T.I.S.P./T.P.S.S.E. Community Meeting 2024

Berlin, 05. – 06.11.2024

IT-Sicherheit in Krankenhäusern

Nico Brüggemann, Fraunhofer SIT

Inhalt

- Hintergrund
- Cyberangriffe auf Krankenhäuser
- IT-Sicherheitsprobleme in Krankenhäusern
- Forschung

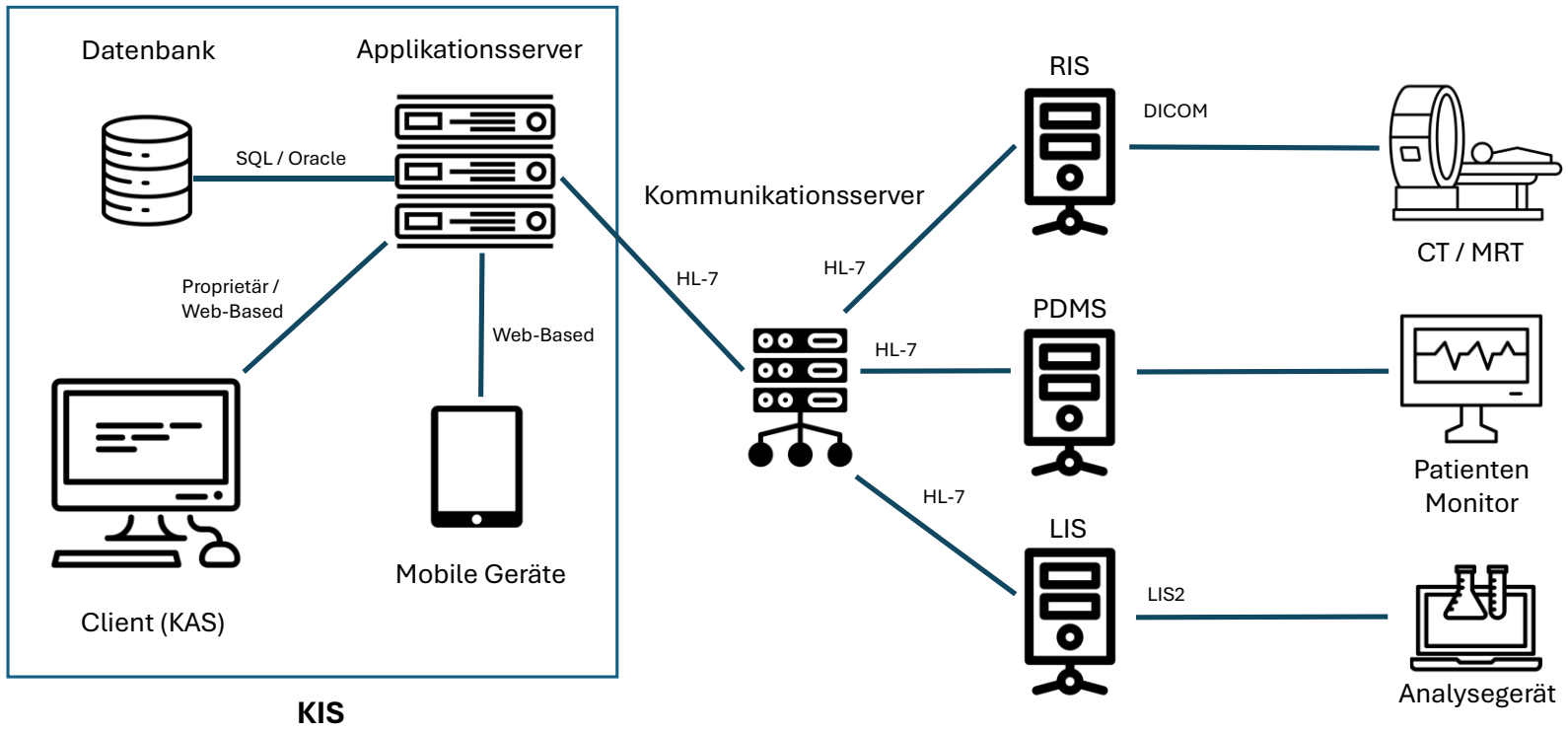
Inhalt

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

→ Hintergrund

Hintergrund - IT-Systeme im Krankenhaus

- Krankenhausinformationssystem (KIS)



