Hessischer Hausärzteverband
Bezirksverband Wiesbaden

Wiesbaden, 26.05.2019

Sehr geehrte Kolleginnen und Kollegen,

Die Digitalisierung ist im Gesundheitssystem angekommen und wirft für uns im Praxisbetrieb neue Fragen auf. Die aktuell wichtigste Frage betrifft den Betrieb des Konnektors, mit dem die Verbindung zum sicheren Netz der Telematikinfrastruktur aufgebaut wird. Die Empfehlungen der KBV und der gematik entpuppen sich dabei als unpraktikabel. Statt Arbeitserleichterung bedeutet die Digitalisierung für uns Mehrarbeit und Mehrkosten für die Praxen.

Ich möchte Ihnen mit diesem Text vereinfacht die Hintergründe erklären und versuchen einige praktische Hilfestellungen zu geben.

Die Digitalisierung des Gesundheitssystems wird aktuell nach dem Motto: „Digitalisierung first, Bedenken second“ vom Bundesgesundheitsministerium unter Jens Spahn erzwungen. Grundsätzlich gibt es viele digitale Anwendungen, die uns Ärzten bei der Versorgung der Patienten in Klinik und Praxis helfen könnten. Doch Gesundheitsdaten gehören nicht ohne Grund zu den besonders schützwerten Daten (§9 DSGVO), weshalb ein gewisses Minimum an Datenschutz eben nicht nur zu „Bedenken“ sind, sondern zu den zentralen Anforderungen an eine funktionierende Telematikinfrastruktur (TI) gehören.

Aktuell müssen sich alle Arztpraxen Deutschlands per Zwang an das Netz der TI anschließen lassen. Zentral für den Aufbau des sicheren Netzes der TI ist dabei ein verschlüsselter Kanal, oder Tunnel, (Virtual Private Network-VPN), über den Daten zwischen den Arztpraxen und künftig auch Krankenhäusern, Apotheken und weiteren Leistungserbringern, aber auch den Krankenkassen, ausgetauscht werden können. Der VPN-Tunnel wird dabei von einem spezialisierten Router, dem Konnektor, aufgebaut.

Seriell oder paralleler Betrieb des Konrektors?

Ab hier beginnt der Schildbürgerstreich in der Digitalisierung des Gesundheitssystems. Der Konnektor kann in den Praxen auf zwei Wegen installiert werden. Entweder wie von der gematik empfohlen im seriellen (Reihen-) Betrieb, oder in einem zweiten, nicht empfohlenen, aber erlaubten Betrieb, dem parallelen-Betrieb. Bei der Installation müssen wir Ärzte uns für eine von diesen beiden Installationen entscheiden.[1]

In persönlichen Kontakten zu einer Vielzahl hessischer Vertragsärzte und bundesweit zu etlichen Hausärzten ist mir keine Praxis bekannt, die den Konnektor im seriellen Betrieb installiert hat. Dieses kleine aber entscheidende Detail ist aber für das Thema des Datenschutzes, der Haftung und der Finanzierung wegweisend.

[1] https://www.gematik.de/fileadmin/user_upload/gematik/files/Publikationen/gem_OPB_Infoblatt_Anschluss_2017-10-BR-DGDV1_web.pdf

Im **seriellen Betrieb (Abb.1)** ist das Internet und das Praxisnetz durch den Konnektor voneinander getrennt. Der Konnektor blockiert das gesamte Internet und baut nur den VPN-Tunnel in das sichere Netz der gematik auf. Diese Installation bietet auf der einen Seite den größten Schutz (deswegen wird der serielle Betrieb auch von der Kassenärztliche Bundesvereinigung (KBV), der gematik und vom Bundesamt für Sicherheit und Informationstechnik (BSI) empfohlen), auf der anderen Seite funktioniert damit nicht mal mehr ein Windows-update, da kein freier Zugang zum Internet mehr besteht (siehe Tabelle auf Seite 6).

