FH MÜNSTER
University of Applied Sciences

Elektronische Patientenakte (ePA) und Telematikinfrastruktur (TI)

Sinnvoll oder unsicher?

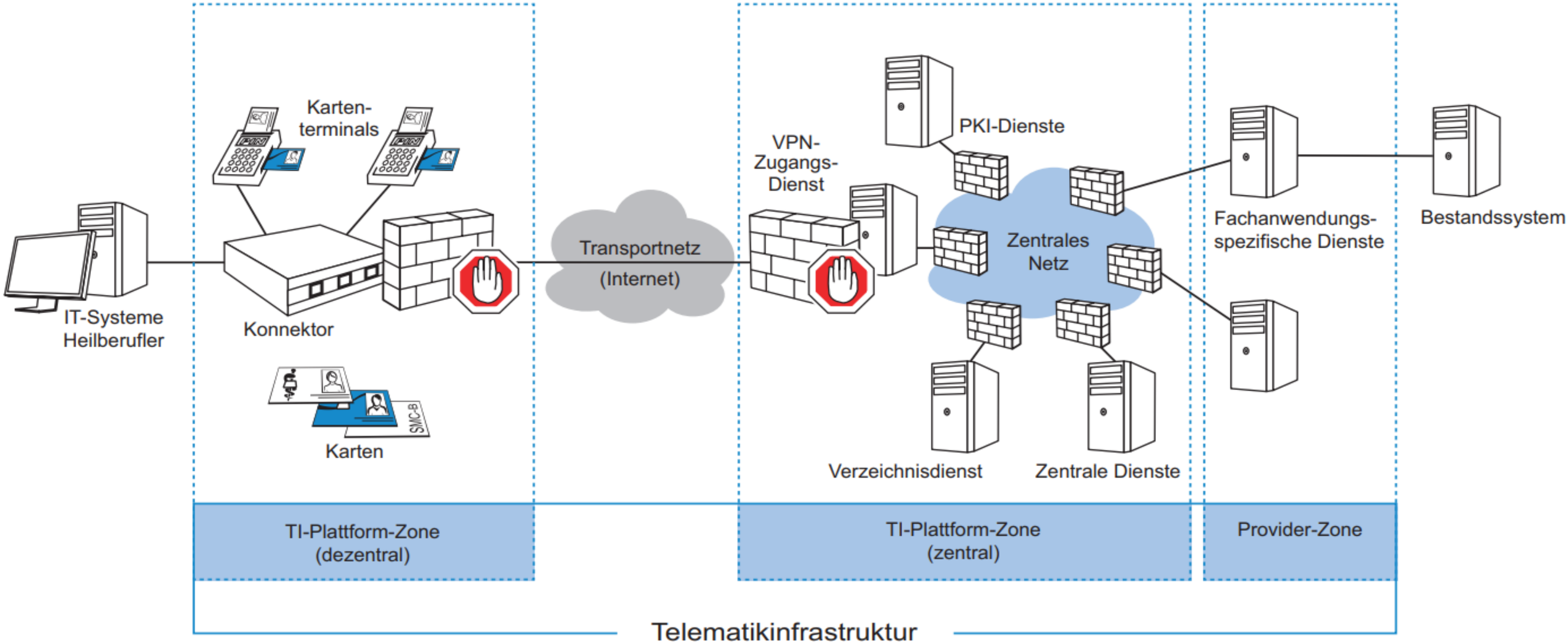
Christoph Saatjohann

Labor für IT-Sicherheit

Email: christoph.saatjohann@fh-muenster.de

Twitter: @SaatChris

EINFÜHRUNG TELEMATIKINFRASTRUKTUR



* https://www.gematik.de/fileadmin/user_upload/gematik/files/Publikationen/gematik_whitepaper_web_Stand_270916.pdf

VSDM, KIM, ePA, eAU

FACHANWENDUNGEN

Versichertenstammdatenmanagement (VSDM)

