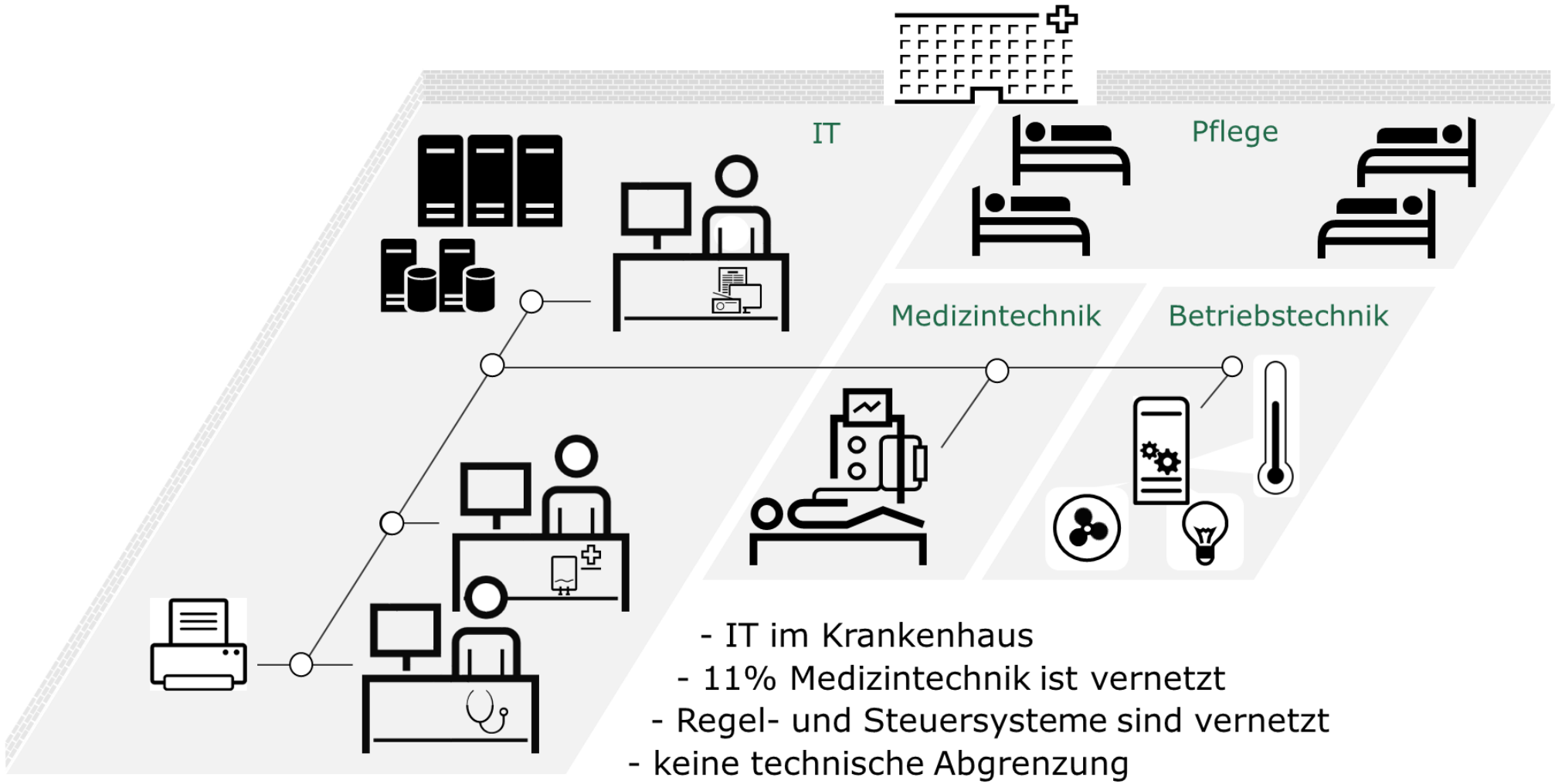
- Anforderung
  - Älter werdende Gesellschaft
  - Zugang zu einer qualitativ hochwertigen Gesundheitsversorgung und Pflege
  - Finanzierung ist zentrale gesundheitspolitische Aufgabe
- wachsende Bedeutung der IT
  - Hoher, steigender Digitalisierungsgrad
  - Zunahme der Datenmengen
  - Standardisierte, systemübergreifende Prozesse
- Fokusthemen
  - Umfassende Verfügbarkeit aller Informationen
  - Einsatz von Expertensystemen, Künstlicher Intelligenz (KI)
  - Verknüpfung von Prozessen, Automation
  - Interoperable Datenstruktur

