



Telematik-Infrastruktur, ePA, KIM & Co, was steckt dahinter?

Teil 2: Herausforderungen für Praxen und mögliche Gefahren

Christoph Saatjohann

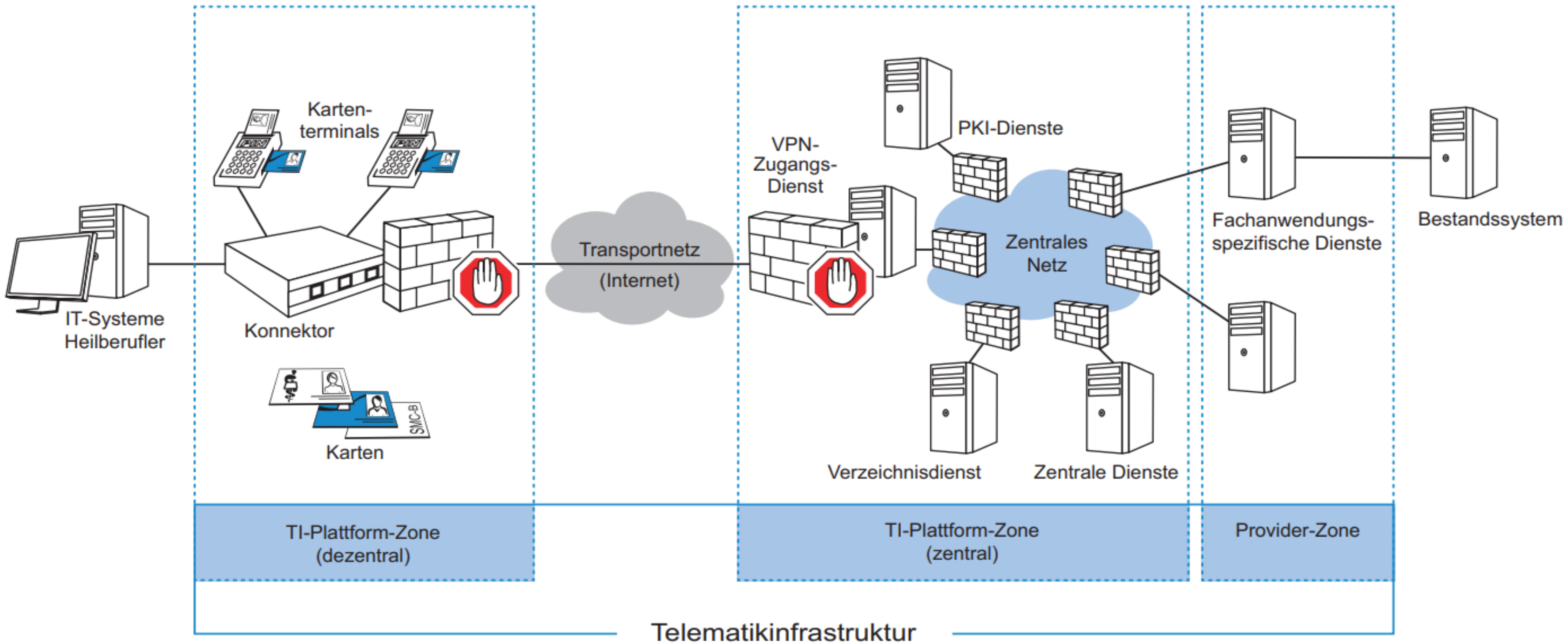
Labor für IT-Sicherheit

Email: christoph.saatjohann@fh-muenster.de

Twitter: [@SaatChris](https://twitter.com/SaatChris)



EINFÜHRUNG TELEMATIKINFRASTRUKTUR





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



Freie
Hansestadt
Bremen

DIE LANDESBEAUFTRAGTE FÜR DATENSCHUTZ

*LDI Bremen

AKTUELLES	WIR ÜBER UNS	DATENSCHUTZTIPPS	PUBLIKATIONEN
-----------	--------------	------------------	---------------

[Datenschutztipps](#) ▶ [Orientierungshilfen und Handlungshilfen](#) ▶ [Telefax ist nicht Datenschutz konform](#)

