bvvp WESTFALEN-LIPPE

REGIONALTREFFEN-
BVVP- WL

03.03.2021

THEMA: IT-RICHTLINIE- EINE ANNÄHERUNG

1. Einleitung: worum es geht und Stand der Dinge
2. Einzelne Beispiel-Anforderungen
3. Konkretisierung Herr Saatjohann: inklusive „Konnektorfarm“-Alternative? u. „TI 2,0“
4. Weiteres: eHBA, Homepage, Mitgliederentwicklung

1/

IT-SICHERHEITS-RICHTLINIE

Einleitung

- DSGVO regelt sicheren Umgang mit personenbezogenen Daten, europaweit, 2018
- Datenverarbeitung bei gesetzlicher Grundlage oder Einwilligung des Betroffenen
- StGB/SGB V (höheres Recht): Schweigepflicht, Offenbarungspflicht
- BSI: Bundesamt für Sicherheit in der Informationstechnik
- IT-Richtlinie: „Kompromiss“ zw. Forderung des BSI und Umsetzungsfähigkeit in Praxis

Einleitung

- Gültig ab 01.01.2021
- Verbindlich: 01.04.2021 / 01.01.2022
- Praxisinhaber verantwortlich, Haftungsrisiko
- Unterteilung in Praxisgröße, Datenumfang, zusätzlich Großgeräte und Dezentrale Komponenten
- Vorteil: bringt uns bei Einhaltung aus der Haftung bei kriminellen Angriffen

Durchzuführende Anforderungen

https://www.kbv.de/media/sp/RiLi___75b_SGB_V_Anforderungen_Gewaehrleistung_IT-Sicherheit.pdf

- „Praxis“: Anlage 1 und 5
- „Mittlere Praxis“: Anlage 1,2 und 5
- „Großpraxis“: Anlagen 1,2,3 und 5

Einleitung: Bestandteile

- Mobile Anwendungen (Apps)
- Office Produkte
- Internet-Anwendungen
- Endgeräte
- Smartphone und Tablet
- Mobiltelefon
- Wechseldatenträger / Speichermedien
- Netzwerksicherheit
- Endgeräte mit dem Betriebssystem MS Windows
- Mobile Device Management

Kritik

- zu ungenau
- zu viel Text
- teils schwer verständlich
- auch für kleinere Praxen „weitere“ Anforderungen (hardware-Firewall)
- es fehlen Erklär-Videos
- es fehlen bessere Musterpläne zur Ausarbeitung der individuellen Praxisstruktur

2/

IM EINZELNEN

Mindestziele/-maßnahmen

- Schutz vor Phishing und Schadprogrammen im Browser
- Verwendung von SIM-Karten-PINs
- Zugriffschutz: Sperrcodes, Bildschirmsperre
- Updates von Betriebssystemen, APPs

Im Einzelnen ab 01.04.2021

- Verzicht auf Cloud-Speicherung
- Beseitigung von Rest-Information vor Weitergabe von Dokumenten
- Keine vertraulichen Daten im Browser speichern
- Nur Internet-Anwendungen mit Authentifizierung nutzen
- Die Zugänge strikt absichern

- Nur verschlüsselte Internet-Anwendungen nutzen
- Sichere und aktuelle APP nutzen
- Mikrophon und Kamera am Rechner deaktivieren und nur temporär aktivieren
- Zugriffsschutz für Smartphone und Tablet
- Absicherung von Netzübergangspunkten

Ab 01.01.2022

- Firewall benutzen (laufend zu aktualisieren)
- Sichere Speicherung lokaler App-Daten
- Regelmäßige Datensicherung
- Sichere Grundkonfiguration für mobile Geräte
- Wechseldatenträger bei jeder Verwendung auf Schadsoftware überprüfen
- Nutzen der Sicherheitsmechanismen von Mobiltelefonen

- Die von der gematik zur Verfügung gestellten Informationen für Installation der TI-Komponenten berücksichtigen
- Hinweise zum sicheren Betrieb der dezentralen Komponenten der TI berücksichtigen
- TI-Komponenten vor Zugriff Unberechtigter schützen
- Sicheres Aufbewahren der Administrationsdaten für die TI-Komponenten

„Zusammenfassung“?