Digitalisierung im Gesundheitswesen



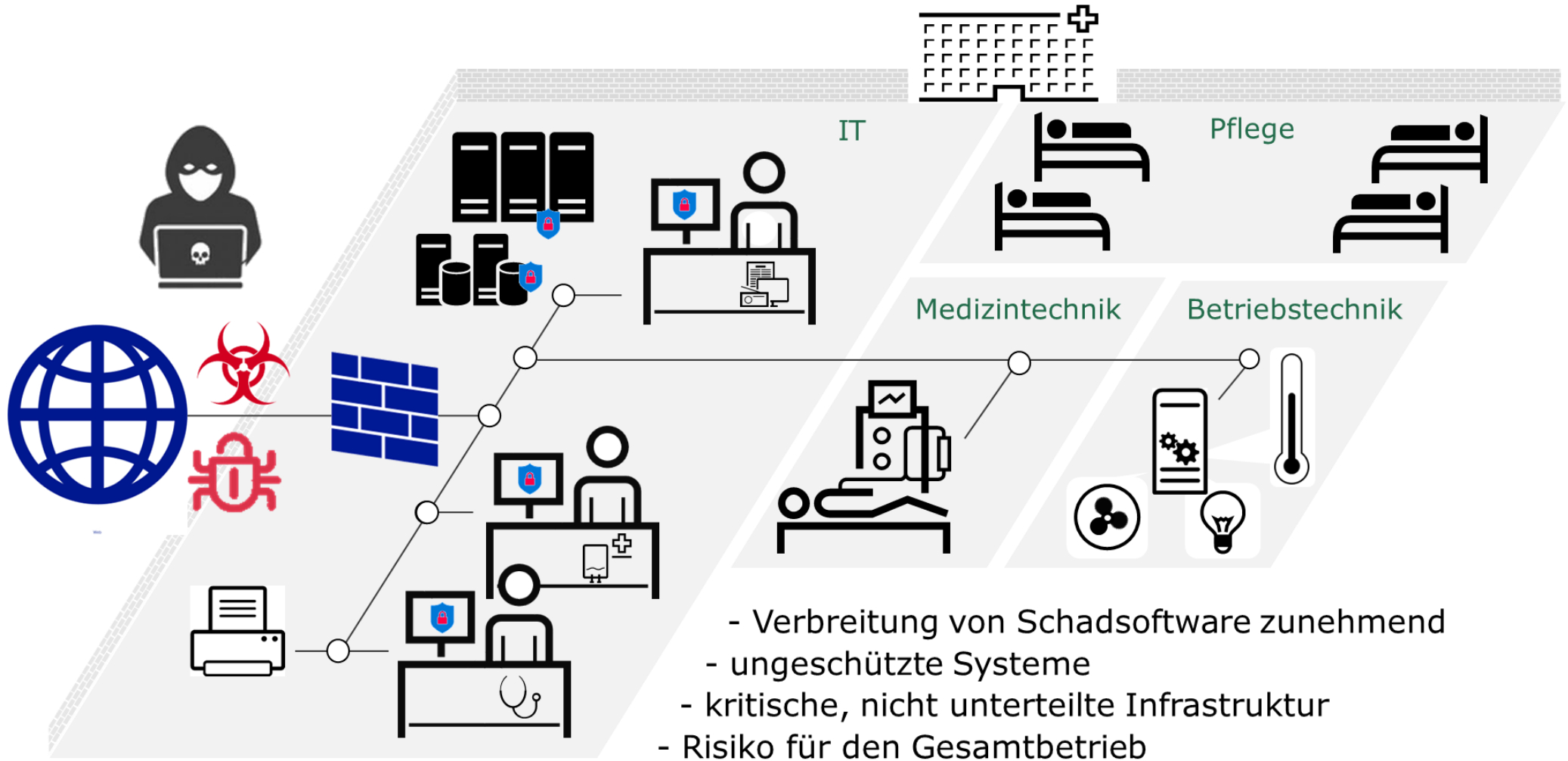
- IT im Krankenhaus

Digitalisierung im Gesundheitswesen