Telefax ist nicht Datenschutz konform



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



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

- 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



The image shows a form for an 'Arbeitsunfähigkeitsbescheinigung 1' (Sickness Certificate 1). The form is yellow and contains several fields for data entry. On the left side, there is a vertical instruction: 'Bitte sofort dem Arbeitgeber vorlegen!'. The form fields include: 'Krankenkasse bzw. Kostenträger', 'Name, Vorname des Versicherten' with a 'geb. am' field, 'Kostenträgerkennung', 'Versicherten-Nr.', 'Betriebsstätten-Nr.', 'Arzt-Nr.', and 'Datum'. There is a QR code next to the 'Versicherten-Nr.' field. Below the form, there are four checkboxes: 'Erstbescheinigung', 'Folgebescheinigung', 'Arbeitsunfall, Arbeitsunfallfolgen, Berufskrankheit', and 'dem Durchgangsarzt zugewiesen'. At the bottom left, there is a field 'arbeitsunfähig seit' followed by five small boxes for date entry. On the right side of the form, there is a box titled 'Ausfertigung zur Vorlage beim Arbeitgeber' and a paragraph of text: 'Der angegebenen Krankenkasse wird unverzüglich eine Bescheinigung über die Arbeitsunfähigkeit mit Angaben über die Diagnose sowie die voraussichtliche Dauer der Arbeitsunfähigkeit übersandt.'

- Digitale Übertragung der eAU an KK per KIM Dienst
- Frist: 01.01.2021
 - Übergangsfrist für bis Oktober 2021 falls Praxen technisch dafür noch nicht ausgerüstet sind
- Weiterleitung an AG: 01.01.2022



FRISTSETZUNGEN UND TERMINE



- eRezept:
 - Spezifikation: 30.06.2020
 - Einführung: 01.07.2021
- ePA:
 - Bereitstellung: 01.01.2021
 - Feingranulare Rechtevergabe: 01.01.2022
 - Forschungsdaten: 01.01.2023
- Fristen durch Gesetze vorgegeben
 - Beispiel: ePA, eAU, IT-Sicherheitsrichtlinie



Probleme bei starren Fristen

- Probleme:
 - IT Implementierung nach starren Fristen hat sich NICHT bewährt
- Besser: Agile Methoden ohne starre Fristen
 - Bsp: sobald 3 Anbieter Zulassung bestanden haben: Frist von einem Jahr zur Einführung beginnt



TEIL 2



- Technik wird immer weiterentwickelt
- Ab 2023 (DVPMG):
 - „Zukunftskonnektor“
 - Digitale Identitäten
 - DSFA durch den Gesetzgeber
- Aber: Spezifikation im Einvernehmen mit dem BSI / BfDI



ALTERNATIVEN ZUR TI?

Rahmenbedingungen einer med. Vernetzung

- Gemengelage mit unterschiedlichen Zielen: Patienten, Ärzte, Kassen, Politik, Unternehmen...
 - Siehe frühe TI Entwicklung und Historie der Gematik
- Abwägung: Komfort, Funktionalität, Sicherheit, Umsetzbarkeit, Finanzierbarkeit...