Hintergrund - Datenaustauschformate

- DICOM
  - Übertragung von medizinischen Bilddaten
  - Protokoll und Datenformat

- HL7
  - Übertragung von medizinischen Daten
  - Alt aber weitverbreitet

- FHIR
  - Übertragung von medizinischen Daten
  - Neues Datenaustauschformat
  - Basiert auf Webtechnologie

Hintergrund - Medizintechnik

- Medizingeräte sind Medizinprodukte

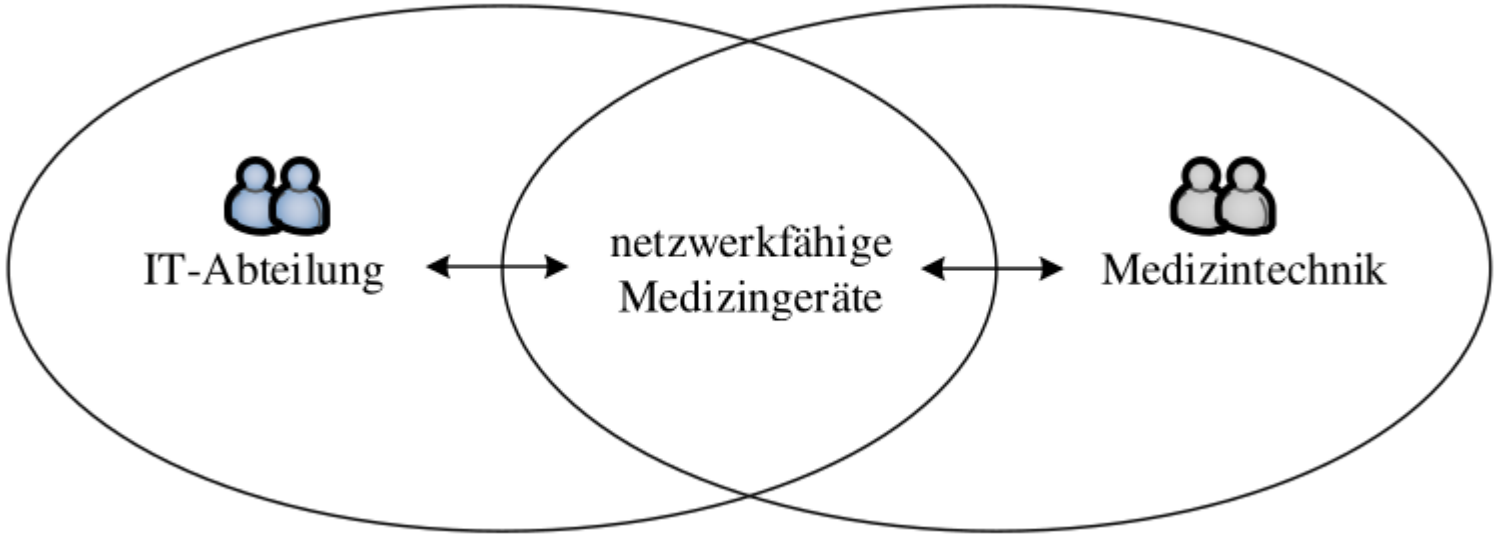
Risiko

Klasse I	Klasse IIa	Klasse IIb	Klasse III
Keine methodischen Risiken	Anwendungsrisiko, mäßig invasiv, kurzzeitig	Erhöhtes Risiko, systemische Wirkung, langzeitig	Besonders hohes Risiko, invasiv, langzeitig
• Rollstühle • Gehhilfen • Patientenbetten • Wiederverwendbare chirurgische Instrument	• Hörgeräte • Kontaktlinsen • Zahnkronen • Dentalmaterial • Diagnostische Ultraschall-Geräte	• Röntgengeräte • Beatmungsgeräte • Blutbeutel • Defibrillatoren • Kondome • Anästhesie-Geräte	• Künstliche Gelenke • Herzklappen • Brustimplantate • Resorbierbares chirurgisches Nahtmaterial