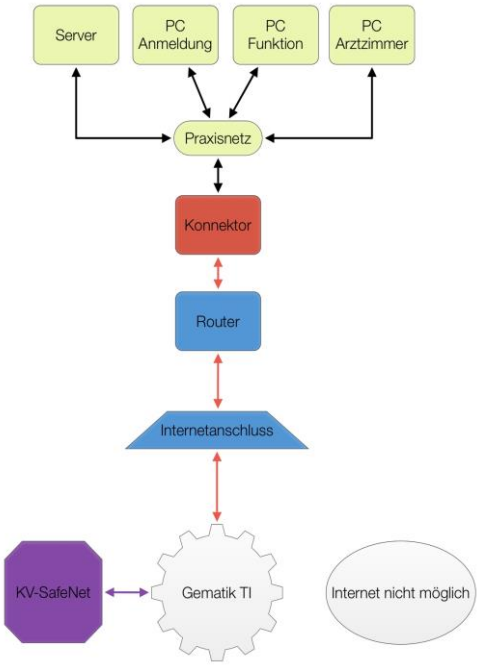

Abb.1: serielle Installation. Vereinfachte Darstellung

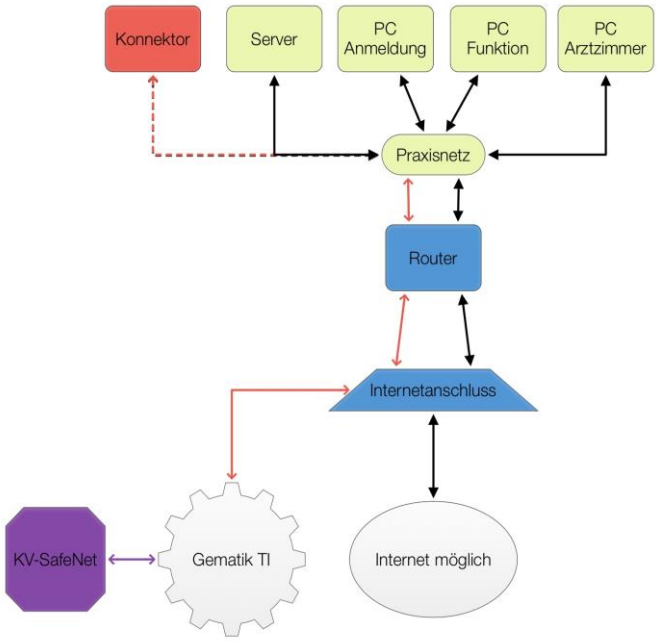

Abb.2: parallele Installation. Vereinfachte Darstellung

Dieses Problem kann man mit dem **parallelen Betrieb (Abb.2)** umgehen. Im parallelen Betrieb ist jedoch kein Computer mehr durch den Konnektor vor unautorisierten Zugriffen geschützt. Damit besteht kein Schutz vor Angriffen aus dem Internet und der Praxisinhaber muss sich selber um einen ausreichenden Schutz (Firewall) kümmern. Die KBV hat sich dazu bereits eindeutig geäußert: „Ärzte und Psychotherapeuten sind nicht für die Sicherheit in der TI verantwortlich, wohl aber für den Datenschutz in ihrer Praxis“, erläuterte Kriedel. Für eine sichere Firewall beim Parallelbetrieb des Konnektors haftet also letztlich der Praxisinhaber.[2]

Der serielle Betrieb ist das Feigenblatt der gematik (siehe Tabelle). Die Sicherheit des gesamten Systems wird im seriellen Betrieb zwar garantiert, doch für eine Digitalisierung des Gesundheitswesens ist dieser Betrieb komplett unzureichend. Es bleibt sogar fraglich, ob die weiteren geplanten Änderungen allein von den Datenmengen (immerhin müssen Zugriffe von 150.000 Arztpraxen, 2000 Krankenhäuser, etlichen Apotheken, Physiotherapeuten und Geschäftsstellen der Krankenkassen auf Labor, Diagnosen, evtl. Bildgebende Verfahren, elektronische Patientenakte (ePA) verwaltet werden) im Netz der gematik, und viel wichtiger über die entsprechenden Server, vernünftig verwaltete werden können.