Nicht trivial ein System zu entwerfen was allen Anforderungen gerecht wird



Beispielhafte weitere Projekte

- Mediverbund Hausärztervernetzung
 - Technisch ähnlich zur TI:
Zentrales Netz, Ärzte verbinden sich per VPN Konnektor (bspw. GUSBox oder HÄVG)
- Westdeutschen Teleradiologieverbund
 - Sichere Übertragung von Bilddateien zwischen Praxen und Krankenhäusern
- Vorschlag Thomas Maus – Telepolis
 - Papierlastig (Versicherungsnachweise)
 - Rechtlich bedenklich:
 - „Versicherungsnachweis nur nach Anfrage bei KK“
 - Bei eRezept Betrug: Auskunftspflicht der Ärzte, Apotheker, Patienten
 - Wenig praktikables System der „Luftschleuse“ beim Arztbrief: „Sichtprüfung der Nachrichten“, „Quarantäne bis Bedrohungslage besser verstanden ist“

- **Mein Wünsche:**
 - Wahlweise Übermittlung von Daten Ende-zu-Ende (E2E) an Patienten -> KIM für Patienten
 - Alle Dienste: Standard-Protokolle mit E2E Verschlüsselung
- **Aber: Eine Alternative ist schon da!**
 - Patient kann sich Daten auf CD mitgeben lassen (DSGVO §20 / BGB § 630g)

Haftung und Verantwortung

Sofern die zugelassenen Komponenten (insbesondere der Konnektor) der TI bestimmungsgemäß verwendet werden und gemäß den mit dem BSI abgestimmten und im Betriebshandbuch der Komponente beschriebenen Anforderungen durch den Leistungserbringer aufgestellt und betrieben werden, scheidet eine Haftung des Leistungserbringers nach der DSGVO in jedem Fall aus.

- Keine Haftung bei TI- oder Konnektor-Hack

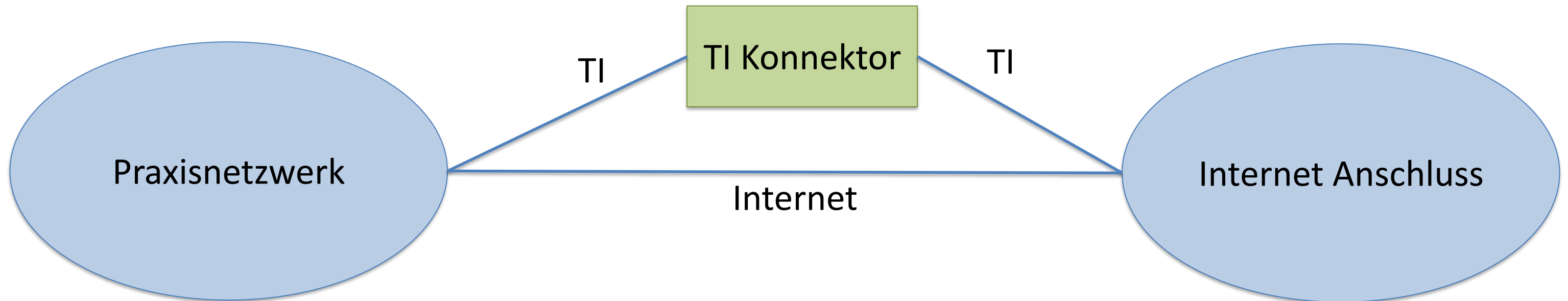
- Aber: PraxenbetreiberInnen haften für Vorfälle innerhalb Ihres Netzwerkes („Verschulden“)
 - Fehlkonfigurationen, nicht upgedatete Software, „Stand-der-Technik“ nicht eingehalten



