Bei diesem Papier handelt es sich um meine persönliche Meinung, welche ich im Rahmen der freien Meinungsäußerung von mir gebe und dessen Richtigkeit ich durch die Bundesregierung in allen Punkten dikutieren möchte, da ich es leid bin, von hohen Funktionären wie Kriedel etc. als „Spinner, welcher angeblich in Einzelfällen Mängel gefunden haben will“ abgetan zu werden. Weiter finde ich es unmöglich, dass ich nahezu täglich von Praxen höre, die Patientendaten verloren haben.

„Rechtliche Grundlagen: Artikel 19 (Meinungs- und Informationsfreiheit)
Jeder Mensch hat das Recht auf Meinungsfreiheit und freie Meinungsäußerung; dieses Recht schließt die Freiheit ein, Meinungen ungehindert anzuhängen sowie über Medien jeder Art und ohne Rücksicht auf Grenzen Informationen und Gedankengut zu suchen, zu empfangen und zu verbreiten.“ [1]

„Grundgesetz Art 5
(1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten.“ [2]

Alle in Blau gestellten Fragen und Forderungen möchte ich im Rahmen des IFG schriftlich beantwortet bzw. kommentiert haben!

Voraussetzungen, Bestimmungen IT

Zum Thema Datenschutz beziehen wir uns regelmäßig auf den IT-Grundschutz. In unseren Augen ist die DSGVO sehr eindeutig. Art. 5 DSGVO, Absatz 1 f besagt:

"Personenbezogene Daten müssen[...] in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);" [3]
Dazu wird oft der **"Stand der Technik"** zitiert. Dieser ist nicht fest definiert, aber das BSI sagt dazu:
‚Stand der Technik‘ ist ein gängiger juristischer Begriff. Die technische Entwicklung ist schneller als die Gesetzgebung. Daher hat es sich in vielen Rechtsbereichen seit vielen Jahren bewährt, in Gesetzen auf den ‚Stand der Technik‘ abzustellen, statt zu versuchen, konkrete technische Anforderungen bereits im Gesetz festzulegen. Was zu einem bestimmten Zeitpunkt ‚Stand der Technik‘ ist, lässt sich zum Beispiel anhand existierender nationaler oder internationaler Standards und Normen von beispielsweise DIN, ISO, DKE oder ISO/IEC oder anhand erfolgreich in der Praxis erprobter Vorbilder für den jeweiligen Bereich ermitteln. Da sich die notwendigen technischen Maßnahmen je nach konkreter Fallgestaltung unterscheiden können, ist es nicht möglich, den ‚Stand der Technik‘ allgemeingültig und abschließend zu beschreiben.“[4]

[1] (Amnesty International Deutschland e. V., 2019)
[2] (Bundesamt für Justiz, 2019)
[3] (intersoft consulting services AG, 2019)
[4] (Bundesamt für Sicherheit in der Informationstechnik, 2019)

Der Grundschutz basiert auf ISO/IEC 2700x, er definiert also den Stand der Technik. Laut DSGVO muss jeder Datenverarbeitende diesen Stand der Technik erfüllen. Man kann sicher immer streiten wo sinnvoll anfängt und aufhört. Allerdings das bewusste Abschalten vorgesehener Sicherheitsmaßnahmen (Firewalls, Transportverschlüsselung...) geht lang am Grundschutz vorbei.

Installationsmängel:

Die Mängel sind allgemeingültig und wurden so in **allen** besichtigten Praxen vorgefunden und dokumentiert. Zusätzlich wurden mir Bilder aus ganz Deutschland dazu gesendet.

Mangel 1 - Fehlerhafter Aufbau

Nach Technikerangaben wird der Konnektor in fast allen Praxen parallel zu allen anderen Netzwerkkomponenten im LAN angeschlossen obwohl keine Schutzeinrichtungen vorhanden sind (vor meinen Veröffentlichungen waren es nach eigenen Ermittlungen über 90%).

Die gematik schreibt dazu in Ihren Unterlagen:
„Im Parallelbetrieb ist keine Komponente des LAN durch den Konnektor vor unautorisierten Zugriffen geschützt. Ohne zusätzliche Sicherungsmaßnahmen haben alle Komponenten im LAN Zugriff aufeinander (somit auch eine potenzielle Schadsoftware auf einem der Geräte). Außerdem besteht kein Schutz vor Angriffen aus dem Internet. […] Da der Konnektor nicht als Firewall im LAN fungiert, ist der Parallelbetrieb nur für medizinische Einrichtungen geeignet, die bereits ein größeres LAN etabliert haben und über entsprechende Sicherheitsfunktionen gemäß dem BSI verfügen.“ [5]

Daraus folgt, dass der Parallelbetrieb nur mit Hardware - Firewall zulässig ist.

Mangel 1 - Problem 1
Die Anschlüsse werden parallel durchgeführt obwohl im Netz keine Firewall vorhanden ist. Das ist den Technikern bewusst, denen aber egal. Die Techniker installieren sogar parallel ohne Firewall, wenn sie direkt darauf hingewiesen werden, dass das gegen die Bestimmungen verstößt. Dabei werden die Ärzte sogar unter Druck gesetzt die Installation zu unterschreiben sonst wird abgebaut und es droht der Honorarabzug. Ein sicherer Aufbau wird den Ärzten trotz Aufforderung verweigert!

Frage1: Was sagt die Regierung dazu, dass die Patientendaten nicht richtig geschützt sind und Hacker diese Daten sehr einfach abziehen können und Ärzte dennoch unter Strafe gezwungen werden sich weiterhin zwangsanschließen zu lassen?

So wie das Gesetz es gefasst wurde, wird es von den Firmen, welche das Gesetz im Auftrag der Bundesregierung (gematik 51% BMG) anwenden und durchsetzen, derartig genutzt, Ärzte in einen Anschluss zu nötigen, welcher die Patientendaten in manchen Fällen sogar nahezu frei ins Netz stellen oder zumindest einfach Zugänglich machen.
Sowohl dem Bundesdatenschutzbeauftragten als auch dem Landesdatenschutzbeauftragten NRW persönlich wurden die eklatanten Mängel vorgeführt. Seit März ist in der Angelegenheit nichts geschehen. Es wird immer auf die angeblich sichere Zertifizierung verwiesen. Unsere Recherchen zeigen jedoch auch Mängel in der Zertifizierung auf! Nimmt ein Arzt die Installation nicht ab, so droht der Honorarabzug, daher unterschreiben die Ärzte,

[5] (gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2018) S.22

wider besserem Wissens, den unsicheren Aufbau. Meiner Meinung nach liegt dieses Verhalten irgendwo zwischen Nötigung und Erpressung.

Frage 2: Wie steht die Bundesregierung zu diesen erpresserischen Methoden?

Frage 3: Wie will die Regierung die bestehenden unsicheren Anschlüsse nachbessern und wann soll das geschehen?

Frage 4: Wie können und sollten sich Ärzte wehren, die durch die DvOs reingelegt wurden, und nun unsicher am Netz hängen?

Frage 5: Was sollen die Ärzte nun tun, die unsicher angeschlossen sind, um nicht weiter gegen die DSGVO zu verstoßen und Patientendaten zu verlieren?

Frage 6 : Sollen alle unsicher angeschlossenen den Internetstecker ziehen?

Mangel 1 - Problem 2
Aus angeblichen Datenschutzgründen nennen die Netzbetreiber nicht die IP Adressen und Ports für eine ordnungsgemäße Firewallkonfiguration. Seit März versprechen gematik und Bundesdatenschutzbeauftragter diese Daten zu besorgen. Sie liegen noch immer nicht vor! (die Daten von zwei Anbietern haben wir uns besorgt bzw. erarbeitet von zwei Anbietern fehlen die Daten bis heute) Damit ist ein sicherer paralleler Anschluss – so wie ihn das BSI vorschreibt –unmöglich. In den meisten Praxen sind die Endgeräte derzeit quasi schutzlos an einem Router angeschlossen.

Frage 7: Warum werden, trotz monatelangem Bitten um Herausgabe dieser wichtigen Daten, die Daten immer noch geheim gehalten?

Forderung 1: Ich fordere unverzüglich die Veröffentlichung aller relevanten IP-Adressen und Ports aller Anbieter! Spezielle Fragen entnehmen Sie dem Zusatzpapier von Herrn Schmirler.

Um hier vollständig zu sein möchte ich zu den Netzbetreibern herausstellen, dass ich die Lösung von Arvato vorbildlich finde, die Informationen sauber über DNS SRV-Einträge verfügbar zu machen. Bei solch einer Arbeitsweise können Firewalls die Informationen selbst beziehen und die Daten müssen nicht veröffentlicht werden. Die Firewalls, welche damit umgehen können sind jedoch beschränkt. Das führt evtl. zu weiteren Kosten für Umrüstungen.

Noch ein Hinweis, was die Sinnlosigkeit der „geheimen Adressen und Ports“ betrifft.
Die "geheimen" Daten ließen sich natürlich empirisch recht einfach ermitteln, was die Geheimhaltungstaktik ein Stück weit ad absurdum führt. In jedem Firewalllog stehen Adressen und Ports in der Liste der blockierten Pakete.

Mangel 1 - Problem 3
Da Antivirenprogramme in die Kommunikation eingreifen, werden sie einfach durch die Techniker abgeschaltet. Das wurde in zahlreichen Praxen dokumentiert (Fotos), sowie Zeugen Johannes Ernst und Jens Ernst, Praxisangestellte und Ärzte der betroffenen und besichtigten Praxen, die alle namentlich benannt werden können.

Mangel 1 - Problem 4
Da auch die eigentlich nicht wirklich gute Windows Firewalls in die Kommunikation

eingreift, wurde diese durch die Installateure entweder komplett abgeschaltet oder es wurden sicherheitsrelevante Funktionen deaktiviert in dem komplette Ports generell ein- und ausgehend komplett freigeschaltet wurden, was gar keinen Sinn ergibt. Dieser Umstand wurde bis heute nicht aufgelöst.

Frage 8: Was hält die Bundesregierung von der Abschaltung bzw. außer Kraft Setzung der wichtigsten und grundlegenden Sicherheitsfunktionen eines Praxisrechners?

Forderung 2: Wenn durch einen DvO Sicherheitsvorrichtungen wie Antivirenprogramme oder Firewallfunktionen außer Kraft gesetzt werden, dann tritt die Firma, welche mit dem TI-Anschluss beauftragt wurde, sofort in die komplette Haftung ein! Das muss gesetzlich geregelt werden!

Die sensiblen Daten hängen also einfach ungeschützt hinter einem Router. Ein Router ersetzt keine Firewall und ist nicht geeignet ein Praxisnetz zu schützen. Aktuelle Untersuchungen zeigen, dass 5 von 6 modernen Routern teils erhebliche, bekannte Sicherheitslücken[6] aufweisen. Die in den meisten Arztpraxen seit Jahren liegenden Speedports mit ewig nicht upgedateter Firmware haben noch größere Lücken. Selbst wenn in einer Praxis eine Firewall vorhanden war, wurde sie nicht richtig konfiguriert. Die Techniker können die Firewalls nicht konfigurieren und umgehen diese deshalb. Selbst wenn ein praxisbetreuender Techniker die Firewall entsprechend konfigurieren wollte, so war das wegen nicht bekannter IPs und Ports nicht möglich.

Selbst große Firmen schätzen die Bedrohung der Daten durch fehlende oder falsch konfigurierte Firewalls vollkommen falsch ein. Genau diese „Sicherheitseinrichtung NAT-Router“ war Teil meiner Kontroverse mit der großen Online Heise Security Redaktion zum Thema TI.

So teilte uns man uns per Mail mit:
„Wie genau kann man über das Internet auf die Patientendaten zugreifen? Wenn ich das richtig verstehe, dann wird der Konnektor im Parallelbetrieb als Client in ein bestehendes Netzwerk gehängt. Anscheinend wird im Zuge der Einrichtung auch die Windows Firewall bei Clients im Praxisnetz abgeschaltet oder es werden zumindest bestimmte Ports freigegeben. Ein Zugriff aus dem Internet ist damit jedoch noch nicht möglich, schließlich sind die Clients über einen Router mit dem Internet verbunden. Und der Router lässt eingehende Verbindungen aus Richtung Internet nur durch, wenn ein Port-Forwarding eingerichtet wurde.“

Die Redaktion wurde wenige Tage nach diesen Mails, trotz Firewall, Opfer solch einer Fehleinschätzung. Dabei wurden über den Port 449 Verbindungen von Rechnern nach außen aufgebaut und Daten gestohlen.

Bei einer richtig konfigurierten Firewall hätte kein Rechner über den Port 449 eine Verbindung nach Außen aufbauen können. **Entscheidend für die Sicherheit von Daten in einem Netzwerk ist nicht, ob ich direkt auf die Daten zugreifen kann. Entscheidend ist, ob die Daten abgezogen werden können.**

[6] (Tremmel, 2018)

Frage 9: Ist für die Bundesregierung ein NAT Router ein ausreichender Schutz für ein Praxisnetz?

Diese Frage muss öffentlich beantwortet werden, da die TI - aufbauenden Unternehmen offensichtlich der Meinung sind, dies sei so. Zahlreiche Papiere belegen das.

Forderung 3: Ich fordere, dass über die offiziellen Papiere der gematik und der KBV usw. klargestellt wird, dass ein Router nicht ausreichend ist, ein Praxisnetz anzuschließen, egal ob seriell oder parallel. (einzige Ausnahme ist eine Reihenschaltung ohne SIS) Wenn in der Praxis Internet vorhanden ist muss eine Hardwarefirewall vorhanden sein! Ohne Firewall kann die DSGVO nicht erfüllt werden! Die Firewall muss BSI konform programmiert werden, so dass ausgehende Ports vollkommen geschlossen sind und nur einzelne benötigte IP zu IP Verbindungen zugelassen werden. Port 80 und 443 sind über Proxyserver zu leiten.

Frage 10: Wer übernimmt die nun entstehenden Kosten für die sichere Anbindung der TI? Sollten nicht die Unternehmen, welche die TI falsch angeschlossen haben, die Kosten tragen?

Forderung 4: Im Gesetz steht, dass der Anschluss an die TI kostenneutral für die Ärzte erfolgen muss. Da die gematik bis heute nicht in der Lage war, diesen Anschluss sicher zu gestalten sind alle Kosten für Hardwarefirewall, dessen Installation und auch die laufenden Kosten von den KVen zu ersetzten!

Die Firma Hasomed schreibt beispielsweise: *„Die gematik setzt einen umgesetzten IT-Grundschutz des BSI voraus. Verantwortlich dafür ist die Praxis. Die Umsetzung des Grundschutzes kann der DvO nicht prüfen.“*. Diese Annahme ist usus bei allen Anbietern. Auch wenn die Praxis nie am Netz hing und die DvOs erst den Internetzugang herstellen und den Rechner erstmalig anschließen. (Denken sie mal bitte über diesen Satz nach…es ist unmöglich, dass der Grundschutz umgesetzt ist, wenn die Praxis nie angeschlossen war!) Da die Unternehmen aus Zeitdruck Menschen in Kurzschulungen herausgeschickt haben um die TI zu installieren, ist auch klar, warum die DvOs das nicht prüfen können. Die Installateure, welche ich kennen gelernt habe, wussten noch nicht ein mal, was ein Port ist, oder dass eine IP nur ein Mal im Netz vergeben werden kann.

Frage 11: Ist diese Vorgehensweise von der Bundesregierung so gewollt, dass die sensibelsten Daten, welche wir Menschen haben von Technikern angeschlossen werden, die offensichtlich keine Ahnung von der Materie haben?

Forderung 5: Der Gesetzgeber ist nun am Zug die Umsetzung der TI zu regeln. Dabei hat er festzulegen: Der DvO hat die örtliche Prüfung durchzuführen. Ist der IT-Grundschutz nicht umgesetzt, ist die Reiheninstallation ohne SIS anzuschließen.

Die Firma Hasomed schreibt Beispielsweise (und so denken und handeln ausnahmslos nach Angaben aller Ärzte, welche ich gesprochen habe, alle Anbieter)
Beachten Sie bitte weiterhin, dass weder unsere Techniker noch HASOMED Bescheinigungen ausstellen können, die bestätigen, dass Ihr Praxisnetz auch nach der Konnektorinstallation über alle der gewählten Installationsweise entsprechende Sicherheitsfunktionen gemäß dem Bundesamt für Sicherheit in der Informationstechnik (BSI) verfügt.

Forderung 6: Der Gesetzgeber ist nun am Zug die Umsetzung der TI zu regeln. Dabei hat er festzulegen: Wenn der DvO parallel angeschlossen hat oder seriell mit SIS, hat der Techniker der Praxis schriftlich zu bestätigen, dass der IT-Grundschutz umgesetzt wurde. Damit ist auch die Haftung des Praxisinhabers auf den DvO zu übertragen.

Wenn die Unternehmen mit in der Haftung stehen, dann wird der Aufbau auf einmal ganz anders erfolgen, „quick and dirty“ ist dann vorbei, da bin ich mir ganz sicher. Kein Unternehmen wird dann mehr der Meinung sein, dass ein Speedport eine ausreichende Sicherheit darstellt.

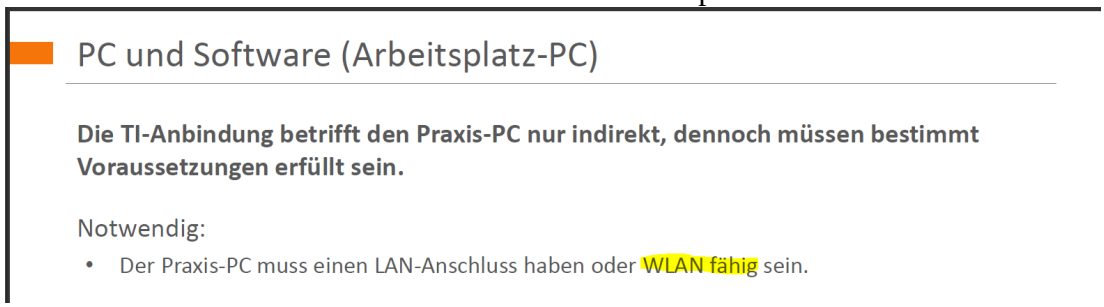
Der schlimmste Fall, den wir bisher hatten!
Die Techniker binden darüber hinaus Praxisnetze mit Kabelmodems einfach an, ohne sich der eingesetzten Technik bewusst zu sein. Kabelmodems mit nachgeschalteten IP-Client Routern bieten nicht einmal Basis-Sicherheitsfunktionen. “***ACHTUNG!*** *Die Firewall ist nicht aktiv, wenn die FRITZ!Box die Internetverbindung eines anderen Routers nutzt ("IP-Client-Modus"). In diesem Fall empfiehlt sich die Einrichtung einer Firewall in dem anderen Router.*“[7]

In einer Arztpraxis in Hagen wurde die TI so angeschlossen und sowohl Firewall als auch Antivirenprogramm abgeschaltet. **Die Patientendaten waren somit vollkommen ungeschützt aus dem Internet direkt erreichbar!**

Die Softwarehersteller haben teils keine Ahnung von IT Sicherheit und wollen sich auch nicht damit auseinandersetzen. Selbst nach meinen Veröffentlichungen werden Papiere veröffentlicht, in denen grobe Fehler an der Tagesordnung sind.
Beispiele:

1. Hasomed: Mail an Hasomed mit Fallschirmpapier von Hasomed (am Schluss angehängt) lesen Sie sich das Papier sowie meine Mail an Hasomed durch, in der ich die vielen Fehler aufdecke!

2. Elefant: Schließt offiziell Rechner mit Patientendaten per WLAN an.

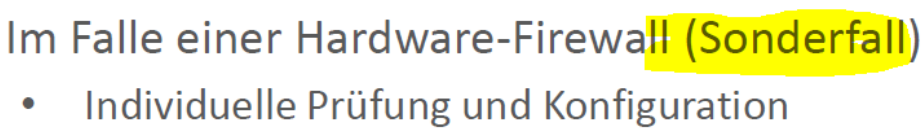

PC und Software (Arbeitsplatz-PC)

Die TI-Anbindung betrifft den Praxis-PC nur indirekt, dennoch müssen bestimmt Voraussetzungen erfüllt sein.

Notwendig:

- Der Praxis-PC muss einen LAN-Anschluss haben oder WLAN fähig sein.

3. auf Seite 5 von Elefant steht: Die Firewall sei ein Sonderfall. (komplettes Dokument angehängt)


Im Falle einer Hardware-Firewall (Sonderfall)

- Individuelle Prüfung und Konfiguration

[7] (AVM Computersysteme Vertriebs GmbH, 2019)

4. Das DGN sagt immerhin halb richtig: „ein Abschalten einer Firewall sollte natürlich nie erfolgen und wird auch nicht von uns empfohlen. Um dem TI-Konnektor den Zugang zu seinen Diensten im Internet zu erlauben, **sind keine Veränderungen an den Firewall- und Filtereinstellungen notwendig**. Für die Kommunikationswege der TI werden lediglich wenige Ports zu zielgerichteten Servern für den VPN-Verbindungsaufbau nach außen benötigt. Eingehende Verbindungen aus dem Internet in das Praxis-Netzwerk werden nicht benötigt. Daher ist es für die Integration des Konnektors nicht erforderlich, eingehende Ports in der Firewall freizuschalten.“[8]

Wenn in einer Praxis eine wie von der gematik geforderte (wie zertifiziert) nach BSI eingerichtete Firewall (Whitelist-Ansatz NET.3.2.A2 Festlegen der Firewall-Regeln) vorhanden ist, kann der Konnektor ohne Änderungen in der Firewall keine Verbindung ins Internet aufbauen. Die Firewall würde alle Datenpakete blocken.

Leider sind die Hersteller nicht gewillt mit mir zu sprechen. Zahlreiche Versuche Verbindung aufzunehmen schlugen fehl. Ich habe Mails gesendet, geändert hat sich nichts. Die falschen Informationen stehen immer noch auf den Webseiten und die Papiere mit den Fehlern werden weiter versendet. Ich bin in den Mails auch auf weitere Fehler eingegangen.

Frage 12: Was will die Bundesregierung unternehmen, um den Firmen, welche die TI aufbauen, wenigstens ein gewisses Sicherheitsniveau beizubringen, damit dieser schlampige Aufbau endlich aufhört? Warum gibt es keinerlei Voraussetzungen, welche ein Unternehmen erfüllen muss um die TI aufzubauen?

Forderung 7: Alle Softwarehersteller PVS usw. sind sofort darüber zu informieren, dass sie die bisherigen Installationspraktiken sofort zu ändern haben. Bei allen parallelen Installationen ohne Hardwarefirewall ist eine Hardwarefirewall unverzüglich nachzurüsten!

Wenn kein Mensch jemals einen Fehler machen würde, wäre ohne Hardwaresicherheitslücken solch ein Router schon eine Barriere, die nur durch Hacker zu überwinden ist.

Mit diesem Satz habe ich bereits drei Probleme aufgezeigt.

1. Menschen machen Fehler, auch Ärzte. Sei es durch unachtsames Öffnen einer Mail oder Benutzen eines infizierten USB Sticks.
2. Die Router haben (sogar bekannte) Sicherheitslücken. Router sind außerdem so nett, sich am Internetanschluss mit ihrer Identität vorzustellen. Das heißt, ich weiß immer, welcher Router da steht und kann die aufgelisteten Sicherheitslücken für den betroffenen Router abarbeiten und mir so Zugriff auf das Netzwerk verschaffen.
3. Die Daten sind so begehrt, dass auch Hacker die Praxen angreifen um Ärzte oder ihre Patienten zu erpressen oder die Daten gewinnbringend zu verkaufen.