Quelle: https://www.clincoach.de/themen/klassifizierung-von-medizinprodukten-3/

Hintergrund - Medizintechnik

- Medizingeräte und IT verschwimmen immer mehr



Inhalt

→ Cyberangriffe auf Krankenhäuser

Cyberangriffe auf Krankenhäuser

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Aktuelle Angriffe

Nr.	Datum	Ort	Land	Unternehmen	Typ
8	Oktober 2024 ?	Münnerstadt	BY	Krankenhaus	
34	Juni 2024	Hausham	BY	Krankenhaus	
84	9. Februar 2024	Coppenbrügge	NI	Krankenhaus	
91	Januar 2024	Berlin	BE	Krankenhaus	
104	24. Dezember 2023	Bielefeld	NW	Krankenhaus	
105	24. Dezember 2023	Herford	NW	Krankenhaus	
106	24. Dezember 2023	Rheda-Wiedenbrück	NW	Krankenhaus	
116	28. November 2023	Esslingen am Neckar	BW	Krankenhaus	
159	6. Oktober 2023	Frankfurt/Main	HE	Krankenhaus	
267	10. Mai 2023	Bremen	HB	Krankenhaus	

Quelle: https://konbriefing.com/de-topics/hackerangriff-deutschland.html

Cyberangriffe auf Krankenhäuser

- Wie läuft ein Angriff auf ein Krankenhaus ab?
- Initial Access über die „Office IT“
  - MS Office, Citrix, VPN, etc.
- Angreifer greifen Krankenhäuser meist „zufällig“ an.

Inhalt

→ IT-Sicherheitsprobleme in Krankenhäusern

IT-Sicherheitsprobleme in Krankenhäusern

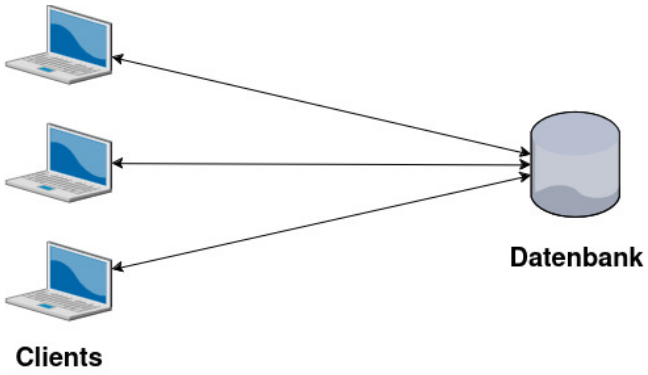
- Gibt also keine Sicherheitsprobleme mit der medizinischen IT?

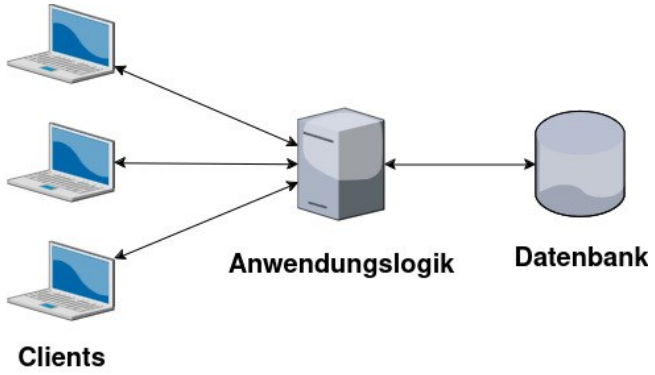
→ Leider doch

- Probleme auf technischer Ebene
  - Veraltete Software
  - Veraltete Protokolle/Datenaustauschformate und fehlende Awareness
  - Medizingeräte

Veraltete Software - Beispiel

- KIS verwenden teilweise veraltete IT-Architekturen.
  - 2-Schicht-Architektur (Client & Datenbank)





Veraltete Software - Beispiel

- Die Softwareverteilung wird über SMB-Netzwerklaufwerke abgewickelt.