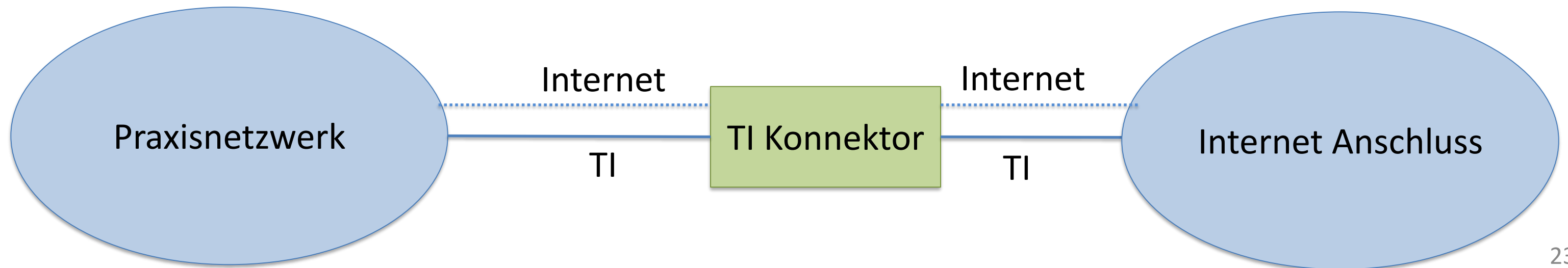
STANDALONE-TI AM INTERNETRECHNER

2 Anschlussmöglichkeiten

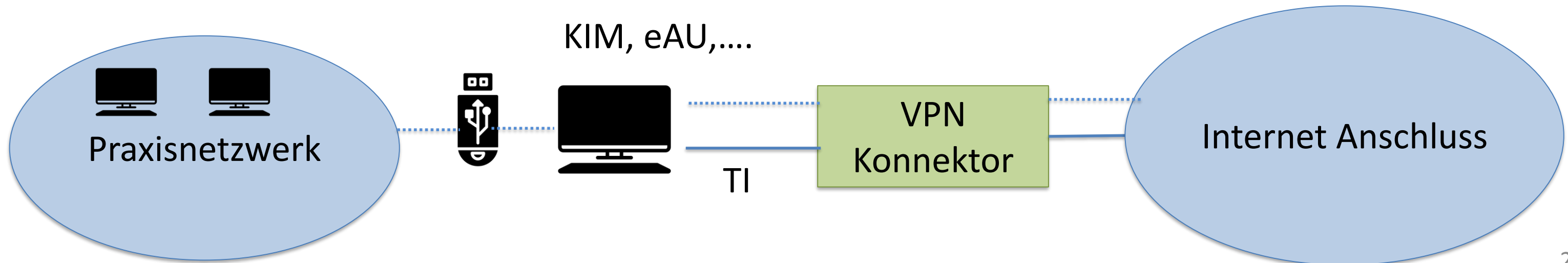
- Parallel: Direktes Internet für das Praxisnetzwerk



- Seriell: Internet für Praxisnetzwerk optional (SIS)