All diese Probleme veranlassen mich zu der Vermutung, dass deutschlandweit die meisten Arztpraxen derzeit nicht sicher an das Internet angeschlossen sind. Eine Ermittlung, wie viele Praxisrechner ohne Firewall unsicherer an einem Router hängen, lehnen alle Verantwortlichen ab. Ohne Erhebung kann so weiter behauptet werden, es handele sich um Einzelfälle. Ein sicherer Anschluss wäre unseren Ergebnissen nach ein Einzelfall.

[8] (DGN Deutsches Gesundheitsnetz Service GmbH, 2019)

Frage 13: Warum ist keine Stelle daran interessiert, eine Ermittlung der Anzahl vorzunehmen, wie viele Rechner unsicher bzw. nicht der Zertifizierung entsprechend angeschlossen sind? Haben Sie Angst, dass aus den „Einzelfällen“ eine Quote von „100%“ wird? Meine Befürchtungen liegen bei 100%!

Ich war letzte Woche bei einer Psychologin, welche sich wirklich ausgiebig mit dem Thema auseinandergesetzt hat und von Ihrem Anbieter, auch gegen den Wiederstand, eine Netztrennung ohne SIS installieren ließ. Soweit hatte sie alles richtig gemacht. Trotzdem hatte der Techniker den Zertifizierten Aufbau zu Nichte gemacht, in dem er wichtige Schutzfunktionen im Kartenlesegerät abgeschaltet hatte (darauf gehe ich gleich noch ein, die Mail der Psychologin an den Bundesdatenschutzbeauftragten finden Sie im Anhang). Dies wusste die Psychologin nicht und ich behaupte mal, hätte sie auch nicht wissen können. Trotzdem war der Aufbau so nicht mehr zertifiziert und die Haftung beim Praxisbetreiber.

Serieller / Reihenanschluss

Bis hierher sind wir davon ausgegangen, der serielle Anschluss sei durch die integrierte Firewall im Konnektor sicher, wie es vollmundig versprochen wird.
Zur Sicherheit bei Reihenbetrieb und Netztrennung schreibt die gematik:
„Durch die integrierte Firewall des Konnektors und den optionalen und gegebenenfalls kostenpflichtigen Secure Internet Service (SIS) wird das LAN optimal vor unautorisierten Zugriffen von außen geschützt.“ (gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2018)

Hinter solch vermeintlich sicheren Anschlüssen befinden sich unter anderem medizinische Geräte und PC ohne Schutzmechanismen, da Ärzte den Sicherheitsversprechen der gematik glauben. Wir können diese Sicherheit nicht bestätigen.

Aufgrund von Berichten über eine Trojaner-Infektion eines seriellen und SIS-geschützen Anschlusses, bat mich ein Arzt eine Datenschutzfolgeabschätzung (DSFA) für seine Praxis zu erstellen. Dazu habe ich eine Anti-Viren-Testdatei (EICAR European Institute for Computer Anti-Virus Research) unerkannt und vollkommen problemlos auf verschiedenste Wege über die TI in das Praxisnetz transferiert.

Zu dem Testfile kann man lesen: *„Der EICAR Testvirus ist eine Textdatei mit einem speziellen Inhalt, die zum Prüfen von Virenscannern verwendet wird. Jeder Virenscanner muss diese Dateien als Virus erkennen – auch wenn diese natürlich völlig harmlos sind. Daher ist es auch normal, dass Ihr Virenscanner Sie beim Download dieser Dateien warnen sollte. […] Wenn Ihr Virenscanner Sie nicht darauf hinweist, dass diese Datei gefährlich für Ihren Computer sein kann, sollten Sie dringend Ihre Virus-Software wechseln.“*[9]

Wir haben das Testfile zu Tests ebenfalls auf unseren Server gelegt. Hier können Sie selbst den Test durchführen.

https://happycomputer.eu/testdaten/eicar.com
https://happycomputer.eu/testdaten/eicar.zip
https://happycomputer.eu/testdaten/eicar.tgz

[9] (ETES GmbH, 2019)

Lediglich bei http (Port 80) wurde der EICAR geblockt.

Weiterhin haben wir getestet, ob ein stehlen der Daten aus dem Praxisnetz möglich sein könnte. Da alle Ports offen sind, ist auch das problemlos möglich. Damit ist ein Rechner hinter einem SIS keines Wegs geschützt. Das entspricht nicht einmal dem Grundschutz Basisanforderung und schon gar nicht dem „Stand der Technik".

Wir haben folgende Ports getestet und keine Firewall hat uns aufgehalten: Sie können hier den Test selbst durchführen. Sie sollten das unten abgebildete Erfolgsfenster nur auf den Ports 443 (HTTPS) und 80 (HTTP) erhalten. Es kann sein, dass es sinnvoll ist, einen weiteren Port frei zu schalten, jedoch nur an eine bestimmte IP. In der Regel sollten sonst **alle Ports** geschlossen sein. Vor allem z.B. Port 53.

21 FTP, 22 SSH, 23 TELNET, 25 SMTP, 53 DNS, 80 HTTP, 110 POP3, 115 SFTP, 135 RPC, 139 NetBIOS, 143 IMAP, 194 IRC, 443 SSL, 445 SMB, 449 Malware, 1433 MSSQL, 3306 MySQL, 3389 Remote Desktop, 5632 PCAnywhere, 5900 VNC, 65000 HighPort zufällig ausgewählt.

Was mit Ihren Daten passieren kann, wenn der Schutz vor Viren, Trojanern (Malware) nicht ausreichend und z.B. der Port 449 ausgehend nicht geschlossen ist, können Sie bei Heise nachlesen.[10] Aber auch über jeden anderen offenen Port können Daten gestohlen werden (z.B. Port 53). Auch dieser war, wie alle Ports vollkommen offen. (https://www.all-about-security.de/security-artikel/plattformsicherheit/single/dns-das-unterschaetzte-datenleck/) lesen Sie, wie einfach man Daten über diesen Port stehlen kann.

Ich habe lange den Aussagen von gematik, Bundesdatenschutz, Landesdatenschutzbeauftragten und Herstellern geglaubt, dass der serielle Anschluss des Konnektors wegen des SIS sicher sei. Dies wurde uns von den Datenschutzbeauftragten persönlich zugesichert. Tests wurden uns übrigens untersagt, wir müssten den Aussagen der gematik vertrauen, so die wörtliche Aussage!

Nach meinen Tests, welche wegen des Testverbotes nur die absolut simpelsten waren, kann ich derzeit keine Anschlussart mit Internet ohne Hardwarefirewall mehr empfehlen.

Wir haben das BSI mit den Umständen konfrontiert und die folgenden Fragen gestellt:

> Hallo
>
> Trotzdem ich auf keine meiner Mails mehr eine Antwort bekomme, schreibe ich erneut.

[10] (Schmidt, 2019)

Der Bundesdatenschutzbeauftragte hat in seinem Tätigkeitsbericht (Seite 59) klargemacht, wie die gesetzliche Lage ist. So ist dort zu lesen:
„Nach dem Anwendungsbeginn der DSGVO im Mai 2018 stellte sich mit Nachdruck die Frage, wer eigentlich Verantwortlicher für die Telematik-Infrastruktur (TI) ist und damit eine Datenschutz-Folgenabschätzung (DSFA) vorzulegen hat (vgl. hierzu auch unter Nr. 15.2.3). ***Viele Arztpraxen sind ihrer gesetzlichen Verpflichtung zur Erstellung einer DSFA nachgekommen.*** *Sie haben dabei allerdings nicht an der Schwelle ihrer Praxisräume Halt gemacht, sondern vielmehr auch die TI in ihre Betrachtungen mit einbezogen. Die gesetzlich vorgeschriebene DSFA der Arztpraxis ergab dann,* ***dass ein Anschluss an die TI nicht vertretbar sei.*** *Viele Ärzte haben sich des-halb an mich gewandt. Die Frage, wer der datenschutzrechtliche Verantwortliche im Sinne der DSGVO für die TI ist, konnte bis zum Redaktionsschluss noch nicht endgültig geklärt werden.“*

Das bedeutet: **Jeder Arzt sollte eine DSFA anfertigen. Der Bundesdatenschutzbeauftragte meint sogar, dass jeder Arzt gesetzlich dazu verpflichtet ist.** Da die gematik jedoch – trotz mehrfacher Aufforderung – nicht in der Lage ist, eine DSFA vorzulegen, kann ein Arzt nur zu dem Ergebnis kommen, dass er sich erst dann an die TI anschließen lässt, wenn die DSFA vorliegt. Trotzdem hat ein Arzt sich anschließen lassen und eine DSFA beauftragt.

Arztpraxen müssen nicht nur die Vorgaben des Grundschutzkatalogs „Basisanforderung“ umsetzen, sondern die Vorgaben des erhöhten Schutzes. Das gilt besonders bei der Konfiguration von Firewall-Regeln und Sicherheitsproxies.

Auch Ärzte, welche über den „sichere“ SIS angeschlossen wurden, müssen eine DSFA erstellen.

Beim ÄND kann man https://www.aend.de/article/197426 nachlesen, was KBV, gematik und Herr Kriedel zu allen Anschlüssen schreiben:
„Die Praxis muss – wie bisher auch schon – spezielle Sicherheitsmaßnahmen wie Firewall und Virenschutz ergreifen, um sich vor Angriffen von außen zu schützen.“

Also muss ein Arzt in jedem Fall testen ob er geschützt ist, egal wie er angeschlossen ist.

Nach meiner Meinung sollte jeder Arzt der sich an die TI anschließen lässt, eine Firewall haben, ob parallel oder seriell. Der Schutz der Patientendaten sollte über allem stehen. Ich bin auch der Meinung, dass die TI in eine DMZ gehört. Nur so kann das Praxisnetz vor Angriffen und Übergriffen aus der TI bzw. über den Konnektor geschützt werden.

Mit einfachsten Testmethoden kann jeder Arzt seine eigene Praxis testen. Dafür muss er im Browser lediglich 2 Links ausführen.

TEST 1

Hier der einfachste und wichtigste Test, welchen jeder Arzt sofort ausführen kann und welcher komplett ohne Risiko ein schnelles Ergebnis bringt.

http://portquiz.net:449/ Bekommt man hier ein Ergebnis, findet ausgehend keine Kommunikationskontrolle statt.

Das Ergebnis muss immer so aussehen:

nicht so!

Kommt eine Ergebnisseite, dann ist ein Abziehen der Daten mit Hilfe von Malware problemlos möglich! (Wie das geht, schauen Sie z.B. hier: https://www.heise.de/ct/artikel/Emotet-bei-Heise-4437807.html) Aber auch jeder beliebige andere Port ist zum Abziehen von Daten geeignet. (https://www.all-about-security.de/security-artikel/plattformsicherheit/single/dns-das-unterschaetzte-datenleck/)

Diesen Test sollte jeder Anschluss bestehen, welcher BSI-konform (Gundschutzkompendium Grundschutzkatalog erhöhte Anforderung) hergestellt wurde!

Kommt hier eine Ergebnisseite muss der IT Dienstleister informiert werden!

Meiner Meinung nach sollte auch sofort der Internetstecker gezogen werden, da die Gefahr besteht, gegen die DSGVO zu verstoßen. Wenn ich eine DSFA erstelle und dieser Link ein Ergebnis bringt, ist mein Ergebnis eindeutig. In der Empfehlung steht dann: Das Praxisnetz sollte sofort vom Internet getrennt werden. Da ich kein Jurist bin, maße ich mir jedoch nicht an, Weisungen zu erteilen.

Nach DSGVO muss der Stecker gezogen werden!!

Auch hier sind die Behörden gefordert, klare Anweisungen herauszugeben, wie Ärzte auf einfachste Weise prüfen können, ob sie gegen Richtlinien des BSI und damit gegen die DSGVO verstoßen. WICHTIG!!! Verstoßen die Ärzte gegen die DSGVO bzw. die Richtlinien des BSI haften sie auch, da der Konnektor nicht wie zertifiziert benutzt wird!!!

TEST 2

Ein weiterer Test, für alle die in der Firewall eine Antivireneinrichtung haben oder die am SIS hängen.

*Der **EICAR Testvirus** ist eine Textdatei mit einem speziellen Inhalt, die **zum Prüfen von Virenscannern** verwendet wird. Jeder Virenscanner muss diese Dateien als Virus erkennen – auch wenn diese natürlich **völlig harmlos** sind. Daher ist es auch normal, dass Ihr Virenscanner Sie beim Download dieser Dateien warnen sollte.*
Urheber dieses einheitlichen Tests ist das EICAR (European Institute for Computer Anti-Virus Research).
Wenn Ihr Virenscanner Sie nicht darauf hinweist, dass diese Datei gefährlich für Ihren Computer sein kann, sollten Sie dringend Ihre Virus-Software wechseln.
(Quelle: https://www.etes.de/downloads/eicar-testvirus/)

Ich wähle extra eine andere Quelle als mich, damit Sie Vertrauen fassen und den Test durchführen. Er ist absolut ungefährlich!

Der Test sieht folgendermaßen aus:

Der Link: https://www.etes.de/downloads/eicar-testvirus/?file=files/etes/downloads/anwenden/eicar.com oder https://happycomputer.eu/testdaten/eicar.com Testet, ob eine Antiviren Testdatei von den Sicherheitseinrichtungen in der Telematik bzw. des SIS erkannt wird. Meldet sich der lokale Virenscanner (und das wird er tun) ist die Testdatei unerkannt **über den (angeblich) sicheren SIS und den (angeblich) schützenden Konnektor auf den Rechner gelangt**. (Es ist mir an dieser Stelle egal, ob das Virus über die TI oder einen anderen Tunnel oder wo auch immer herkommt. Der Konnektor ist Bestandteil der TI und damit kommt das Virus durch die TI auf den Rechner! Entscheidend ist, er kommt nicht durch den Internetanschluss sondern durch den SIS). **Das beweist, dass es keinen wirksamen Schutz gegen Malware (Viren und Trojaner) gibt.** (Dieser Test ist für den seriellen Anschluss wichtig. Bei einem parallelen Anschluss kann es richtig sein, dass sich der lokale Virenscanner meldet, wenn in der Firewall kein Virenscanner eingerichtet ist) Von einem als „SICHER“ verkauften Anschluss kann ein Arzt einen entsprechenden Virenscanner erwarten!

Konsequenz: Hinter solch einem Anschluss müssen alle Geräte durch den Praxisinhaber geschützt werden. Der SIS schützt Sie nicht ausreichend!! Medizinische Geräte, auf denen kein Virenschutz installiert werden kann dürfen sich nicht im selben Netz befinden!! DAS IST WICHTIG!!!

Auch an dieser Stelle eine weitere Differenzierung. Es ist mir egal, welche Dienstleistungen von wem angeboten werden. Ich muss aber ehrlich sagen was der

angebotene Anschluss leistet, damit der Kunde sich entsprechend verhält.
Wenn ich die Aussage mache: *„Durch die integrierte Firewall des Konnektors wird das LAN optimal vor unautorisierten Zugriffen von außen geschützt. “* wie im Informationsblatt der gematik steht, dann ist das für jeden Arzt missverständlich. Ich bin sogar der Meinung, dass hier ein Werbeversprechen gegeben wird, das nicht gehalten wird. Da keinerlei Kommunikationskontrolle von innen nach außen stattfindet, frage ich mich wirklich, was den SIS denn überhaupt noch zu einem sicheren Anschluss macht?

Was ist der Unterschied ob ein Arzt sein System an einer FRITZ!Box hat oder an einem SIS? Für die Bedrohung des Praxisnetzes sehe ich kaum einen Unterschied. Lediglich Port 80 wird gescannt? Das reicht einfach nicht! Auch hier bin ich der Meinung, dass ich nicht nachvollziehen kann, wie das BSI-Konform und zertifiziert sein kann?

Das hat verheerende Konsequenzen: Informationen, welche aus den Konnektoren in die Praxisnetze gelangen, werden ungefiltert bearbeitet, da die Konnektoren im Praxisnetz die höchste Vertrauensstufe „LAN“ besitzen. Dies vereinfacht Angriffe aus der TI heraus und kann sogar zu einem Zusammenbruch des Gesundheitssystems führen.

Der §1 BSIGesetz sagt:
„Das Bundesamt [für Sicherheit in der Informationstechnik] ist zuständig für die Informationssicherheit auf nationaler Ebene.“
Ich fordere das BSI auf:
Kümmern Sie sich um die Sicherheit unserer Gesundheitsdaten.
Die TI ist ein Risiko für unsere sensibelsten und intimsten Daten.

IT-Sicherheit kennt keine Kompromisse.

Hier nun meine Frage an das BSI sowie die Datenschutzbehörden.

Wir wissen ganz sicher, dass Sie auch wissen, dass der überwiegende Teil aller Arztpraxen in Deutschland falsch und nicht sicher angeschlossen sind und auch heute noch angeschlossen werden. Uns liegen zahlreiche Beschwerden an Sie alle in schriftlicher Form vor.

Wie gedenken Sie das Problem zu lösen?
Was geschieht, wenn die Daten von Patienten auf Grund Ihrer Untätigkeit weiter gestohlen werden? Tragen Sie eine Mitverantwortung?
Ist es richtig, dass der SIS absolut keine Kommunikationskontrolle durchführt und alle Ports ausgehend offen sind?
Haben Sie, das BSI, das wirklich so zertifiziert?
Ist es richtig, dass der SIS keinen wirksamen Schutz gegen Malware hat?
Haben Sie das so zertifiziert?
Ist es richtig, dass wir dann zukünftig im Grundschutzkatalog stehen haben, dass keine Kommunikationskontrolle mehr stattfinden braucht um den Grundschutz erhöhte Anforderungen zu erfüllen?(macht meine Arbeit leichter und dürfte in einigen Gerichtsprozessen für die Angeklagten sprechen) Oder gelten die Normen und Richtlinien

nur so lange der „kleine Mann“ sie umsetzt, die Politiker dürfen ungestraft jeden Unsinn machen und werden durch die Ämter und Ministerien gedeckt?
Ist ein Router ausreichender Schutz für ein Praxisnetz?
Ist es richtig, dass der Konnektor keine wirksame Firewall zur Verfügung stellt, die das Praxisnetz ausreichend schützt, wenn alle Port ausgehend offen sind?

Das sind einfache Fragen, die Sie beantworten können sollten. Versuchen Sie es! Wenn Sie eine Frage nicht beantworten wollen, beantworten Sie einfach die nächste. Aber antworten Sie!

Nach unzähligen Mahnungen und der noch folgenden Nachricht:

Sehr geehrte Damen und Herren,

Wie bereits am Freitag 5.07.2019 telefonisch besprochen, schicke ich Ihnen die Fotos mit den 2 neu eingerichteten Arbeitsplätzen, nach der Installation des Konnektors. Dieser wurde am 04.06.2019 von der Firma Varicom aus Saarland, auf meinen ausdrücklichen Wunsch seriell angebunden. Ich verwende als Praxissoftware MCS.Isynet.

Nach dem Absturz des 2.Arbeitsplatzes infolge des monatlichen Updates ,sah ich mich am 03.07. gezwungen die Hotline anzurufen. Nach einer Stunde wurde endlich der Fehler in der Netzkonfiguration beseitigt. Anschließend musste ich jedoch feststellen, dass Windows- Firewall mit Absicht abgeschaltet wurde. Auf die Nachfrage bei der Firma Varicom, wurde mir mitgeteilt ,daß trotz des Abschaltens, das System sicher sei .

Ich bin allerdings, durch die Foren im Internet (insbesondere auf facharzt.de) und den Artikel im Augenarzt Nr. 3 (Juni 2019), auf das Ihnen telefonisch mitgeteilte Problem aufmerksam geworden.

In der Hoffnung bald mit Ihrer Hilfe, die o.g. Sicherheitslücke zu beseitigen, verbleibe ich,

oder diese:

dieses Mal in Mz gefunden. Habe ich heute fotografiert. Damit legt meine kleine, nicht repräsentative Stichprobe nahe, dass parallel Standard ist.

Ich habe bisher nur mit einem "Installateur" gesprochen, aber der verhielt sich genau so, wie Sie es mal geschildert haben. Es lief daraus hinaus, dass er mich fragte, warum ich mich überhaupt um seinen Kram kümmern würde. Er würde alles so machen, wie es in der Schulung (von arvato) kommuniziert worden wäre. Und ich solle mich doch um meinen eigenen Kram kümmern. Fast hätte er Recht gehabt, aber da diese Praxis zur Praxisgemeinschaft meiner Frau gehört und der Serverraum in meiner Zuständigkeit liegt, hat er eben nur fast Recht gehabt ;-)

Der Eindruck liegt nahe, dass die "Installateure", sofern sie Ahnung haben, wissen, was sie in den Praxen für einen Schrott hinterlassen.

Aber der wirtschaftliche Druck, möglichst viele Installationen in möglichst kurzer Zeit, lässt ihnen keine Wahl.

Dass arvato jetzt den Auftrag erhalten hat, für die nächsten 8 Jahre die TI zu administrieren - das ist der Bock als Gärtner. arvato ist Bertelsmann - und was ein Kommunikationskonzern wie Bertelsmann mit sensiblen Daten anstellen kann.

Gruß

Eine weitere finden Sie als Anhang.

Das kann Sie doch nicht kalt lassen!!

Sind Sie nicht für den Schutz der Daten verantwortlich? Tun Sie endlich etwas! Beantworten Sie wenigstens meine Mails!

Mit freundlichen Grüßen

Jens Ernst

Habe ich die folgende Antwort erhalten:

Sehr geehrter Herr Ernst,

vielen Dank für Ihre Anfrage und Ihren Anregungen zum Thema der Telematikinfrastruktur (TI).

In einem neu gestalteten Bereich Ihrer Webseiten unter:
https://fachportal.gematik.de/erste-schritte/anschluss-medizinischer-einrichtungen/
hat sich die gematik der hauptsächlichen und dringenden Fragen in diesem Kontext angenommen und entsprechende zusätzliche Informationen bereitgestellt.

Hier sind nun neben einem allgemeinen
Informationsblatt "Technische Ausstattung einer medizinischen Einrichtung"
auch Informationen zu den Anforderungen bezügl. der Betriebsarten des Konnektors, Checklisten für Praxen und ein Muster-Installationsprotokoll "Sichere TI-Installation" hinterlegt, mit dem der Dienstleister vor Ort - aber auch der Praxisinhaber/- inhaberin selbst noch einmal Schritt für Schritt die sach- und fachgerechte TI-Installation nachvollziehen kann.

Zu beachten ist hier, dass der BSI- zertifizierte Konnektor beim Anschluss an die Telematikinfrastruktur hierbei eine Schutzfunktion für sich selbst sowie hierdurch für die über Ihn an die TI angeschlossenen Komponenten vor Angriffen aus dem Transportnetz übernimmt, die im Rahmen der Zertifizierung bestätigt wurde. Hierbei werden Angriffe mit hohem Angriffspotential abgewehrt.
Der Zugang zum offenen Internet über den SIS ist für den Praxisinhaber optional und muss durch diesen - bzw. dem von ihm beauftragten Dienstleister - im Bedarfsfall aktiviert werden.
(Siehe auch
https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Service/Anschluss_medizinischer_Einrichtungen_an_die_Telematikinfrastruktur__DVO_/Informationsblatt_Betriebsarten-Konnektor_V1.0.0.pdf)
Detaillierte Informationen zum Leistungsangebot des SIS sowie eventuelle zusätzliche Konfigurationsmöglichkeiten diesen betreffend sind über den jeweilig vom Praxisinhaber beauftragten Zugangsdienstbetreiber erhältlich.
Der VPN-Zugangsdienst mit dem Secure Internet Service selbst werden nicht durch das BSI zertifiziert, unterliegen jedoch für eine gematik-Zulassung den obligatorischen Anforderungen in den entsprechenden Spezifikationen.
Details zu den Anforderungen sind z.B. in dem von der gematik zum Download zur Verfügung gestellten Dokument "Spezifikation VPN-Zugangsdienst"
enthalten.