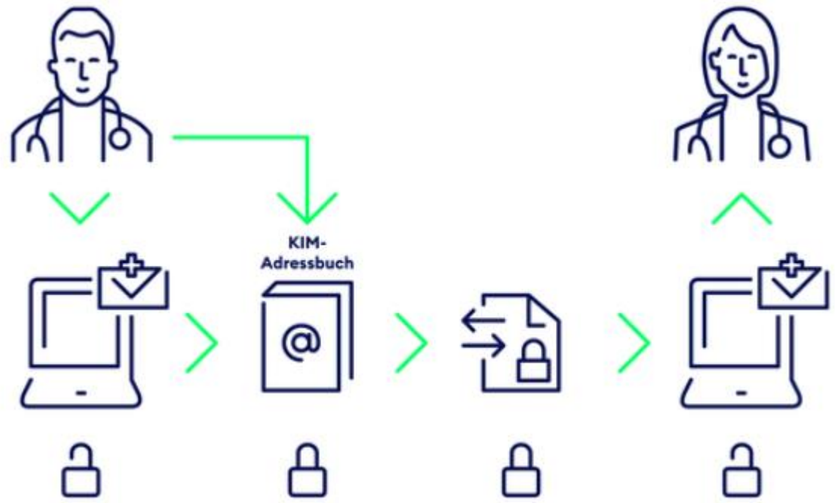
- Online Update der Versichertendaten auf der eGK
  - Beim Einlesen der Karte wird der Krankenkassenserver nach Aktualisierungen gefragt
- Erste produktive Anwendung der TI
  - Wird auch gleichzeitig als TI-Anschluss Nachweis verwendet
- Sichere Ende-zu-Ende-Verschlüsselung zwischen eGK und Krankenkasse

Sichere Kommunikation im Gesundheitswesen

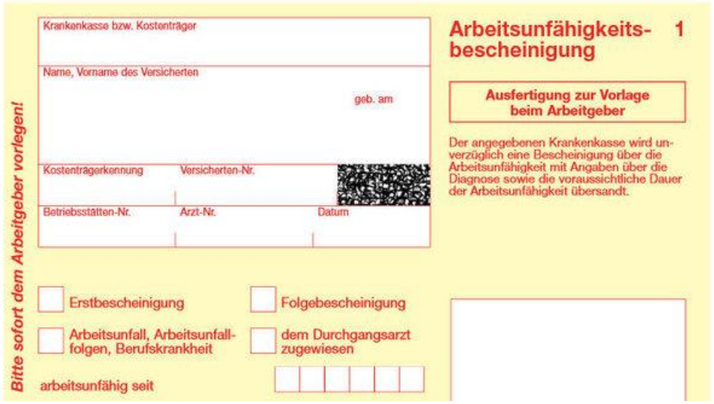
*LDI Bremen

Kommunikation im Medizinwesen (KIM)

- Sichere Email Kommunikation zwischen Ärzten, Psychotherapeuten, Apothekern….
- Grundlage für eAU, eArztbrief, HKPs
- Komplette Email (samt Betreff) wird signiert und Ende-zu-Ende verschlüsselt



eAU



- Digitale Übertragung der eAU an KK per KIM Dienst
  - Aktuell geplant: Ab 1.10.2021
- Weiterleitung an AG: 1.07.2022
  - Weiterleitung durch KK
- Inhalt der eAU bleibt der gleiche wie heute
  - Insbesondere auch bei der Meldung an AG

Elektronische Patientenakte

ePA

Elektronische Patientenakte (ePA)

- Freiwillige patientengeführte Akte
  - Patient vergibt zeitlich limitierte Lese- Schreibrechte
  - Patient kann Daten lesen, löschen, schreiben
- ePA ‚liegt' beim Krankenkassen Dienstleister
  - Nicht auf der eGK, nicht bei der Krankenkasse
  - Daten werden beim Arzt/Patienten verschlüsselt

ePA Rechtemanagement

- Ab 2021: **Vom Patienten ermächtigte** Leistungserbringer (LE) können **komplette** Akte einsehen
- 2022: Individuelle Dokumente oder Gruppen von Dokumenten können **pro Arzt individuell** freigegeben werden
- Feingranulare Rechtevergabe per Smartphone App

Patienten-Sicht

- Informierte Behandlung
  - Direkte „Patientenquittung“ mit gestellten Diagnosen
- Einfaches Verwalten von Unterlagen
  - Impfpass, Zahnbonus, Medikationsplan, ….