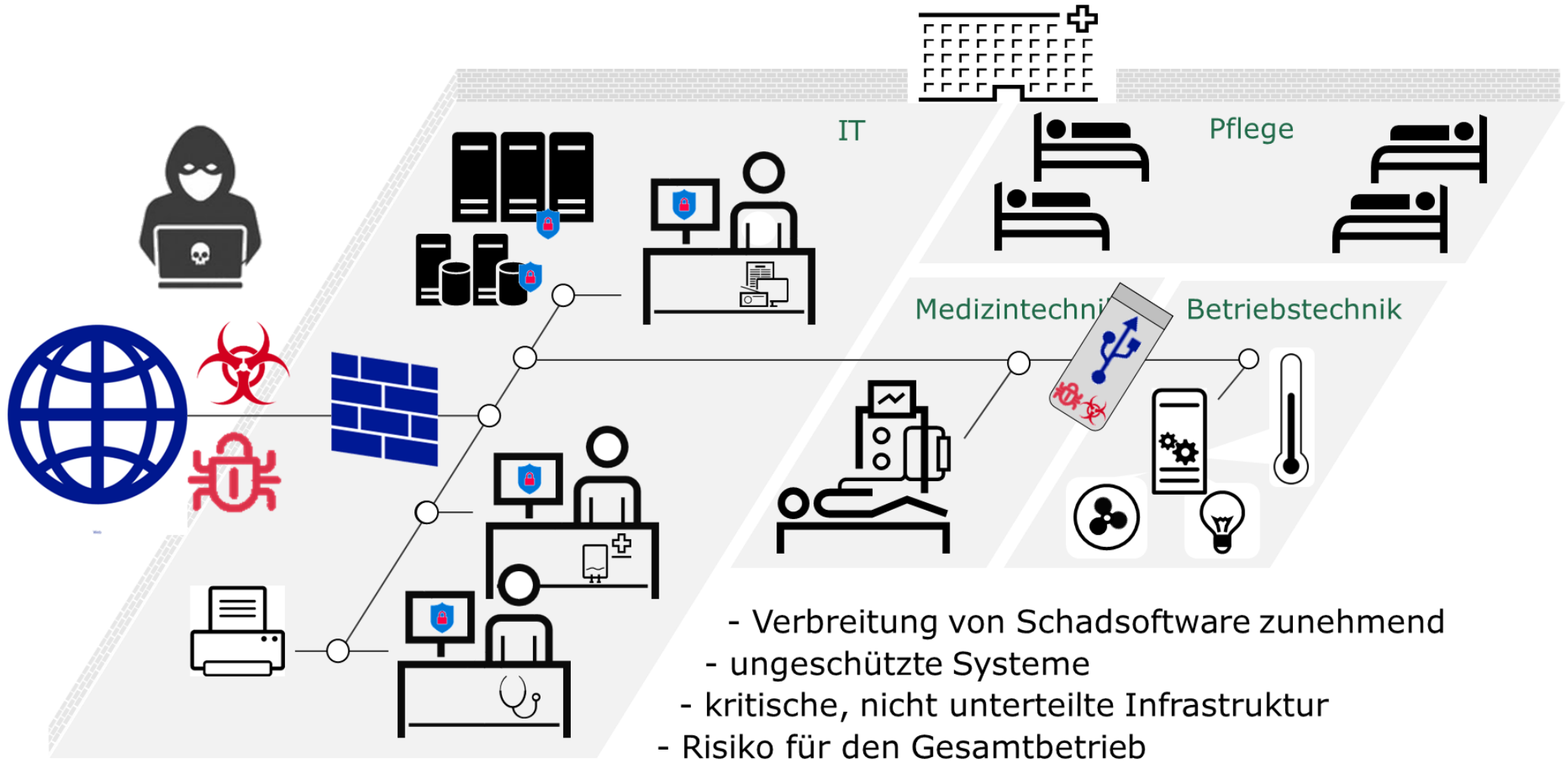
- IT im Krankenhaus
- 11% Medizintechnik ist vernetzt
- Regel- und Steuersysteme sind vernetzt
- keine technische Abgrenzung

