Sehr geehrte Damen und Herren,

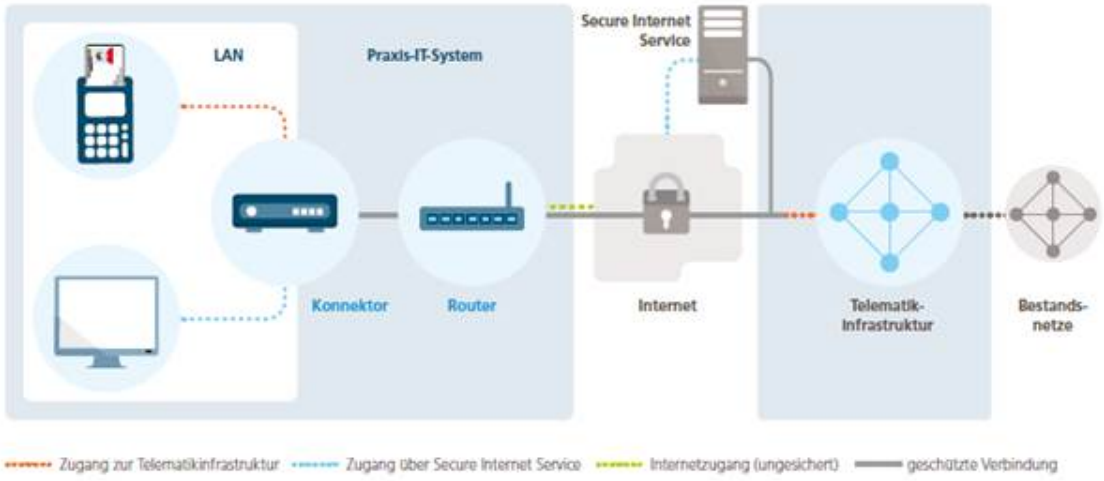
da ich immer noch nicht das Gefühl habe, dass ich es geschafft habe, die Menschen zu überzeugen, dass wir auf einer tickenden Zeitbombe sitzen, möchte ich an dieser Stelle noch einmal eine Zusammenfassung der absolut gesicherten und nachprüfbaren Fakten machen. Dabei versuche ich das so zu beschreiben, dass jeder Laie dies ganz einfach prüfen kann. Ich werde immer noch gefragt, ob meine Behauptungen haltbar seien, da bereits über 100.000 Installationen durchgeführt wurden und noch nichts passiert sei. Ich kann den bereits entstandenen Schaden nicht abschätzen, möchte jedoch die Fakten zusammentragen und für jeden verständlich erklären.
Die Gematik hat beim BSI die Telematik zertifizieren lassen. Dabei wurden am Internet drei verschiedene Methoden zugelassen.

Quelle z.B.: https://www.bzaek.de/fileadmin/PDFs/t/gem_2017-12-IB-AME_anschluss_medizinische_einrichtung_online.pdf

Mir wurde dieses Dokument vom Landesdatenschutzbeauftragten zugesendet. Daher gehe ich erst einmal von der Richtigkeit des Dokumentes aus. Ich werde mich mit allen Bildern und Zitaten auf dieses Dokument beziehen.

1. **Reihenbetrieb**

   Dabei wird der Konnektor mit dem LAN (Local Area Network /Lokales Netz) Anschluss an den Rechner angeschlossen und mit dem WAN (Wide Area Network/Internetanschluss) Anschluss ans Internet angebunden. In dieser Betriebsart ist das Praxis Netz nur über eine geschützte Verbindung mit dem Netz der Telematik verbunden. (graue Linie)



Ein Internetzugang zu allen anderen Diensten (E-Mail, Abrechnungssyteme usw.) ist dabei nicht vorgesehen.