Auch auf die Fragen zur DSGVO und deren Bewertung werden auf obig bereits referenzierter Seite https://fachportal.gematik.de/erste-schritte/anschluss-medizinischer-einrichtungen/
unter dem Punkt "Bitte beachten Sie auch die Hinweise der gematik zu Datenschutz und Haftung in der Telematikinfrastruktur" noch näher eingegangen.

Wir hoffen, Ihnen mit diesen Informationen weiter helfen zu können und verbleiben mit freundlichen Grüßen,

Im Auftrag

Anabela da Silva Santos

Bundesamt fuer Sicherheit
in der Informationstechnik

Service-Center

Damit steht fest, das BSI hat den SIS nicht zertifiziert, die Firewall schützt nur den Konnektor und das Transportnetz. Der SIS schützt das Praxisnetz bei weitem nicht ausreichend vor Malware bzw. davor, Daten über z.B. Malware zu verlieren. Die eingebaute und vom BSI zertifizierte Firewall im Konnektor hat also nichts mit dem SIS zu tun. Eine ausgehende Kommunikationskontrolle fehlt. Das ist nicht einmal Grundschutz Basisanforderung BSI und. **Damit ist eine Hardware-Firewall auch bei einem seriellen Anschluss mit SIS immer zwingend nötig!**

Weiter steht fest, dass die gematik einen SIS **verkauft**, welcher nicht den Bestimmungen des BSI genügt und vor allem nicht Stand der Technik ist, damit sehe ich die gesamte Zertifizierung des seriellen Anschlusses mit SIS gefährdet! Was nutzt mir eine verschlossene unüberwindliche Stahltür, wenn das Fenster daneben sperrangelweit offen steht?

Fazit bisher, alle Praxen, die über einen Internetanschluss verfügen **sind nicht sicher angeschlossen**. Selbst mit Hardware-Firewall ist auf Grund der fehlenden Informationen eine sichere Anbindung nur möglich, wenn man sich die IP-Adressen aus den Logs fischt. Auf Grund der unverschlüsselten Kommunikation im Netz ist das wahrscheinlich jedoch bereits ein Verstoß gegen die DSGVO, da ich auch Echtdaten von Patienten sehen kann. Außerdem wurden uns solche Log-Auswertungen untersagt.

Frage 14: Ist der Bundesregierung bekannt, dass der SIS keinerlei Kommunikationskontrolle von innen nach außen durchführt und somit mit jeder beliebigen Malware alle Daten abgezogen werden können und ist das für die Bundesregierung richtig so?

Forderung 8: Bei allen Reiheninstallationen ohne Hardwarefirewall ist der SIS unverzüglich abzuschalten. Er darf erst nach Aufrüstung einer Hardwarefirewall wieder hinzugeschaltet werden!

Versprechen wie diese, sind nicht umgesetzt:

3.5.4 Firewall

Die Firewall des T-Systems Konnektors schützt die Kommunikation zwischen Ihrem Netzwerk und anderen Netzen. Es wird grundsätzlich sämtlicher ein- und ausgehender Datenver-

kehr auf die Einhaltung der vorgegebenen Kommunikationsregeln überprüft. Dies ist notwendig, da Sie bei Verwendung der Online-Funktionalität des Konnektors mit Kommunikationspartnern in verschiedenen Netzen verbunden sein können.

Die Firewall setzt Kommunikationsregeln sowohl für das Netz des Leistungserbringers und das WAN, als auch für den Datenverkehr innerhalb der aufgebauten VPN-Tunnel durch. Die angewandten Filterregeln sind im Security Target des Verfahrens BSI-DSZ-CC-0928 beschrieben.

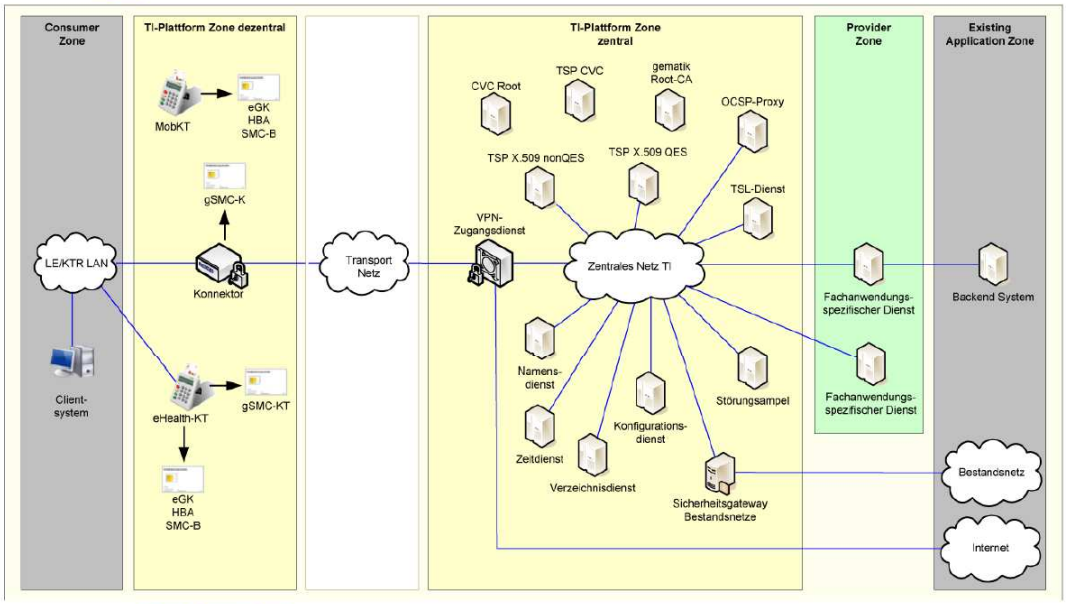


Abbildung 2 Übersicht des Gesamtsystems der TI

Die grundlegende Sicherheitsregel (policy) der T-Systems Konnektor-Firewall besteht darin, dass sämtlicher Datenverkehr, der nicht vom Konnektor initiiert wurde oder nicht an Dienste des Netz- und Anwendungskonnektors gerichtet ist, blockiert wird. Ein aktiver Zugriff auf Ihr Netzwerk über den T-Systems Konnektor ist nicht möglich. Zudem filtert die integrierte Firewall den Datenverkehr dahingehend, dass ausschließlich zulässige Protokolle und Fachdienste Zugriff auf die jeweiligen Netze erlangen.

Die Firewall ist eng mit der Sicherheitsprotokollierung verknüpft. Wird eine Regelverletzung erkannt, so wird diese im Sicherheitsprotokoll des Konnektors protokolliert. Sie können sich in Kapitel 7.10 über die Auswertung des Sicherheitsprotokolls informieren.

In BSI-DSZ-CC-0928 (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/Reporte09/0928ma2b_pdf.pdf;jsessionid=ADBE006BE373F97486CB879DC3E57184.2_cid360?__blob=publicationFile&v=2) ist jedoch klar geregelt, dass das LAN Vollzugriff auf den SIS erhält, jedoch die Aussage „Zudem filtert die integrierte Firewall den Datenverkehr dahingehend, dass ausschließlich zulässige Protokolle und Fach dienste Zugriff auf die jeweiligen Netze erlangen." ist vom SIS nicht umgesetzt! Die BSI Grundschutz Basisanforderung ist nicht erfüllt, schon gar nicht die erhöhten Anforderungen.

Nächstes Problem in Verbindung mit beiden Anschlussmethoden:

Die Techniker schließen die Rechner an das Internet an, ohne die Rechner upzudaten. In einer Praxis wurde beispielsweise ein sein 6 Jahre in Betrieb befindlicher Rechner ohne ein Update weder Windows Update noch Virenschutz, einfach an einen Speedport angeschlossen (parallel). Den Technikern war das vollkommen egal. Das wurde übrigens auch vom Bundes- und Landesdatenschutz in Augenschein genommen, kann also auch von dort angefragt werden. Sie können sich auch den Beitrag https://www.br.de/nachrichten/deutschland-welt/sicherheitsluecken-probleme-mit-der-elektronischen-patientenakte,RRmEPve ansehen, da spricht der Arzt selbst im Fernsehen.

Forderung 9: Die DvOs werden verpflichtet, beim Anschluss von Praxen ans Internet, diese komplett auf den „Stand der Technik" zu bringen, wie es das BSI fordert und zertifiziert hat.

Ein weiteres Problem ist das Kartenlesegerät. Es sollte einen absolut geheimen Sicherheits PIN haben. Bei der Eingabe ertönt ein Rauschen um die Eingabe nicht abhören zu können.

3 Probleme werden von den DvOs eingebaut:

1. Das Rauschen wird von den Technikern abgeschaltet. (Zeugen, Ärzte, vorhanden)
2. Der 8-stellige PIN des Lesegerätes ist egal ob Köln, Hagen oder Schwerte: 12345678 Vermutlich der Ausgangs PIN
3. Der 6 Stellige Ärzte PIN ist 123456

Frage 15: Warum werden bei solch wichtigen Funktionen, wie das Rauschen, überhaupt Abschaltfunktionen eingebaut?

Frage 16: Warum wird eine zu einfache PIN Eingabe nicht durch eine entsprechende Programmierung verhindert? Warum darf die Transport PIN weiter genutzt werden?

Frage 17: Findet die Bundesregierung einen PIN 12345678 sicher?

Ich kann dazu nur sagen, dass ich schon mindestens 100 Menschen nach einem 8-Stelligen PIN gefragt habe, 12345678 war immer unter den ersten 3 Antworten dabei!

Forderung 10: Über die offiziellen Kanäle ist die Anweisung zu erteilen, dass alle Praxen mit den PINs 12345678 oder 123456, ihre PINs in geheime sichere PINs ändern müssen, sonst verstoßen diese gegen die DSGVO. Eine entsprechende Anweisung und eine entsprechende Informationsschrift mit einer Anleitung ist von den Betreibern unverzüglich den Praxen zur Verfügung zu stellen!

Und noch eine Meldung zu den Kartenlesegeräten hat mich erreicht.

> Danach konnten wir uns dann mit dem nächsten Spaß beschäftigen, nämlich dass die Telematik immer kurze Zeit nach Praxisstart abstürzte - einzige Lösung, alle Komponenten in der richtigen Reihenfolge neustarten und hoffen, dass man länger als 10Min hatte, bevor man dies wieder tun musste. […] Was war's? (Bzw. ist es noch?)
>
> Nun, jede KVK-Karte ist mit einem elektronischen Zertifikat pro Krankenkasse gesichert (also jede Krankenkasse hat ein eigenes Zertifikat). Der Kartenleser holt sich über die SMC-B Karte, über den Konnektor, VPN-Tunnel usw. sozusagen das "Gegen-"Zertifikat um zu schauen ob die Karte echt ist. Für diese "Gegen-"Zertifikate gibt es 8 Speicherplätze (pro alle Kartenleser einer BSNR), die je einmal belegt werden können und nicht mehr freigegen werden (außer man schaltet alles aus).
>
> Na, Sie ahnen es schon? Es gibt dummerweise mehr als 8 Krankenkassen in unserem Lande, wer konnte denn nur sowas ahnen.
> Und so lange man den ganzen Tag nur Patienten behandelt, die zur gleichen Kasse gehören oder einfach eh nur 8 Patienten am Tag macht, läuft die Telematik auch prima.
> Und zur Sicherheit hat man bei den Testes der ganzen Telematik auch einfach nur mit 5 Karten gearbeitet, bevor man den Mist auf die Menschheit losgelassen hat, wie uns der zuständige Entwickler berichtete.

Frage 18: Ist diese Schilderung richtig? Ein Argument für die TI war die Prüfung der Karte und der dadurch wegfallende Misbrauch! Wie werden die Karten dann auf echtheit geprüft, wenn diese Funktion angeschaltet werden muss für eine andauernde Funktion?

Ein weiteres Problem in Zusammenhang mit den Konnektoren sind die Passwörter.

Die geheimen Passwörter (die wenigstens komplex sind) der Konnektoren werden auch gegen den Willen der Ärzte aufgeschrieben und mitgenommen. Daher bin ich nach Köln gefahren um das PW eines Konnektors zu ändern.

Frage 19: Gibt es Regelungen über die Mitnahme geheimer Passworte aus den Praxen? Hält es die Bundesregierung für richtig, dass sogar bei Zeitarbeitsfirmen rekrutierte Mitarbeiter, welche nach wenigen Wochen schon nicht mehr in dem Bereich arbeiten, Kenntnis über Zugangsdaten von Konnektoren mitnehmen?

Forderung 11: Die Konnektoren haben neben dem Admin einen Superuser. Das PW des Superusers ist für die Firmen. Das Passwort des admins gehört ausschließlich in die Praxis. Die DvOs haben die Passwörter aufgeschrieben und mitgenommen. Meiner Meinung nach verstößt das gegen mehrere Gesetze unter anderem gegen §203 StGB. Auch würde ich das mitnehmen von solchen Passworten als Vorbereitung zu einer Straftat bewerten. Diese Passwörter sind durch die betroffenen Ärzte zu ändern. Eine entsprechende Anweisung und eine entsprechende Informationsschrift mit einer Anleitung sind von den Betreibern unverzüglich den Praxen zur Verfügung zu stellen!

Ein weiteres Problem sind die Router, welche von den DvOs keine Beachtung bekommen. Die Softwarestände der Router werden nicht geprüft. Die Softwarestände sind uralt. Für ein

Telefon mag das ausreichend sein für eine Praxis nicht! Wenn dann noch nicht einmal eine Hardwarefirewall vorhanden ist und sogar die lokalen Firewalls abgeschaltet werden, dann sind die Daten vollkommen Schutzlos im Internet.

Forderung 12: Die DvOs sind anzuweisen, die Softwarestände der Router auf den neuesten Stand zu bringen und alte Router auszutauschen!

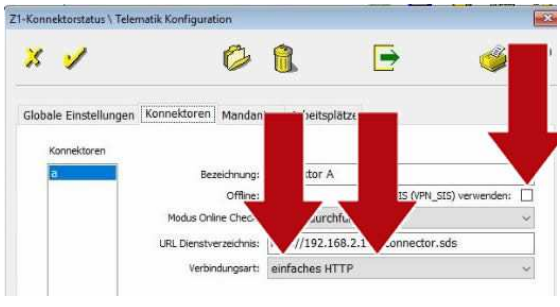
Das nächstes Problem ist das WLAN. In ein WLAN kann vergleichsweise einfach eingedrungen werden. Außer eine 802.1x Verbindung (selbst die ist nicht 100% sicher, und die wird bestimmt nicht installiert) ist kein WLAN sicher!!!!!
Selbst WPA3 mit seinem neuartigen Butterfly-Handshake ist bereits gehackt worden, bevor ich überhaupt ein Gerät gesehen habe, welches WPA3 kann.
https://www.computerbase.de/2019-04/wpa3-schwachstellen-dragonblood-wlan-passwort-hacken-unsicher/
Zu WPA2 Das sind allein die Sicherheitslücken, welche für WPA und WPA II bereits bekannt sind. CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088 Sie wollen wissen, wie einfach das geht? https://www.heise.de/security/artikel/KRACK-so-funktioniert-der-Angriff-auf-WPA2-3865019.html Diese Anleitungen im Internet sind so simpel, dass Ihnen sehr schnell klar sein muss, dass es keine Hacker Kenntnisse bedarf, um sich in ein WLAN zu hacken.

Wie aus zahlreichen Unterlagen ersichtlich ist (Hasomed, Elefant, DGN usw.) wird das von den Unternehmen toleriert. Techniker schließen sogar Praxisrechner mit sensiblen Daten im Zuge des TI Anschlusses per WLAN an. (Auch hier gibt es sogar im Zuge des TI Anschlusses gehackede Arztpraxen. Das TI-Anschließende Unternehmen war Ergosoft. Auch hier wieder eine psychologische Praxis.)

Frage 20: Gibt es von Seiten der Bundesregierung Vorgaben zur Nutzung eines WLAN in einem Praxisnetz? Wenn nicht, warum nicht?

Forderung 13: WLAN in den Praxisnetzen sind zu verbieten. Das muss durch gematik und KBV ganz klar kommuniziert werden! Außerhalb des Praxisnetzes (Netztrennung vor dem Konnektor auf der WAN-Seite) ist es zulässig, aber nur dort.

Darauf aufbauend haben wir einen weiteren bereits erwähnten groben Mangel der Kommunikation aufgedeckt, welcher gegen Art. 6 DSGVO verstößt. Die Kommunikation im LAN verläuft in Klartext, also unverschlüsselt. Bei der Programmierung wurde eine SSL-Verschlüsselung der Verbindung explizit vorgesehen, von den Technikern aber vermutlich aufgrund des Mehraufwandes nicht umgesetzt. Auch hier ein Beispielbild aus einer Supportsitzung, damit Sie mir das glauben.



Das macht die Daten im Netz nicht nur sicht- sondern auch manipulierbar. Es ist das Äquivalent einer wiederbeschreibbaren Postkarte. Jeder kann mitlesen und neu beschreiben. Darüber hinaus kann ein Angreifer aus dem WLAN heraus eine Verbindung in die TI herstellen. Das BSI schreibt dazu:
„Zwischen den lokalen Netzen der Leistungserbringer und der zentralen Telematikinfrastruktur-Plattform werden zu schützende Daten der TI und der Bestandsnetze ausgetauscht. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten unbemerkt manipulieren können. Der Absender von übertragenen Daten muss eindeutig bestimmbar sein.“

Die gematik schreibt dazu per Mail auf Anfrage von Teletrust:

> *der Konnektor wurde spezifiziert, um in den Verschiedensten Umgebungen zu funktionieren und unterschiedlichen Anforderungen gerecht zu werden. Daraus resultieren die Konfigurationsmöglichkeiten des Konnektors.*
> ***Zum eine betrifft dieses die Möglichkeit, Kommunikation zum Primärsystem nicht per TLS zu verschlüsseln. Diese Betriebsart ist nicht empfohlen, wurde aber aufgenommen, um interoperabilität mit sehr alten Systemen zu erlauben.***
>
> *Der Konnektor bietet die Möglichkeit über seine zertifizierte Firewall das Netz des Leistungserbringers gegen das Internet abzuschirmen wenn er in Reihe geschaltet wird (WAN-Buchse mit dem Internetrouter verbunden und entsprechende Konnektorkonfiguration). In dieser sicheren Konfiguration kann das Internet nur über den SIS-Service des VPN-Zugangsdienstes genutzt werden, oder der Internetzugang kann komplett gesperrt werden. Für Praxen, die sich nur wegen der TI mit dem Internet verbinden, ist dieses das Ideale Szenario. Sicherheitsbewußte Ärzte sollten auf dieses Szenario bestehen.* ***Der gematik wurde zugetragen, dass dieses Szenario selten installiert wird. Einen Direkten Einfluss hat die gematik hierauf jedoch nicht.*** (Anmerkung Jens Ernst: Die wissen genau, dass fast ausschließlich parallel installiert wird)
>
> ***Die Parallelinstallation ist vorgesehen, für Praxiennetze, welche sich bereits anderweitig gegen Bedrohungen aus dem Internet absichern und erlaubt eine TI-Anbindung, welche nicht mit der sonstigen Internetnutzung interferriert. Dem Arzt muss bei diesem Szenario klar sein, dass der Konnektor keine Sicherheit gegenüber dem Internet bieten kann und mit anderen Mitteln für die Sicherheit der in seinem Netz gespeicherten medizinischen Daten sorgen muss.***
>
> *Die KBV hat Richtlinien für einen sicheren Betrieb von Informationstechnik in Arztpraxen herausgegeben. Selbstverständlich gehören dazu Firewalls und Virenschutz. Selbstverständlich können Firewalls und Virenschutz auch bei einer TI-Anbindung genutzt werden.*
> *Leider hat sich gezeigt, dass detaillierte Kenntnisse über die Konfigurationsmöglichkeiten des Konnektors notwendig, sind, um den Konnektor optimal in eine Umgebung zu integrieren. Dieses bietet Dienstleistern jedoch auch die Möglichkeit, sich gegenüber den* ***verbreiteten 08/15 Installationen*** *zu profilieren.* (Anmerkung Jens Ernst: Die wissen genau, dass verbreitet 08/15 installiert wird)
>
> *Sollten wir innerhalb der nächsten sieben Tage keine Rückmeldung von Ihnen erhalten, schließt sich das Ticket automatisch.* (Anmerkung Jens Ernst: Mehr braucht man ja bei solch einem Skandal nicht zu tun, 295 Wörter schreiben, fertig, Problem gelöst)

Das war übrigens die Antwort der gematik auf meine Meldung der Probleme beim Anschluss der TI bei Teletrust. Der Betreff ist auch sehr aufschlussreich: *Ihr #Ticket ID-0000081602# mit dem Titel "WG: TeleTrusT-AG "SICCT": "Skandal bei Telematik-Infrastruktur"" wurde*

gelöst. Mit dieser Mail betrachtet die gematik das Problem als gelöst. Da fühlt man sich doch richtig ernst genommen.
Noch eine Anmerkung, auf **meine** Anfragen bei der gematik habe ich bis heute noch keine Antwort erhalten. Ich bin offensichtlich nicht würdig genug, eine Antwort zu bekommen. Das oben genannte Ticket wurde von der Firma Teletrust eröffnet, welche ich ebenfalls um Hilfe gebeten hatte.

Zurück zum meinem Satz: „Bei der Programmierung wurde eine SSL-Verschlüsselung der Verbindung explizit vorgesehen, von den Technikern aber vermutlich aufgrund des Mehraufwandes nicht umgesetzt.“ Hier ist ein weiterer wesentlicher Kritikpunkt bei der Umsetzung der TI enthalten. Ich möchte nicht alle Techniker für komplett unfähig halten. Es wird mit Sicherheit Techniker geben, die vielleicht alles richtig machen wollen und vielleicht sogar welche, die alles richtiggemacht haben. Unsere Erfahrung mit dem Anschluss der TI an ein Praxisnetz ist eine Andere. Die Techniker werden pauschal bezahlt**.** Darum wird nur das allernötigste getan um das System einmalig vorgeführt zu haben. Dann verschwinden die Techniker und lassen nicht arbeitsfähige Praxen und unsichere Anschlüsse zurück. Es wird weder geprüft, ob ein paralleler Anschluss überhaupt geschaltet werden dürfte, noch werden andere wichtige sicherheitsrelevante Konfigurationen wie TLS durchgeführt. Funktioniert etwas nicht, werden Stück für Stück alle Sicherheiten abgeschaltet bis der Stammdatenabgleich funktioniert. Ziel scheint lediglich eine schnelle Unterschrift zum abkassieren der Installationspauschale zu sein. Eine Beratung hat bisher kein Arzt mit dem ich gesprochen habe, je erhalten. Die Datenschutzbeauftragten können das bestätigen (poststelle@bfdi.bund.de, poststelle@ldi.nrw.de). Die haben auch mit den Ärzten gesprochen und hatten sogar einen guten Fragenkatalog vorbereitet. Sie bekommen bestimmt die vor Ort ausgefüllten Daten zur Verfügung gestellt. Die Theorie und die Wirklichkeit sind komplett gegenteilig

Frage 21: Wie steht die Bundesregierung zur fehlenden Verschlüsslung?