Digitalisierung im Gesundheitswesen



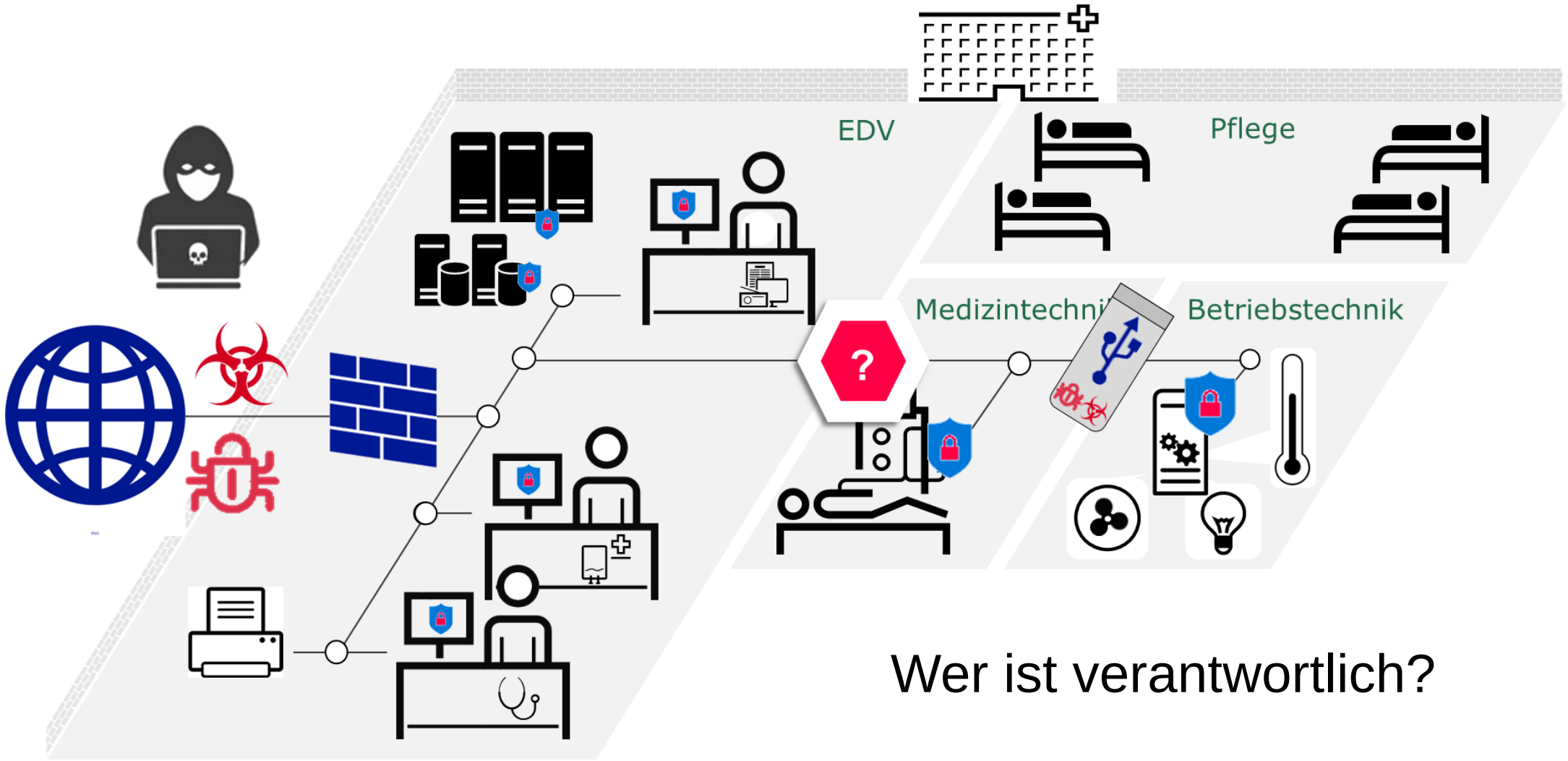
- Verbreitung von Schadsoftware zunehmend
- ungeschützte Systeme
- kritische, nicht unterteilte Infrastruktur
- Risiko für den Gesamtbetrieb

Digitalisierung im Gesundheitswesen



- Verbreitung von Schadsoftware zunehmend
- ungeschützte Systeme
- kritische, nicht unterteilte Infrastruktur
- Risiko für den Gesamtbetrieb

Digitalisierung im Gesundheitswesen



Wer ist verantwortlich?

Cyberangriffe auf Gesundheitseinrichtungen

06.10. 17.10. 28.11. 24.12. 30.01. 12.02.

CSO DEUTSCHLAND

Die Maternus-Kliniken AG ist Opfer eines Cyberangriffs geworden.

CSO | 19. OKTOBER 2023 08:40 UHR

Die Maternus Kliniken AG wurde gehac

Thieme kma Online

Home Aktuelles Themen Markt & Partner Stellenmarkt Termine Mediathek

Cyberangriff

Daten gelöscht bei digitalem Einbruch ins Klinikum Esslingen

Unbekannte haben sich Zugang zu den IT-Systemen des Klinikums Esslingen verschafft. Neben Einschränkungen der bildgebenden Untersuchungsverfahren wurden bei dem Cyberangriff auch Verwaltungsdaten gelöscht. Die Polizei ermittelt.