ZITAT aus dem oben genannten Dokument:

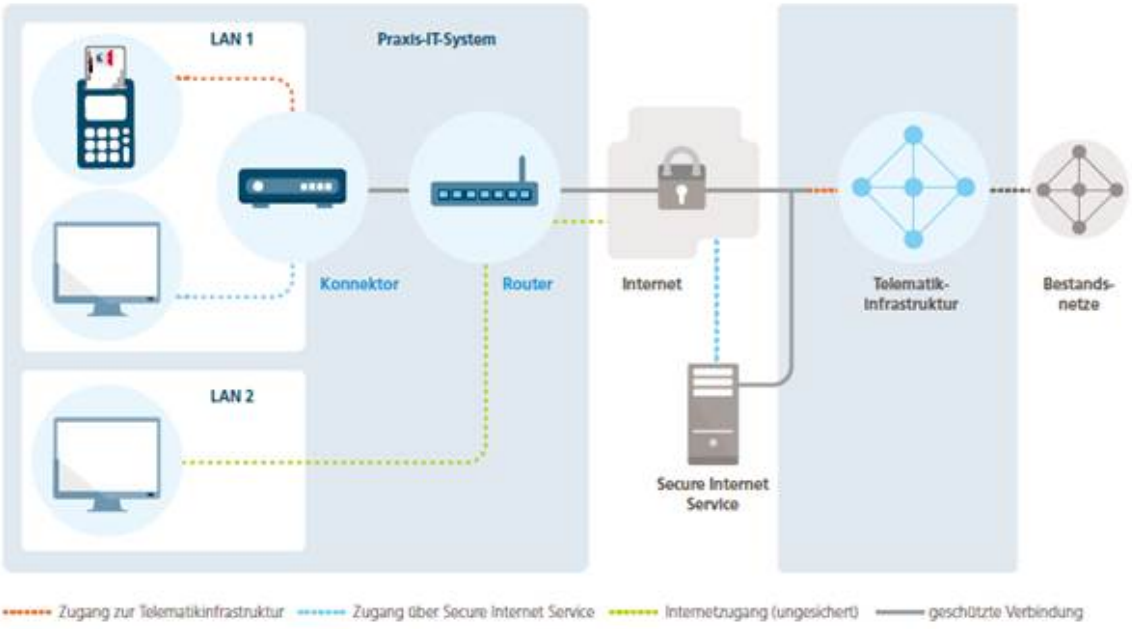
Im Reihenbetrieb befinden sich alle Komponenten im selben Praxisnetzwerk (LAN) und erhalten Zugang über den Konnektor zur Telematikinfrastruktur. Durch die integrierte Firewall des Konnektors und den optionalen und gegebenenfalls kostenpflichtigen Secure Internet Service wird das LAN optimal vor unautorisierten Zugriffen von außen geschützt.

Diese Betriebsart ist leicht zu konfigurieren und gewährleistet eine vertrauliche Übertragung medizinischer Daten.

2. **Netztrennung**

Dabei wird der Konnektor mit dem LAN (Local Area Network /Lokales Netz) Anschluss an den Rechner angeschlossen und mit dem WAN (Wide Area Network/Internetanschluss) Anschluss ans Internet angebunden. In dieser Betriebsart ist der mit der Telematik verbundene Praxisrechner nur über eine geschützte Verbindung mit dem Netz der Telematik verbunden. (graue Linie). Einen Internetzugang zu allen anderen Diensten (E-Mail, Abrechnungssyteme u.s.w.) ist dabei nicht vorgesehen.
Ein oder mehrere andere Rechner werden gemeinsam mit dem WAN Anschluss des Konnektors parallel an das Internet angebunden (grüne Linie). Diese Rechner hätten

dann Zugriff auf Mails Abrechnungssysteme, Internet allgemein. Auf diese Rechner gehören dann absolut keine Patientendaten!!!!!