[2] https://www.kbv.de/html/1150_40271.php

Die Sicherheit der TI ist für die Arztpraxis nur im seriellen Betrieb in die Haftung der gematik eingeschlossen. Zumindest wenn es um Angriffe aus dem Internet geht. In der parallelen Installation haftet die Arztpraxis alleine.

Durch den seriellen Betrieb entstehen (theoretisch) kaum **weitere Kosten**. Die Frage, wie man allein ein update von Windows oder dem Praxisverwaltungsprogramm bekommt wird nicht beantwortet. Im parallelen Betrieb entstehen durch die Wartung, Pflege, die Updates, etc. natürlich weitere Kosten. Doch diese Folgekosten werden bei der Erstattung nicht berücksichtigt.

Welche Folge eine unzureichende Finanzierung hat, konnten wir bei dem Datenskandal in England gut sehen.[3] Dort wurden aufgrund fehlender Finanzierungen wichtige updates nicht aufgespielt und es konnten Patientendaten aus einem Krankenhaus entweder werden. Bis Januar 2020 müssen alle Praxen z.B. auf Windows 10 umsteigen. Die Digitale Welt mag das Potential haben Kosten einzusparen, doch die Frage muss schon heißen: für wen?

Die niedergelassenen Ärzte werden mit den Folgekosten der Digitalisierung alleine gelassen. Als Grundlage der Finanzierung wird uns mit dem seriellen Betrieb des Konnektors ein nicht praktikables, dem Gedanken der Digitalisierung sogar entgegenstehendes Model empfohlen.

Der Anschluss in der Praxis

Aktuell müssen Ärzte, die nicht an die TI angeschlossen sind mit 1% KV-Honorarabzug rechnen. Jens Spahn nächster e-Heath-Gesetzentwurf sieht einen Strafabzug von 2,5% ab 2020/2021 vor.[4]

Kolleginnen und Kollegen, die mit diesen Abzügen leben können, oder in den nächsten Jahren in Rente gehen möchten, können beruhigt auf den TI-Anschluß verzichten. Aktuell gibt es keine Anwendungen, die der direkten Patientenversorgung dienlich ist. Es werden keine Praxisabläufe unterstützt oder vereinfacht (es dauert sogar alles eine Spur länger). Die geplanten Applikationen wie Notfalldatensatz, elektronische Patientenkarte, e-Rezept, etc. sind zwar vorgedacht, aber es existieren noch nicht einmal vernünftige, veröffentlichte Modelle. Die App Vivy (ein Portal für eine durch Patienten geführte Ansammlung von Arztberichten) oder die ePA der Techniker Krankenkasse sind hier am weitesten, jedoch für uns im alltäglichen Einsatz eher eine Arbeitsbelastung. Den: irgendwer muss die Daten ja pflegen, eingeben, bearbeiten, korrigieren. Eine Arbeit bei der Jens Spahn in seinen neuen eHealth Gesetzentwurf an Hausärztinnen und Hausärzte als billige Erfüllungshilfen denkt.[5]

[3] https://www.futurezone.de/digital-life/article214159475/Patientendaten-aus-hunderten-Krankenhaeusern-gestohlen.html
[4] https://www.tagesspiegel.de/politik/gesetzentwurf-des-gesundheitsministers-spahn-will-aerzte-und-kassen-zu-digitalisierung-zwingen/24345002.html
[5] https://e-health-com.de/details-news/digitale-versorgung-gesetz-der-rundumschlag/