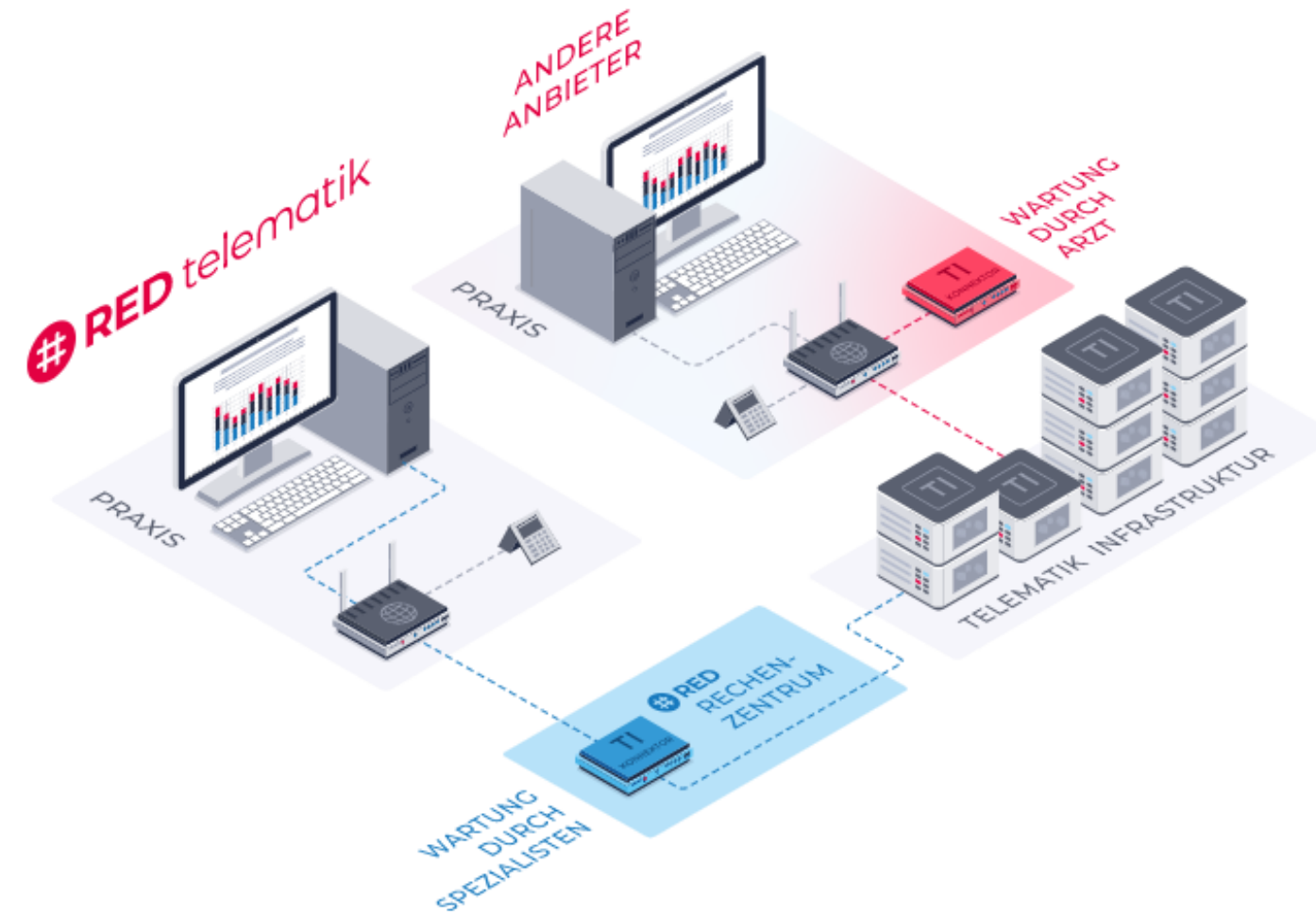


- Stand-Alone-PC - “Airgap”