Das Klinikum Esslingen wurde gehackt: Am 28. November gegen 17 Uhr verzeichnete das Unternehmen

Thieme kma Online

Home Aktuelles Themen Markt & Partner Stellenmarkt Termine Mediathek

Auswirkungen

Cyberangriff wirft Uniklinikum Frankfurt zurück in die 80er

Der Cyberangriff auf das Universitätsklinikum Frankfurt ist noch nicht überstanden. Erreichbar ist weiterhin nur die Übergangswebseite. Das Rechnungswesen hat notgedrungen Fax und Papier wieder für sich entdeckt.

Thieme kma Online

Home Aktuelles Themen Markt & Partner Stellenmarkt Termine Mediathek

Top-Themen

Podcast-Staffel 2 | Digitalkolumne | Krankenhausreform | Fachkräftemangel | Insolvenzen

kma-online.de > Aktuelles > IT & Digital Health > Bezirkskliniken Mittelfranken Opfer von Cyberangriff

Daten verschlüsselt

Bezirkskliniken Mittelfranken Opfer von Cyberangriff

An den Bezirkskliniken Mittelfranken kam es zu einem Hackerangriff. Unbekannte drangen in die IT-Systeme ein und verschlüsselten gezielt Daten. Polizei und Staatsanwaltschaft untersuchen zusammen mit einem Krisenstab den Ausmaß des Schadens.

KHO

Katholische Hospitalvereinigung Ostwestfalen gGmbH

IT-Systemausfall nach Cyberattacke

In den frühen Morgenstunden des 24.12.2023 ist das gesamte IT-System der Krankenhäuser Fra Vinzenz Hospital Rheda-Wiedenbrück und Mathilden Hospital Herford ausgefallen. Patientenrele den jeweiligen Homepages.

Unbekannte haben sich Zugang zu den Systemen der IT-Infrastruktur der Krankenhäuser verschafft erste Prüfung ergab, dass es sich wahrscheinlich um eine Cyberattacke durch Lockbit 3.0 handelt, noch nicht absehbar ist. Aus Sicherheitsgründen wurden direkt nach Bekanntwerden noch in der Na und alle nötigen Personen und Institutionen informiert. Zum Ausmaß des Schadens sowie zu event gen können zum jetzigen Zeitpunkt noch keine Angaben gemacht werden. „Wir haben noch in der N und mit der Analyse der Situation begonnen. Die Zugänge zu allen Systemen wurden unmittelbar ge systeme sind Patientendaten für die Behandlung der Patienten aber noch verfügbar." sagt Dr. Jan S gGmbH. Die zuständigen Behörden wurden informiert und die internen wie externen IT-Sicherheitsspezialisten arbeiten mit Hochdruck an der Aufklärung des Sachverhaltes und der Sic rungsarbeiten laufen auf Hochtouren. Die Patientenversorgung ist weiterhin gewährleistet und der K nische Einschränkungen weiter, wir haben uns jedoch aus Sicherheitsgründen von der Notfallversor tretende Geschäftsführer Philipp Herzog.

IT LAHMGELEGT

Cyberangriff auf Krankenhaus Lindenbrunn

In letzter Zeit häufen sich die Meldungen über Hackerangriffe auf deutsche Kliniken. Jetzt ist das Krankenhaus Lindenbrunn in Niedersachen betroffen.

Von Julia Mutzbauer

CSO | 12. FEBRUAR 2024 11:35 UHR

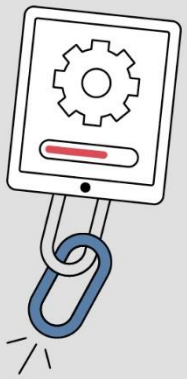
Das Krankenhaus Lindenbrunn ist Ziel einer Cyberattacke geworden. Die

Sicherheitslücken vernetzter Medizinprodukte

- gewachsene System- oder Softwarearchitekturen
- Mangelndes Verständnis für die spezifische Bedrohung der IT-Sicherheit durch die breite Vernetzung von IT- und Medizintechniksystemen
- Ungenügende Motivation im Risikomanagement IT-Security systematisch zu analysieren und zu beherrschen
- Fehlendes Verantwortungsbewusstsein für das Produkt und den Kontext eines Klinik-IT-System

Lage der IT-Sicherheit in Deutschland 2023 im Überblick

Mehr als **2.000** **Schwachstellen** in Softwareprodukten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**



Graubereich: Medizintechnik, Gebäudeautomation, IoT

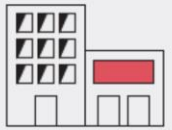
Ransomware

ist weiterhin die größte Bedrohung.