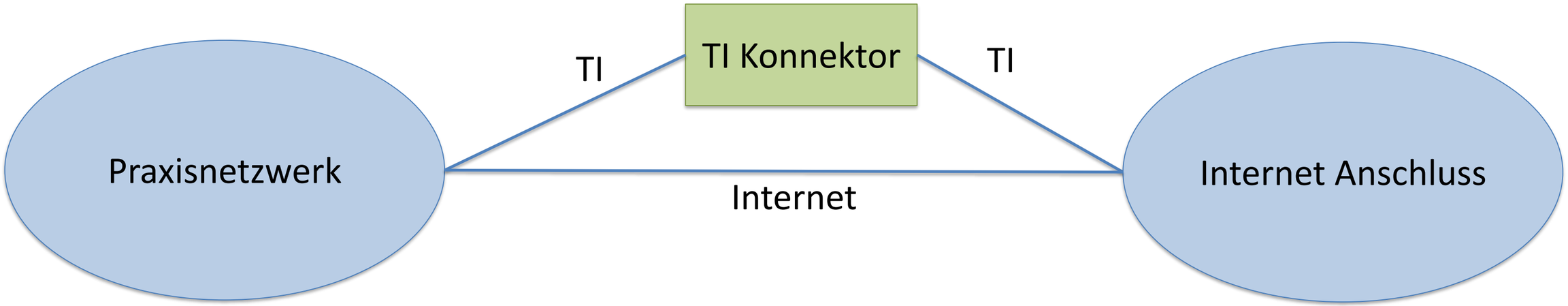
Leistungserbringer-Sicht

- Einfache Erfüllung des Auskunftsanspruchs gegenüber Patienten
  - ePA integriert in PVS/KIS - Freigabe „per Klick“
- Einfache Kommunikation mit Nachbehandlern
  - Statt DVDs/Arztbriefe: Eintrag in ePA
- Potentieller Mehraufwand
  - Neue Prozesse müssen erlernt werden
  - Vermehrte Erläuterungen durch direkte Pat-einsicht in Akten?

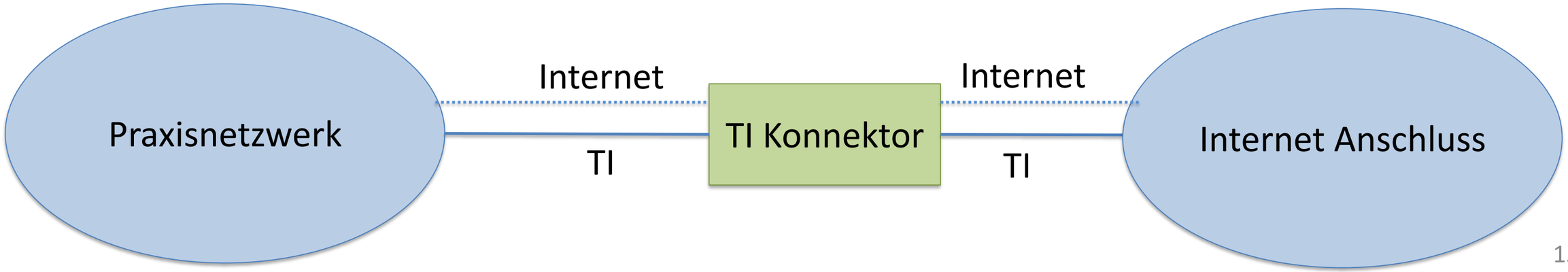
SICHERHEIT?