Forderung 14: Die Verschlüsselung ist unverzüglich in allen Praxen einzuschalten und zu nutzen. Es muss eine offizielle Anweisung der KBV und der gematik geben, dass bei fehlender Verschlüsselung gegen die DSGVO verstoßen wird!

Ein weiterer Punkt, welchen ich ungeheuer finde. Ein Arzt lässt sich zwangsweise anschließen, will aber einen TI-Anschluss ohne SIS und Internet, um nicht das Risiko zu haben, gehacked zu werden (da dem Arzt fundierte IT Kenntnisse fehlen und sich die Anbieterinformationen wiedersprechen, wie wir hier auch dargelegt haben).

Das wird dem Arzt verweigert. Man sagt ihm, er könne nur den Anschluss mit SIS haben. Auch den Arzt kann ich benennen. Auch das ist an die Behörden gemeldet, keine Reaktion! Darüber, dass andere Ärzte genötigt werden sich parallel anzuschließen, obwohl sie keine Hardwarefirewall haben, hatte ich bereits berichtet.

Frage 22: Ist es richtig, dass Firmen die Art des Anschlusses vorschreiben dürfen und Patientendaten auf diese Art nicht sicher ins Internet gehängt werden?

Forderung 15: Beim Zwangsanschluss an die TI handelt es sich um einen fundamentalen Eingriff in das Netzwerk einer Praxis. Darum sollte ein Arzt auch frei entscheiden dürfen, wie

er angeschlossen werden möchte (sicher oder unsicher, mit oder ohne Internet). Bisher beziehen sich die Betreiber der TI auf die Vertragsfreiheit und sind der Meinung ausschließlich unsichere Anschlüsse anbieten zu dürfen. Hier müssen die Rechte der Patienten und damit die fundamentalen Menschenrechte auf Unversehrtheit (und damit meine ich auch die digitale Unversehrtheit) sowie die Rechte des Grundgesetzbuches über der Vertragsfreiheit stehen. Dies ist unverzüglich ins Gesetz aufzunehmen und fest zu schreiben!

In diesem Blog habe ich noch etwas Interessantes gelesen:
https://www.vondoczudoc.de/viewtopic.php?f=11&t=6676&start=0

„nach langem hin und her und zig Anrufen bekam ich nun heute einen Anruf einer Zeitarbeitsfirma, die im Auftrag der CGM die Telematik installieren will."

Wenn bei Zeitarbeitsfirmen in einem 2 Tageskurs Menschen rekrutiert werden die TI zu installieren, dann ist die katastrophale Umsetzung der TI kein Wunder.

Frage 23: Warum ist beim Aufbau der TI auf ausgebildetes bzw. zertifiziertes Personal verzichtet worden. Es war mal angedacht, dass den Aufbau ausschließlich zertifizierte Techniker vornehmen sollten.

Forderung 16: Es dürfen nur noch ausgebildete IT-ler die TI aufbauen, welche wenigstens Grundlagenwissen im Bereich IT haben. Ich bin für ausschließlich zertifiziertes Personal. In der Zertifizierung ist eine Prüfung nötig, in der die Grundkenntnisse Grundschutz abgefordert werden müssen!

Die Mängel sind allgemeingültig und wurden mir aus ganz Deutschland mit Bildern bestätigt.

Die gematik betont immer wieder, es würden keine medizinischen Daten übertragen. Trotz mehrfacher Aufforderungen, das richtig zu stellen, tut sie das nicht. Daher die Informationen zur Aufklärung an alle, die das noch nicht wissen.

Diese Daten werden übertragen:

In der ersten Rollout-Phase (VSDM) der Telematikinfrastruktur in 2019 sollen nach Angaben der gematik zunächst die gemäß § 291 SGB V auf der elektronischen Gesundheitskarte gespeicherten Daten übertragen und abgeglichen werden. Hierbei handelt es sich um folgende Daten:

- Die Bezeichnung der ausstellenden Krankenkasse, einschließlich eines Kennzeichens für die kassenärztliche Vereinigung, in deren Bezirk der Versicherte seinen Wohnsitz hat,
- den Familiennamen und Vornamen des Versicherten,
- das Geburtsdatum des Versicherten,
- das Geschlecht des Versicherten,
- die Anschrift des Versicherten,
- die Krankenversicherungsnummer des Versicherten,
- den Versichertenstatus, für Personengruppen nach § 264 Abs. 2 SGB V den Status der auftragsweisen Betreuung,
- den Zuzahlungsstatus des Versicherten,
- den Tag des Beginns des Versicherungsschutzes,

- bei befristeter Gültigkeit der elektronischen Gesundheitskarte das Datum des Fristablaufs.

In § 291 Abs.2 Nr.7 SGB V wird darüber hinaus auf den § 264 Abs.2 SGB V verwiesen, also die Vorschrift „Versichertenstatus, für Personengruppen nach § 264 Abs.2 der Status der auftragsweisen Betreuung“. Gemäß § 264 Abs.4 S.3 und 4 SGB V gilt als Versicherungsstatus die Statusbezeichnung „Mitglied“, „Rentner“ oder „Familienversicherter“. Der Status der auftragsweisen Betreuung nach § 264 Abs. 2 kann die Werte „SGB XII“, „Asylbewerberleistungsgesetz“ und „Krankenhelfer“ haben.

Die tatsächlich auf der elektronischen Gesundheitskarte speicherbaren Daten zum Versichertenstatus ergeben sich aber aus untergesetzlichen Normen, namentlich aus dem „Fachkonzept Versichertenstammdatenmanagement“ der gematik und aus der „technischen Anlage zu Anlage 4 Bundesmantelvertrag-Ärzte (BMV-L)“. Gesetzliche Grundlage für den Erlass der technischen Normen sind § 291 b Abs.1 Nr.2 und §§ 291 Abs.3, 87 Abs.1 S.2 SGB V. In den beiden technischen Spezifikationen ist unter anderem geregelt, dass auf der EGK ein „DMP-Kennzeichen“ gespeichert wird, das folgende Werte haben kann:

- Diabetes Mellitos Typ 2
- Brustkrebs
- Koronare Herzkrankheit
- Diabetes Mellitos Typ 1
- Asthma Bronchiale
- COPD

siehe: „Fachkonzept Versichertenstammdatenmanagement“, Seite 43, abrufbar unter https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Spezifikationen/Basis-Rollout/Fachanwendungen/gematik_VSD_Fachkonzept_VSDM_V270.pdf

Bei gespeicherten Daten zu diesen chronischen Erkrankungen handelt es sich zweifellos um besondere personenbezogene Daten im Sinne von Art.9 Abs.1 DSGVO. Gerade die vorgenannten DMP-Zeichen und die daraus ersichtlichen Informationen über chronische Erkrankungen des betroffenen Patienten können ganz eindeutig als Score-Wert gegen die Interessen des Betroffenen verwendet werden. Die Eintrittswahrscheinlichkeit und der Schaden der Rechte und Freiheiten im Sinne von Art.35 DSGVO würde in diesem Fall ein hohes Risiko für die Betroffenen bedeuten.

(Quelle: https://de.wikipedia.org/wiki/Versichertenstatus)
Da kann man nachlesen:

```
.---------  Versichertenstatus
| .-------  Stichprobenzuordnung
| |..-----  Geburtsjahr
| ||| .---  Versicherstenstatus-Ergänzung
| --- |

1    9
3 000 1
5 651 9
```

Status RSA	Erg.	Beschreibung
1		Versicherungspflichtige und -berechtigte
3		Familienversicherte

5		Rentner in der Krankenversicherung der Rentner und deren familienversicherten Angehörige
	000	Versicherter ohne Stichprobenbeteiligung
	1..	weiblich, ohne EU-/BU-Rentenbezug
	2..	männlich, ohne EU-/BU-Rentenbezug
	3..	weiblich, mit EU-/BU-Rentenbezug
	4..	männlich, mit EU-/BU-Rentenbezug
	5..	wie 1, nur vor 1900 geboren
	6..	wie 2, nur vor 1900 geboren
	7..	wie 1, nur nach 1999 geboren
	8..	wie 2, nur nach 1999 geboren
	.JJ	Geburtsjahr
		1 Versicherter aus alten Bundesländern
		4 Sozialhilfeempfänger, § 264 SGB V
		6 Betreute Ausländer im Inland, BVG inkl. OEG, IfSG, SVG, ZHG, HHG, PrVG sowie BEG
		7 Sozialversicherungsabkommen, nach Aufwand, Grenzgänger
		8 Sozialversicherungsabkommen, pauschal
		9 Versicherter aus neuen Bundesländern
		D wie 1, und Disease-Management-Programme für Asthma Bronchiale
		F wie 9, und Disease-Management-Programme für Asthma Bronchiale
		A wie 1, und Disease-Management-Programme für Brustkrebs
		C wie 9, und Disease-Management-Programme für Brustkrebs
		S wie 1, und Disease-Management-Programme für COPD
		P wie 9, und Disease-Management-Programme für COPD
		E wie 1, und Disease-Management-Programme für Diabetes mellitus Typ 1
		N wie 9, und Disease-Management-Programme für Diabetes mellitus Typ 1
		M wie 1, und Disease-Management-Programme für Diabetes mellitus Typ 2
		X wie 9, und Disease-Management-Programme für Diabetes mellitus Typ 2
		K wie 1, und Disease-Management-Programme für Koronare Herzkrankheit
		L wie 9, und Disease-Management-Programme für Koronare Herzkrankheit

Forderung 17: Ich fordere, dass die gematik hier zukünftig an die Wahrheitspflicht erinnert wird! Die Aussage, es werden derzeit noch keine medizinischen Daten übertragen stimmt einfach nicht!

Noch eine Kleinigjeit, welche mich aber ärgert. Beim Aufbau der TI wird in Systemen (dessen Aufbau wir begleitet haben) der Google DNS (8.8.8.8) verwendet und abgeprüft. Es kann doch nicht sein, dass bei solch einem wichtigen Unternehmen wie die TI nicht auf eigene DNS Server gesetzt wird! In Zeiten von CLOUD Act und Calea kann es nicht sein, dass wir für so wichtige Daten amerikanische Dienste nutzen. Arvato macht dies übrigens richtig.

Frage 24: Warum wird bei den TI Anfragen der Google DNS genutzt?

Forderung 18: 8.8.8.8 ist aus allen Konfigurationen und Testprogrammen zu entfernen. Google hat jetzt bereits eine Datenbank mit TI Anschlüssen allein auf Grund der Testtools.

Jetzt komme ich zu einer richtig perfiden Geschichte, die mir von einem Psychologen berichtet wurde, welcher ebenfalls parallel ohne Firewall an die TI angeschlossen wurde. Es geht um die Haftungsfragen. Da der Psychologe mit der Technik überfordert ist und die TI nur so installiert wurde (eine Reihenanschluss wurde verweigert) möchte er sich nun einer „Diffusionsgemeinschaft“ anschließen. Ich habe erst einmal nachfragen müssen, was das bedeuten soll. Ja, er schließt sich einer Gemeinschaft an, in der Patientendaten in die Cloud geladen werden. Damit können Patienten nicht mehr beweisen, dass die Daten bei dem Psychologen gestohlen wurden und der Arzt ist aus der Haftung (Beweispflicht). Allein einem Arzt solch ein Angebot zu machen halte ich für kriminell. Es sind aber die Auswüchse der Spahn Politik, die mit Hochdruck und Zeitdruck den Ärzten ein unsicheres System aufzwingt. Die Ärzte sehen keinen Ausweg.

Frage 25: Wie steht die Bundesregierung zu solchen Methoden, sich aus der Haftung zu schleichen, so dass geschädigte Patienten noch nicht einmal einen Schadensersatz geltend machen können? Wie verhält sich die rechtliche Lage in den Rechenzentren in denen Konnektoren gehostet werden? Ist das Hosten von Konnktoren überhaupt Datenschutzkonform?

Forderung 19: Ich fordere, dass die Rechte der Patienten dahingehend gestärkt werden, dass sowohl der Arzt als auch die Diffusionsgemeinschaften oder Rechenzentren jede auch für sich allein voll haften. Wenn Patientendaten durch den Anschluss der TI öffentlich werden und Menschen dadurch geschädigt werden, dann muss den Opfern der TI auch ein Schadensanschpruch zustehen.

Bei den Abrechnungen mit den KVen bzw. KZVen wird teilweise immer noch Java für Abrechnungen verwendet. Java ist nicht sicher! Darum wird es auch von keinem einzigen Browser mehr unterstützt.

Seit Ende 2015 steht fest, dass Java nicht mehr von den Browsern unterstützt wird. Die Praxen müssen deshalb auf den Internetexplorer 11 zurückgreifen.
Das sagt Microsoft dazu?

„In einem technischen Blogbeitrag klärt Chris Jackson, bei Microsoft verantwortlich für die Cybersicherheit, schonungslos über die Gefahren bei der Verwendung des Explorers auf.“ Jackson schreibt, dass der Internet Explorer technisch vollkommen veraltet sei. Und er beschreibt, dass Microsoft jahrelang keine Rücksicht auf Internet-Standards genommen habe. Wer heute eine neue Webseite erstellt und sie im Internet Explorer aufruft, der laufe Gefahr, so Jackson, dass sie mit 20 Jahre alten Implementierungen gerendert wird. Die Weiterentwicklung des Internet Explorers, Version 11 wurde 2015 beendet.

Also sowohl Java als auch der Internet Explorer sind nicht sicher!!!
Forderung 20: Wenn Sie die Digitalisierung einläuten wollen, dann schaffen Sie die Voraussetzungen. Alle Hersteller von Software PVS usw. aber auch alle KVen und KZVen sind verpflichtet, die Software auf den neuesten Stand zu bringen, dass Patentendaten nicht weiter gefährdet sind!

Etliche zigtausendfach verbreitete Praxisprogramme sind mit Uralt-Entwicklungsumgebungen erstellt, die teils wie VB 6 schon 2001 abgekündigt wurden, und trotzdem wurde in den beiden größten Praxissoftware Konzernen einfach weiter damit programmiert. Beispiele:

TurboMed im CGM Konzern mit ca. 13.000 Installationen verwendet VB 6 und VB-Skript
x.isynet im medatiXX Konzern mit ca. 10.000 Installationen verwendet VB 6
x.concept im medatiXX Konzern mit ca. 7000 Installationen verwendet Visual FoxPro

Wenn Probleme gefunden werden, wird also in diesem Falle Microsoft garantiert nicht mehr reagieren, denn die Entwicklungsumgebungen sind zeitlich schon lange aus dem erweiterten Microsoft Support rausgefallen.

Frage 26: Warum werden von Seiten der Bundesregierung solche Softwarevoraussetzungen nicht reglementiert? Wer haftet bei einem Datenverlust?

Die TI ist nicht schuld, der Anschluss an das Internet schon! Haften wird wahrscheinlich wieder der Praxisbetreiber!

Forderung 21: Wenn die Systeme mit Internet an die TI angeschlossen werden, dann müssen die PVS auch auf dem neuesten Stand und sicher sein. Seit fast 20 Jahren abgekündigte Entwicklungsumgebungen sind wahrscheinlich nicht mehr zulässig! Wer ein solches PVS einsetzt, sollte nicht mit am Internet hängen, sondern muss einen Reihenanschluss ohne SIS wählen. Um den Praxisbetrieb weiter aufrecht erhalten zu können ist die Methode der Netztrennung möglich ohne SIS. Das sollte durch die gematik und die KBV ebenfalls veröffentlicht werden!

Wir zwingen weltweit Menschen neue EDV Systeme anzuschaffen, weil Serverbetriebssysteme oder Betriebssysteme von Workstation aus dem Windows Support fallen. Bei solch wichtigen Systemen, in denen Patientendaten gehalten werden, ist uns das jedoch egal? So lange die Systeme nicht am Internet angeschlossen waren, war das auch vertretbar. Nun ist das eine Sicherheitsverletzung, welche nicht hinnehmbar ist.

Zahlreiche Praxen sind seit dem Anschluss an die TI gehacked worden.

Am 07.06.2019 habe ich mich deshalb an die Datenschutzbehörden gewendet.

> Hallo
> Ich muss mich leider erneut bei Ihnen melden. Die Lage wird immer dramatischer. Nach meinem Interview haben sich zahlreiche Ärzte und Systemadministratoren bei mir gemeldet.
> Die Meldungen sind äußerst besorgniserregend. Ärzte werden gegen ihren ausdrücklichen Willen falsch angeschlossen und genötigt, dies hinzunehmen. Unterschreiben die Ärzte nicht, dass die Installation ordnungsgemäß erfolgt ist, droht man ihnen mit weiteren Kosten bzw. dem Honorarabzug , da die TI ja nicht installiert wurde.
> Noch schlimmer sind 3 Meldungen von Systemadministratoren, welche mich erreicht haben. Hier zwei Beispiele:
>
> Sehr geehrter Herr Ernst,
> vielen Dank für Ihre Expertise, die ich mit großem Interesse gestern Abend … erlebt

habe.
Zu diesem Thema hätte auch ich einiges zu berichten:
Auch ich bin IT-ler, und seit Jahren an verschiedenen Systemen auch bei Ärzten um Stabilität und um Sicherheit bemüht.
Das, was Sie feststellen, ist noch nicht einmal die Spitze des Eisberges.
Vor einigen Wochen hatte ich darüber sogar mit der KV-Pfalz, den Datenschützern in MZ, Bonn und Berlin, und mit der „Beauftragten der Bundesregierung für die Belange der Patientinnen und Patienten Prof. Dr. Claudia Schmidtke" in Berlin besprochen / per Fax schriftlich zur Kenntnis gegeben.
Das Ergebnis ist wie in solchen Fällen immer „sehr übersichtlich".
Das, was Sie feststellen, kann ich als Dipl.- Ing., VDE, nur unterstreichen…..

Eine weitere Mail lautet:

Hallo Herr Ernst.
….. leiste meinen EDV Support im Rahmen des Ehrenamtes unentgeltlich.
Das bedeutet allerdings, dass ich auch in diesem Zusammenhang „unterschrieben" habe, (DSGVO) was mich von meiner Verantwortung freistellt.
Daher ist es mir nicht möglich Ärzte, denen ich helfe, in die Pfanne zu hauen. (Die wissen aber, was sie an mir haben)
Ein Supporter, Subcontrakter, aus dem Stuttgarter Raum, der Psychologen bedient, Telematik aufbaut, wollte kürzlich von uns verlangen, den Datenbestand einer psychologische Praxis voll aufs Netz zu legen…
Dagegen legte ich als dort verantwortlicher Sysop mein entschiedenstes Veto ein!
Wiederum Wochen vorher hatte man mich dort hin gerufen, weil das Sicherheitsteam der Telekom der Psychologin den Internetzugang gesperrt hatte, weil vom Anschluss aus Malware/Botware ausging. Sie solle einen Profi rufen, der sich um das Problem kümmert..
Als ich kam, hatte ich drei Tage Arbeit.
Ergebnis: 446 Trojanische Pferdchen verschiedenster Kategorien.
Kein Antivirus. Keine Firewall.
Trotz gefilterter VPN-Verbindung via GUS-Box gab das Systemhaus (Ergosoft) den Rat, man solle zum Zwecke des Supports einen AVM-Fritz-WLAN-Stick in den PC stecken, anmelden, und dann könnte das Systemhaus Fernwartung machen. (?!?)
Das allererste, was ich gemacht hatte, können Sie sicher raten: Ich hab diesen USB-Stick entfernt.
Viren und Trojaner wurden alle entfernt, und waren weg.
Ob, und wohin die sensiblen Daten, zum Teil die persönlichsten Dinge von Patientinnen und Patienten noch gegangen sind, weiß nur Gott…
Bis bei der Umstellung ein recht junger Mann mit Bart, aus Stuttgart, uns einen „parallelen" Anschluss mit dem Konnektor liefern wollte.
Wir hätten kein Internet auf dem Praxisrechner…
Das sei so üblich. Ich erklärte meine Anwesenheit, meine Bedenken, und meine Vorsicht.
Darauf meinte der Mann, er habe bisher 129 (!!!) paralleler Systeme genau so konfiguriert.
Die Praxisinhaberin war mit dabei, und ich stellte die Frage zwei Mal. Wir haben uns also nicht „verhört".
Überall würde das so laufen…

Ich wollte wissen, ob es nicht auch anders ginge.
Zögerlich meinte er, ja, in serieller Form.
Das hat er dann auch so umgesetzt.
Als Sysop habe ich die Verantwortung für die Datensicherheit…..
Diese Situation ist bei Leibe kein Einzelfall.
Das werden Sie verstehen.
Es gibt da einige Praxen, bei denen ich helfe.
Und überall gibt es einen gemeinsamen Hauptnenner.
Es ist das Markenzeichen unserer Politik, die uns Sicherheit vorgaukelt, wo keine Sicherheit ist.
Die Frage, die ich seit Monaten gebetsmühlenartig an Politik, Behörden und Verwaltung (KV) gegeben habe, war die:
Wie kann es denn sein, dass zum wiederholten Mal die Netzwerkumgebung des Bundestages, und der Bundesregierung gehackt wurden, wo doch dort „die Oberliga“ (Dipl.-Inf., Dr. – Inf.), spielt, und nicht nur „der dumme ……“
Immer wird nur abgewiegelt, und verharmlost.
Namen: BSI, Landes- / Bundesdatenschutzbeauftragte, KV-Pfalz, Kaufmännische Krankenkasse, Patientenbeauftragte der Bundesregierung.
Passiert ist nichts.
Eine mächtige Lobby!
Hut ab vor Ihrer Initiative.
Haben Sie eine „kugelsichere Weste“?

Weiter habe ich mit einem Systemadmin telefoniert, der mir berichtete, dass er selbst in einer Praxis ebenfalls einen mit hunderten Trojanern befallenen Rechner „platt gemacht hat“ auf Weisung des Arztes. Das System wurde komplett neu aufgesetzt, um zu verhindern, dass man jemals herausbekommen könnte, dass die Praxis gehackt wurde.

Bisher wird von allen Seiten immer so getan, als ob ich der einzige „Spinner“ bin, dem da was aufgefallen sei und das es sich um einen Einzelfall handle. Nun lese ich mehrfach Meldungen, dass es sehr wohl weitere Administratoren gibt, welche sich hilfesuchend auch an die Datenschutzbehörden gewendet haben sollen. Lügen die alle? Ich bitte um eine Bestätigung, ob es weitere Meldungen von anderen Administratoren gibt. Ich weiß nun auf jeden Fall ganz sicher, dass es sich nicht um Einzelfälle handelt, sondern, dass ein richtiger Anschluss ein Einzelfall ist.
Weiter geht also nicht mehr darum, dass Daten auf Grund der Fehler beim Anschluss an die TI potentiell abgefischt werden könnten, sondern das ist bereits mehrfach geschehen. Die Dunkelziffer schätze ich auf Grund der enormen Strafen und der unfreiwilligen aufgezwungenen unsicheren Anschlussmethode sehr hoch ein.
Die Ärzte sagen zu Recht: „Ich wollte das nicht, die Techniker schließen mich an, die Politik zwingt mich dazu und nun soll ich dafür haften und Strafen zahlen? Das sehe ich nicht ein, sollen die mir das doch erstmal beweisen, dass ich gehackt wurde, ich vernichte alle Beweise.“
Zur Aufklärung der Vorfälle, und damit auch zur Erfassung der Vorfälle, ist meiner Meinung nach eine Amnestie von Nöten, die Ärzte, welche unwissentlich in die Falle getappt sind, von einer Bestrafung frei stellen. Sonst werden wir nie das Ausmaß ermitteln können.