Für uns wird die Digitalisierung auf absehbare Zeit keine Arbeitserleichterung bringen. Wir werden diejenigen sein „dürfen“, durch deren Arbeit dieses System überhaupt erst aufgebaut wird. Vielmehr dient die Digitalisierung vor allem der Verschlankung der Krankenkassen (administrativen Strukturen), einer besseren Kontrolle der Ärztinnen und Ärzte und meiner Meinung nach der wichtigste Punkt: der dritte Gesundheitsmarkt[6] (eHealth durch Investoren mit der Illusion der Patienten mehr Kontrolle über ihre eigenen Daten zu haben) wird auf Kosten des ersten (alle durch die GKV finanzierten Gesundheitsleistungen) und zweiten Gesundheitsmarktes (alle privat finanzierten Gesundheitsleistungen) gestärkt.

Da die Digitalisierung des Gesundheitssystems mit der TI aber politisches Programm ist, haben viele Kolleginnen und Kollegen, die mit den angedrohten Strafabzügen nicht leben wollen, bereits bestellt und erwarten den Einbau des Konnektors im Laufe des Jahres.

Praktische Empfehlungen für den Anschluss

Hier würde ich aus eigener Erfahrung empfehlen, dass man an einem Rechner in der Praxis (Büro, Labor, u.ä.) noch das alte Kartenlesegerät installiert lässt und das neue Kartenlesegerät mit Konnektoranschluss an der Anmeldung installiert (beide Lesegeräte an einem Rechner gehen nicht, bitte hierzu eigenen PVS-Anbieter kontaktieren). Damit hätte man bei Netzausfällen, oder anderen Fehlern, immer noch das altes System, solange es funktioniert, als Backup. Rückmeldungen zur Stabilität der neuen Kartenlesegerät und dem Konnektoranschluss an die TI fallen sehr unterschiedlich aus. Ich habe Rückmeldungen von „funktioniert tadellos“ bis hin zu „fällt dauernd aus“ erhalten; bei uns selber gab es nur vereinzelte, kurz anhaltende Fehler (Abb.3).

Ob nun Konnektor oder nicht. Der Internetzugang sollte immer mit einer ausreichenden Firewall und die Rechner mit einem aktuellen Virenschutzprogramm geschützt werden. In vielen Routern gibt es integrierte Firewalls. Diese sollten auf jeden Fall den Sicherheitsstandard ELA4+[7] erfüllen (Abb.3).

Der Internetzugang über das Hauptsystem sollte im besten Fall nur für die Updates und die Fernwartung genutzt werden. Zudem empfehle ich, angesichts der zunehmenden Bedrohung durch Viren und Trojaner, eMails nicht über das Hauptsystem zu empfangen. Man könnte ein, vom Hauptsystem unabhängiges, WLAN in der Praxis installieren und die eMails können so sicher über ein Tablett oder einen unabhängigen Rechner ohne PVS-Anschluß bearbeitet werden (Abb.3). Auch Internetrecherchen können so sicher und unabhängig durchgeführt werden.

6 https://www.zukunftsinstitut.de/fileadmin/user_upload/Publikationen/Auftragsstudien/Zukunftsinstitut_Philips_Gesundheitsstudie_2015.pdf

7 https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ITSicherheitskriterien/CommonCriteria/eal_stufe.html