„Wenn man seinen Praxiscomputer ohne Mikro und ohne Kamera in einem abgeschlossenen Raum in Reihe hinter dem Konnektor geschaltet hat, er ein Zugangspasswort besitzt, die Office-Software nicht in eine Cloud geht, das Betriebssystem und eine Antivirensoftware regelmäßig upgedatet wird, Daten regelmäßig auf einem externen Datenträger abgesichert werden, keine Patientendaten (auch keine Telefonnummern) auf dem Handy sind oder man ein eigenes Praxishandy hat, auf dem möglichst keine weiteren Apps aufgespielt sind und welches mit einem SIM-Karten-PIN geschützt ist, erfüllt man die Anforderungen der Richtlinie mit relativ großer Sicherheit schon zum wesentlichen Teil.“

- bei Parallel-Anschluss: mindestens eine Hardware-Firewall zusätzlich !?

3/

KONKRETISIERUNG

CHRISTOPH SAATJOHANN

Email: christoph.saatjohann@posteo.de

Twitter: @SaatChris

KBV/KZBV IT-Sicherheitsrichtlinie

- **! Unabhängig von der TI !**
- Begrifflichkeiten teilweise aus dem BSI Grundschutz übernommen
  - Kann als Anhaltspunkt zur Interpretation dienen
- Allgemein: Viele Unklarheiten, doppelte/sich widersprechende Punkte

Beispielhafte offene Fragen

- Anzahl der ständig mit der DV betrauten Personen entscheidend:
  - Sicherheitsanforderung einer 4er Psychotherapeuten Praxis geringer als einer mittleren Zahnarztpraxis?
  - Was gilt bei einer Praxisgemeinschaft?
- Verantwortlicher:
  - SGB V §75b: Verbindlich für Leistungserbringer
  - Richtlinie: Praxisinhaber*in verantwortlich
- Regeln für das Home Office?

FIREWALL IN DER PRAXIS

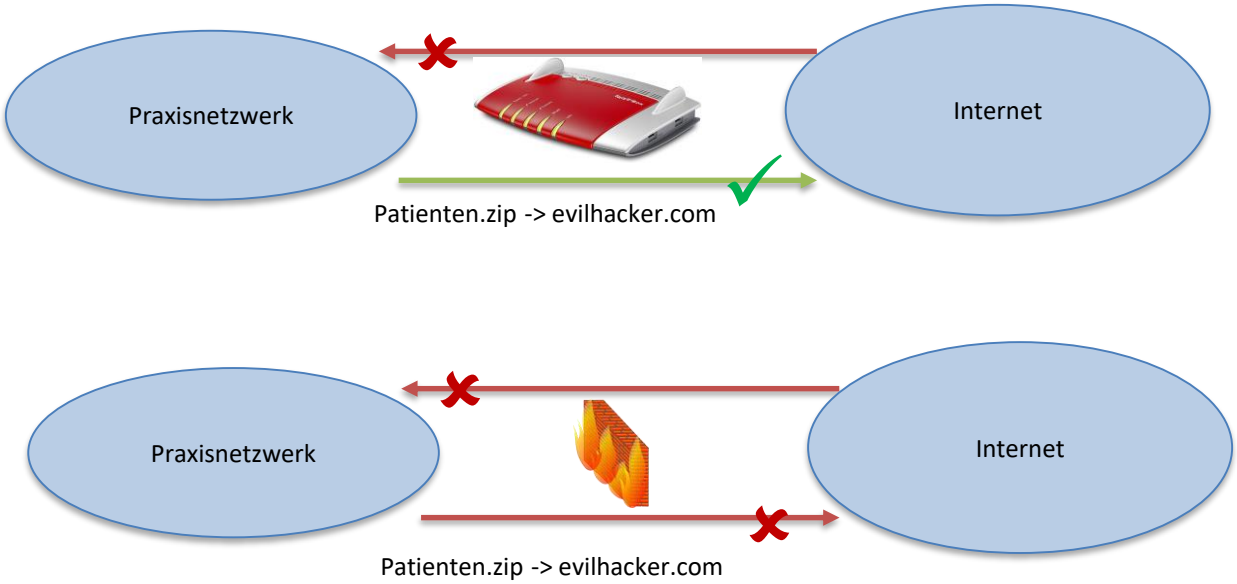
(01.04.2021 – A1, 32.)