Ich bitte also darum, diese Straffreiheit für die Ärzte für einen begrenzten Zeitraum zu gewähren, damit wir Ärzte dazu überreden können, die Sachen offen zuzugeben und eventuell auch ermitteln können, wie der Hackerangriff ursächlich geführt wurde. Das ist wirklich wichtig.
Ich bitte um eine schnelle Antwort.

Frage 27: Ich möchte meine Bitte bzw. Frage an die Bundesregierung weiter geben. Ist es möglich eine zeitlich begrenze Amnestie auszurufen um die Fälle aufzuklären? Wenn die Beweise vernichtet werden aus Angst vor den Strafen, dann werden wir das Problem nie in den Griff bekommen, weil wir ja noch nicht einmal wissen, wie viele Daten täglich abgezogen werden.

Ein weiterer wesentlicher Punkt ist die fehlende DSFA.
Kein PKW darf ohne Straßenzulassung fahren! Aber bei den Daten von 80.000.000 Menschen verzichten wir auf die DSFA? Das kann doch nicht wahr sein!

Frage 28: Von der IT sowie den Ärzten wird immer Vertrauen verlangt. Dieses wird ständig als Vorschuss gewährt und wir stellen im Nachhinein fest, dass dieses Vertrauen falsch war. Wann können wir endlich mit einer DSFA rechnen?

Frage 29: Wann werden PEN Tests durchgeführt und können die Ergebnisse von unabhängigen Experten untersucht werden?

Führende Experten in hohen Gremien haben mit mir gesprochen und mir versichert, dass bereits die Einordnung in die Schutzprofile fehlerhaft vorgenommen wurde!

Frage 30: Es gibt unterschiedliche Aussagen zu den Common Criteria Schutzprofil und Sicherheitsniveau für alle Konnektoen. Ich möchte wissen, welche Sicherheit alle Konnektoren bieten. Dabei interessieren mich sowohl das Evaluation Assurance Level als auch das Sicherheitsniveau die VAN. Ein Konnektor soll nicht BSI zertifiziert sein ist das richtig? Welche Sicherheit bietet dieser und wer hat das dann zertifiziert?

Wir können sagen, dass schon bei der derzeitigen Zertifizierung wesentliche Angriffsszenarien in den Schutzprofilen nicht behandelt wurden: Zum einen die Angriffe gegen die Praxis aus der TI heraus, zum anderen Angriffe über die Fernwartungsfunktion der Konnektoren. 2016 hat eine zwei Jahre ignorierte Sicherheitslücke im Fernwartungsprotokoll (TR-069) bei Routern zum Ausfall von fast 1.000.000 Anschlüssen geführt. Wir sollten diesen Fehler nicht wiederholen.
Stellen Sie sich vor, z.B. die Fern-Update Funktion der Konnektoren würde wie in 2016 die Übernahme der Speedport Router, genutzt werden, um einen gezielten Angriff auf das Gesundheitswesen zu führen. Terroristen könnten so alle Ärzte Deutschlandweit mit einem gezielten Angriff außer Betrieb setzten. Das ist durchaus ein reales Szenario. Sind auch noch Apotheken und Krankenhäuser sowie alle Pflegeeinrichtungen angeschlossen würde das zum totalen Zusammenbruch des gesamten Gesundheitswesens führen! Hier müss die höchste Sicherheit Anwendung finden.

Frage 31: Ist es richtig, dass diese beiden Angriffsszenarien nicht behandelt wurden und auch nicht behandelt werden, weil man die Netze der TI und KV sowie den Konnektor für absolut

sicher bis in alle Ewigkeit hält?

Das BSI hat mit auf Anfrage, ob das BSI das wirklich so zertifiziert hat, mitgeteit:

> „Das BSI hat einzelne Komponenten der Telematikinfrastruktur (TI), wie z.B. Konnektoren, Kartenterminals, eGK usw., nach Common Criteria (CC) bzw. nach Technischer Richtlinie (TR) zertifiziert.
> **Es gibt jedoch keine Zertifizierung für die Telematikinfrastruktur insgesamt und auch keine gesonderte konkrete BSI-Zertifizierung für die Dienstleister vor Ort (DVO). Daher ist Ihre Aussage in dieser Hinsicht völlig korrekt.**“

Frage 32: Ist es für die Bundesregierung richtig, dass es keine Zertifizierung für die TI gibt? Halten Sies es für ausreichend, wenn einzelne Komponenten zertifiziert wurden?

Frage 33: Welche Komponenten der gesamten TI sind überhaupt vom BSI getestet und zertifiziert worden? Ich bitte um eine Aufstellung der Komponenten der TI mit den jeweiligen Anforderungen und Status hinsichtlich Zertifizierung und Zulassung .

Eine Kette ist nur so stabil, wie das schwächste Glied. Eine Kette aus dem härtesten Stahl hat keinen Sinn, wenn ein Kettenglied aus Papier ist.

Hier eine Zusammenfassung von Prof. Dr. Hartmut Pohl zum Zulassungsprozess von Hardware und Software:

> Digitalisierung ist ein in der Bevölkerung weitverbreitetes gesellschaftliches Ziel – insbesondere bei Technik-Affinen. Die – meist im Internet oder angeschlossenen Netzen – verarbeiteten Daten werden dabei gegen Veränderung (Integrität) und Einsichtnahme (Vertraulichkeit) geschützt. Unverzichtbar ist auch, dass die Daten zeitnah verarbeitet werden können (Verfügbarkeit), was angesichts der Vielzahl der eingesetzten Hardware- und Software-Komponenten aufwändige Maßnahmen erfordert. Diese Notwendigkeit zeigt auch die Vielzahl der Ausfälle und der kriminellen Fälle von Datendiebstahl weltweit. Zukünftig stärker im Blickpunkt werden allerdings die Fälle von Datenmanipulation (Sabotage) stehen, die bei Medizingeräten und Patientenakten erhebliche – auch **lebenswichtige** – Auswirkungen haben können.
>
> **Bewertung der TI-Situation auf der Grundlage des Stands der Technik**
>
> 1. Sicherheit ist kein absoluter Begriff, **Sicherheit ist nicht zu 100% erreichbar** – auch und erst recht nicht in der Informationstechnik. Eine Aussage wie „die Telematik-Infrastruktur ist sicher“ ist daher nicht sachgerecht, weil sie technisch nicht erreichbare 100% Sicherheit suggeriert.
>   Vielmehr muss das erreichte Sicherheitsniveau beschrieben werden. Benutzt wird daher häufig eben nicht der Begriff Sicherheit als vielmehr der Begriff **Vertrauenswürdigkeit**[11] als Nachweis durchgeführter Sicherheitsprüfungen.
> 2. Bei der Verarbeitung von Daten – auch von Gesundheitsdaten – hat eine **Bewertung** der Daten zu erfolgen: Risikoanalyse und Requirements für Security Maßnahmen (Datenschutz).

[11] Aus Praktikabilitätsgründen wird hier gleichwohl der umgangssprachliche Begriff Sicherheit benutzt.

3. Ein System kann nur dann als sicher bezeichnet werden, wenn alle Komponenten sicherheitsgeprüft wurden. Dies gilt für alle Software-Komponenten und die eingesetzte **Hardware** (Prozessoren, Chips, Router, Gateways etc.). Beispielsweise muss unverzichtbar bei der Komponente TI-Konnektor die eingesetzte Hardware gleichermaßen geprüft werden. So erlaubt z.B. die in fast jedem PC installierte ‚Intel Management Engine' ein nicht-erkennbares real-time Mitlesen und Verändern aller verarbeiteten Daten durch Unberechtigte; andere Hersteller bauen funktional vergleichbare Komponenten ein: Die eingesetzten Komponenten mit Ihrer Architektur sind jedenfalls offenzulegen, um das Sicherheitsniveau bewerten zu können.

4. Die Sicherheitsprüfungen müssen sich naturgemäß auch auf die Kommunikation zwischen Komponenten und Teilkomponenten sowie zur TI erstrecken.

5. Alle Security Test müssen nach einem anerkannten **Stand der Technik** auf der Basis des international anerkannten Standards ISO 27034 durchgeführt werden.

6. Sicherheit bedeutet nicht nur den Einbau von Sicherheitsfunktionen wie z.B. Firewalls sondern auch die Prüfung, ob diese selbst sicher sind und nicht etwa manipulierbar (Qualität der Sicherheit); so gilt für Verschlüsselungsprogramme nicht nur die Überprüfung des mathematischen Algorithmus sondern auch der **Implementierung**, der Programme.

7. Sicherheitsprüfungen müssen sich also auf die vollständigen Ebenen von **Software, Firmware, Microcode und Apps** erstrecken.

8. Sicherheitsgeprüfte Systeme müssen nach Änderungen sowie mindestens 3-monatlich und einer vollständigen **Wiederholungsprüfung** unterzogen werden.

9. Auch die **Installation** der Komponenten muss kontrolliert werden.

Stand der Technik der Entwicklung sicherer Software und Geräte

Um sichere Software zu generieren, reicht es aus, die möglichen Angriffspunkte zu eliminieren – also die Sicherheitslücken zu identifizieren und zu beheben. Um Sicherheitslücken zu vermeiden, ist ein ganzheitlicher Prozess erforderlich. Dieser sichert nicht nur medizinische Anwendungen ab, sondern alle Kommunikationswege der Geräte und Software. Um dies zu erreichen muss von Grund auf sicher entwickelt werden. Stand des Security Testing ist der Einsatz eines Security Testing Prozesses gem. ISO 27034 [1] mit 6 Methoden über den gesamten Life Cycle der Software-Entwicklung:

- **Security Requirements Analysis:** Software wird auf der Grundlage funktionaler Anforderungen erstellt – dabei dürfen Sicherheitsaspekte nicht vernachlässigt werden: Die Requirements entsprechen dem Wert der verarbeiteten Daten. Der Wert muss festgelegt werden.
- **Threat Modeling des Security Designs:** Da etwa die Hälfte aller Sicherheitslücken in Software auf Designfehler zurückzuführen sind, müssen Sicherheitsmaßnahmen während der Designphase berücksichtigt werden. In dieser Phase sind die Fehlerbehebungskosten im Vergleich zur Implementierungsphase vergleichsweise gering. Threat Modeling hilft dabei, Bedrohungen zu identifizieren – unabhängig von der Komplexität der Architektur. Die Methode unterstützt die Entwicklung eines vertrauenswürdigen Security Designs. Dazu wird systematisch und methodisch eine vollständige Bedrohungsmodellierung durchgeführt – mit dem Ziel, die Auswirkungen der erkannten Bedrohungen zu reduzieren oder sogar zu

eliminieren. Alternative Architekturen – wie z.B. zentrale/dezentrale Speicherung von Daten – werden untersucht.

- **Conformance Testing:** Jedes Produkt hat spezielle Security Requirements. Es wird überprüft, ob ein Produkt festgelegte Security Requirements korrekt implementiert. Conformance Testing fällt damit unter die Klasse der nicht funktionalen Tests. Der Fokus liegt insbesondere auf der Sicherheit eines Produkts, eines Systems, eines Netzwerks o.ä. Conformance allein reicht jedoch noch lange nicht aus, um Software abzusichern. Daher sollte ein Produkt unverzichtbar den weiteren Tests unterzogen werden.
- **Static Source Code Analysis:** Ab der Implementierungsphase wird die Korrektheit des Quellcodes der Zielsoftware mit formalen Methoden auf Einhaltung syntaktischer Programmierkonventionen der Programmiersprache sowie auf Einhaltung der Programmierrichtlinien überprüft. Dieses Verfahren ist vergleichbar mit einem Parser, der eine lexikalische, syntaktische und semantische Analyse des Programmcodes durchführt.
  Aufgrund lexikalischer Regeln der verwendeten Programmiersprache und den semantischen Zugehörigkeiten benötigen Fehler im Allgemeinen einen manuellen Audit, um false positives auszuschließen und entsprechende Behebungsstrategien zu entwerfen. Die Qualität und Quantität des Analyse-Resultats hängt somit maßgeblich von der Auswahl geeigneter Tools ab.
- **Penetration Testing:** Dabei werden kontrollierte Angriffe durchgeführt und den Methoden der Angreifer eingesetzt: Es werden systematisch und methodisch gezielt Sicherheitslücken identifiziert. Dabei werden jedoch nicht nur die ohnehin schon bekannten und veröffentlichten Sicherheitslücken erkannt, sondern insbesondere die bisher nicht-bekannten Zero-Day-Vulnerabilities identifiziert. Die Komplexität der Systeme ist dabei unerheblich.
- **Dynamic Analysis – Fuzzing:** Manuelle Überprüfungen auf sicherheitskritische Fehler und Sicherheitslücken von IT-basierten Target Systems sind angesichts des meist großen Binärcode-Umfangs nicht praktikabel. Der Einsatz herkömmlicher Verfahren zur Behebung funktionaler Fehler und insbesondere nicht erkannter Sicherheitslücken (Vulnerabilities) ist sehr kostenaufwändig – viele Vulnerabilities werden daher erst nach der Auslieferung der Software an Kunden – z.T. auch von Dritten erkannt.
  Sicherheitslücken in Soft- und Hardware/Firmware und Microcode (!) können kostengünstig identifiziert werden. Fuzzing ist auf jede Art Software anwendbar – angefangen von Protokollen bis hin zu Individualsoftware, Standardsoftware wie ERP, CRM, Datenbanksysteme und auch auf unternehmensspezifische Anpassungen an Standardsoftware (Customizing), Web-Applications, Betriebssysteme und auch in Hardware und Embedded Systems.

Frage 34: Ist es richtig, dass dieser absolut übliche Verfahrensprozess bei der Entwicklung der TI nicht eingehalten wurde? Wenn ja, warum?

Zu den Angriffen aus der TI heraus habe ich mir ebenfalls Gedanken gemacht.
Denken wir mal an Locky, der 2016 das gesamte „sichere“ Bahnnetz befallen hat. Nur ein Fehler hat dazu geführt, dass das gesamte Netz verschlüsselt wurde. Ich halte solch ein Szenario auch für die TI für durchaus möglich. Da alle Praxen Tag und Nacht an der TI hängen wären im Nu alle Praxen verschlüsselt und nicht mehr arbeitsfähig. Später kämen auch alle Krankenhäuser, Pflegeeinrichtungen und Apotheken dazu. Wir müssen uns immer vor Augen halten, dass bei der derzeitigen Konfiguration der Konnektor die höchste Vertrauensstufe LAN hat. Das bedeutet, er genießt das volle Vertrauen aller im Netzwerk

befindlichen Geräte. Alle von dort kommenden Informationen werden ungeprüft verarbeitet. Auch ein unbemerktes systematisches ausspionieren der Praxis durch Kriminelle aber auch durch zum Beispiel korrupte Mitarbeiter der KV oder bei arvato ist so vollkommen problemlos möglich. Denken wir an die Steuer CDs, die wir Deutschen so gern gekauft haben. Das waren gestohlene Daten von Menschen, die dafür viel Geld bekommen haben. Was glauben Sie, was die Gesundheitsdaten der Deutschen wert sind? Ein Vermögen. Übrigens geben wir diese Daten freiwillig dem Konzern arvato/Bertelsmann, welcher ein Medienkonzern ist, zu der mit der AZ Direkt ein großer Adresshändler ist, und die Arvato-Tochter Infoscore bietet Inkassoservice sowie Wirtschafts- und Bonitätsauskünfte an. Die verdienen mit Daten über Menschen eine Menge Geld. Die bekommen nun die Hoheit über alle Patientendaten? Die Macht über diese Daten macht arvato zu einem übermächtigen Konzern. Diese Daten gehören nicht in die Hände von privaten Firmen!

Erst wenn all diese Dinge wirklich geklärt sind und man immer noch solch ein Netz haben möchte, sollte eine Inbetriebnahme erfolgen. Dann aber richtig mit gesetzlichen Regelungen was die Haftung betrifft und strengen Regeln, wie draußen angeschlossen wird. Und das muss kontrolliert werden.

Meiner Meinung nach gehört die Telematik in jeder Praxis wegen der geschilderten Angriffsmöglichkeiten, aber auch wegen des Layer2 Tunnels, in eine DMZ. Als Demilitarisierte Zone bezeichnet ein extra an der Firewall angeschlossenes Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Geräte. Das bedeutet, ich kann exakt genau steuern, welche Informationen ausgetauscht werden dürfen und wie diese Informationen auszusehen haben. Eine Verbreitung von Malware über die TI und aus der TI in das Praxisnetz wird dadurch weitestgehend unterbunden.

Frage: Diese Frage möchte ich provokativ stellen. Wie viele Patientenakten müssen wir der Bundesregierung vorlegen, damit die Bundesregierung endlich etwas unternimmt?

Auf diese Frage können Sie natürlich nicht antworten, darum ist sie auch nicht blau. Aber glauben Sie mir, es ist derzeit problemlos möglich an Patientendaten zu kommen! Auch Hacker wissen das und haben bereits reagiert. Wir wissen von bereits zwei gezielten Angriffswellen gegen Ärzte und Apotheken. (z.B. TK Virus)

Jeder Mensch macht Fehler, das ist mir bewusst. Daher ist es durchaus plausibel, dass es auch mal zu einem fehlerhaften Anschluss kommt. Wenn jedoch jeder Anschluss fehlerhaft ist, dann drängt sich mir die Vermutung auf, dass eine gewisse Absicht dahintersteckt. Selbst bei vorwiegend unfähigem Personal müsste eine korrekte Installation einmal vorzufinden sein. Ich habe noch nicht eine Installation gesehen, die einer BSI Zertifizierung standgehalten hätte.

Auf diese Art kann bei jedem Datenverlust schon beim ersten Blick auf die Installation sofort offensichtlich gezeigt werden, dass der Aufbau nicht der Zertifizierung entspricht. Damit werden keine weiteren Untersuchungen durchgeführt und die Haftungsfrage ist sehr schnell geklärt. Der Praxisbetreiber haftet!

Frage 35: Wie erklärt sich die Bundesregierung die unbestreitbare Tatsache, dass jeder Anschluss, welchen ich bisher gesehen habe, nicht dem zertifizierten Aufbau entspricht?

Frage 36: Wie gedenkt die Bundesregierung ein Qualitätsmanagement einzuführen, damit wenigstens jede zigste Praxis kontrolliert wird?

Was auf der Strecke bleibt, sind die fundamentalsten Grundrechte eines jeden Menschen in Deutschland!
Ich bin der Meinung, dass wir es uns als Land gar nicht leisten können, alle Ärzte zu kriminalisieren und in ungeklärte Haftungsfragen zu verstricken! Wir haben jetzt bereits einen Ärztemangel. Einige Ärzte hätten noch einige Jahre praktiziert, sehen aber in der TI Pflicht keinen Nutzen und unnötige Risiken und haben aufgehört oder denken offen und laut darüber nach aufzuhören. Steigen die Strafen, hören sie sicher auf. An die TI anschließen werden sie sich nicht lassen, das Risiko ist zu groß. Technische EDV Kenntnisse fehlen ihnen. Andere Ärzte geben ihre Kassenärztliche Zulassung zurück und behandeln nur noch Privatpatienten. (entsprechende Veröffentlichungen existieren bereits https://www.aend.de/article/197809) Die deshalb steigenden Wartezeiten für Kassenpatienten sollen dann mit Gesetzen wie dem Terminservice- und Versorgungsgesetz – TSVG in den Griff gebracht werden, stürzen Ärzte aber in noch kritischere Situationen, da wichtige Behandlungsstunden verloren gehen! Erste Ärzte kündigen bereits Klagen an. (https://www.medical-tribune.de/meinung-und-dialog/artikel/vertragsaerzte-und-psychotherapeuten-protestieren-gegen-das-tsvg/) Das alles hilft unserem Land nicht weiter! Hat Herr Spahn schon mal darüber nach gedacht? Er macht statt dessen Vorschläge wie: *"Wenn von einer Million Pflegekräften 100.000 nur drei, vier Stunden mehr pro Woche arbeiten würden, wäre schon viel gewonnen"* Vielleicht sollten die Ärzte auch ein wenig mehr arbeiten. Ich kann ihnen versichern, dass viele, die im Gesundheitswesen und in der Pflege arbeiten, dies selbst mit privatem Engagement bis an ihre Grenzen tun! Solche Vorschläge sind ein Schlag ins Gesicht für all die.

Frage 37: Ist die Bundesregierung bereit, mit mir zusammen in einer beliebigen Stadt Kontrollbesuche in beliebigen Praxen durchzuführen um sich die Probleme anzusehen und zu handeln?

Heute erreichte mich eine Mail aus Ihrem Haus an eine besorgte Ärztin (3 Monate Bearbeitungszeit finde ich bei solch wichtigen Problemen zu lang!).

> **Von:** Buergerservice BMG <Buergerservice.BMG@bmg.bund.de>
> **Datum:** 6. August 2019 um 10:24:39 MESZ
>
> **Betreff: Ihre E-Mail vom 6. Mai 2019 an das Bundesministerium für Gesundheit;**
>
> *Sehr geehrt.……..,*
>
> *vielen Dank für Ihr Schreiben vom 6. Mai 2019, in der Sie die Gefährdung der Patientendaten durch den Parallelbetrieb der Hardware zur TI ansprechen und sich auf die Datensicherheit und den Datenschutz der TI beziehen.*

Ich verweise auf die Stellungahme der gematik (https://www.gematik.de/news/news/stellungnahme-zu-den-musterschreiben-von-medi-geno-bezueglich-des-ti-konnektors-1/), die Sie nachfolgend finden:

Grundsätzliche Verantwortung der gematik

Die Fachanwendungen, Komponenten und Dienste der TI werden entsprechend den gesetzlichen Vorgaben – dies umfasst auch die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) – spezifiziert. Die Komponenten und Dienste der TI sowie deren Anbieter werden auf Grundlage der Spezifikationen von der gematik geprüft und zugelassen sowie anschließend der sichere und datenschutzgerechte Betrieb der TI von der gematik überwacht.

An dieser Stelle möchte ich das erste Mal eingreifen. Es nutzt nichts, wenn etwas spezifiziert wird, aber die Spezifikationen nicht eingehalten werden! Der SIS erfüllt nicht die Schutzfunktion, die er gemäß Grundschutz erfüllen müsste! Das haben wir hier dargelegt und kann gern jeder Zeit geprüft werden. (der SIS ist ein Dienst) Ich habe keine Ahnung, wie die Anbieter geprüft werden, aber nach dem Sie dieses Papier hier gelesen haben müssen Sie doch zugeben, dass hier nicht so gearbeitet wird, dass die DSGVO erfüllt wird! Die Aussage: *„datenschutzgerechte Betrieb der TI von der gematik überwacht“* ist einfach nicht wahr! Die gematik har klar gestellt, dass sie nicht den Aufbau und die Praxen kontrolliert. Und das nie tun wird. Sie zieht sich auf den Standpunkt zurück, bei der Zertifizierung sei alles richtig gemacht worden. Das müsse reichen! Für den Rest sei sie nicht verantwortlich! Sie weigert sich sogar zu ermitteln, wie viele Praxen parallel ohne Firewall angeschlossen wurden. Von einer Überwachung kann keine Rede sein. Wie hätte es sonst passieren können, das mehr als 100.000 Praxen angeschlossen wurden und ich hier behaupte, dass die Mehrzahl (ich würde sogar sagen fast alle) der Praxen nicht wie zertifiziert also nicht sicher angeschlossen wurden.