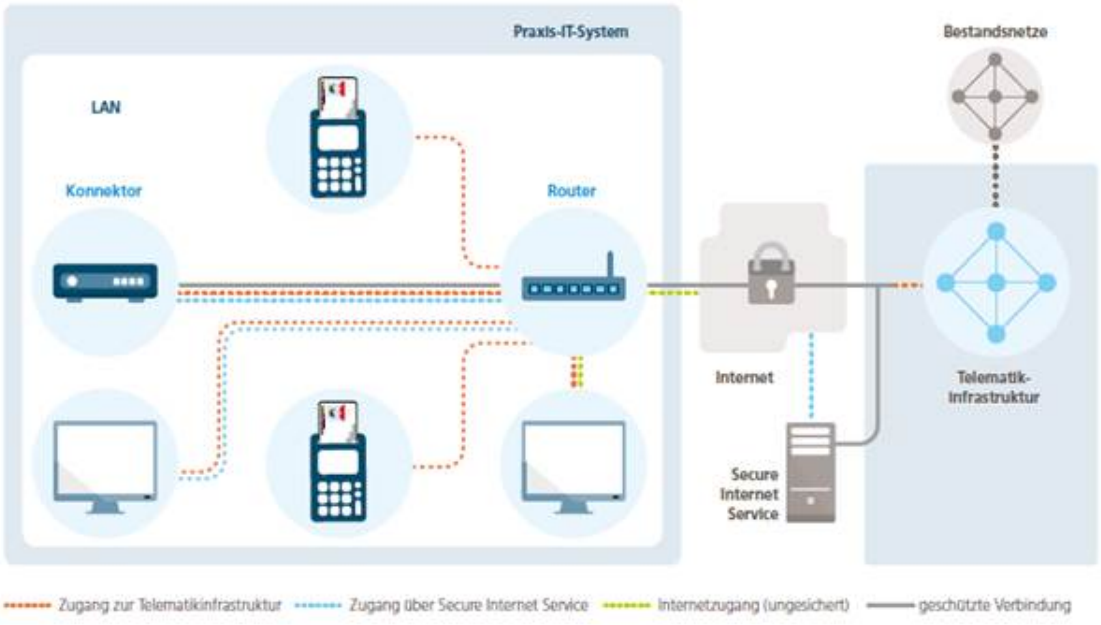


ZITAT aus dem oben genannten Dokument:
Durch die integrierte Firewall des Konnektors ist das LAN 1 sowohl vor Zugriffen aus dem Internet als auch aus dem LAN 2 geschützt. Die Komponenten im LAN 2 sind allerdings nicht durch den Konnektor abgesichert. Die Konfiguration aller beteiligten Komponenten in der Praxis ist bei dieser Betriebsart etwas aufwendiger; gegebenenfalls ist ein zusätzlicher Netzwerkverteiler (Switch) erforderlich.

Die Netztrennung bietet eine hohe Sicherheit im LAN 1 und damit einen durchgängigen Schutz bei der Übermittlung medizinischer Daten. Durch das LAN 2 kann die Praxis zudem

3. Parallelbetrieb

Diese Betriebsart ist sehr leicht zu erkennen. Der WAN Anschluss des Konnektors wird nicht benötigt. Der Konnektor ist nur mit dem LAN verbunden.



ZITAT aus dem oben genannten Dokument:

Wichtig: 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. Zudem müssen alle Netzwerkkomponenten bei dieser Betriebsart unterschiedlich konfiguriert werden.

*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 Bundesamt für Sicherheit in der Informationstechnik verfügen.*

Das bedeutet, diese Betriebsart ist nur zulässig, wenn eine Hardwarefirewall das gesamte Netzwerk schützt.

Um aber eine **Hardwarefirewall** richtig zu programmieren, müssen

a. Quell IP-Adresse (Praxisrechner)
b. Ziel IP Adresse (Telematik Infrastruktur Server oder Konzentratoren) und
c. der Port, über den kommuniziert werden darf bekannt sein.

Sie müssen sich das so vorstellen, als ob Sie ein Paket von Ort a) zum Ort b) transportieren wollen. Es gibt natürlich unendlich viele Orte. Und von allen Orten werden über die Straßen Pakete transportiert. Dabei stehen Ihnen verschiedene Transportmittel zur Verfügung. (von mir aus PKW/LKW/Bus/Pferd usw.) Es gibt verschiedene Straßen von Ort a) zu Ort b) und alle auf der Welt dürfen die Straßen benutzen. Aber auf der einen Straße dürfen nur PKW fahren, auf der anderen nur LKW und so weiter.