Firewall

Der Übergang zu anderen Netzen insbesondere das Internet muss durch eine Firewall geschützt werden.	01.04.2021

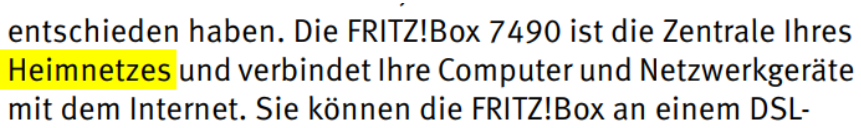
- Was für eine Firewall wird benötigt (FritzBox?)
- KBV Empfehlung: HW-Firewall mit Allowlist
- Grundschutz: Firewall mit Allowlist (NET 3.2.A2)

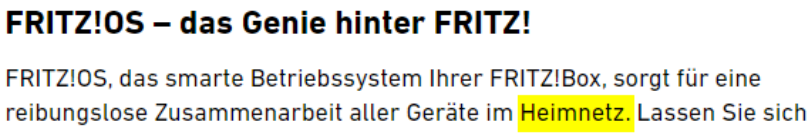
FritzBox vs. „HW-Firewall“



- **Nur explizite erlaubte Datenverbindungen in das Internet sind erlaubt (Allowlist)**

FritzBox


entschieden haben. Die FRITZ!Box 7490 ist die Zentrale Ihres Heimnetzes und verbindet Ihre Computer und Netzwerkgeräte mit dem Internet. Sie können die FRITZ!Box an einem DSL-


FRITZ!OS – das Genie hinter FRITZ!

FRITZ!OS, das smarte Betriebssystem Ihrer FRITZ!Box, sorgt für eine reibungslose Zusammenarbeit aller Geräte im Heimnetz. Lassen Sie sich

- FritzBox ist für den **privaten** Gebrauch konzipiert und nicht für den professionellen Einsatz gedacht!

Firewall Fazit

- Sicherer (Technisch & Haftung): HW Firewall/UTM
- Wichtig: **Konfiguration der Firewall (auch im Konnektor)**
- Aber: Explizit vorgeschrieben ist nur „Firewall“
  - Unternehmerische Entscheidung ob nur FritzBox genutzt wird (Bsp. Internet Nutzung nur für TI und Updates)