- Ableitung:
  - Viele Fehlerquellen (Berechtigung, etc.)
  - Betreiber hab mehr Verantwortung.

Quelle: KI generiert mit Chatgpt 4o

Veraltete Software - Absicherung

- KIS-Hersteller müssen auf moderne Architekturen umsteigen.
  - Beispiel: Webtechnologien

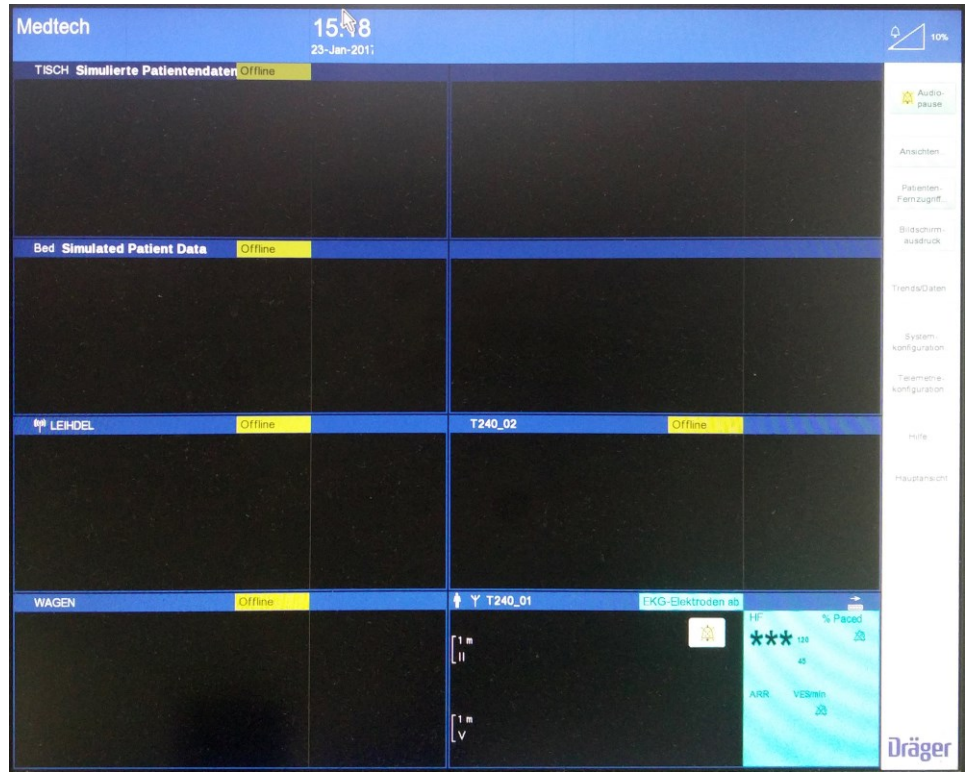
Medizingeräte

- Medizingeräte dürfen nicht verändert werden.
- Medizingeräte haben eine hohe Lebenszeit.

- Ableitung:
  - Alte Softwarestände
  - Systeme können selbst kaum abgesichert werden.