In der Firewall sage ich dann, dass ich keine Pakete von all den Straßen annehme oder versende. In den Paketen könnten ja Bomben sein. Nur wenn ich weiß, dass der Fahrer mit dem PKW von dem Ort a) ein Paket zu mir Ort b) transportiert hat, dann nehme ich das Paket an. Genau so nimmt Ort b) nur das Paket von Ort a) an wenn es von dem Fahrer mit dem PKW geliefert wurde.

So funktioniert eine Firewall. Dabei gibt es Straßen, welche jeder benutzt (von mir aus Autobahnen) das ist bei der Internetkommunikation der z.B. Port 80.

Wenn ich nun in der Firewall gezwungen werde alle Pakete anzunehmen, welche über die Autobahn kommen (generelle Freischaltung des Port 80 in der Firewall) anzunehmen, wo bleibt dann die Sicherheit?

Aber genau das wird nun von mir verlangt.

Mail vom Support:

> *„Sehr geehrter Herr Ernst,*
> *Leider stehen uns auch nicht mehr Informationen zur Verfügung.*
> *Wir speichern allein aus Datenschutzrechtlichen Gründen keine IP Adressen. Als Standard IP Adresse nehmen wir, wenn sie frei ist, die x.x.x.190 für den Konnektor.*
> *Die x.x.x.191 oder x.x.x.195 wird für die Kartenlesegeräte genommen. Der Port 4742 wird für die Kommunikation im internen Netzwerk genommen. Also Kartenlesegerät auf Konnektor und auf Client.*

Einen Proxy Server vor die KocoBox zu schalten sehe ich nicht als optimal an. Da dort auch keine http Seiten besucht werden, sondern nur gesicherte Seiten der Gematik ist es auch nicht sinnvoll.
Ein generelles sperren aller Ports ist sinnvoll. Dort sollten nur die von mir genannten Ports freigegeben werden.“

Wir schalten also aus Datenschutzgründen die Sicherheit und damit den Datenschutz ab!

Laut den mir also vorliegenden Informationen, sind die IP Adressen geheim. Damit ist eine sichere Programmierung einer Firewall nicht möglich.

Ich habe keine Kontrolle über die Daten.

Nun zu den Feststellungen.

1. Ich habe bisher noch nicht eine Reiheninstallation gesehen. Alle mir zugetragenen Daten weisen auf einen Parallelbetrieb hin. Der Support von cgm hat mir gegenüber bestätigt, dass der WAN nicht genutzt wird. Die gematik schreibt mir über den sichereren Reihenbetrieb: „Der gematik wurde zugetragen, dass dieses Szenario selten installiert wird“
   und weiter
   „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.“
   Wenn der Konnektor nur mit einem Kabel angeschlossen ist, liegt immer nur der Parallelbetrieb vor! Das ist leicht zu prüfen!
   Keinem Arzt ist das klar, es ist an Ihnen, den Ärzten das mitzuteilen!! Jeder Arzt muss dann selbst entscheiden!

2. In den allermeisten Arztpraxen, die ich bisher gesehen habe, sind keine Hardwarefirewalls vorhanden!! Sogar die Windows Firewall wird von den Technikern teilweise abgeschaltet, weil die Techniker entweder zu faul sind oder nicht in der Lage sind diese zu programmieren (!).

   Einer der zertifizierten Installationspartner versucht nun Schadensbegrenzung und schiebt den schwarzen Peter an die Ärzte weiter.

Als ich mich beim Support beschwerte, dass mein Kunde verlassen wurde, ohne dass die Windows Firewall wieder eingeschaltet wurde und das Virenschutzprogramm abgeschaltet wurde, wurde mir gesagt, man würde alles abschalten, da die Windows Firewall denen zu sehr rumpfuschen würde. Dafür habe ich Zeugen.

