Berufsverband
der Augenärzte
Deutschlands e.V.

der Augenarzt

Telematikinfrastruktur: Anbindung mit Sicherheitsrisiko

der Augenarzt 3/2019
S. 121–128

Eine Publikation
des Kaden Verlags

KADEN

Telematikinfrastruktur: Anbindung mit Sicherheitsrisiko

Nachgefragt bei Jens Ernst, Happycomputer GmbH

Derzeit biegt die Anbindung der Telematikinfrastruktur (TI) aus Sicht der Politik auf die Zielgerade ein. Die Angaben darüber, wie viele Praxen an die TI angebunden sind, variieren ja nach Quelle. Das liegt an der sehr einseitigen Information der Öffentlichkeit und der Ärzteschaft durch die Kassenärztliche Bundesvereinigung, die gematik und des Bundesgesundheitsministeriums. Zwischen 20 und 40 % der Ärzte sind noch nicht angebunden und wollen dies teilweise auch zukünftig nicht. Da Gesundheitsminister Jens Spahn immensen Druck aufbaut und höhere Honorarstrafen für die „Verweigerer" plant, sind kritische Fragen und Nachrichten über Probleme eher unwillkommen. Jens Ernst ist Inhaber eines IT-Unternehmens in Schwerte, das auch die EDV und Netzwerkarchitektur von Arztpraxen betreut. Im April 2019 stieß er auf eklatante Probleme in Praxen, die zur Einhaltung der gesetzlich vorgegebenen Fristen Ende Juni 2019 kurzfristig an die TI angebunden worden waren.

Jens Ernst
Happycomputer GmbH

der Augenarzt: Bei der TI-Anbindung gibt es strenge gesetzliche und regulatorische Vorgaben. Der Konnektor wird versiegelt und unter besonderen Sicherheitsvorkehrungen angeliefert und wird von geschulten und zertifizierten Technikern angeschlossen. Zumindest kann man das den Aussagen der gematik und der Anbieter so entnehmen.

Die Anbindung erfolgt nicht entsprechend der gesetzlichen Vorgaben und nicht durch zertifizierte Techniker.

J. Ernst: Diese Aussage muss ich zunächst einmal korrigieren. Die Anbindung erfolgt nicht entsprechend der ursprünglich verbreiteten gesetzlichen Vorgaben – das fängt schon damit an, dass sie nicht von zertifizierten Technikern durchgeführt wird. Bei meiner Recherche hat sich gezeigt, dass die Techniker teilweise noch nicht einmal wissen, was eine IP-Adresse oder ein Port ist, geschweige denn, wie man eine Firewall konfiguriert.

der Augenarzt: Die Techniker sind nicht zertifiziert?

J. Ernst: So ist es. Jeder kann nach einer kurzen, teilweise lediglich online durchgeführten Schulung die TI aufbauen. Das ist eine Schande. Die Ärzte können die TI sogar selbst installieren, was sicherlich auch nicht im Sinne der Vorschriften ist.

der Augenarzt: Das klingt nicht vertrauenerweckend.

Windows-Firewall und Virenschutz werden absichtlich abgeschaltet.

J. Ernst: Das stimmt. Da nach dem Einsatz eines solchen Technikers in einer von mir betreuten Praxis alles andere nicht mehr funktionierte, habe ich mich auf die Fehlersuche begeben. Dem Konnektor wurde vom Techniker eine IP-Adresse mit der Ziffer 190 am Ende zugewiesen (Beispiel: 192.168.2.190). Das machen diese Firmen immer so, unabhängig davon, ob die Adressen frei sind oder nicht. Da die zugewiesene IP-Adresse bereits durch die Telefonanlage besetzt war, konnte sich der Techniker nicht mit seinem Rechner auf den Konnektor einloggen.
Er demonstrierte den Damen an der Rezeption dann wohl, dass er ohne Netzwerk mit seinem Laptop problemlos auf den Konnektor zugreifen kann. Folglich trennte er alle Geräte vom Switch und änderte die IP-Adresse des Rechners, woraufhin natürlich keine Firewallregel mehr funktionierte. Da die Telefonanlage nicht mehr angebunden war, klappte nun zwar der Zugriff auf den Konnektor, die Telefonanlage selbst funktionierte jedoch nicht mehr. Der Techniker schaltete daraufhin die Windows-Firewall und den Virenschutz ab, der Konnektor bekam den Router als Standardgateway, und

der Techniker konnte demonstrieren, dass die Versichertenkarte eingelesen werden kann.

der Augenarzt: Es entstand also ein komplettes Chaos, nur weil der Techniker dem Konnektor eine bereits vergebene IP-Adresse zugeteilt hat?