2 Ransomware-Angriffe auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.

68 erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

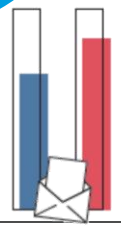
15 davon richteten sich gegen IT-Dienstleister.



Mehr als **2.000** **Schwachstellen** in Software-Produkten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

Eine Viertelmillion neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.

66% aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe: **34%** Erpressungsmails, **32%** Betrugsmails



84% aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Phishing	*Ransomware* Abhängigkeit innerhalb der IT-Supply-Chain Schwachstellen, offene oder falsch konfigurierte Online-Server	*Ransomware* APT Schwachstellen, offene oder falsch konfigurierte Online-Server

Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.

370 **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.

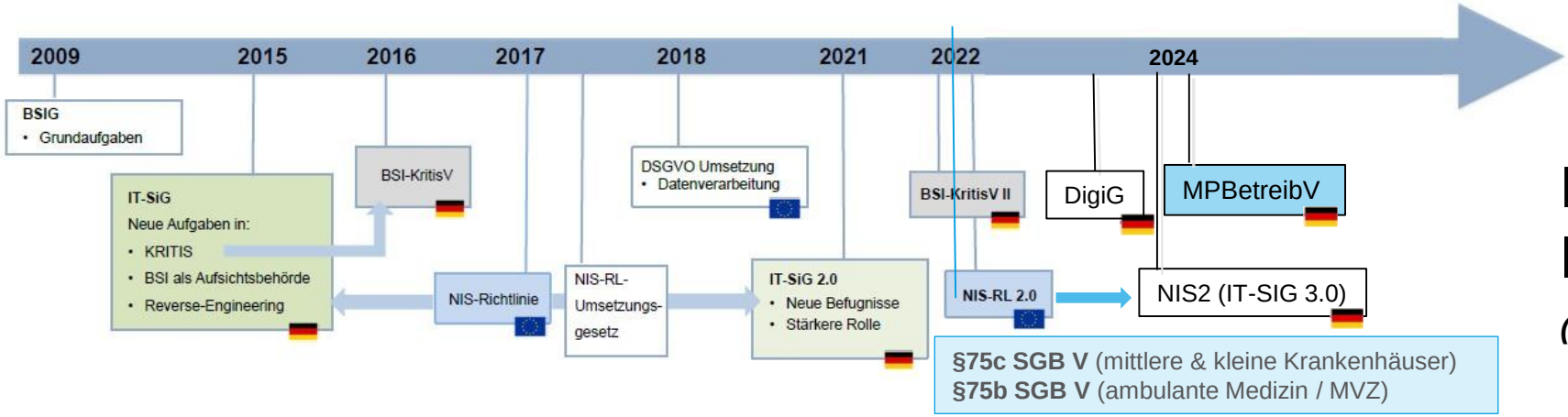
6.220 (2022)
5.100 (2021)

7.120 Teilnehmer hatte die Allianz für Cyber-Sicherheit im Jahr 2023.

Deutschland **Digital•Sicher•BSI•**

Quelle: BSI, Stand: Oktober 2023, BSI - Die Lage der IT-Sicherheit in Deutschland (bund.de)

wichtige nationale Rechtsvorschriften



§75c SGB V (mittlere & kleine Krankenhäuser)
§75b SGB V (ambulante Medizin / MVZ)

Forderung von Informationssicherheit

(aller vernetzter Geräte inkl. Medizintechnik)

KRITIS-Verordnung

Sektor Gesundheit:
> 30.000 vollstationäre Fälle
= Maximalversorger

Umsetzung nach IT-Grundschutz,
B3S Branchenstandard (DKE)

IT-Sicherheitsanforderungen an Kliniken/Krankenhäuser gemäß Patientendatenschutzgesetz (PDSG) bzw. des § 75c SGB V

PDSG

Alle Kliniken und Krankenhäuser in Deutschland

Umsetzung nach Stand der Technik,
B3S Branchenstandard (DKE)

KBV – Richtlinie

Alle kassenärztlichen Sitze
MVZ, Praxen, Ambulanzen
Praxen mit medizinischen Großgeräten: Zugriff, Konfiguration, Segmentierung

MPBetreibV

verbundene MP – Eignung muss überprüft werden

2024: Maßnahmen zur Gewährleistung der Informationssicherheit

nach Stand der Technik = B3S

Anforderungen aus dem Branchenstandard Gesundheit, u.a.:
-> Vorfallerkennung und Behandlung
-> Schutz vor Schadsoftware
-> Intrusion Detection / Prevention
-> Protokollierung

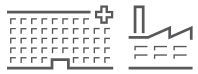
DEUTSCHE KRANKENHAUS GESELLSCHAFT DKG

Betreiber Kritischer Infrastrukturen ab dem **1. Mai 2023 verpflichtet,** [...] Systeme zur Angriffserkennung (SzA) [...] einzusetzen,...