Installation und Betrieb des Konnektors

Die Ausstattung bzw. der Anschluss der medizinischen Einrichtungen an die TI liegen außerhalb des Verantwortungsbereiches der gematik und erfolgen durch die jeweiligen IT-Dienstleister der Leistungserbringer. Dies betrifft insbesondere den Konnektor.

Die gematik hat vorsorglich Kontakt zu allen relevanten Anbietern von Zugangsdiensten zur TI aufgenommen, weil nur diese über die Dienstleister-vor-Ort („DVO“)/AIS-Dienstleister auf eine sichere Installation der Konnektoren hinwirken können.

Die gematik hat erst reagiert, nach dem der Bundesdatenschutz sich der Angelegenheit angenommen hat. Der war bei mir zu Besuch und hat sich Ärzte angesehen. Auf meine Meldung hat die gematik nicht reagiert. Wenn es eine Kontrolle gegeben hätte, dann wäre meine Meldung nicht nötig gewesen. Auch heute wird noch falsch installiert. Es hat sich nichts geändert. Es wird sich erst etwas ändern, wenn Sie die DvOs und die Betreiber in die Haftung nehmen!

Die gematik unterstützt die DVO/AIS-Dienstleister beispielsweise durch Hinweise und Dokumente in ihrem Fachportal: https://fachportal.gematik.de/erste-schritte/hinweise-fuer-dienstleister-dvo/

Eine sach- und fachgerechte Installation der Anbindung an die TI durch den DVO/AIS-Dienstleister setzt daher grundsätzlich die Einhaltung der Hinweise und Dokumente des Bundesamtes für Sicherheit in der Informationstechnik und der gematik voraus.

Was sollen uns diese „sinnlosen“ Sätze sagen? Den DvOs sind die Unterlagen egal! Sie werden pauschal bezahlt. Sie installieren ja sogar gegen den Willen der Ärzte falsch! Dazu habe ich ja nun diese Fragen gestellt. Ohne eine Haftung der Unternehmen wird sich nichts daran ändern!

> *Schutzfunktion des Konnektors*
>
> *Der Konnektor kann die Systeme der Leistungserbringer, die daran angeschlossen sind, vor Angriffen aus dem Internet zusätzlich schützen, sofern die Konfiguration „seriell“ gewählt wird. Sehr wichtig ist aber, dass mit der Installation eines Konnektors keinesfalls die in den medizinischen Einrichtungen bereits umgesetzten Sicherheitsmaßnahmen für den IT-Praxisbetrieb obsolet werden, so dass z. B. Virenschutz oder die Netzabsicherung nach wie vor unerlässlich sind.*

Ich habe keine Ahnung, ob der Konnektor vor Angriffen schützen könnte. Ich kann nur sagen, das er es auch bei einer seriellen Anbindung nicht ausreichend tut, sobald der SIS geschaltet ist. Ob das Problem beim Konnektor liegt oder nur am SIS ist mir jetzt mal egal. Es ist mir auch egal, ob der Konnektor das können sollte. Ich fordere nur eine ehrliche und richtige Aufklärung der Ärzte! Wenn Sie den Ärzten sagen, dass die immer eine Firewall benötigen, da der SIS nicht ausreichend schützt, dann ist das für mich in Ordnung! Mehr will ich doch gar nicht, nur absolute Ehrlichkeit!

> *Haftung bei Verwendung des Konnektors*
>
> *Die gematik legt funktionale Vorgaben für den Produkttyp „Konnektor“ fest, ist selbst aber weder Anbieter, Hersteller oder Betreiber des Konnektors. Betreiber des Konnektors im Sinne der Ausübung der tatsächlichen Sachherrschaft und bestimmungsgemäßen Nutzung ist vielmehr die jeweilige Leistungserbringerorganisation, sprich „die Praxis“.*
>
> *Insofern ist zu jeglichen auf Basis der aktuellen MEDI GENO-Musterschreiben gewünschten Bestätigungen über den Ausschluss einer Haftung und/oder eines Mitverschuldens von Leistungserbringern für aus der bzw. über die TI erfolgende Angriffe und daraus resultierende Folgen zu bemerken, dass die gematik uneingeschränkt zu der grundsätzlichen Einschätzung hinsichtlich des Ausscheidens einer Haftung eines Leistungserbringers* ***im Falle der bestimmungs- und anforderungskonformen Verwendung und Aufstellung zugelassener TI-Komponenten steht*** *(siehe unser Informationsblatt Datenschutz und Haftung in der Telematikinfrastruktur).*

Sie haben schon mitbekommen, dass Sie die Haftung einschränken auf: „***im Falle der bestimmungs- und anforderungskonformen Verwendung und Aufstellung zugelassener TI-Komponenten steht“*** Da kein Konnektor den ich bisher gesehen habe den „***bestimmungs- und anforderungskonformen Verwendung und Aufstellung zugelassener TI-Komponenten“*** entspricht, versprechen Sie nichts als Luft! Geanau das ist ja das Problem! Dann kann ich Ihnen auch versprechen ein Schloss zu schenken, wenn sie aus eigener Kraft ohne Hilfe einen Rundflug über dem Ministerium machen. Es ist eine ernst gemeinte aber vollkommen leere Versprechung!
An dieser Stelle Bitte ich Sie, schaffen Sie endlich die juristischen Voraussetzungen! Haftung für die aufbauenden Unternehmen oder die gematik. Öffentliche Meinungsbekundungen ohne Gesetze sind eben nur Meinungsbekundungen. Richter haben sich an Gesetze zu halten! Diese gesetzlichen Regelungen fehlen immer noch! Das ist ja auch Bestandteil der Forderungen!

> *Einer über diese generelle Beurteilung hinausgehenden Würdigung der Sach- und Rechtslage im individuellen Einzelfall steht jedoch zum einen entgegen, dass die gematik die individuellen technischen und organisatorischen Gegebenheiten in den einzelnen Leistungserbringerpraxen*

nicht aus eigener Kenntnis heraus bewerten kann und dass zum anderen diesbezügliche Wertungen der gematik auch keinerlei Bindungswirkung gegenüber dem im einzelnen Streitfall mit einer konkreten Haftungsfrage befassten Gericht entfalten würde.

Datenschutz-Folgenabschätzung

Von der gematik werden im Rahmen der Spezifikation von Anwendungen der elektronischen Gesundheitskarte und der Produkte der TI auch die Risiken für die Rechte und Freiheiten natürlicher Personen in den Datenschutz- und Sicherheitskonzepten betrachtet und hierbei Überprüfungen, die in Art und Umfang im Wesentlichen einer Datenschutz-Folgenabschätzung mit den gesetzlich geforderten Inhalten entsprechen, durchgeführt und dokumentiert.

Es erscheint also legitim, dass sich Leistungserbringer bei ihrer eigenen Datenschutz-Folgenabschätzung für die Verarbeitungsprozesse im Konnektor auf die Analyse der gematik stützen. Zu diesem Zweck bereitet die gematik eine Mustervorlage für die Erstellung einer Datenschutz-Folgenabschätzung zur Verwendung durch die Leistungserbringer vor, in welcher die relevanten technischen Informationen und Beurteilungen enthalten sind.

Zu berücksichtigen ist auch, dass gemäß Erwägungsgrund 91 der DSGVO eine Datenschutz-Folgenabschätzung zwar insbesondere bei umfangreichen Verarbeitungsvorgängen erstellt werden sollte, nach Satz 4 des Erwägungsgrundes die Verarbeitung personenbezogener Daten jedoch dann nicht als umfangreich gilt, wenn sie Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen solle eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein. Diese Erwägung dürfte aus Sicht der gematik trotz oder gerade wegen der Verwendung des Konnektors einschlägig bleiben, da, wie vorstehend dargelegt, seitens der gematik sowohl bei der Spezifikation und Zulassung des Produkttyps „Konnektor“ als auch bei der Überwachung des sicheren und datenschutzgerechten Betriebs höchste Standards und intensive Abstimmungen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Tragen kommen.

An dieser Stelle möchte ich den Bundesdatenschutzbeauftrgten zitieren.
Der Bundesdatenschutzbeauftragte hat in seinem Tätigkeitsbericht (Seite 59) klar gemacht, wie er die gesetzliche Lage sieht, und der sollte es wissen und seinem Wort möchte ich an der Stelle mehr Glauben schenken. So ist dort zu lesen:
„Nach dem Anwendungsbeginn der DSGVO im Mai 2018 stellte sich mit Nachdruck die Frage, wer eigentlich Verantwortlicher für die Telematik-Infrastruktur (TI) ist und damit eine Datenschutz-Folgenabschätzung (DSFA) vorzulegen hat (vgl. hierzu auch unter Nr. 15.2.3). ***Viele Arztpraxen sind ihrer gesetzlichen Verpflichtung zur Erstellung einer DSFA nachgekommen.*** *Sie haben dabei allerdings nicht an der Schwelle ihrer Praxisräume Halt gemacht, sondern vielmehr auch die TI in ihre Betrachtungen mit einbezogen. Die gesetzlich vorgeschriebene DSFA der Arztpraxis ergab dann,* ***dass ein Anschluss an die TI nicht vertretbar sei.*** *Viele Ärzte haben sich des-halb an mich gewandt. Die Frage, wer der datenschutzrechtliche Verantwortliche im Sinne der DSGVO für die TI ist, konnte bis zum Redaktionsschluss noch nicht endgültig geklärt werden.“*

Das bedeutet für mich, j**eder Arzt hat eine gesetzliche Verpflichtung eine DSFA zu erstellen.** Dem ist nichts hinzuzufügen! Wem sollen wir bei dem Meinungs-Chaos überhaupt noch was glauben? Schaffen Sie endlich ordentliche Richtlinien, welche die Patientendaten

und die Ärzte schützen! Ohne DSFA wüssten wir noch nicht einmal von den Installationsproblemen! Was machen Praxen mit mehreren Ärzten ohne DSFA? Das sind doch alles nur Ausreden! Die DSFA der TI ist zu erbringen!

Worte an Herrn Span persönlich:

1. Bevor Sie den nächsten Schritt machen, bringen Sie bitte erst einmal das Chaos in Ordnung, was durch Druck aus Ihrem Ministerium und mangelnde Sorgfalt bei der Umsetzung entstanden ist! Da das BGM auch Eigentümer der gematik ist, die für die Umsetzung verantwortlich ist, fällt das in Ihre Verantwortung! Der Mensch und die Menschenrechte sollten das höchste Gut sein und kein Geld und Fortschritt dürfen den Menschen herabsetzten.
2. Ich habe gehört, Sie sind homosexuell. Heute dürfen Sie sich offen dazu bekennen ohne etwas befürchten zu müssen, und das ist gut so. Das muss aber nicht so bleiben! Schauen Sie mal in die Geschichte! Und ich möchte bewusst in Deutschland bleiben. In der Weimarer Republik durften homosexuelle Menschen auch ohne Bestrafung relativ frei agieren. Es wurden jedoch so genannte „rosa Listen“ geführt. Als die Nazis an die Macht kamen, haben die die Listen genutzt, um all diese Menschen in KZs zu verschleppen und zu ermorden. Kommen wir zum hier und jetzt. Was ist, wenn über einen homosexuellen Menschen, auf Grund der schlampig angeschlossenen TI in einer Praxis, Daten im Internet öffentlich werden, während dieser sich in einem Land befindet, in dem Homosexualität verboten ist. Ja auch das gibt es heute noch! Der würde im völligen Einklang mit den dort herrschenden Gesetzen hingerichtet werden! Finden Sie das richtig? Schauen Sie sich um. Den Rechtsruck durch Europa und den Rest der Welt kann man nicht übersehen. In einem Bundesstaat der USA steht seit Anfang des Jahres die Abtreibung unter 99 Jahren Gefängnis. Weitere Bundesstaaten wollen nachziehen. Wer sagt uns, dass die Daten, welche Sie da fleißig sammeln, selbst wenn sie vor Hackern sicher blieben, was ich bestreite, nicht irgendwann von Anderen gegen uns Menschen verwendet werden?
   Was ist mit z.B. jungen Musliminnen, welche von Ihrer Ärztin Kontrazeptiva verschrieben bekommen. Wenn die Eltern das in der Gesundheitsakte lesen ist die Verschleppung in die Heimat noch das Humanste, was denen droht. Haben Sie schon mal von Ehrenmorden gehört? Das gibt es wirklich, auch in Deutschland!
   Was ist mit Jugendlichen, welche mit Ihren Eltern ein Problem haben. Wie sollen die sich bei einem Psychologen offen, wenn die Eltern Zugriff auf die Akte haben? Den Jugendlichen kann nicht mehr geholfen werden.
   Das sind nur ein paar Beispiele. Rufen Sie mich an, sie können mich immer erreichen, ich habe noch viel mehr Beispiele, diese schienen mir aber gerade passend.
   Eine grundlegende ethische und moralische Debatte muss unbedingt geführt werden!
3. Wenn die Ärzte nach „Volkes Willen“ angeschlossen werden, müssen unabhängige Whitehackintests zugelassen werden! Den Vertrauensvorschuss, den wir Ihnen alle entgegen gebracht haben, haben Sie verspielt. Lesen Sie das Dokument, dann wissen Sie warum. Lassen Sie unabhängige Tests zu und Loben Sie ein Bug-Bounty-Programm aus, nur so bekommen wir ein gewisses Maß an Sicherheit hin!
4. Bis heute hat die gematik keine Risikofolgeabschätzung vorgelegt trotz mehrfacher Aufforderung seit Jahren. Auch der Bundestatenschutzbeauftragte hat diese eingefordert! Meiner Meinung nach ist das bereits ein Verstoß gegen die DSGVO! Das ist wie das Fahren eines Autos ohne Zulassung. Die Ärzte tragen derzeit das gesamte Risiko, obwohl sie von der

IT-Materie absolut keine Ahnung haben. Die „ (leider nicht) zertifizierten Techniker“ die das aufbauen, bringen die Ärzte an den Rand der Existenz. Die Ärzte bringen den „Technikern“ ein Vertrauen entgegen, welches diese ausnutzen und für eine Installationspauschale genau nur so viel tun, dass das einmalige Karte einlesen funktioniert. Mehr nicht! Das gern gebrauchte Zitat: „Die Verantwortung des Arztes endet beim Konnektor“ wird genutzt um den Ärzten vermeintlich eine Sicherheit vorzugaukeln, welche aber nicht gegeben ist. Es handelt sich rein um eine freie Meinungsäußerung ohne jeden juristischen Hintergrund. Diese Haftungsfragen müssen juristisch aufgearbeitet und in Gesetze gegossen werden. Eine Haftungsbefreiung wird heute noch den Ärzten versprochen, wenn sie, wie zertifiziert angeschlossen sind. Ich habe noch keine Installation gesehen, welche dem Zertifizierten Aufbau entsprochen hat. Die Ärzte wissen das jedoch nicht! Bei der hohen Anzahl von parallelen Schaltungen ohne Firewall sind alle diese Ärzte in der Haftung. Den Ärzten ist ganz offensichtlich in der Praxis sogar das Recht genommen, sich sicher anschließen zu lassen. Meldungen an alle Behörden werden ignoriert. Die Unternehmen drängen den Ärzten einen unsicheren Anschluss auf, wenn die nicht unterschreiben gibt es den Honorarabzug. Also unterschreiben die. Um dann aus der Haftung zu kommen treten sie „Diffusionsgemeinschaften“ bei. Was auf der Strecke bleibt sind die Patienten und damit die fundamentalsten Menschenrechte. Datenschutz ist nicht etwas für gesunde. Die haben keine Daten zu verlieren! Der Datenschutz ist besonders für die Kranken wichtig! Die haben Daten zu verlieren, die bei Bekanntwerden den Lebenslauf der Menschen ändert.

5. Nach meinen Informationen sind 15% der praktizierenden Ärzte an der Altersgrenze (Quelle: Dr. Stefan Bültmann) weitere 5% der Ärzte überlegen auf die Kassenärztliche Zulassung zu verzichten und Privatpraxen zu eröffnen, wenn die Fragen weiter ungeklärt bleiben. Kann es sich Deutschland leisten, auf 20% der Ärzte zu verzichten? Ich glaube nicht!
6. Das BSI hat versucht Smartphone als sicher zu zertifizieren. Da die Handys von Hause aus bereits mit Spionagesoftwere ausgestattet sind, ist das nicht möglich! Die Gesundheitsdaten mit dem Handy zugänglich zu machen ist mit Sicherheit nicht sicher möglich! Fragen Sie das BSI! Bitte hören Sie auf, solche Dinge zu fordern. Fragen Sie erst Experten, ob solche Dinge möglich sind! Das BSI hat meines Wissens nach bereits Stellung dazu genommen. Hören Sie auf diese Menschen, die wissen wovon die reden! Zusätzlich werden Handys durch Apps ausspioniert. Die Gesundheitsdaten haben nichts auf einem Handy zu suchen! Übrigens ist ende Juni der erste Handychip vom BSI als Smartcard zertifiziert worden „Snapdragon 855“. Selbst dieser Handychip hat eine höhere CC Klasse als jede einzelne Komponente der TI; die gesamte TI ist ja nicht einmal zertifiziert! Die Zertifizierung des aus Hardware, Firmware und Betriebssystem bestehenden Sicherheitselements erfolgte laut dem BSI nach **Common Criteria (ISO/IEC 15408) EAL 4 + ALC_DVS.2 und AVA_VAN.5.** Die Evaluierungsstufe EAL 4 + ALC_DVS.2 AVA_VAN.5 bietet eine Widerstandsfähigkeit des Produktes gegen Angreifer mit hohem Angriffspotenzial.

Literaturverzeichnis

Amnesty International Deutschland e. V. (2019). *https://www.amnesty.de/*. Von Alle 30 Artikel der Allgemeinen Erklärung der Menschenrechte: https://www.amnesty.de/alle-30-artikel-der-allgemeinen-erklaerung-der-menschenrechte abgerufen 3.8.2019

AVM Computersysteme Vertriebs GmbH. (2019). *https://avm.de*. Von Sicherheitsfunktionen (Firewall) der FRITZ!Box: https://avm.de/service/fritzbox/fritzbox-7590/wissensdatenbank/publication/show/57_Sicherheitsfunktionen-Firewall-der-FRITZ-Box/ abgerufen 3.8.2019

Bundesamt für Justiz. (28. 03 2019). *https://www.gesetze-im-internet.de*. Von Grundgesetz für die Bundesrepublik Deutschland: https://www.gesetze-im-internet.de/gg/BJNR000010949.html abgerufen 3.8.2019

Bundesamt für Sicherheit in der Informationstechnik. (2019). *https://www.bsi.bund.de/*. Von Fragen und Antworten zum Inkrafttreten des IT-Sicherheitsgesetzes: https://www.bsi.bund.de/DE/Service/FAQ/IT-Sicherheitsgesetz/faq_node.html abgerufen 3.8.2019

DGN Deutsches Gesundheitsnetz Service GmbH. (24. April 2019). *https://www.dgn.de*. Von TI-Installation: Das ist beim Parallelbetrieb zu beachten: https://www.dgn.de/unternehmen/ti-installation-das-ist-beim-parallelbetrieb-zu-beachten/ abgerufen 3.8.2019

ETES GmbH. (2019). *https://www.etes.de*. Von EICAR Testvirus: https://www.etes.de/downloads/eicar-testvirus/ abgerufen 3.8.2019

gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH. (24. Oktober 2018). Anschluss medizinischer Einrichtungen an die Telematikinfrastruktur - Ein Überblick für Dienstleister vor Ort (DVO). Berlin, Berlin, Deutschland.

intersoft consulting services AG. (2019). *https://dsgvo-gesetz.de*. Von Art. 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten: https://dsgvo-gesetz.de/art-5-dsgvo/ abgerufen

Schmidt, J. (6. Juni 2019). *https://www.heise.de*. Von Trojaner-Befall: Emotet bei Heise: https://www.heise.de/ct/artikel/Trojaner-Befall-Emotet-bei-Heise-4437807.html abgerufen 3.8.2019

Tremmel, M. (5. Oktober 2018). *https://www.golem.de*. Von Fünf von sechs Routern enthalten bekannte Sicherheitslücken: https://www.golem.de/news/sicherheit-fuenf-von-sechs-routern-enthalten-bekannte-sicherheitsluecken-1810-136957.html abgerufen 3.8.2019

Jens Ernst

Von: Jens Ernst <jens.ernst@happycomputer.eu>
Gesendet: Montag, 10. Juni 2019 17:36
An: 'info@hasomed.de'
Betreff: WG: DSGVO, Grundschutzkatalog usw.
Anlagen: ElefantTI_Statement_Praxissicherheit_2019-06-05.pdf

Sehr geehrte Damen und Herren

Ich bin der „böse Systemadministrator“, der gerade den Aufbau der TI bemängelt. Mit Verwunderung habe ich Ihr Statement Praxissicherheit gelesen. Als erstes möchte ich feststellen, dass Sie eine Software für Psychotherapeuten herstellen. Damit gehören die Daten in der Software und auf den Rechnern allgemein, in solch einer Praxis, zu den sensibelsten Daten, die ein Mensch haben kann, anders als z.B. bei einem Zahnarzt. Gerade bei Ihnen sollten ausschließlich die höchsten Anforderungen gelten.

Ihr Schreiben zeigt mir, dass Deutschland derzeit definitiv noch nicht bereit ist für eine TI ist.

Ich finde es erst einmal gut, dass Sie sich nach meinen Veröffentlichungen mit der Materie auseinandersetzen, bin aber über das Ergebnis enttäuscht. Haben Sie sich wirklich auch nur annähernd den Grundschutzkatalog angesehen? Mir ist sehr wohl klar, dass der in seinem vollen Umfang kaum umsetzbar ist, besonders bei kleinen Praxen. Aber was Sie da schreiben verstößt meiner Meinung nach ganz klar gegen jede Regel.

Zu
WAS EMPFIEHLT DIE KBV?

„[...] Zudem würden häufig die Konnektoren in Form eines „Parallelbetriebs“ angebunden werden, sodass die Schutzfunktionen des Konnektors [**hier der Reihenbetrieb gemeint, Anmerkung von HASOMED**] für die Praxis nicht genutzt werden“.[3]

Ihre Anmerkung ist falsch. Die KV hat recht. Bei einem Parallelbetrieb werden die Schutzfunktionen des Konnektors nicht genutzt. Dem gibt es nichts hinzuzufügen.

zu
4. Ist das Telefon mit dem PC verbunden? Wenn ja, spricht dies für Parallelbetrieb.
Auch das ist nicht richtig. Wenn die Telefonanlage parallel zu dem Konnektor angeschlossen wird ist Telefonie und Reihenschaltung kein Problem. Will man auch noch CAPI Dienste nutzen ist eine weitere Schnittstelle allein zur Telefonanlage ohne Internetanbindung möglich. Um die Sicherheit der Daten zu gewährleisten, sollte jeder Arzt 10 €/Rechner, der CAPI nutzen will, für eine weitere Schnittstelle ausgeben.