Da das eine absolute Katastrophe wäre, versucht nun der zertifizierte Dienstleister der Compugroup Schadensbegrenzung zu betreiben. Nach dessen Auskunft wird die Firewall natürlich bei allen abgeschaltet, da man DIE LOKALEN Geräte nicht anfassen würde. (Das soll natürlich nur so lange anhalten, bis die Dienstleister vor Ort die Freigaben eingetragen haben) **Ich halte selbst diese Vorgehensweise, wenn sie stimmen würde, für unverantwortlich, da die Rechner in der Zeit vollkommen ungeschützt im Internet stehen.** Man würde dann den Ärzten eine Liste mit Ports und Adressen hinterlassen, welche freigeschaltet werden müssen. Ich habe die Ärzte mit den Vorwürfen konfrontiert. Die bestreiten ganz vehement, dass das die Wahrheit ist. Natürlich ist das nicht wahr. Ich habe den Techniker vor Ort am Telefon gefragt, was ich frei schalten soll. Der Techniker wusste von keinem Port und IP Adressen kannte er auch nicht. Wo soll dann die Liste herkommen?

Hat ein Arzt also keine Firewall, ist die Sicherheit der Patientendaten nicht mehr gegeben.

Ärzte, die nie den Rechner am Internet hatten, bekommen von den zertifizierten Technikern den Rechner ans Internet gehängt ohne dass die Ärzte über das Risiko informiert werden. Da die Ärzte den zertifizierten Technikern vertrauen und denken, die wüssten was die Techniker tun, werden die Ärzte unwissentlich in eine schwierige Lage gebracht.

Konsequenzen

Verstöße gegen die DSGVO sind zusätzlich zur Bestrafung nach DSGVO noch nach dem StGB zu bestrafen.

Im § 203 StGB ist zu lesen:

„Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe."

Da Ärzte Geld für ihre Leistungen abrechnen, gilt der §203 StGB!

Außerdem bitte ich um Beachtung des Art 5 und Art 83 der DSGVO.

Artikel 5 (f) sagt, dass die Daten

> *„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");*

Der Arzt ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht")."

Wenn er das nicht macht, droht ihm Artikel 83, Abs. 5:

„Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

1. *die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;*
2. *die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;*
3. *die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;*
4. *alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;*
5. *Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die*

Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1."

Alle Ärzte stehen mit einem Bein im Gefängnis und sind von Kriminalisierung und hohen Strafen bedroht. Das kann doch nicht im Sinne des Gesetzgebers sein! Wie können die Ärzte mit Honorareinbußen bedroht werden und dann in die Kriminalität gedrängt werden?
Das sind die ersten Fakten, welche durch jeden ganz einfach geprüft werden können. Diese Fakten beruhen nicht auf Fachwissen oder Beobachtungen von mir, sondern auf Daten, die jeder selbst prüfen kann. Die Telematik ist also bereits heute ein gigantisches Netzwerk von 100.000 Rechnern, welche nicht richtig und nicht sicher am Internet angeschlossen sind und all unsere Patentendaten beinhalten.

Weitere Kritikpunkte auf die ich hier im Einzelnen nicht so detailliert eingehen möchte.
Noch etwas, selbst der zertifizierte Aufbau, den der Bundesdatenschützer anpreist, hat meiner Meinung nach große Probleme, da auch dieser Aufbau zu kurz gedacht ist. Durch fehlende Updatemöglichkeiten (Reihenbetrieb) und ein vollkommen inhomogenes Netz von 200.000 VPN Tunneln mit vollkommen unterschiedlicher Hard- und Software und jeder fehlenden Möglichkeit Updates ordentlich zu pflegen ist es eine tickende Zeitbombe und es kommt der Tag an dem wieder alle Daten im Netz sind, das wette ich schon heute.