Bundesamt für Sicherheit in der Informationstechnik

Die [...] Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem **laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten... bezieht IT und OT (M-IT) mit ein**
[Quelle: § 8a Absatz 1a Satz 1, 2 **BSIG;**]

wichtige bevorstehende EU-Rechtsvorschriften

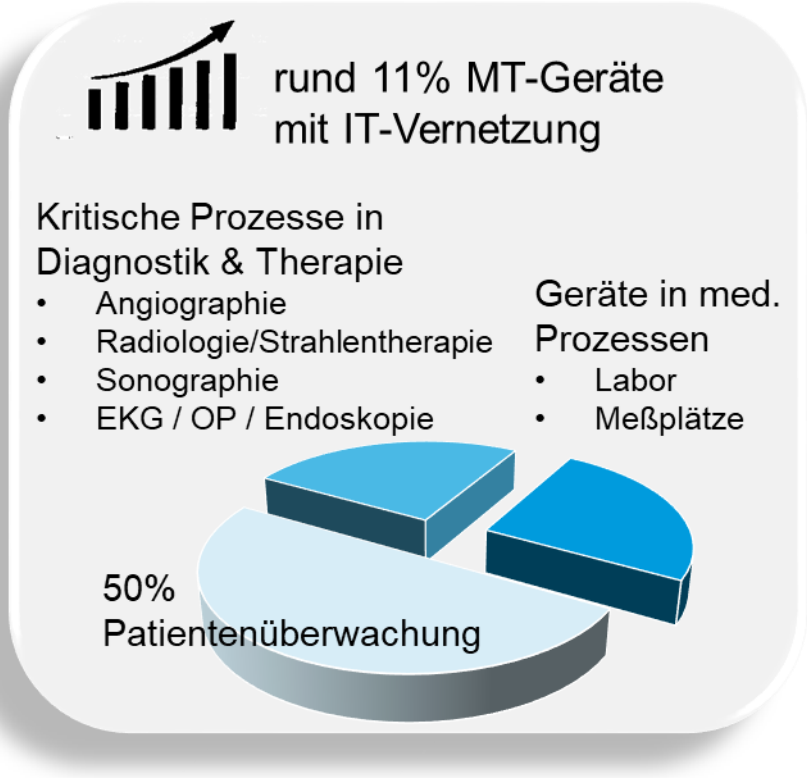


	2022				2023				2024				2025				Max Bußgelder
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
EU NISD	Anwendbar												Aufgehoben durch NIS2				
EU CSA	Anwendbar																
CyberSecurity Act, Verordnung zur Cybersicherheit, Zertifizierungsrahmenwerk für ITK-Produkte und -Dienstleistungen durch ENISA																	
EU NIS2	Vorschlag					Angenommen							Anwendbar				2% Jahresumsatz
Network and Information Security (NIS) Directive, regelt die Cyber- und Informationssicherheit von Unternehmen und Institutionen																	
EU CRA				Vorschlag													2,5% Jahresumsatz
Cyber Resilience Act, legt Anforderungen an die Cyber Sicherheit für Produkte mit digitalen Bestandteilen verbindlich fest																	
EU AIA	Vorschlag					Angenommen							Anwendbar				4% Jahresumsatz
Artificial Intelligence Act, europäischer Ansatz für künstliche Intelligenz																	
EU EHDS			Vorschlag														
europäischer Gesundheitsdatenraum, EU-weiter Austausch von Patientendaten und Nutzung von Gesundheitsdaten																	
EU Data Act			Vorschlag														4% Jahresumsatz
Vorschriften für den fairen Zugang zu und die Nutzung von Daten im EU-Raum																	
EU CER Act	Vorschlag					Angenommen							Anwendbar				
Cyber Resilience Act, reguliert Resilienz bei Kritischen Infrastrukturen in der EU, fordert Ausfallsicherheit bei Betreibern																	

Quelle: © Siemens Healthineers, 2023

Anforderungen und Rahmenbedingungen

B3S stellt an **Medizintechnik** insgesamt 87 Anforderungen



Dokumentation

- CAFM
- IT-Parameter
- Schutzziele
- Netzwerktopologie
- Schnittstellenübersicht