NETZPLAN

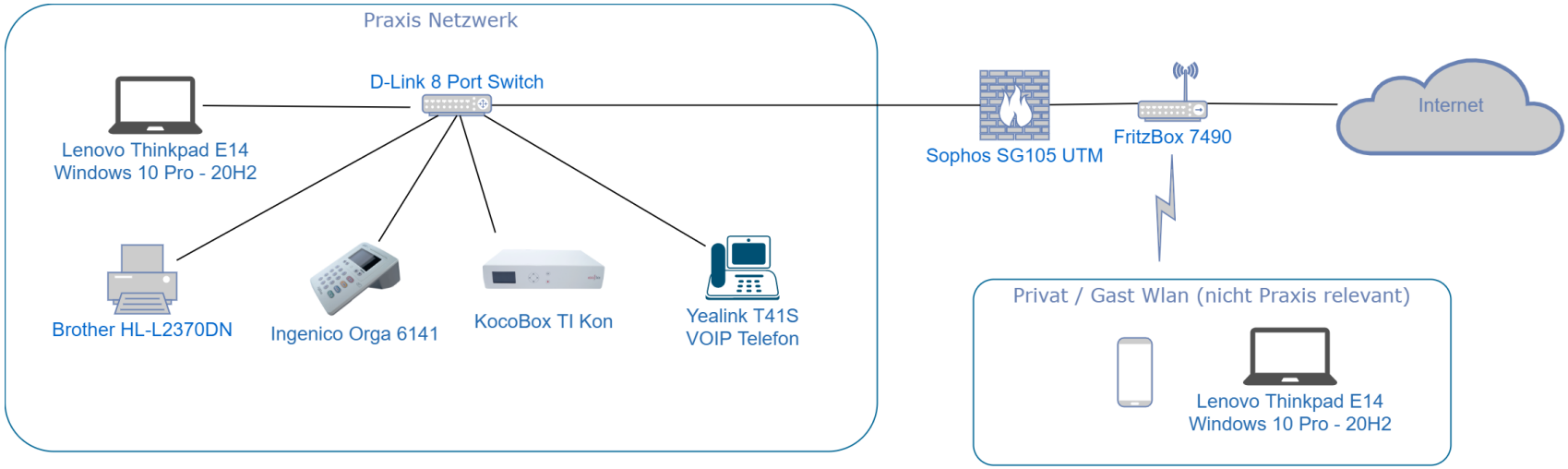
(01.04.2021 – A1, 33.)

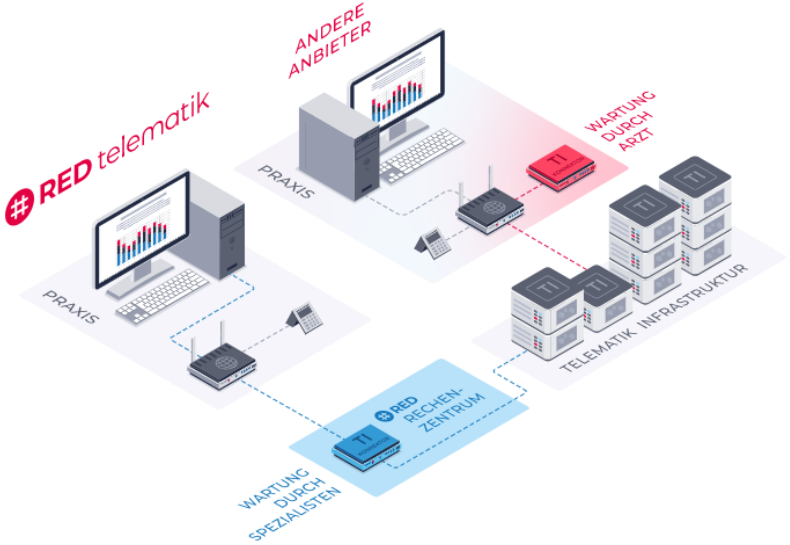
Netzplan

- Grundschutz Definition (BSI Standard 100-2 - 4.2.2.):
  - IT-Systeme, d. h. Client- und Server-Computer, aktive Netzkomponenten (wie Switches, Router, WLAN Access Points), Netzdrucker etc.
  - Netzverbindungen
  - Minimalsatz von Informationen: eindeutige Bezeichnung, Typ und Funktion, Platform, Standort, etc.

Beispiel Plan - Einzelpraxis

- Erstellt mit draw.io (Vorlage wird verschickt)