J. Ernst: Genau, es funktionierten weder die Drucker, noch die Telefonanlage, denn beide waren vom Netzwerk getrennt. Wir teilten der Telefonanlage dann eine andere IP-Adresse zu und schauten uns die ganze Konfiguration genauer an. Was wir dabei vorfanden, war unfassbar: Das komplette System war ohne Schutz – und noch dazu an einen Internetanschluss von Unitymedia angebunden, der bauartbedingt ein Modem statt eines NAT-Routers nutzt. Das Netz hatte keine Firewall, keine Paketfilter oder ähnliches – ich hätte von außen direkt auf alle Daten zugreifen können. Ich rief beim Support dieses TI-Installateurs an und beschwerte mich über den Techniker. Dazu wurde mir lediglich mitgeteilt, dass man das „immer so mache“, da die Windows-Firewall „immer so dazwischenfunken würde“. Da kam mir ein erster Verdacht.

der Augenarzt: Nach etwas Hilfe konnte in der Praxis wieder gearbeitet, gedruckt und telefoniert werden – war das Problem damit behoben?

J. Ernst: Leider nicht. Da die für eine ordnungsgemäße Konfiguration der Firewall benötigten Regeln aus Datenschutzgründen geheim gehalten wurden, war eine ordnungsgemäße Inbetriebnahme der TI gar nicht möglich.
Die Firewall schützt die Praxis, die ans Internet angeschlossen ist, samt Telefonanlage und Computern vor unerlaubten Zugriffen aus dem Internet sowie vor Hacker-Angriffen. In manchen Routern sind die Grundfunktionen einer Firewall eingebaut. Da nach aktuellen Tests jedoch fünf von sechs Routern erhebliche Sicherheitslücken aufweisen und kein Router eine richtige Firewall enthält, welche stündlich mit den neuen Angriffsszenarien gefüttert wird, ist bei sensiblen Daten – besonders bei medizinischen Daten – Wert auf erhöhte Sicherheit zu legen und deshalb eine zusätzliche, eigene Firewall nötig.

der Augenarzt: War das Abschalten der Firewall ein Versehen?

J. Ernst: Davon bin ich zunächst ausgegangen, bis ich das in anderen Praxen genauso erlebt habe. Auch dort bestätigte mir dann bei einem Beschwerdeanruf der Support, dass man das „immer so machen würde“. Das war offenbar kein Versehen, sondern Absicht, da es so einfach schneller geht. Schließlich werden die Techniker pauschal bezahlt, und da zählt jede Minute.

der Augenarzt: Ist die Installation ohne zusätzliches Firewall-Gerät einfacher? Hätte man nicht einfach dem Konnektor eine andere IP-Adresse geben können, statt der Telefonanlage, die dann komplett neu programmiert werden musste?

J. Ernst: Die Installation ohne Firewall ist natürlich einfacher aber eben auch unsicher. Und ja, der Techniker vor Ort hätte jede beliebige freie IP-Adresse nutzen können. Im Nachhinein ist das leider nicht so einfach abzuändern, da sowohl das Kartenlesegerät als auch der Rechner die IP des Konnektors mitgeteilt bekommen. Da war es für uns einfacher, die Telefonanlage zu erneuern. Auch die Firewall musste komplett neu programmiert werden.

der Augenarzt: Kommen wir zu einer technischen Frage, die sich bei der Installation der TI stellt: Was bedeutet „parallel“ oder „seriell“ installiert – in einfachen Worten?

Wird der Konnektor parallel (mit nur einem Netzwerkkabel) angeschlossen, so ist das System unsicher und nicht zulässig.

J. Ernst: Seriell bedeutet ganz einfach, dass alle Datenpakete, die sich nicht im lokalen Netz der Praxis befinden, ausschließlich über den Konnektor ins Internet bzw. zur TI gelangen können. Erkennen kann man den Anschluss daran, dass der Konnektor mit zwei Netzwerkkabeln und einem Stromkabel verbunden sein muss. Beim parallelen Anschluss existieren zwei Wege ins Internet: Der erste Weg über die Firewall und der zweite Weg über den Konnektor. Der Praxisrechner ist also parallel mit dem Konnektor an einem Switch angeschlossen. Der Konnektor ist dann – wie der Rechner auch – nur mit einem Netzwerkkabel versehen. Hierfür ist jedoch eine richtig eingerichtete Firewall vorgeschrieben. Um die Firewall richtig einrichten zu können, und um das Netz BSI-konform – also nach den Vorschriften des Bundesamtes für Sicherheit in der Informationstechnik – zu betreiben, müssen die richtigen Regelwerke in der Firewall hinterlegt werden. Das ist eine Menge Arbeit. Wenn diese Informationen für die Konfiguration von den Anbietern geheim gehalten werden, ist eine richtige Einrichtung nur möglich, wenn man im Netzwerk die geblockten Pakete mitschneidet und auswertet. Aber Vorsicht! Sobald man im Netz Datenpakete mitschneidet, betreibt man laut Bundesdatenschutz „Hacking“ und macht sich strafbar. Das ist zwar nicht sinnvoll, ist aber so.

der Augenarzt: Die Informationen beziehungsweise Regeln für die Konfiguration sind also so geheim, dass selbst der Praxisinhaber sie nicht wissen darf?