TI Anschluss in der Praxis / KH

- Parallel: Direktes Internet für das Praxisnetzwerk



- Seriell: Internet für Praxisnetzwerk optional (SIS)



2020: Probleme mit dem TI Anschluss *

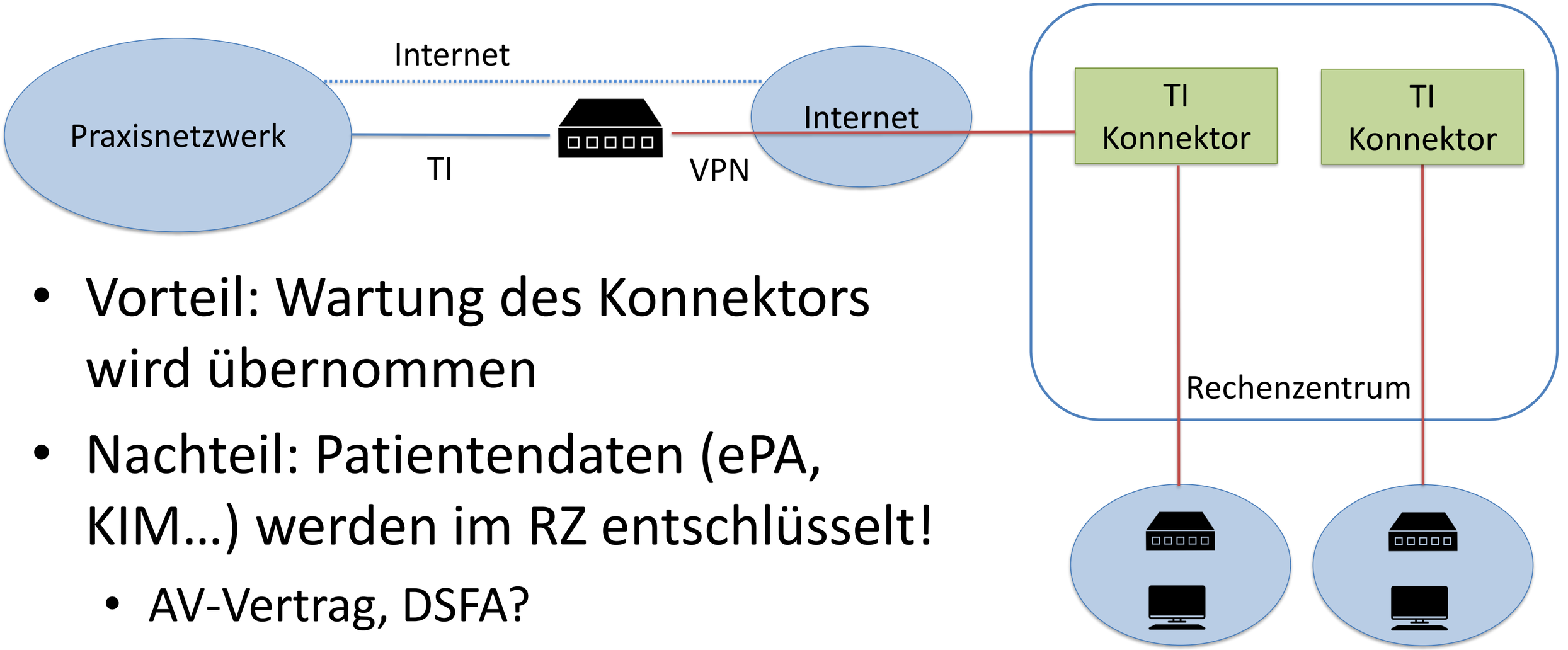
- ~ 200 Konnektoren im Internet erreichbar
  - 133 Secunet Administrator-Oberflächen
  - 67 Konnektoren mit erreichbarer PVS Schnittstelle
  - **29 Konnektoren erreichbar OHNE Authentifizierung!**
- Ursache: Fehlkonfiguration das Praxisnetzwerks

Laut Praxis wurden die Ports geschlossen, Firewall wird von einem bekannten des Herrn Dr. betreut

Unnötige Portfreigaben wurden durch den Techniker entfernt

* https://media.ccc.de/v/rc3-11342-tut_mal_kurz_weh_neues_aus_der_gesundheits-it

Rechenzentrums-Konnektor



- Vorteil: Wartung des Konnektors wird übernommen
- Nachteil: Patientendaten (ePA, KIM…) werden im RZ entschlüsselt!
  - AV-Vertrag, DSFA?