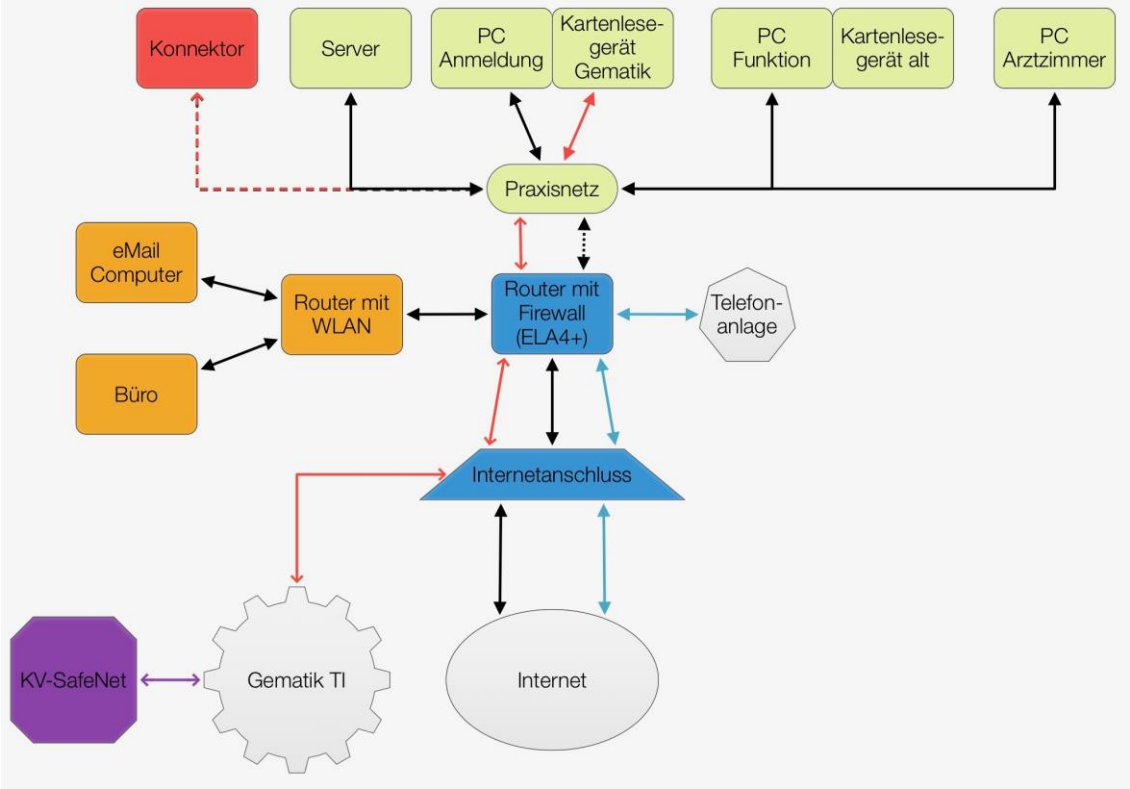

Abb.3 Beispiel für eine Netzarchitektur in der Praxis

Fazit

Der Aufbau der Digitalisierung des Gesundheitssystems in Deutschland wird auf dem Rücken der Ärzte ausgetragen. Die finanzielle Förderung entspricht nur dem Reihenbetrieb, mit allen weiteren Kosten und vor allem mit der Haftung werden in Deutschland 150.000 Ärztinnen und Ärzte von der Politik alleine gelassen.

Der hessische Hausärzteverband hat auf der KVH-Vertreterversammlung (18. Mai 2019) und auf dem Hausärztetag ins Erfurt (10./11. Mai 2019) die Politik aufgefordert für eine bessere finanzielle Ausstattung der Arztpraxen zu sorgen, damit die geplante Digitalisierung für Ärzte und Patienten nutzbringend und sicher umgesetzt werden kann.