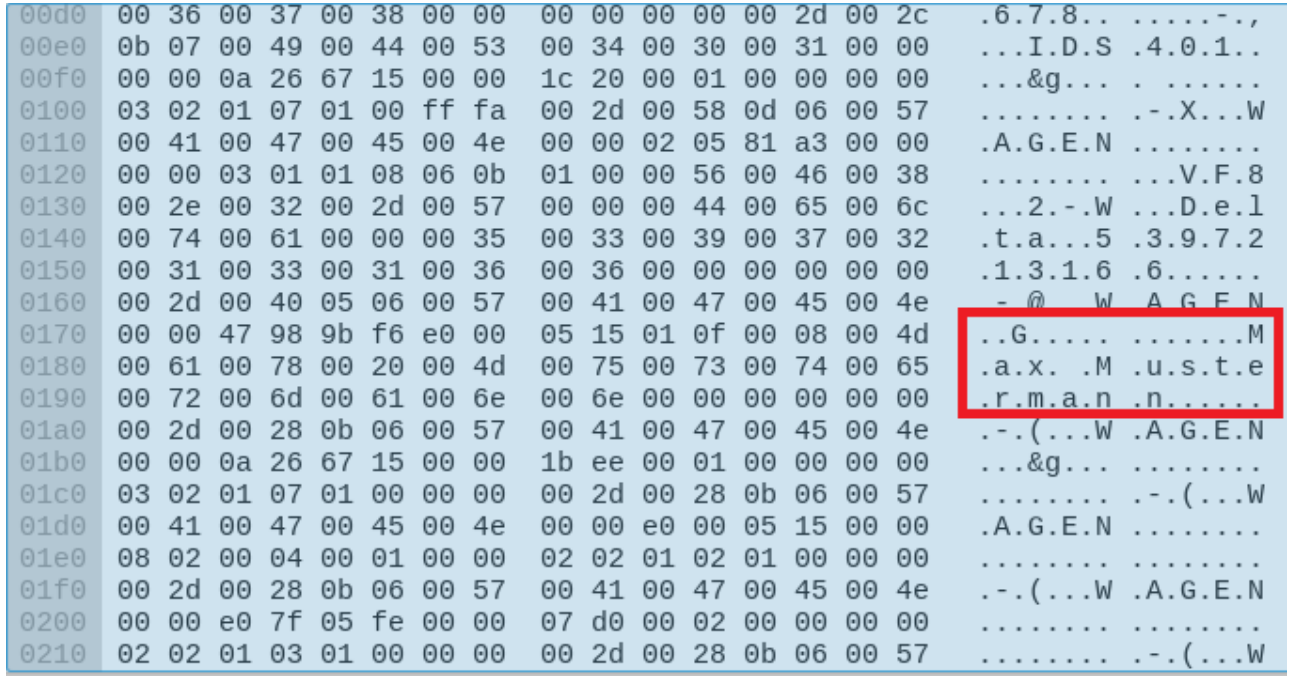
Medizingeräte

- Beispiel Syn Flood



Medizingeräte

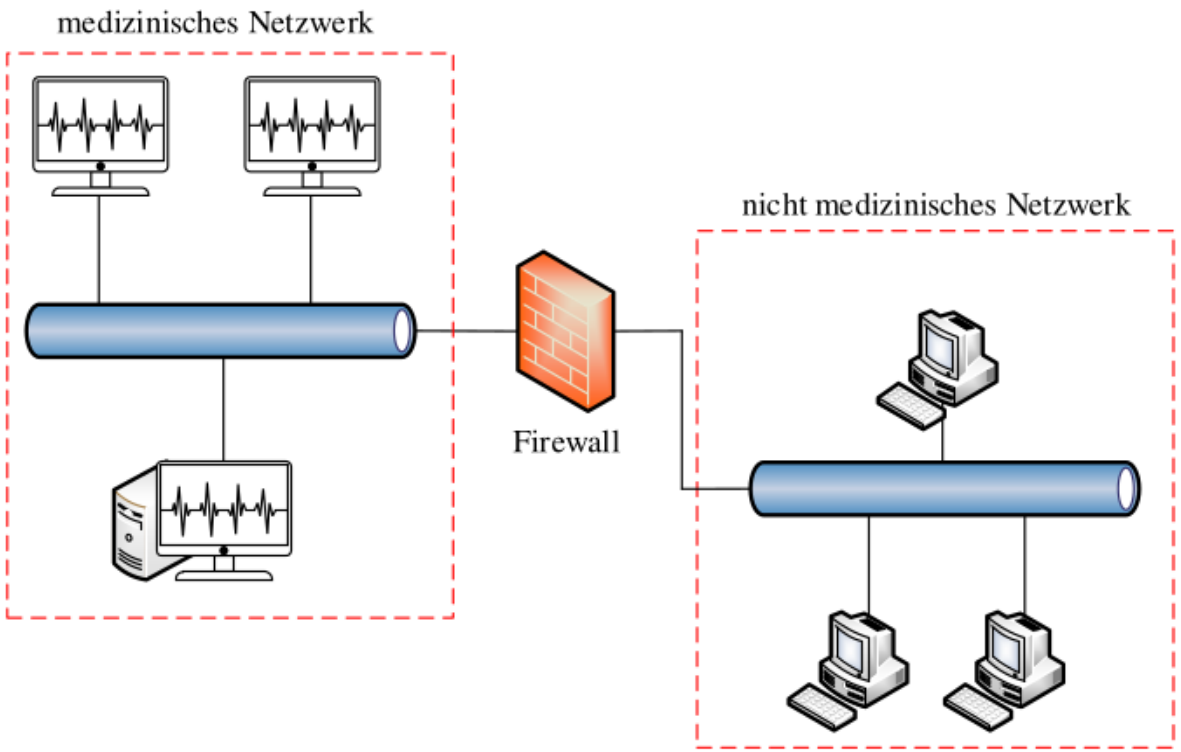
- Beispiel MITM

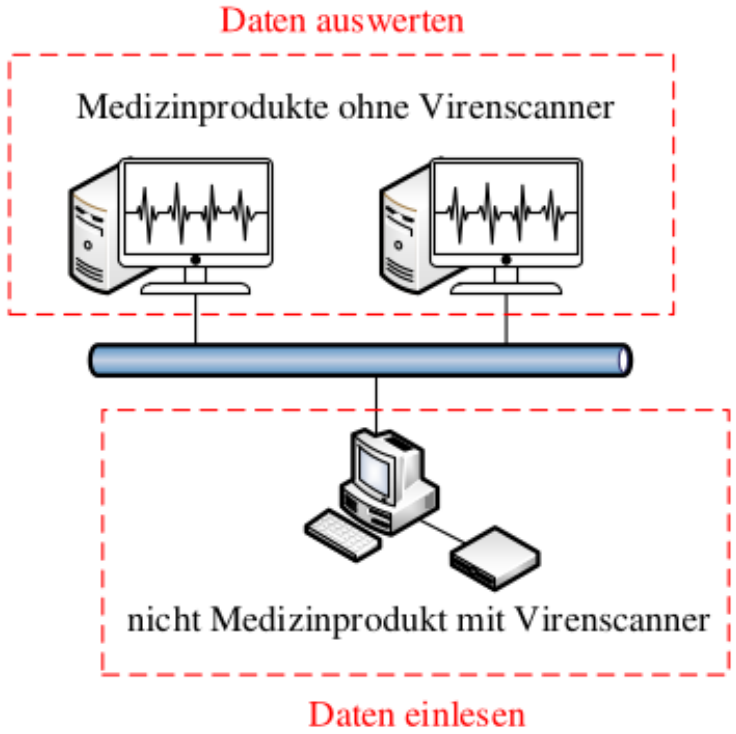


```
00d0  00 36 00 37 00 38 00 00  00 00 00 00 00 2d 00 2c   .6.7.8.. .....-.,
00e0  0b 07 00 49 00 44 00 53  00 34 00 30 00 31 00 00   ...I.D.S .4.0.1..
00f0  00 00 0a 26 67 15 00 00  1c 20 00 01 00 00 00 00   ...&g... . ......
0100  03 02 01 07 01 00 ff fa  00 2d 00 58 0d 06 00 57   ........ .-.X...W
0110  00 41 00 47 00 45 00 4e  00 00 02 05 81 a3 00 00   .A.G.E.N ........
0120  00 00 03 01 01 08 06 0b  01 00 00 56 00 46 00 38   ........ ...V.F.8
0130  00 2e 00 32 00 2d 00 57  00 00 00 44 00 65 00 6c   ...2.-.W ...D.e.l
0140  00 74 00 61 00 00 00 35  00 33 00 39 00 37 00 32   .t.a...5 .3.9.7.2
0150  00 31 00 33 00 31 00 36  00 36 00 00 00 00 00 00   .1.3.1.6 .6......