Richtlinien / Konzepte

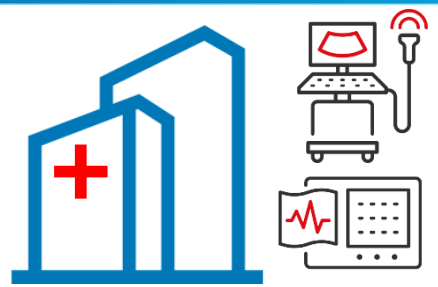
- Management von:
  - Änderungen
  - Schwachstellen
  - IS-Vorfällen
  - …

Risikomanagement

- systematisches IT-Risikomanagement

Situation = statisch, unvollständig, intrasparent

CyberSecurity Service für Medizingeräte im Krankenhaus-IT-Netz



Klinisches
Informations-System

passives scannen des
IT-Datenverkehrs

MT/BT/IoT CyberSecurity Tool

- Asset Erfassung
- Netzwerktopologie
- Softwarearchitektur
- Angriffserkennung
- Schwachstellenerkennung

- Policies

- Risk score
- Impact score
- Handlungsempfehlung

- MDS2 Papiere
- Sicherheitshinweise

Managed Active Services

Aktives
Risikomanagement

Nutzungsanalayse
med. Geräte

Aktive
Angriffserkennung

Standort- und
Gerätetracking

Aktives
Alarmsystem

Risikotransparenz

vSecure - Security as a Service

von der Erkennung zur Behebung von Gefahrenstellen

3

vSolve – Gefahrenbehebung

- Medizingerät
- IT-Infrastruktur

MT

2

vCon – Security Beratung

- Reporting-Analyse und Bericht
- Organisationstransfer / Arbeitsaufträge

MT

1

vCloud – Betrieb und Gefahrenerkennung

- Bereitstellung der HW-SW Infrastruktur
- Betrieb auf Applikationsebene / asimily

IT

IoT

MT

0

Dark- und Deepnet Analyse

- Suche und Analyse nach Schwachstellen
- 24/7 Echtzeit Überwachung

Onetime and continious security

Gefahrenstellen finden und beseitigen

3

2

1

0

Security Quickcheck

- AD Scan & Dark-/Deepweb-Check, Pentest für Versicherungen
- Nutzer-, Anmelde- und Unternehmensdaten
- => Reporting und Handlungsempfehlungen

Kontinuierliche 24/7-Echtzeit-Überwachung

- Dark- und Deepweb (Add-on threat intelligence)
- mtl. Report mit Risikoeinschätzung und Handlungsempfehlungen
- Echtzeitsuche, Alarmierung, Beseitigung

vCloud
Sicherer Betrieb und Nutzung

Open Telekom Cloud

asimily

Sichere Infrastruktur

- Deutsche hochsichere Cloud-Lösung
- Best in class Analysesoftware

2 weeks

1 YEAR

Schnell – Sicher – Günstig

- Bereitstellung innerhalb von 2 Wochen
- monatliche Gebühr • kein Invest
- keine Mindestlaufzeit • jährlich kündbar

vCon
Security-Beratung

3

2

1

0

Analyse der Ergebnisreports

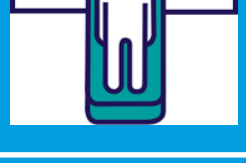
- Lesen und verstehen
- Bewerten und priorisieren

Vom Report in die Organisation

- Generierung von Serviceaufträgen
- Kommunikationsmanagement IT, MT, IS, BT und EK

vSolve
Gefahrenbehebung

3



Medizingerät

- Hotfix • Update • Upgrade
- Herstellerkommunikation
- Kommunikation Fachabteilung

IT-Infrastruktur

- IT-Architektur anpassen
- Segmentierung (VLAN)
- Netzwerkkonfiguration/-regeln

Vielen Dank für Ihre Aufmerksamkeit!

Andreas Kalz
Bereichsleiter Business Development
Digitale Transformation

Am Bahnhof Westend 9-11
14059 Berlin

+49 172 3257060

Andreas.Kalz@vamed.com
www.vamed.de

+49 173 2771284

Rene.Knab@vamed.com
www.vamed.de

René Knab
Risk Manager Medizintechnik
Leitung Medical IT

Paradigmenwechsel Medizintechnik

- Aufbrechen von Fachgebietsgrenzen
- Interdisziplinäre Zusammenarbeit
- Abteilungsübergreifendes Prozessmanagement
- Ausrichten der Prozesse auf die Kundenbedürfnisse