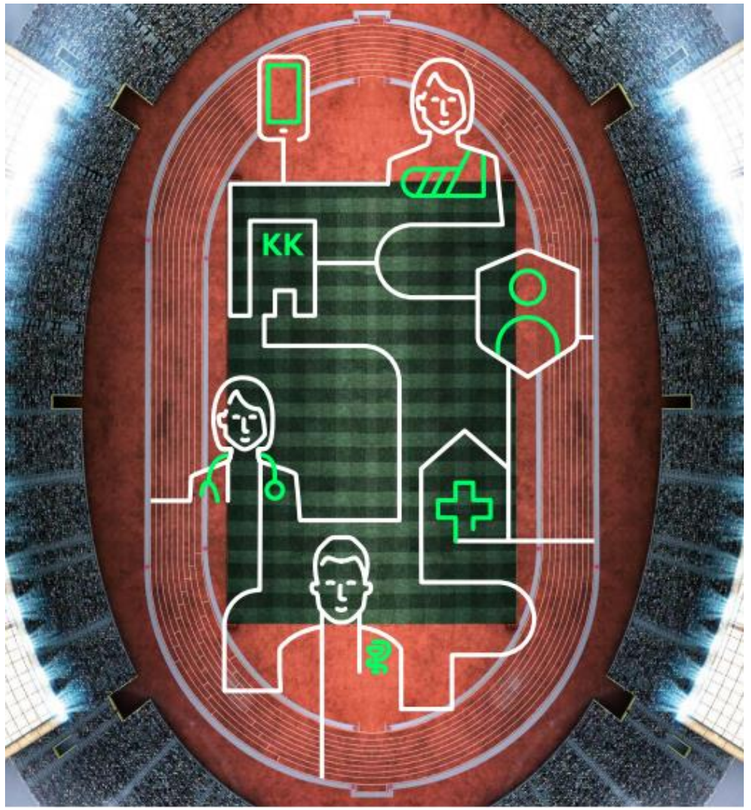
ePA Sicherheit?

- **100% Sicherheit gibt es nicht!**
- Skalierbarer Datendiebstahl der ePA eher unwahrscheinlich
  - Hoher Schutz (Betreiberausschluss & 2 getrennte Systeme)
- Wahrscheinlicher: Einbruch in einzelne Praxen/MVZ/KHs
  - Mehrere konkrete Angriffe bekannt: Praxis Hannover (Okt ‘19), Uniklinik Düsseldorf (Sept ‘20)…
  - In 2020: 43 Angriffe auf Gesundheitsdienstleister *

https://www.faz.net/aktuell/wirtschaft/digitec/mehr-hacker-angriffe-auf-kliniken-und-kritische-infrastruktur-17062421.html

Ausblick

- Technik wird immer weiterentwickelt -> TI 2.0*
  - Vorteil: Separates TI-Netz entfällt
  - Größerer Patientenfokus
  - Mögliche Nachteile: ePA Integration in europäische Lösungen schwierig (Interoperabilität)



* https://www.gematik.de/mediathek/publikationen

Fazit

TI mit-verantwortlich für Diskussionen über IT-Sicherheit und Datenschutz im Medizinsektor

Dezentrale Praxen/KHs == Hunderttausende mögliche Angriffsziele

Nutzung der verfügbaren Techniken immer auch eine persönliche Risiko/Nutzen Abwägung

Email: christoph.saatjohann@fh-muenster.de
Twitter: @SaatChris