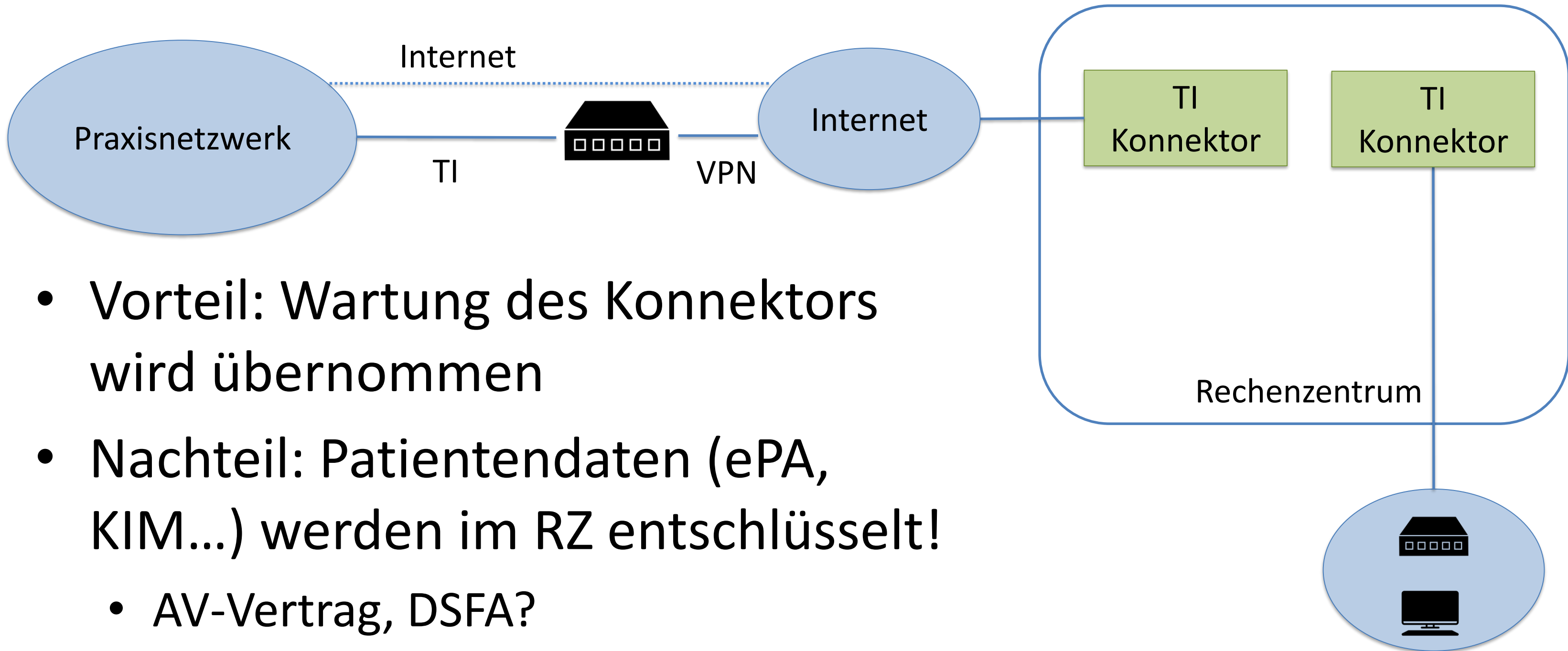
24

- TI-PC: eGK Einlesen, KIM, eAU, eRezept...
- Behandler-PC: Patientenakte
- Problem: Zusammenhängende Daten: Im- und Export von Daten zur Patientenakte
- Ganz ohne Kommunikation nicht möglich!
 - Wie sichere Kommunikation herstellen?
 - Updates für den Behandler-PC?



CLOUD-BASED-TELEMATIKINFRASTRUKTUR?