Zu
6. Hat die Praxis einen WLAN-Drucker? Wenn ja, spricht dies für Parallelbetrieb.
Ein WLAN hat in einer Praxis mit solch sensiblen Daten nicht zu suchen!!!! Außer eine 802.1x Verbindung (selbst die ist nicht 100% sicher, und die haben Sie bestimmt nicht installiert) ist kein WLAN sicher!!!!!
Selbst WPA3 ist bereits gehackt worden, bevor ich überhaupt ein Gerät gesehen habe, welches WPA3 kann.
https://www.computerbase.de/2019-04/wpa3-schwachstellen-dragonblood-wlan-passwort-hacken-unsicher/
zu WPA2 Das sind allein die Sicherheitslücken, welche für WPA und WPA II bereits bekannt sind.
CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088
Sie wollen wissen, wie einfach das geht? https://www.heise.de/security/artikel/KRACK-so-funktioniert-der-Angriff-auf-WPA2-3865019.html
Es ist an uns, den Ärzten den WLAN auszureden!!! Übrigens haben auch die Gerichte mehrfach in Filesharingverfahren festgestellt, dass jedes WLAN unsicher ist. Damit dürfte die Haftung des Arztes bereits bestätigt sein. https://von-wegen-abmahnung.de/blog/bgh-urteil-wlan-schluessel

Zu

Niemals sollte ein sicherheitsrelevanter Rechner direkt mit dem Internet verbunden werden. **Bis hier stimme ich mit Ihnen überein.** Die Verbindung sollte stets zumindest über einen Router mit NAT-und Firewall-Funktionalität erfolgen. [HASOMED: Die aktuellen Router wie eine FRITZ!Box oder Speedport der Telekom erfüllen diese Anforderung.]

An dieser Stelle möchte ich entschieden Intervenieren.

1.) Fünf von sechs Routern enthalten bekannte Sicherheitslücken
https://www.golem.de/news/sicherheit-fuenf-von-sechs-routern-enthalten-bekannte-sicherheitsluecken-1810-136957.html
Dabei handelte es sich um moderne neue Router, nicht die alten Speedports, die in Arztpraxen seit Jahren ohne Updates vor sich hin laufen!!!!
2.) Selbst das BSI hat neue Richtlinien zu sicheren Routern herausgegeben.
https://www.ccc.de/de/updates/2018/risikorouter
Hier kann man nachlesen, dass selbst die nicht weit genug gehen!!!!
3.) Zitat aus BSI Grundschutz:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_2_Firewall.html

Die gesamte Kommunikation zwischen den beteiligten Netzen MUSS über die Firewall geleitet werden. Es MUSS sichergestellt sein, ***dass von außen keine unbefugten Verbindungen in das geschützte Netz aufgebaut werden können****.* ***Ebenso DÜRFEN KEINE unbefugten Verbindungen aus dem geschützten Netz heraus aufgebaut werden.***

Für die Firewall MÜSSEN eindeutige Regeln definiert werden, die festlegen, welche Kommunikationsverbindungen und Datenströme zugelassen werden. Alle anderen Verbindungen MÜSSEN durch die Firewall unterbunden werden (Whitelist-Ansatz). Die Kommunikationsbeziehungen mit angeschlossenen Dienst-Servern (z. B. E-Mail-Servern, Web-Servern), die über die Firewall geführt werden, MÜSSEN in den Regeln berücksichtigt sein.

Es DÜRFEN KEINE IT-Systeme von außen über die Firewall auf das interne Netz zugreifen (siehe Vorgaben aus dem Baustein NET.1.1 Netz-Architektur und -design). *Etwaige Ausnahmen zu dieser Anforderung werden in den entsprechenden anwendungs- und systemspezifischen Bausteinen geregelt.*

Es MÜSSEN Verantwortliche benannt werden, die Filterregeln entwerfen, umsetzen und testen. Zudem MUSS geklärt werden, wer Filterregeln verändern darf. Die getroffenen Entscheidungen sowie die relevanten Informationen und Entscheidungsgründe MÜSSEN dokumentiert werden.

Bitte zeigen Sie mir, wie Sie mit einer Fritzbox oder einem Speedport diese äußerst wichtigen Punkte umsetzen wollen? Nur so zur Info, mit dem Konnektor wird der Praxisrechner Teil des geschützten Netzes!

Übrigens, eine kleine wahre Begebenheit dazu. Die gleiche Diskussion habe ich mit Heise Security geführt. Dort war man auch der Meinung, dass eine Fritzbox mit einer Firewall ausgerüstet, oder ein NAT Router ausreichend als Schutz sei. Selbst setzt Heise aber Firewalls ein. Diese waren aber offensichtlich nicht so konfiguriert, wie es der Grundschutzkatalog fordert. Kurz nach unserer „Mail-Diskussion“ ende April ist Heise nur wenige Tage später am 13.05.2019 Opfer eines Trojaners geworden. Unter https://www.heise.de/ct/artikel/Emotet-bei-Heise-4437807.html kann man nun nachlesen, was das für Heise bedeutet. So kann man lesen:

Zitat:
Das änderte sich Mittwochnachmittag, als in den Firewall-Logs reihenweise Verbindungen zu bekannten Emotet-Servern auffielen. Ein schneller Check zeigte, dass bereits eine ganze Reihe von Rechnern über

*seltsame Verbindungen etwa auf TCP-Port 449 nach draußen kommunizierte. Das bedeutete: „**ROTER ALARM!**“*

Mit einer richtig konfigurierten Firewall nach Grundschutzkatalog wäre das nicht möglich gewesen. Lesen Sie den Artikel mal komplett durch!

Weiter heißt es:
Welche Daten die Kriminellen bereits abziehen konnten, ist noch nicht ausreichend geklärt. Die Verantwortlichen haben den Vorfall jedenfalls bei der zuständigen Datenschutz-Aufsichtsbehörde gemeldet, wie es die DSGVO fordert.

Ganz Aktuell ist seit dem 05.06.2019 eine gezielte Angriffswelle auf Arztpraxen und Apotheken mit einem Trojaner gestartet.
https://www.aerztezeitung.de/politik_gesellschaft/krankenkassen/article/989934/trojaner-tk-warnt-arztpraxen-gefaelschten-mails.html
https://www.deutsche-apotheker-zeitung.de/news/artikel/2019/06/06/apotheker-und-aerzte-warnen-vor-krankenkassen-trojaner
https://www.kvhessen.de/tk-fake-mail/
https://www.aerzteblatt.de/nachrichten/103703/Warnung-vor-Trojanern-in-falscher-TK-Mail

Wir haben uns den Trojaner von einem Psychologen schicken lassen. Wir wollten untersuchen, was der tut. Das Macro haben wir bereits offen und die Programmierung ist sogar kommentiert. Das spricht für einen professionellen Trojaner. Dieser lädt erst aus dem Internet den Schadcode. Dieser kann sich daher sogar von Mal zu Mal ändern. Ohne Internetanschluss oder hinter unserer Firewall ist der Virus wirkungslos. Wir müssen nun, um weiteres herauszubekommen, ein schlechtes Netz mit einem Router (und wir werden die neueste Fritzbox dafür einsetzen, um zu beweisen, dass auch moderne Router mit einer Firewall nicht ausreichen) aufbauen, um die Funktionsweise des Trojaners zu ermitteln und herauszubekommen, ob dieser Trojaner sogar Daten stiehlt. Sollte das der Fall sein, wären erneut unzählige Daten im Internet gelandet, denn es wurden einige Arztpraxen infiziert. Möglich wird dies durch fehlende gesetzliche Regelungen, wie die TI aufgebaut werden MUSS. Ich habe bereits mehrere Meldungen vorliegen, wonach Praxen, auch Psychologen, nach der TI Anbindung befallen wurden. Ein Systemadmin berichtete mir von 446 Trojanern. Das muss aufhören!!!!

zu
• WLAN ist erlaubt, aber verschlüsselt
Dazu hatte ich mich geäußert.

Ärzte müssen das nicht wissen. Es ist an uns, den ITlern, die darüber aufzuklären und Dinge abzuschalten, die so nicht richtig sind!

Zu:
Szenario 3 (laut „Technischer Anlage Datenschutz“ nicht optimal, aber in Ordnung)
• Parallele Anbindung
• Router mit NAT-Firewall
• WLAN mit WPA2 und MAC-Filter
• Laptop oder PC mit Windows 10, guten Passwörtern, Bildschirmsperre, Antivirus, Personal Firewall, ver-schlüsseltes PVS (Elefant Zusatzmodul Security-Mode), Festplattenverschlüsselung

Auch der MAC Filter rettet Sie nicht. Es ist ein leichtes eine bestehende oder schon einmal verbundene Mac zu fälschen!!

Laut den Medien soll es Einzelfälle gegeben haben, bei denen die Sicherheitsfunktionen auf dem Computerabgeschaltet worden sind.
Wir haben uns das zusammen mit dem Bundesdatenschutz und dem Landesdatenschutzbeauftragen angesehen. Leider waren es keine Einzelfälle. Ich habe Bilder aus ganz Deutschland bekommen mit abgeschalteten Firewalls, sogar richtig teure Softwarefirewalls. Hier ein Beispiel aus der Antwort von mir an den Arzt.

Ich meine so etwas sollte da stehen:

Da ich täglich unzählige Mails, übrigens kostenlos, beantworte, habe ich Ihr Dokument nur überflogen. Da finden sich bestimmt noch mehr Dinge. Ich möchte Sie bitten, dieses Dokument noch einmal zu überarbeiten. Ich werde diese Mail auch an den Bundesdatenschutzbeauftragten und Landesdatenschutzbeauftragten weiterleiten. Ich bin der Meinung, dass hier ganz klare gesetzliche Regelungen zwingend erforderlich sind. Wie soll ein Arzt sich in dem Chaos an Informationen, welche sich alle wiedersprechen, zurechtfinden. Und Ihr Unternehmen ist viel größer als meins. Warum sollten mir dann die Ärzte glauben?

Ich bin ebenfalls der Meinung, dass solch ein Dokument Ihre Rechtsabteilung noch einmal prüfen sollte, da sich hieraus ein Haftungsanspruch ergeben könnte.

Ich weiß gar nicht, wie ich weiter argumentieren soll. Ich verdiene damit keinen EURO. Mir sind lediglich die Daten der Menschen wichtig und ich kann die Umsetzung der TI in der Form, wie ich sie bisher gesehen habe nur auf das Schärfste kritisieren. Alle weisen nur die Schuld auf Andere. Der Patient bleibt mit seinem Problem allein und hat nicht die Möglichkeit zu verhindern, dass seine Daten im Netz landen. Wer kommt für die Schäden auf, die dabei entstehen?

Ihre für mich entscheidenden Sätze sind:

Die gematik setzt einen umgesetzten IT-Grundschutz des BSI voraus. Verantwortlich dafür ist die Praxis. Die Umsetzung des Grundschutzes kann der DvO nicht prüfen. Hat die Praxis diesen Grundschutz nicht umgesetzt, soll die Reiheninstallation vorgenommen werden.

Meine Anmerkung dazu ist: **Der Gesetzgeber ist nun am Zug die Umsetzung der TI zu regeln. Dabei hat er festzulegen: Der DvO hat die örtliche Prüfung durchzuführen. Ist der IT-Grundschutz nicht umgesetzt, ist die Reiheninstallation anzuschließen.** Dem ist nichts hinzuzufügen. Nur so ist der Schutz der Daten zu gewährleisten! Und die sind an der Stelle das einzig Wichtige! Ob der Arzt WLAN möchte oder er dann die

Telefonnummer mit der Hand wählen muss ist mir vollkommen egal! Will er mehr Luxus, dann muss der den Grundschutz umsetzen!

Beachten Sie bitte weiterhin, dass weder unsere Techniker noch HASOMED Bescheinigungen ausstellen können, die bestätigen, dass Ihr Praxisnetz auch nach der Konnektorinstallation über alle der gewählten Installationsweise entsprechende Sicherheitsfunktionen gemäß dem Bundesamt für Sicherheit in der Informationstechnik (BSI) verfügt.

Meine Anmerkung dazu ist: **Der Gesetzgeber ist nun am Zug die Umsetzung der TI zu regeln. Dabei hat er festzulegen: Wenn der DvO parallel angeschlossen hat, hat der Techniker der Praxis schriftlich zu bestätigen, dass der IT-Grundschutz umgesetzt wurde. Damit ist auch die Haftung des Praxisinhabers auf den DvO zu übertragen.** Dem ist nichts hinzuzufügen. Wenn die Unternehmen mit in der Haftung stehen, dann wird der Aufbau auf einmal ganz anders erfolgen, da bin ich mir ganz sicher. Kein Unternehmen wird dann der Meinung sein, dass ein Speedport eine ausreichende Sicherheit darstellt.

Ich glaube, mit den zwei Vorschlägen können viele Ärzte sich anfreunden.

Ich würde mich freuen, wenn Sie mir antworten. Bitte verstehen Sie diese Mail als konstruktive Kritik. Mir geht es nicht darum ihnen einen Euro aus Ihrem Geldsäckel zu nehmen. Ich mache auf Grund der geringen Kundenanzahl die Ärzte sind gar keine TI Installation. Aber meine Ärzte wurden von mir sicher angeschlossen und die TI Techniker haben die Sicherheit außer Kraft gesetzt. Dagegen habe ich mich gewehrt. Nun weiß ich, dass in ganz Deutschland Probleme beim Aufbau der TI aufgetaucht sind. Das sin keine Einzelfälle.

MFG

Jens Ernst

Happycomputer GmbH
Alfred-Klanke-Straße 5A
58239 Schwerte

Tel.: 02304/776677
Fax: 02304/776678

info@happycomputer.eu

Registergericht Hagen HRB 8734
Geschäftsführer: Jens Ernst

HASOMED
Elefant®
Die Praxissoftware

HINWEISE ZUR PRAXISSICHERHEIT

WAS SIND DIE UNTERSCHIEDE ZWISCHEN REIHEN- UND PARALLELBETRIEB?

Eine gute Erklärung hierzu liefert die KVNO auf ihrer Webseite unter:
https://www.kvno.de/60neues/2019/19_07_ti-anschluss/index.html

WAS EMPFEHLEN IHRE BERUFSVERBÄNDE?

Empfehlung des VPP: „Vergessen Sie die Reihenschaltung und nehmen Sie unbedingt die Parallelschaltung!“[1]

Empfehlung des BVVP: „Die Empfehlung der gematik für Einzelpraxen lautet klar, die TI im Reihenbetrieb zu installieren. Die Lösung gewährt den derzeit besten Schutz für die Daten. Da der PC nicht separat mit dem Internet verbunden ist, sind auch die Haftungsrisiken minimiert. Aus datenschutzrechtlicher Sicht, sind nur Reihenbetrieb oder Netzwerktrennung zulässig. Daher sollten Sie eine dieser beiden Anschlussarten wählen.“[2]

WAS EMPFIEHLT DIE KBV?

„[...] Zudem würden häufig die Konnektoren in Form eines „Parallelbetriebs“ angebunden werden, sodass die Schutzfunktionen des Konnektors [hier der Reihenbetrieb gemeint, Anmerkung von HASOMED] für die Praxis nicht genutzt werden“.[3]

WAS EMPFIEHLT DIE GEMATIK?

Die gematik setzt einen umgesetzten IT-Grundschutz des BSI[4] voraus. Verantwortlich dafür ist die Praxis. Die Umsetzung des Grundschutzes kann der DvO nicht prüfen. Hat die Praxis diesen Grundschutz nicht umgesetzt, soll die Reiheninstallation vorgenommen werden.
In der Checkliste[5] für Praxisinhaber steht jedoch nur:

Entsprechende Funktionalität am Installationstag prüfen:
- Ist ein »Secure Internet Service« (Sicherer Internetzugang) gewünscht?
- Ist ein Zugang zum »Sicheren Netz der KVen« gewünscht?

WARUM WERDEN SO VIELE KONNEKTOREN PARALLEL INSTALLIERT?

Die meisten Praxen haben bereits einen bestehenden Internetanschluss für ihr Praxisnetz und für die genutzten Anwendungen, u.a. für Softwareupdates, Fernwartung und elektronische Kommunikation. Dies sind insbesonders:

- SafeNet-Router für das Sichere Netz der KVen
- VPN per USB-Stick für die hausärztliche Versorgung
- GUSboxen
- VoIP und Internettelefonie
- Fernwartung / TeamViewer
- Medizintechnik
- Standortvernetzung
- Updates von Elefant
- Updates der Medikamentendatenbank
- E-Mail und Internet Zugang

Somit treffen unsere Techniker im Regelfall bereits auf bestehende Praxisinstallationen.

1 https://www.vpp.org/meldungen/19/190124_techniktipps.html
2 Mitgliederinformation vom 07.05.2019
3 Stellungnahme der KBV vom 22.05.2019
4 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html
5 https://www.gematik.de/fileadmin/user_upload/gematik/files/OPB-Infomaterialien/gem_2017-12-CL-PTP_checkliste_psychotherapeutenpraxis_online.pdf

Ver. 2019-06

Unsere Techniker haben die Anweisung, dass die Installation der TI den Praxisbetrieb nicht blockieren darf.

Aus diesem Grund prüfen Sie insbesondere folgende Gegebenheiten:

1. War der Praxis-PC vorher schon direkt mit dem Internet verbunden? Wenn ja, spricht dies für den Parallelbetrieb.
2. Hat der Kunde den Internetanschluss extra für die TI organisiert? Wenn ja, spricht dies für Reihenbetrieb.
3. Möchte der Kunde mit dem Praxis-PC nicht ins Internet? Wenn ja, spricht dies für Reihenbetrieb.
4. Ist das Telefon mit dem PC verbunden? Wenn ja, spricht dies für Parallelbetrieb.
5. Ist der Praxis-PC ein Laptop und kann nur im WLAN betrieben werden? Wenn ja, spricht dies für Parallelbetrieb.
6. Hat die Praxis einen WLAN-Drucker? Wenn ja, spricht dies für Parallelbetrieb.
7. Soll ein größeres Praxis-Netzwerk mit mehreren Praxis-PCs an den Konnektor angeschlossen werden? Wenn ja, spricht dies für Parallelbetrieb.

Eine allgemeine Vorgabe an den Techniker, in Reihe zu installieren ohne den Praxisablauf zu stören (z.B. WLAN Drucker nicht mehr erreichbar?!) ist also nicht machbar. Es wird in jeder Praxis individuell entschieden.

Der Parallelbetrieb hat den geringsten Einfluss auf die Praxis-IT. Vor allem dann, wenn der Praxis-PC schon vorher mit dem Router und somit dem Internet verbunden war. Die parallele Installation hat keinen Einfluss auf das Sicherheitsniveau der Praxis. Dieses bleibt unverändert. HASOMED oder die Techniker haben keinerlei Vorteil durch die parallele Anbindung!

UND NUN? EINE HERLEITUNG...

1. In den ***Besonderen Geschäfts- und Sicherheitsbedingungen – Telematikinfrastruktur*** (Be-GSB-TI) wird vereinbart, dass die Praxis für ihrr eigene Praxisicherheit verantwortlich und eine sichere Praxis die Grundlage der TI-Installation ist: „Überlegungen des BSI, zum IT-Grundschutz sowie Empfehlungen der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung zu Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, sind der Ausgangspunkt für den Zugang und den Austausch von Informationen zwischen den Beteiligten im Gesundheitswesens mittels Konnektor bei Verwendung der elektronischen Gesundheitskarte (eGK) gemäß § 291a SGBV. Die Kunden der HASOMED verpflichten sich aus diesem Grund zur Anerkennung und strikten Einhaltung der im Folgenden aufgeführten Sicherheitsforderungen, wobei diese keinen Anspruch auf Vollständigkeit erheben, um den Konnektor in Betrieb zu nehmen und gemäß der den Kunden eingeräumten Rechte zu nutzen.“[1]
2. Der IT-Grundschutz des BSI[2] umfasst 850 Seiten. Die Umsetzungshinweise[3] noch einmal 1.040 Seiten. Wir halten es für unrealistisch, dass ein Praxisinhaber diese Lektüre studiert.
3. Hilfreicherweise veröffentlichte die KBV im Juni 2018 gemeinsam mit der Bundesärztekammer das 12-seitige Dokument ***Technische Anlage zu den Hinweisen und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis***[4]. Dies sollte jeder Arzt und Psychotherapeut sehr gut kennen!

WAS EMPFEHLEN KBV UND BUNDESÄRZTEKAMMER IN DER TECHNISCHEN ANLAGE FÜR DIE TI-ANBINDUNG?

- Aktuelles Betriebssystem [HASOMED: Windows 10 ab 2020]
- Aktueller Virenscanner (auch auf Offline-Computern) [HASOMED: Wir empfehlen die Kaufvarianten der Virenscannner, da diese oft deutlich bessere Leistungen haben als die kostenfreien Varianten.]
- Bei einzelnen Rechnern bietet die Installation einer sogenannten Personal-Firewall oder der Betrieb mit aktiviertem Windows-eigenen Firewall zumindest einen Basisschutz.
- Theoretisch wäre die höchste Sicherheit für das Praxisverwaltungssystem gegeben, wenn dieses nicht an Gesundheitsnetze und vor allem nicht an das Internet angebunden wäre, d.h. wenn das Praxisverwaltungssystem offline betrieben würde. Praktisch benötigen die Systeme aber zumindest regelmäßige Updates. [HASOMED: Das heißt Internetanbindung zum Download der Updates.]
- Es wird empfohlen, für die Nutzung des Internets für medizinische Recherchen, Online-Banking, Soziale Netzwerke, Online-Shopping usw. einen dedizierten Rechner zu verwenden, welcher über keinen direkten Zugriff auf Patientendaten oder einen anderen vernetzten Rechner mit Patientendaten verfügt.
- Niemals sollte ein sicherheitsrelevanter Rechner direkt mit dem Internet verbunden werden. Die Verbindung sollte stets zumindest über einen Router mit NAT-und Firewall-Funktionalität erfolgen. [HASOMED: Die aktuellen Router wie eine FRITZ!Box oder Speedport der Telekom erfüllen diese Anforderung.]
- WLAN ist erlaubt, aber verschlüsselt
- Powerline (DLAN) ist erlaubt, aber verschlüsselt

1 https://www.hasomed.de/fileadmin/user_upload/Elefant/Downloads/Elefant_Be-GSB_TI_2018-03.pdf
2 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html
3 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/umsetzungshinweise_node.html
4 https://www.kbv.de/media/sp/Technische_Anlage_Datenschutz.pdf

HASOMED
Elefant®
Die Praxissoftware

WELCHE SZENARIEN GIBT ES NUN FÜR DIE AMBULANTE PRAXIS?

Szenario 1 (optimal)
- Der IT-Grundschutz des BSI ist in der Praxis umgesetzt.[1]
- Die Praxis kann parallel oder in Reihe installiert werden.
-

Szenario 2 (Empfehlung der gematik, wenn kein Grundschutz besteht)
- Reihenanbindung des Konnektors
- Downloads für Updates (für Windows, Antivirus, Firewall und Elefant) und Fernwartungstools per SIS-Power (7,00 Euro pro Monat)
- Smartphone, Tablet oder Zweitrechner für Webrecherchen nutzen

Szenario 3 (laut „Technischer Anlage Datenschutz" nicht optimal, aber in Ordnung)
- Parallele Anbindung
- Router mit NAT-Firewall
- WLAN mit WPA2 und MAC-Filter
- Laptop oder PC mit Windows 10, guten Passwörtern, Bildschirmsperre, Antivirus, Personal Firewall, verschlüsseltes PVS (Elefant Zusatzmodul Security-Mode), Festplattenverschlüsselung

HINWEISE ZUR REIHENSCHALTUNG

Reihenschaltung des Konnektors mit dem Sicheren Internet Service (SIS) bietet den optimalen Schutz durch die Sicherheitsfunktionen des Konnektors, unterliegt aber auch Einschränkungen:
- Das monatliche Datenvolumen ist beschränkt auf 5 GB (30 GB mit Zusatzkosten)
- SIS ist sicherer, weil
  a) Kommunikationsdaten bei unverschlüsselter Kommunikation gescannt und gefiltert werden
  b) im Browser eingebebene Webseiten bei einer „Blacklist" geprüft und im Fall der Auflistung geblockt werden. Derzeit ist nicht bekannt, ob die Möglichkeit zur Freischaltung ggf. falsch geblockter Adressen besteht.
- Es gibt derzeit keine Aussagen zur Verhinderung von Profilbildung aus Logdateien, insbesondere wenn die Kommunikation mit dem Mailserver unverschlüsselt stattfindet (d.h. ohne SSL): Welcher Therapeut schreibt E-Mails an wen (Patienten)? Welcher Therapeut ruft welche Internetseiten auf?
- Findet die Kommunikation im Webbrowser und E-Mail verschlüsselt statt, kann die E-Mail durch SIS zwar nicht gescannt und auch der Empfänger nicht ausgelesen werden, allerdings kann der SIS diese Inhalte dann auch nicht prüfen und leitet den Datenverkehr in diesem Fall ungeprüft durch.
- Hat der Konnektor keine Verbindung zur TI, ist die Praxis mit dem Einzelrechner offline. Auch eine Fernwartung durch den Support ist in diesem Fall nicht mehr möglich.
- Derzeit stellen wir fest, dass bei Reiheninstallationen mindestens die Virenscanner von „Kaspersky" und „ESET" keine Updates über SIS herunterladen können.