Mit kollegialen Grüßen,
Ihr Christian Sommerbrodt

Hessischer Hausärzteverband
Bezirksverband Wiesbaden

Was geht: Betrieb des Konnektors in Arztpraxen

	Serieller Betrieb	Paralleler Betrieb
Haftung für TI	**gematik**	**Arztpraxis**
Haftung für Praxisnetz und Datenschutz allgemein	**Arztpraxis**	**Arztpraxis**
Empfohlen von: BSI, gematik, KBV		 nur auf eigenes Risiko möglich
Firewall	im Konnektor integriert, mit Haftung auf Seite der gematik	einrichten, betreiben und warten einer eigenen Firewall nötig, mit Haftung auf Seite der Arztpraxis
Internet	• kein freier Zugang zum Internet • um Internet zu nutzen muß ein zweiter Zugang mit eigenem Rechner, unabhängig vom Praxisnetz, eingerichtet werden	• voller Internetzugang über das Hauptsystem möglich • Eigenverantwortlicher Aufbau entsprechender Sicherheitsvorkehrungen
Stärkt digitale Prozesse		
KV-SafeNet		
KV-Connect		
Windows und Office-Update		
PVS-Update und Fernwartung (Praxisverwaltungssystem)		
online-Laborabruf		
HzV-online-Key		
Internet, e-Mail, Bank online-Überweisungen, etc.		
VPN für Homeoffice, Hausbesuche, Nebenbetriebsstellen		
Videosprechstunde		
Online-Terminsprechstunde	 nur möglich ohne Anbindung an den Terminkalender im PVS	

Weiterführende Links

https://www.bundesaerztekammer.de/recht/aktuelle-rechtliche-themen/datenschutzrecht/
- Richtiger Umgang mit Patientendaten, Schutz der Patienteninformationen, Schweigepflicht, Wahrung des Patientengeheimnis und Datenschutzrecht.

https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/Bekanntmachung_Datenschutz-Check_09.03.2018.pdf
- Allgemeine Checkliste zum Thema Datenschutz

https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/Hinweise_und_Empfehlungen_aerztliche_Schweigepflicht_Datenschutz_Datenverarbeitung_09.03.2018.pdf
- „Ärzte verarbeiten im Rahmen ihrer Tätigkeit Gesundheitsdaten. Es handelt sich dabei um eine „besondere Kategorie personenbezogener Daten“ gem. Art. 9 Abs. 1 DSGVO. Diese Daten sind besonders schutzbedürftig.“
- „Soweit eine Verbindung mit dem Praxisrechner erfolgt, sollten die Patientendaten auf dem Praxiscomputer verschlüsselt gespeichert und eine leistungsfähige, regelmäßig gewartete und aktualisierte Firewall verwendet werden.“

https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Telemedizin_Telematik/Sicherheit/Schweigepflicht_Technische_Anlage_2018.pdf
- Im Rahmen der Einführung und Gewährleistung von effizienten und effektiven IT-Sicherheitsmaßnahmen muss eine Vielzahl von Prozessen betrachtet werden. Bei der Umsetzung kann das IT-Grundschutz- Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [5] in Verbindung mit dem BSI-Standard 200–2, die Vorgehensweise nach IT-Grundschutz unterstützen.“
- „Virenschutzprogramme müssen so konfiguriert werden, dass sie Datenträger und Netze (Gesundheitsnetz, Intranet und Internet) überwachen. Des Weiteren sollten auch Rechner ohne Anbindung an Netze über Virenschutzprogramme verfügen, um eine versehentliche Virenverschleppung auf das vernetzte System zu vermeiden. Es wird dringend empfohlen, die Virenschutzprogramme stets auf dem aktuellen Stand zu halten (bei Bedarf mit Offline-Prozeduren, Kap. 2.3), da aufgrund sich schnell ausbreitender neuer Viren auch eine Anpassung des Virenscanners nötig ist, um den Schutz weiterhin zu gewährleisten.“
- „Informationen und Daten, welche in einem internen Netzwerk zur Verfügung stehen, sind einem überschaubarem Risiko ausgesetzt. Werden diese Netze oder ein Rechner jedoch über das Internet mit einem Gesundheitsnetz verbunden, wird dringend empfohlen, ein speziell für diesen Zweck vorgesehenes sog. dediziertes Hardware-Gerät (z. B. Router) mit Firewall- und VPN- Funktionalität zu verwenden.“
- Systeme mit Gesundheitsnetz-Anschluss sollten in einer eigenen Sicherheitszone betrieben (also als DMZ be- trachtet) werden und über eine Firewall von den Patientendaten-Systemen getrennt werden. Die Policy für die Kommunikationsbeziehungen sollten so restriktiv wie möglich gestaltet werden: Am Besten sollte Datenverkehr nur von den internen Systemen auf die exponierten Systeme erlaubt sein.