Noch eine Anmerkung:
Ein Kunde (Zahnarzt) hat mich angerufen. Der musste die Abrechnung nach der Umstellung machen (schließt seine Praxis jetzt für 2 Wochen). Da wird ein Java Programm im Internetexplorer gestartet und nimmt Zugriff auf das Kartenlesegerät der Telematik um die Abrechnung zu übertragen. Im Reihenbetrieb würde das wahrscheinlich gar nicht gehen.
Java wird von keinem Browser mehr unterstützt. Nur der seit 2011 nicht mehr gepflegte Internetexplorer, dessen Umgang und Sicherheit ich nach 8 Jahren ohne Softwarepflege für zweifelhaft halte, kann die Java Anwendungen überhaupt ausführen. Übrigens müssen bei Ausführung alle Sicherheiten abgeschaltet werden. Auch der Virenschutz (Maximum Security) muss deaktiviert werden sonst geht das nicht. Das wurde dem Praxispersonal so gesagt (stimmt natürlich nicht, wird aber seit Jahren so gehandhabt).

Ich bin sprachlos und sehe mich als der Netzwerkbetreuer, der davon nichts weiß, auf einmal auch in der Verantwortung.

Der interne Datenverkehr wird nicht gesichert. Es gibt die Möglichkeit intern https zu nutzen, diese Funktion wird bewusst nicht genutzt, sodass Angreifer Netzwerkintern jeglichen Datenverkehr mindestens mitschneiden und speichern können.

Die Gematik nimmt folgendermaßen Stellung dazu:
„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.“

Trotz dem die Gematik schreibt, dass die unverschlüsselte Kommunikation nicht empfohlen wird, ist das der einzige Aufbau, der vorgenommen wird. In verschiedenen Portalen können Sie nachlesen, dass die Administratoren sich darüber wundern. Prüfen Sie es selbst bei sich nach!!! Das ist wichtig. Dokumentieren Sie das!!! Außerdem halte ich die unverschlüsselte Kommunikation für absolut inakzeptabel. Wir können uns bei so wichtigen Dingen nicht am schlechtesten orientieren!
Zudem hat fast jede Praxis ein WLAN, und die Sicherheitsproblematik unter WPA 2 UND WPA 3 im Butterfly Handshake sind hinreichend bekannt. Ins interne Netz einzudringen ist also nicht mal zu schwer. Viele Router haben immer wieder Sicherheitslücken (zuletzt D-Link und ASUS), manche Systemsoftware (ASUS Live Update) bringt Probleme mit. Eine Expertengruppe hat sich zuletzt in eine Radiologie Zugang verschafft und CT und MRT Aufnahmen „angegriffen“. Ich bin als Systemadministrator mit dem Bewusstsein der sicherheitstechnischen Verfehlungen in einer Haftung, die ich nicht verantworten kann und will.
Würde man das Netz der TI physisch trennen und die Firewall würde eine DMZ-Anbindung an das VPN Netz generieren, während der PC ins Internet über eine zweite Leitung oder Route geht, dann sehe ich da keine so argen Probleme. (Netztrennung, zertifizierter Betrieb)
Dann noch die Kommunikation über einen Proxyserver ggf. mit Deep-Packet Inspectation und Stateful Inspection Firewall sowie dynamische Firewall, um Angriffe zu erkennen und zu isolieren.
Man könnte sogar die Anbindung an die TI komplett mit einer einzelnen Firewall mit nur 3 Schnittstellen (WAN/LAN/DMZ) realisieren.

Fazit:
Jeder Arzt sollte selbst entscheiden, ob er das Risiko weiter eingehen möchte. Dazu gehört natürlich, dass die Ärzte erst einmal davon erfahren müssen und ihre eigene IT kontrollieren.
Jeder Arzt sollte seinen Itler des Vertrauens kontaktieren und diese Informationen vorlegen. Nach einer Beratung kann die Entscheidung nur sein, dass die Telematik grundsätzlich umgebaut werden muss.

Die Ärzte zu informieren ist nun Ihre Aufgabe.

MFG

Jens Ernst

Happycomputer GmbH
Alfred-Klanke-Straße 5A
58239 Schwerte
info@happycomputer.eu
Registergericht Hagen HRB 8734
Geschäftsführer: Jens Ernst