0160  00 2d 00 40 05 06 00 57  00 41 00 47 00 45 00 4e   .-.@...W .A.G.E.N
0170  00 00 47 98 9b f6 e0 00  05 15 01 0f 00 08 00 4d   ..G..... .......M
0180  00 61 00 78 00 20 00 4d  00 75 00 73 00 74 00 65   .a.x. .M .u.s.t.e
0190  00 72 00 6d 00 61 00 6e  00 6e 00 00 00 00 00 00   .r.m.a.n .n......
01a0  00 2d 00 28 0b 06 00 57  00 41 00 47 00 45 00 4e   .-.(...W .A.G.E.N
01b0  00 00 0a 26 67 15 00 00  1b ee 00 01 00 00 00 00   ...&g... ........
01c0  03 02 01 07 01 00 00 00  00 2d 00 28 0b 06 00 57   ........ .-.(...W
01d0  00 41 00 47 00 45 00 4e  00 00 e0 00 05 15 00 00   .A.G.E.N ........
01e0  08 02 00 04 00 01 00 00  02 02 01 02 01 00 00 00   ........ ........
01f0  00 2d 00 28 0b 06 00 57  00 41 00 47 00 45 00 4e   .-.(...W .A.G.E.N
0200  00 00 e0 7f 05 fe 00 00  07 d0 00 02 00 00 00 00   ........ ........
0210  02 02 01 03 01 00 00 00  00 2d 00 28 0b 06 00 57   ........ .-.(...W
```