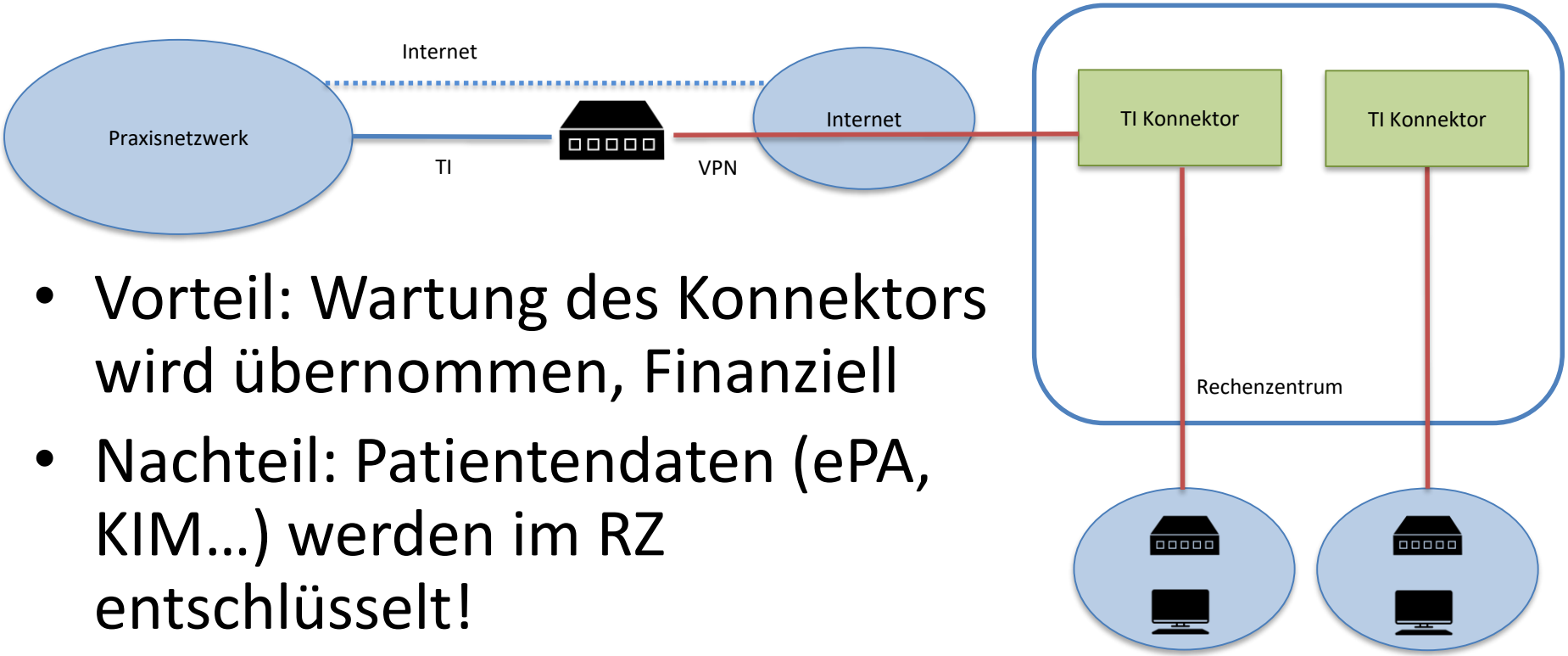




CLOUD-BASED-TELEMATIKINFRASTRUKTUR?

* https://www.redmedical.de/telematik-praxis

Rechenzentrums-Konnektor



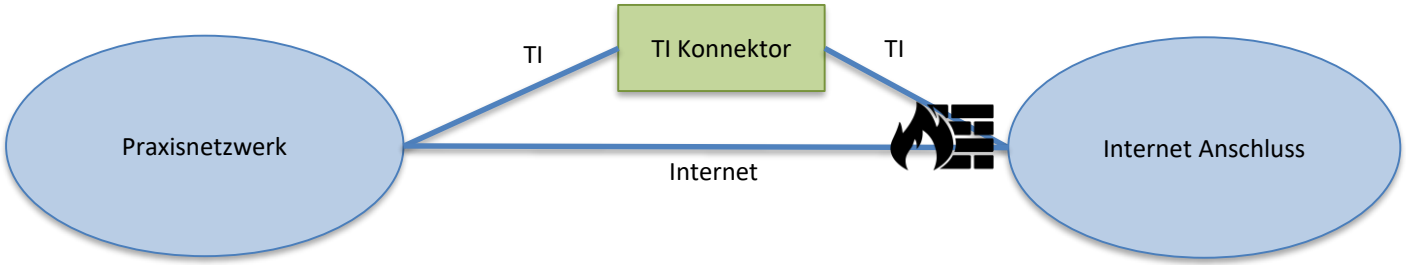
- Vorteil: Wartung des Konnektors wird übernommen, Finanziell
- Nachteil: Patientendaten (ePA, KIM…) werden im RZ entschlüsselt!
  - AV-Vertrag, DSFA?