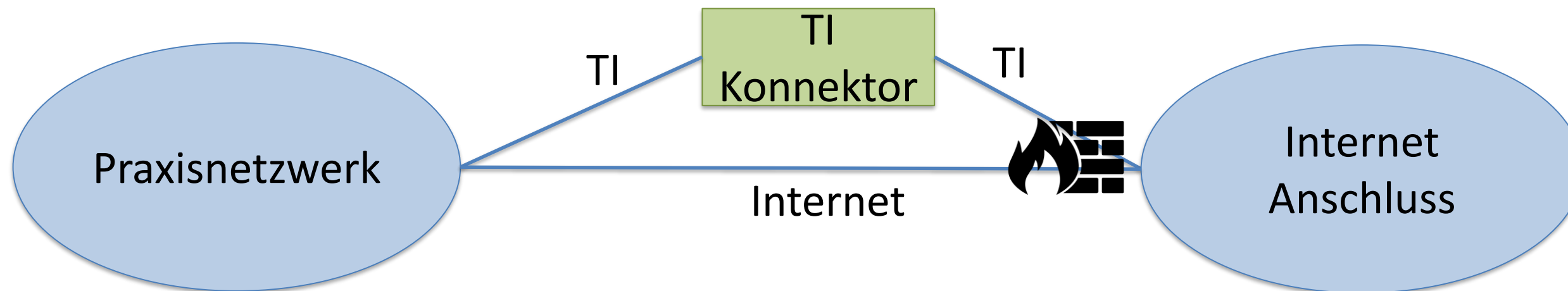
Rechenzentrums Konnektor



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

„Meine Lösung“ in unser Zahnarztpraxis

- Paralleler Anschluss mit Firewall/UTM



- Individuelle Entscheidung anhand der Rahmenbedingungen

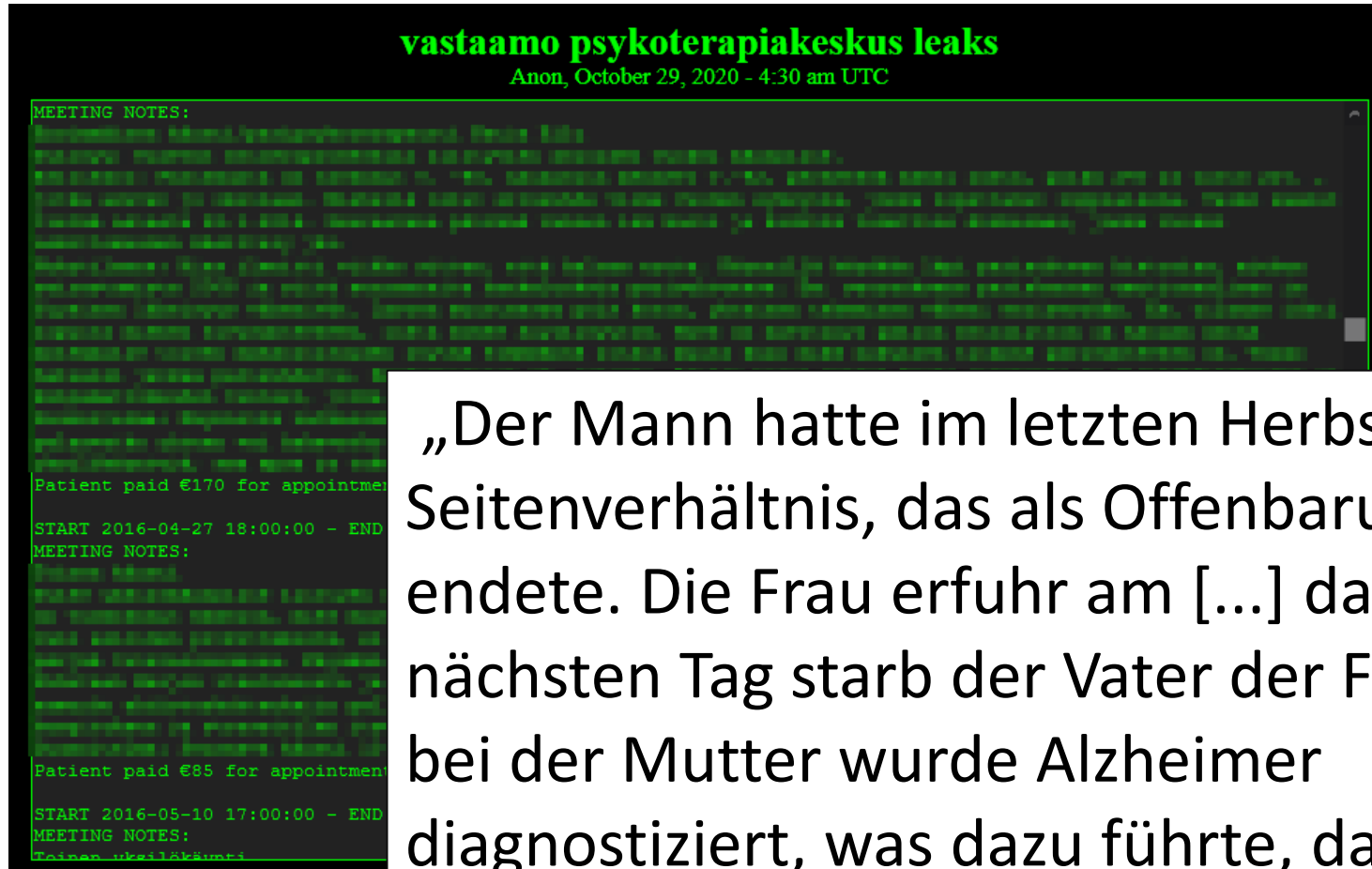
Wichtig: Geräte müssen entsprechend konfiguriert werden!