Medizingeräte - Absicherung

- Netzsegmentierung





Veraltete Protokolle/Datenaustauschformate und fehlende Awareness

- DICOM

Standard:

- Transportverschlüsselung (TLS), Authentication (Kerberos, JWT, MFA-fähig), Verschlüsselung Data-at-Rest, Integritätssicherung (MACs / digitale Signaturen).

Praxis:

- Sicherheitsfeatures werden nicht verwendet.

Veraltete Protokolle/Datenaustauschformate und fehlende Awareness

- HL7

Standard:

- HL7 v2.x definiert Sicherheitsaspekte ausdrücklich als „Implementor-specific“ und gibt keine weiteren Hinweise auf einen sicheren Einsatz.

Praxis:

- Da der Standard selbst keine Sicherheitsfeatures definiert, werden die HL7-Nachrichten unverschlüsselt und ungesichert übertragen.

Veraltete Protokolle/Datenaustauschformate und fehlende Awareness

- FHIR

Standard:

- Der Standard selbst definiert keine zwingend erforderlichen Sicherheitsfunktionen.
- Es werden einige Möglichkeiten und konkrete Empfehlungen zur Absicherung durch die HL7-Organisation beschrieben.

Praxis:

- Durch die Webtechnologien ist die Transportverschlüsselung via TLS einfach zu implementieren.
- standardisierte Autorisierungsprotokollen wie OAuth2.
- Protokollierung mit FHIR-Audit-Events

Veraltete Protokolle/Datenaustauschformate und fehlende Awareness

GESUNDHEITS-IT

Tut mal kurz weh

rC3

Röntgenbilder auf ungeschützten Servern und aus dem Internet erreichbare Praxen: Die Gesundheits-IT hat viele Sicherheitsprobleme.