Konnektor-as-a-Service

- Relevante Entscheidungsgrundlagen:
  - Weniger Wartungsaufwand
  - Finanzielle Vorteile
  - Datenschutzbedenken gegen TI/Konnektor

„Meine Lösung“ in unser Zahnarztpraxis

- Paralleler Anschluss mit Firewall/UTM



- Individuelle Entscheidung anhand der Rahmenbedingungen

<u>Wichtig:</u> Geräte müssen entsprechend konfiguriert werden!

Wie sieht es im Home-Office aus?

TELEMATIKINFRASTRUKTUR 2.0

TI 2.0

- Diskussionsgrundlage für Neugestaltung der TI
  - Kein festgeschriebener Fahrplan
  - Noch keine technischen Spezifikationen
- IT Systeme sind immer im Wandel
  - Nach der TI 2.0 dann irgendwann „TI 3.0“….
- Sollte NICHT als Entscheidungsgrundlage für aktuellen TI-Anschluss dienen

4/

WEITERES:

EHBA, HOMEPAGE, MITGLIEDERENTWICKLUNG

Elektronischer Heilberufsausweis
Elektronischer Psychotherapeutenausweis eHBA

- **Für ÄPT**: Für die Bestellung die Portalseite der Ärztekammer Westfalen-Lippe (ÄKWL) aufrufen. Es gibt 4 Anbieter: Bundesdruckerei GmbH, Medisign GmbH, SHC Stolle und Heinz Consultants GmbH oder T-Systems international GmbH. Kosten vergleichbar, bei Bundesdruckerei einmalig für 5 Jahre. Die Identifizierung mit Personalausweis auch per Post-Ident online möglich.

  https://www.aekwl.de

- **Für PP und KJP**: Die Psychotherapeutenkammer NRW ist dafür zuständig, die Daten der Antragstellenden gegenüber dem gewählten Anbieter zu verifizieren. **Aktuell kann der elektronische Psychotherapeutenausweises noch nicht bestellt werden.** Die Kammer wird ihre Mitglieder rechtzeitig darüber informieren, wann die elektronischen Psychotherapeutenausweise ausgegeben werden können.

  https://www.ptk-nrw.de/berufsstand/epsychotherapeutenausweis

Homepage des Landesverbands

https://westfalen-lippe.mein-bvvp.de/

- Überarbeitung und Pflege durch professionelle Betreuung der Firma „odecologne webdesign“
- Derzeit aktuelle praxisrelevante und berufspolitische Themen unter „Home“
- „Westfalen-Lippe aktuell“: Termine von Mitgliederversammlungen, Regionaltreffen, Seminaren oder Videoberatungen (in Planung)
- Was sind Ihre Wünsche bzgl. unserer Landeshomepage?

Mitgliederentwicklung

- Positive Entwicklung: 38 neue Mitglieder bei 9 Kündigungen
- Von den 38 Neumitgliedern 21 durch MwM-Aktion
- Derzeit: 221 ÄP, 110 PP, 46 KJP, 4 KJP/PP, 14 PiA
- Aufgrund des hohen Altersdurchschnitts vor allem bei den ÄP ist in den nächsten Jahren mit Mitgliedschaftbeendigungen zu rechnen
- Daher weiter Mitgliederwerbung wichtig
- Die Erfahrung zeigt: Mitglieder sorgen sehr erfolgreich für Nachwuchs in unserem Verband

Vielen Dank für Ihre Aufmerksamkeit !