VASTAAMO-HACK



- Datendiebstahl zwischen Nov 2018 – März 2019
 - Intern bekannt seit März 2019
- Sept 2020: 450.000 Eur Forderung an Vastaamo
 - Keine Zahlung, Einschalten der Behörden
- Oktober 2020: Teilweise Veröffentlichung der Daten:
 - Patienten konnten sich für 200 - 700 Eur „freikaufen“
- Veröffentlichte Daten:
 - Mehrere hundert Berichte
 - Für kurze Zeit war eine 10GB Datei online



„Der Mann hatte im letzten Herbst ein Seitenverhältnis, das als Offenbarung endete. Die Frau erfuhr am [...] davon. Am nächsten Tag starb der Vater der Frau und bei der Mutter wurde Alzheimer diagnostiziert, was dazu führte, dass sich die Behandlung der Untreue verzögerte.“

Aus dem Forum:

"will literally kys myself if they are released"

- Keine detaillierten technischen Informationen veröffentlicht
 - Aber: Tendenz geht Richtung „aus dem offenen Internet erreichbaren Datenbankserver“
- Verstöße durch CEO -> IT-Einbruch war bekannt!
- Einordnung: Finnland betreibt seit Jahren ‚Kanta‘
 - Hier: Datenleak aus privater Firma!

- **100% Sicherheit gibt es nie!**
- Datendiebstahl der ePA in diesem Ausmaß unwahrscheinlich
 - Sehr hoher Schutz (2 getrennte Schutz-Systeme)
- **Wesentlich 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.aend.de/article/209051>



WAS IST ZU TUN?



Richtlinien / Empfehlungen zur IT Sicherheit

- KBV Technische Anlage*, diverse Handreichungen anderer Institutionen
- SGB 5 §75b: KBV/KZBV erstellt verbindliche Empfehlungen
 - Eigentliche Frist: 30. Juni 2020

* https://www.kbv.de/media/sp/Technische_Anlage_Datenschutz.pdf

IT-Sicherheitsrichtlinie – Was ist passiert?

- 1. Entwurf: Profil für „IT-Grundschatz“
 - Gesamtes ‚Kompendium‘ 816 Seiten
 - Grundschatz: Verschiedene Bausteinen und Sicherheits-Anforderungen
- KBV 12. Juni: Resolution: Keine Richtlinie ohne gesonderte Finanzierung der Praxen
- KBV-VV 11.09.: Bestätigung der Resolution

IT-Sicherheitsrichtlinie – Wie gehts weiter?

- Verbindliche Richtlinie wird **dringend** benötigt!
 - Rechtliche Sicherheit der Psychotherapeuten/Ärzte
 - Transparenz der Kosten für IT-Sicherheit
- Aber Auch ohne Richtlinie: **Art. 32 DSGVO** - Pflicht zur Umsetzung „Stand der Technik“
 - Auch ohne TI relevant!
 - Mehrheit der Praxen nutzen IT Systeme:
Backup, Passwörter, Telefonie, Video-Konferenz, Emails,
Online-Terminvergabe,



Persönliche Empfehlung für Ihre IT

- Regionaler Systembetreuer mit Referenzen im Medizin Sektor
- Stand-der-Technik („Technische Anlage“) befolgen
- Mindestmaß an Dokumentation
 - Aussagekräftige Verträge / Leistungsbeschreibungen
- Evtl. Cyber-Risk Versicherung



TI verantwortlich für Diskussionen über IT-Sicherheit und
Datenschutz!

Aber: Alle bisherigen Sicherheitsvorfälle unabhängig der TI!

Dezentrale Praxen/KHs == Hunderttausende mögliche Angriffsziele

Email: christoph.saatjohann@fh-muenster.de

Twitter: [@SaatChris](https://twitter.com/SaatChris)