Ein Bericht von Moritz Tremmel

30. Dezember 2020, 13:55 Uhr

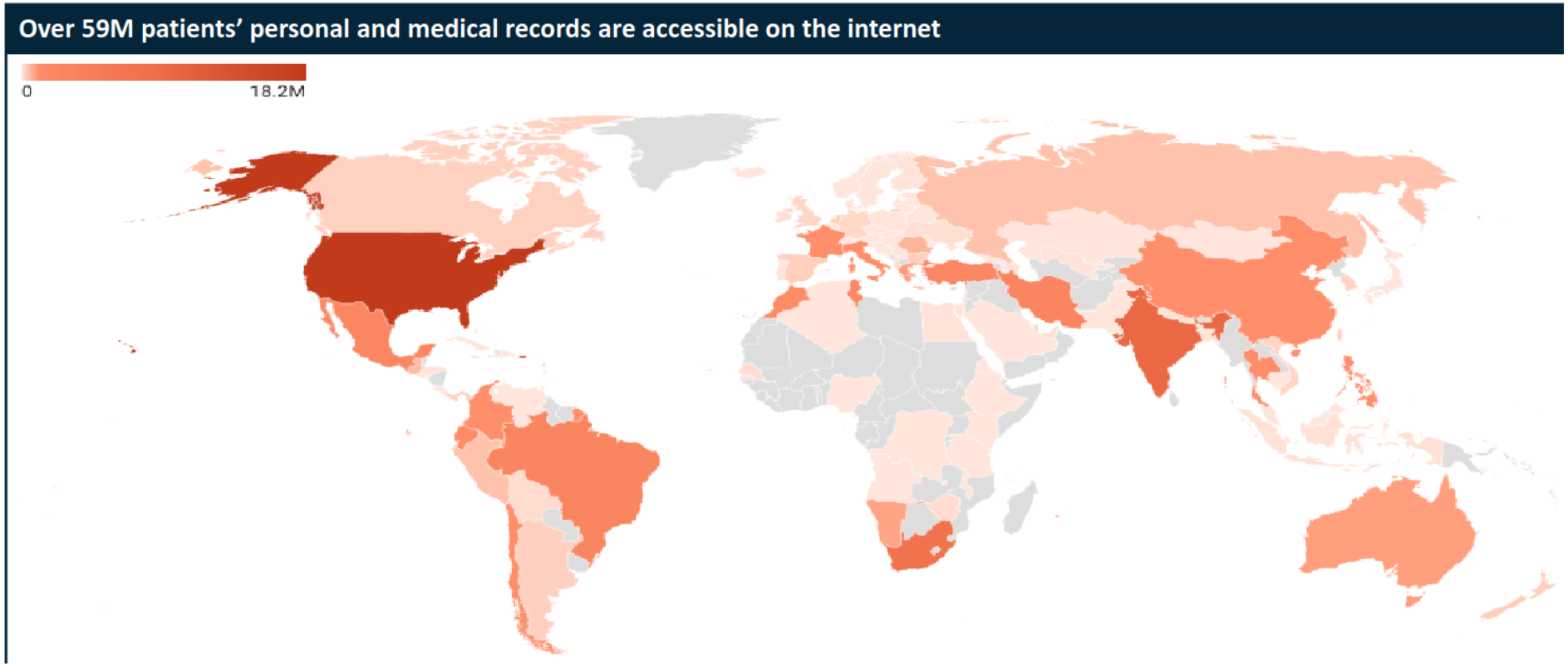
in Pocket speichern | merken

(Bild: Mohamed Hassan/Pixabay)

Wie impft man eigentlich Gesundheits-IT?

Quelle:https://www.golem.de/news/gesundheits-it-tut-mal-kurz-weh-2012-153097.html

Veraltete Protokolle/Datenaustauschformate und fehlende Awareness



Quelle: https://i.blackhat.com/EU-23/Presentations/EU-23-Yazdanmehr-Millions_of_Patient_Records_at_Risk.pdf

Inhalt

→ Forschung

Forschung

- Internetweiter Scan nach HL7, FHIR und DICOM

- Forschungsfragen:
  - Wie viele Hosts sind auffindbar?
  - Was hat sich im Vergleich von alten Scans zu den neuen Scans verändert?
  - Verwenden die Hosts Authentifizierung?
  - Welche Software / Version wird eingesetzt?
  - Gibt es Auffälligkeiten bei IPv6 Hosts?

Forschung

- Methode

Forschung

- Herausforderungen
  - IPv6 Scanning
  - Es gibt zu viele Adressen. Wie sieht das Vorgehen aus?
  - Wie können IPv4- und IPv6-Hosts unterschieden werden?
  - Patientendaten
  - Der Scan wird so gestaltete, dass keine Patientendaten heruntergeladen werden.

Kontaktdaten

Nico Brüggemann
wissenschaftlicher Mitarbeiter

Fraunhofer-Institut für Sichere Informationstechnologie SIT
Stegerwaldstraße 39
48565 Steinfurt

E-Mail: nico.brueggemann@sit.fraunhofer.de
Web: https://www.sit.fraunhofer.de