WAS IST AN DEN VORWÜRFEN ZUR DEINSTALLATION VON FIREWALLS UND VIRENSCANNERN DRAN?

Laut den Medien soll es Einzelfälle gegeben haben, bei denen die Sicherheitsfunktionen auf dem Computer abgeschaltet worden sind.

Dazu unsere Stellungnahme:

1. Unsere Techniker deaktivieren keine Sicherheitsfunktionen in Ihrer Praxis, weder an Ihrem Internetrouter noch auf Ihrem Elefant PC.
2. Die Installation des Konnektors verschlechtert nicht das Sicherheitslevel Ihrer Praxis.
3. Wenn Sie die Einhaltung der Sicherheitsvorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der gematik in Ihrer Praxis überprüfen lassen wollen, wenden Sie sich gern an unsere Service-Partner oder einen lokalen IT-Dienstleister. Unsere Techniker können dies im Rahmen der TI-Installation nicht leisten.

1 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

Ver. 2019-06

HASOMED
Elefant®
Die Praxissoftware

Ob Ihr Konnektor in Reihe oder parallel angeschlossen wurde, können Sie dem Installationsprotokoll entnehmen, dass Sie per E-Mail erhalten haben:

Beispiel Parallelbetrieb

Installationstyp	**Parallel**
Route für SNK wurde eingerichtet	☑
Internet-Modus	**IAG**
Aktiviertes Bestandsnetz	**KVRLP**
Zugriff auf KVSafeNet aktiviert	☑

Beispiel Reihenbetrieb

Installationstyp	**In Reihe**
SIS Power	**SIS Standard enthält 5 GB Datenvolumen und ist der Pflege und Wartung des Konnektors vorbehalten. Für Privatnutzung muss SIS Power (30 GB) gebucht werden (7 Euro brutto monatlich, wird nicht erstattet).**
SIS Power verbindlich buchen	☐
Internet-Modus	**SIS**
Aktiviertes Bestandsnetz	**KVBW**

WAS KÖNNEN SIE TUN, WENN DIE TI BEREITS IN IHRER PRAXIS INSTALLIERT WURDE UND SICH NUN EINE UND SICH NUN EINE REIHENSCHALTUNG WÜNSCHEN?

Wir prüfen derzeit die Möglichkeit zur Erstellung einer Installationsanleitung, damit Sie die Umstellung selbst vornehmen könnten (nur für fachlich versierte IT-Anwender geeignet). Alternativ können unsere Techniker nochmal zu Ihnen in die Praxis kommen und den TI-Betrieb kostenpflichtig (160,00 Euro netto) umstellen.

Wir sind der Überzeugung, dass die fachlich korrekte parallele Installation keinen Mangel darstellt und nicht zur kostenfreien Nachbesserung berechtigt. Auf Nachfrage wird Ihnen der BVVP auch mitteilen, dass mit der in der Mitgliederinformation angegebene Formulierung „In diesem Falle sollten Sie Ihr Softwarehaus kontaktieren und eine entsprechende Nachbesserung einfordern." kein kostenfreier Einsatz gemeint ist.

Bitte haben Sie Verständnis, dass wir die Umstellung von parallelen Installationen auf Reihe bei der Terminplanung nachrangig zu den Erstinstallationen Ihrer Kollegen priorisieren.

Beachten Sie bitte weiterhin, dass weder unsere Techniker noch HASOMED Bescheinigungen ausstellen können, die bestätigen, dass Ihr Praxisnetz auch nach der Konnektorinstallation über alle der gewählten Installationsweise entsprechende Sicherheitsfunktionen gemäß dem Bundesamt für Sicherheit in der Informationstechnik (BSI) verfügt. Wir können Ihnen jedoch bestätigen, dass das Sicherheitsniveau Ihrer Praxis gemäß BSI IT-Grundschutz-Kompendium durch die TI-Installation nicht verschlechtert wurde. Bitte klären Sie mit dem Administrator Ihrer Praxis, ob die unabhängig von der TI-Installation geltenden Sicherheitsbestimmungen des BSI in Ihrer Praxis erfüllt sind.

HASOMED
Elefant®

Informationen zur Telematikinfrastruktur

In diesem Handout finden Sie die wichtigsten Informationen zu den Voraussetzungen für die TI-Anbindung und deren Umsetzung bei Elefant. Bitte nehmen Sie sich hierfür einen Moment Zeit.

Inhalt

Telematikinfrastruktur

Was ist die Telematikinfrastruktur (TI)?

Die Telematikinfrastruktur (TI) ist die sichere Vernetzung verschiedener IT-Systeme im Gesundheitswesen. Die sogenannte Datenautobahn ermöglicht einen schnellen, sicheren und papierlosen Informationsaustausch und optimiert Qualität, Transparenz und Wirtschaftlichkeit in der Gesundheitsversorgung. Voraussetzung ist die Anschaffung neuer technischer Komponenten.

Wer muss an der TI teilnehmen?

Ärzte, Psychotherapeuten, Zahnärzte, Krankenhäuser und Apotheken sind gesetzlich verpflichtet bis zum 31.12.2018 (nach derzeitigem Stand) ihre Praxis/Klinik/Apotheke an die TI anzubinden bzw. ab dem 01.01.2019 den Versichertenstammdatenabgleich durchzuführen.

Wer übernimmt die Kosten für die technische Ausstattung?

Nach den gesetzlichen Vorgaben sind die Krankenkassen verpflichtet, die Kosten für die Erstausstattung der Praxen und den laufenden Betrieb in voller Höhe zu übernehmen. KBV und GKV-Spitzenverband haben sich dazu unter Moderation des Bundesschiedsamtes auf eine Vereinbarung zur Finanzierung der TI geeinigt. Die Vereinbarung ist ab 1. Juli 2017 gültig. Die Finanzierungsvereinbarung ist auf der Homepage der KBV veröffentlicht.

Technische Komponenten

Welche technischen Komponenten werden benötigt?

Die TI-Anbindung und die damit verbundene Nutzung der elektronischen Anwendungen erfordert die Anschaffung neuer technischer Komponenten, wie:

- Internet
- Intranet
- PC und Praxissoftware
- Stationäres eHealth-Kartenterminal (eHKT)
- TI- Konnektor
- Sicherer Internetzugang (VPN-Zugangsdienst)
- Praxis- oder Institutionskarte

Auf den nachfolgenden Seiten finden Sie die Details zu den Voraussetzungen.

Internet

Ein Internetanschluss ist Voraussetzung für die Anbindung an die TI!

Optionen für den Internet-Anschluss

- Empfohlen: DSL-, Kabel- oder Glasfaseranschluss
- Alternativ: UMTS Router mit Netzwerkanschluss

Mindestanforderungen an den Internet-Anschluss für VSDM

- 1 Mbit im Download und 128 Kbit im Upload

Anforderungen an den Router

- Empfehlung: FRITZ!Box, alternativ ist jeder derzeit handelsübliche Router geeignet
- Adminzugang muss vorhanden sein (Admin-Login und Passwort)
- Mindestens ein freier LAN-Port (Netzwerkanschluss)
- Einwahldaten zum Provider müssen vorhanden sein

Im Falle einer Hardware-Firewall (Sonderfall)

- Individuelle Prüfung und Konfiguration

Sie haben keinen Internetanschluss oder wissen nicht, ob Ihr Anschluss alle Voraussetzungen erfüllt? Lassen Sie sich zum Praxis-Check beraten.

Intranet (internes Netzwerk)

Der Auf- bzw. Ausbau eines Netzwerkes ist Voraussetzung für die TI!

Geräte im Netzwerk: PC, Konnektor, Lesegerät(e), Switch, Router

LAN oder dLAN

- Der Konnektor und die Lesegeräte haben kein WLAN. Der Anschluss muss über LAN (Netzwerkkabel) oder dLAN (LAN über Stromkabel) hergestellt werden, damit Patientenkarten eingelesen werden können.

WLAN

- Die Nutzung von WLAN ist nur für den Praxis-PC möglich.

Router

- Stehen am Router nicht genügend LAN-Anschlüsse zur Verfügung, wird ein Switch benötigt.

Zwei mögliche Szenarien für den Anschluss der Praxis an den Internetzugang

- Sie waren vor der TI online: Praxis PC direkt am Router anschließen.
- Sie waren vor der TI offline: Praxis-PC hinter den Konnektor anschließen.

Die Elefant Service-Partner stehen Ihnen bei dem Aufbau Ihres Netzwerks unterstützend zur Seite? Lassen Sie sich zum Praxis-Check beraten.

PC und Software (Arbeitsplatz-PC)

Die TI-Anbindung betrifft den Praxis-PC nur indirekt, dennoch müssen bestimmt Voraussetzungen erfüllt sein.

Notwendig:

- Der Praxis-PC muss einen LAN-Anschluss haben oder WLAN fähig sein.

Dringend empfohlen:

- Windows 7 oder neuer (Windows XP und Vista werden nicht mehr unterstützt und müssen ersetzt werden)
- Aktivieren Sie die Windows-Updates und führen diese durch.
- Aktivieren Sie die Updates Ihres Praxisverwaltungsprogrammes.

Installiertes PVS:

- Ihr PVS benötigt die Zulassung durch die gematik. **Elefant hat seit Nov. 2017 die Zulassung.**

Stationäres eHealth-Kartenterminal (eHKT)

Die Nutzung eines stationären Health-Kartenterminal ist Voraussetzungen für die TI.

Die neuen E-Health-Kartenterminals sind notwendig, um eGK-Anwendungen der elektronischen Gesundheitskarte nutzen zu können, wie z.B. das Versichertenstammdatenmanagement.

Über die Geräte erfolgt auch die Anmeldung der Praxis an die TI: Dazu wird der Praxisausweis (authentifiziert die Praxis für die Teilnahme an der TI) in das Kartenterminal eingesteckt. Die Geräte müssen von der gematik zugelassen sein.

Das Elefant TI-Komplettpaket enthält das „ORGA 6141 online“. Das stationäre eHealth Kartenterminal ist speziell für den gematik Online-Produktivbetrieb-Stufe 1 (OPB1) konzipiert ist.

Konnektor

Die Nutzung eines Konnektors ist Voraussetzung für die TI!

Der Konnektor ist vom Grundprinzip vergleichbar mit einem Router, allerdings auf einem viel höheren Sicherheitslevel. Datenschutz steht im Vordergrund der TI. Der Konnektor bindet Praxissysteme hochsicher in die Telematikinfrastruktur ein und eröffnet so den Zugang zu den eGK-Anwendungen.

Für den Konnektor gelten daher die gleichen Sicherheitsanforderungen wie für Ihren Elefant-PC, da er für die Verarbeitung von personenbezogenen Daten genutzt wird.

Das bedeutet Dritte dürfen keinen unbeaufsichtigten Zugang zum Konnektor haben.

Das Elefant TI-Komplettpaket enthält den „Secunet Konnektor“. Dieser basiert auf der bewährten Hochsicherheitslösung SINA, der auch die Bundesregierung vertraut.

VPN Zugang, Praxiskarte und eHBA

Sicherer Internetzugang (VPN-Zugangsdienst)

Der VPN-Zugangsdienstanbieter stellt den Zugang zur TI bereit.

Vergleichbar mit einem VPN-Zugangsdienst mit einem Internetprovider, der den Zugang zum Internet bereitstellt.

Praxisausweis

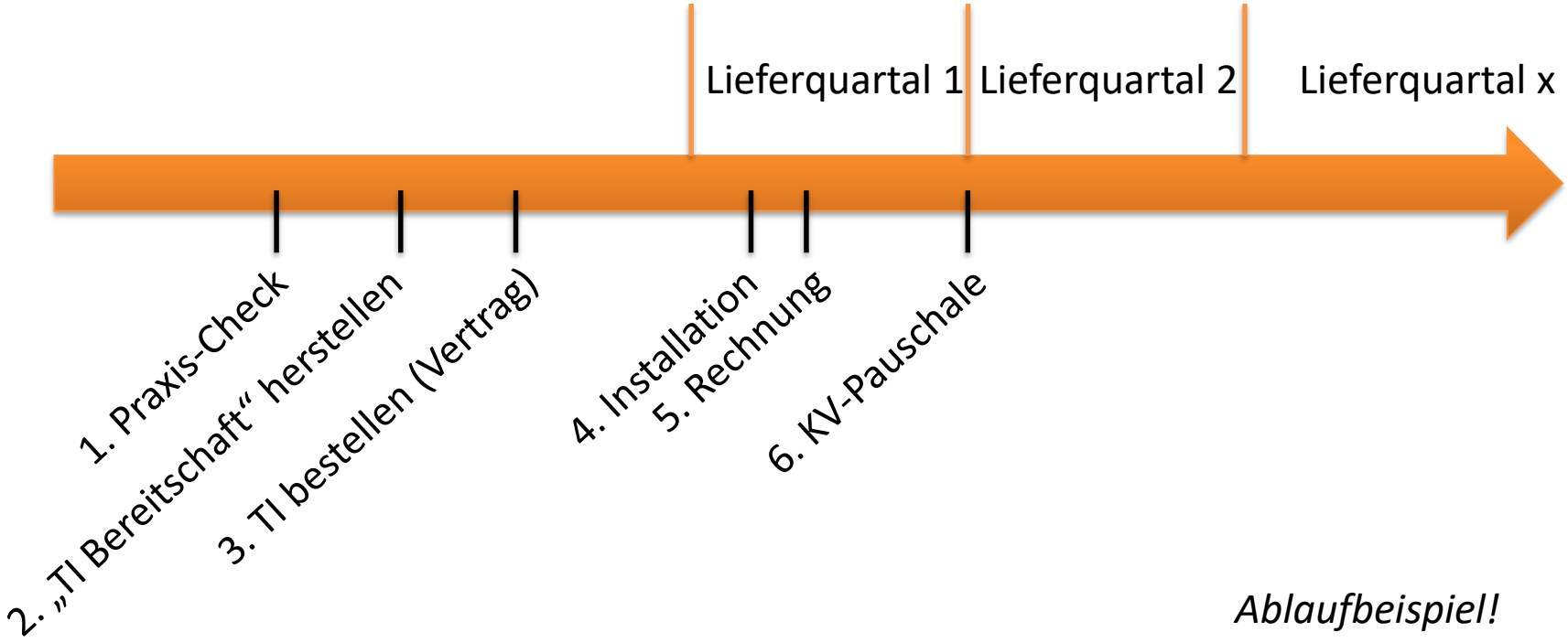
Der Praxisausweis wird für die Verbindung zur TI benötigt, sie repräsentiert die Praxis. Er wird bei der Installation der TI-Technik in eines der stationären Kartenterminals eingelegt und über eine PIN freigeschaltet. Ihren Praxisausweis können Sie über unseren Kooperationspartner medisign bestellen.

Elektronischer Heilberufsausweis (eHBA)

Der elektronische Heilberufsausweis (eHBA) ist eine Chipkarte für Ärzte und Psychotherapeuten. Mit dem eHBA kann eine rechtssichere digitale Unterschrift erstellt werden, die qualifizierte elektronische Signatur (QES). Der eHBA ist **nicht** notwendig für die Anbindung an die TI.

So kommt die Praxis zur Telematik Infrastruktur

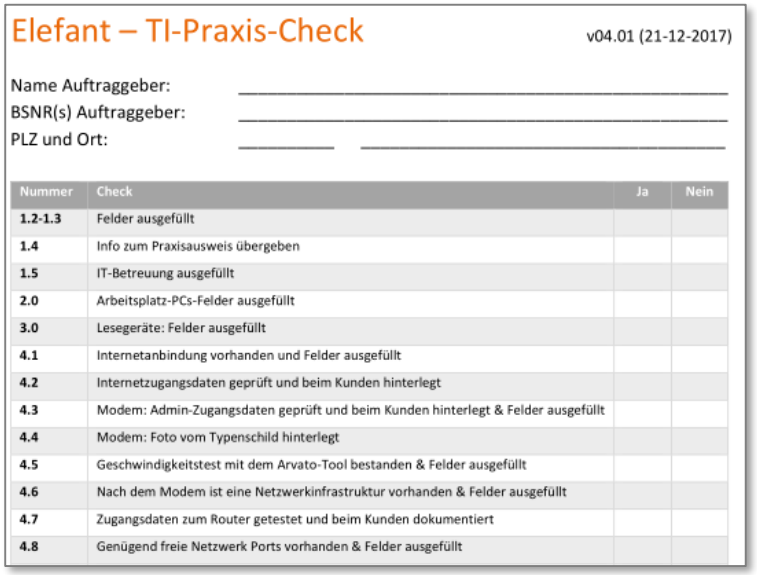
Beginnend mit dem Praxis-Check (1) und den Vorbereitungen zur TI-Installation (2) kann das TI Paket bestellt werden (3). Nach der Installation (4) wird unmittelbar die Rechnung (5) fällig. Durch den Abgleich einer Gesundheitskarte über die Telematik Infrastruktur überweist die KV die gültige Pauschale mit der Quartalsabrechnung.



Ablaufbeispiel!

Elefant TI-Praxis-Check

Im Praxis-Check wird die Bereitschaft der Praxis zur TI Installation geprüft (Dauer ca. 1 Stunde). Wesentliche Punkte dabei sind:



Elefant – TI-Praxis-Check v04.01 (21-12-2017)

Name Auftraggeber: _____

BSNR(s) Auftraggeber: _____

PLZ und Ort: _____ _____

Nummer	Check	Ja	Nein
1.2-1.3	Felder ausgefüllt		
1.4	Info zum Praxisausweis übergeben		
1.5	IT-Betreuung ausgefüllt		
2.0	Arbeitsplatz-PCs-Felder ausgefüllt		
3.0	Lesegeräte: Felder ausgefüllt		
4.1	Internetanbindung vorhanden und Felder ausgefüllt		
4.2	Internetzugangsdaten geprüft und beim Kunden hinterlegt		
4.3	Modem: Admin-Zugangsdaten geprüft und beim Kunden hinterlegt & Felder ausgefüllt		
4.4	Modem: Foto vom Typenschild hinterlegt		
4.5	Geschwindigkeitstest mit dem Arvato-Tool bestanden & Felder ausgefüllt		
4.6	Nach dem Modem ist eine Netzwerkinfrastruktur vorhanden & Felder ausgefüllt		
4.7	Zugangsdaten zum Router getestet und beim Kunden dokumentiert		
4.8	Genügend freie Netzwerk Ports vorhanden & Felder ausgefüllt		

- ☑ Ist der Internetzugang schnell genug?
- ☑ Sind alle Zugangsdaten vorhanden?
- ☑ Muss noch ein Praxisnetzwerk (Kabel) installiert werden?
- ☑ Kann der Konnektor sicher aufgestellt werden?
- ☑ Ist der Router konfigurierbar?
- ☑ Sind spezielle Gegebenheiten zu berücksichtigen (z.B. Firewalls)?
- ☑ Handelt es sich um eine Praxisgemeinschaft?
- ☑ Wird KV-SafeNet genutzt?
- ☑ …

Wir empfehlen dringend den Praxis-Check durchzuführen, denn stellt sich zum Installationstermin heraus, das Voraussetzungen nicht erfüllt sind, so können Folgekosten höher ausfallen. Weiterhin ist ausschließlich das Onlinedatum, also der erfolgreiche TI-Anschluss, relevant für die Förderungshöhe.

Elefant TI-Komplett-Paket

Die HASOMED GmbH/Praxissoftware Elefant bietet Ihnen einen Komplett-Service für technische Erstausstattung sowie für die Wartung im laufenden Betrieb an.

Gesamtpaket – einmalige Kosten: 3.110,00 €

- 1 Konnektor
- 1 Lesegerät (stationär)
- TI-Modul Elefant
- Secure Internet Service (SiS)
- Lieferung (sichere Lieferkette), Installation und Inbetriebnahme
- Einweisung der Praxismitarbeiter

Servicegebühr - monatliche Kosten: 82,67 €

- VPN-Zugangsdienst
- TI-Modul Elefant (Pflege)
- SiS Datenvolumen von 5 GB pro Monat
- Support

Nutzen Sie dieses Paket für Ihre sichere und bequeme Anbindung an die TI. Das Bestellformular finden Sie auf der Webseite.

Einzel- oder Gemeinschaft: Was wird benötigt?

ⓘ Jede BSNR erhält beim Stammdatenabgleich die Pauschale

Einzelpraxen benötigen:

- 1 Konnektor
- 1 Praxisausweis
- 1 Lesegerät

Praxisgemeinschaften benötigen:

- 1 Konnektor (gilt für PVs mit Elefant, Epikur, Psychodat, Psyprax oder Smarty)
- 1 Praxisausweis pro BSNR
- 1 Lesegerät pro Therapeut
- Überschuss für Konnektor-Nachkauf

Gemeinschaftspraxen benötigen:

- 1 Konnektor
- 1 Praxisausweis
- 1 Lesegerät pro Therapeut

Neben dem TI-Komplettpaket haben Praxisgemeinschaften über das TI-Ausbaupaket fehlende Komponenten zu bestellen. Das Bestellformular finden Sie auf der Webseite.

KV Dienste

KV-S@feNet

- Die Telematikinfrastruktur ersetzt das sichere Netz der KVen: Für Ihren KVSafeNet – Anschluss gibt es ein Sonderkündigungsrecht, wenn Sie erfolgreich an die TI angeschlossen sind. Bitte informieren Sie sich dazu bei Ihrer KV.

KV Connect

- KV Connect stellt Dienste auf Basis eines sicheren Netzes (TI oder SafeNet) bereit: Wir empfehlen Ihnen diesen zu behalten z.B. für die Online-Abrechnung.

  Bitte informieren Sie sich dazu bei Ihrer KV.

Kontakt Elefant TI-Team

HASOMED GmbH
Praxisverwaltung Elefant

Sie erreichen uns unser TI-Team
Mo - Do von 09 bis 17 Uhr und Freitags von 09 bis 16 Uhr.

Hotline: 0391 6107-633
Fax: 0391 6230-113
Mail: praxischeck@hasomed.de
Web: www.hasomed.de

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

HASOMED
Elefant®

Muss beim Parallelbetrieb die bestehende Firewall in der Praxis abgeschaltet werden?

Keinesfalls - ein Abschalten einer Firewall sollte natürlich nie erfolgen und wird auch nicht von uns empfohlen. Um dem TI-Konnektor den Zugang zu seinen Diensten im Internet zu erlauben, sind keine Veränderungen an den Firewall- und Filtereinstellungen notwendig. Für die