https://www.kvb.de/fileadmin/kvb/dokumente/Praxis/TI/KVB-Infoblatt-FAQ-Telematikinfrastruktur.pdf

- „Sollte es auf Grund fehlender Datenschutzmaßnahmen innerhalb des Praxisnetzwerks, z.B. fehlende Absicherung der Hard- oder Software mittels Firewall, Zugriffsbeschränkung o.ä., zu einem Missbrauch kommen, ist hier die Praxis bzw. der verantwortliche Arzt/Psychotherapeut verantwortlich."
- „Laut der BfDI endet diese Verantwortung beim Konnektor, der Schnittstelle zwischen der Praxis und der TI. Ab dem Konnektor liegt die Verantwortung für den sicheren Betrieb der TI grundsätzlich bei der gematik und weiteren Netzanbietern. Die Architektur der TI wurde maßgeblich von der gematik definiert und entwickelt. Die Sicherheitsanforderungen an die TI wurden dabei vom Bundesamt für Sicherheit in der Informationstechnik (BSI) - also von der höchsten Instanz für IT-Datensicherheit in Deutschland - festgelegt. Die Einführung der TI wird laufend vom BSI und der BfDI begleitet."

https://www.gematik.de/fileadmin/user_upload/gematik/files/Publikationen/gem_OPB_Infoblatt_Anschluss_2017-10-BR-DGDV1_web.pdf

- Anschluss des Konnektors, Pralle oder Reihe

https://www.kbv.de/html/1150_40271.php

- Der Reihenbetrieb zeichnet sich dadurch aus, dass der Konnektor alle Verbindungen zwischen Internet (Secure Internet Service) und TI vom Praxisnetzwerk kapselt und dadurch die Praxis schützen kann. Durch die integrierte Firewall wird dabei nicht nur die TI vor Angriffen von außen geschützt, sondern auch das gesamte Netzwerk der Praxis.
- Bei der Parallelinstallation fungiert der Konnektor nicht als Firewall im Netzwerk, und die Praxis muss wie heute schon entsprechende Sicherheitsmaßnahmen treffen. „Daran ändert sich mit dem Anschluss an die Telematikinfrastruktur nichts", betonte Kriedel.
- Auch für die Haftung im Falle eines Datenschutzvorfalls muss die gesamte Datensicherheit betrachtet werden: „Ärzte und Psychotherapeuten sind nicht für die Sicherheit in der TI verantwortlich, wohl aber für den Datenschutz in ihrer Praxis", erläuterte Kriedel. Für eine sichere Firewall beim Parallelbetrieb des Konnektors haftet also letztlich der Praxisinhaber.

Weitere Beispiele für Datenpannen in Gesundheitssystemen

- https://patientenrechte-datenschutz.de/2019/01/30/datenleck-in-der-smart-city-singapur-daten-von-14-200-hiv-patienten-die-in-singapur-erhoben-wurden-sind-ins-internet-gelangt/
- https://www.moobilux.com/2017/03/uk-skandal-deepmind-hatte-zugang-zu-millionen-patientendaten/
- https://www.aerzteblatt.de/nachrichten/75706/Cyber-Attacke-legt-Krankenhaeuser-in-England-lahm
- https://www.gdv.de/de/themen/news/kostbare-beute-patientendaten-31284
- https://www.datenschutzbeauftragter-info.de/patientendaten-aus-deutschen-krankenhaeusern-im-freien-umlauf/
- https://www.tagesschau.de/inland/apotheken-datenleck-101.html