J. Ernst: Eine BSI-konforme parallele Einrichtung auf legalem Weg ist so nicht möglich. Von einem Anbieter (CGM) haben wir seit ein paar Tagen die Regeln vorliegen, wie regelkonform eingerichtet werden muss. Diese funktionieren auch. Da diese Regeln jedoch bislang geheim gehalten wurden, glaube ich, dass alle bisher installierten parallelen Anschlüsse unsicher aufgebaut sind. Dies liegt daran, dass eine generelle Portöffnung – beispielsweise der Ports 80, 443 und 53 – einen Proxybetrieb, welcher laut BSI vorgeschrieben ist, unmöglich macht. Außerdem reißen die generellen Portöffnungen solche Sicherheitslöcher in die Firewall, dass man mit der einfachsten Malware Daten abfischen kann. Hinzu kommt, dass bei allen Netzen, die ich bisher gesehen habe, die TLS-Verschlüsselung nicht aktiviert war.

WLAN ist immer unsicher!

Damit werden die Daten im LAN (innerhalb der Praxis) im Klartext für jeden sichtbar kommuniziert. Das ist ein Skandal. Die gematik hat in einer Mail an mich ausdrücklich darauf hingewiesen, dass eine solche Kommunikation nicht gewünscht ist. Befindet sich in dem Netzwerk noch ein WLAN, können Patienten oder Nachbarn sich den Zugang zum Praxis-WLAN erschleichen und alle Daten mitlesen. WLAN ist immer unsicher!

der Augenarzt: Wie für uns alle war die neue TI-Technologie auch für Sie ein Novum. Wird man als Fachmann von den Herstellern oder von der gematik zu den Details informiert?

Der TI-Aufbau in den Praxen unterscheidet sich maßgeblich vom zertifizierten Testaufbau der gematik.

J. Ernst: Bis vor zwei Monaten hatte ich noch nichts von der Telematikinfrastruktur gehört. Wegen der Probleme, die bei meinen Kunden entstanden sind, musste ich mich gezwungenermaßen mit dem Thema auseinandersetzen. Der Aufbau bei den Ärzten vor Ort hat nichts mit dem zertifizierten Testaufbau der gematik zu tun. Das muss an dieser Stelle ganz deutlich gesagt werden. Der zertifizierte Aufbau soll angeblich sicher sein.
Ich fand bei meinen Kunden enorme Sicherheitslücken und eklatante Nachlässigkeiten nach der TI-Installation und erkannte das Sicherheitsrisiko. Alle Informationen zur gematik habe ich mir selbst aus dem Internet angelesen. Wir als Praxisbetreuer wurden nicht informiert, noch nicht einmal über die Änderungen, welche die Techniker vorgenommen haben. Es gibt bei YouTube auch ein Selbstinstallationsvideo für den Konnektor „KoCoBox“. Da ist absolut keine Rede von Sicherheit, Firewall oder Reihenbetrieb. Dieses Video dürfte meiner Meinung nach so nicht im Internet verbreitet werden. Wir haben uns das zusammen mit Datenschützern angesehen, passiert ist aber bisher nichts – man kann es immer noch ansehen. Für mich unbegreiflich.

der Augenarzt: Wie kann ich als Praxisbetreiber erkennen, dass etwas faul ist?

J. Ernst: Ganz einfach: Bei einem Reihenanschluss sind am Konnektor der LAN und der WAN angeschlossen – also zusätzlich zum Stromkabel zwei Netzwerkkabel. Allerdings, bei unserem Zahnarzt wurde der Konnektor mit zwei Kabeln angeschlossen, jedoch eins am Router und eins am Switch hinter der Firewall. Somit waren zwar zwei Kabel angeschlossen, jedoch nur zum Zwecke der Umgehung der Firewall. Also die Existenz von zwei Kabeln allein genügt nicht für eine stich-

haltige Aussage zur Sicherheit, lediglich wenn nur ein einziges Kabel angeschlossen ist, ist eine sichere Konfiguration so gut wie ausgeschlossen. Ich habe Bilder und Erklärungen von rund 50 Praxen aus dem gesamten Bundesgebiet bekommen, mit je nur einem angeschlossenen Netzwerkstecker.
Ein einziger Praxisinhaber berichtete mir von einer Reihenschaltung. Daraufhin habe ich recherchiert, welche Firma die Installation vorgenommen hatte. Es stellte sich heraus, dass der Arzt über IT-Kenntnisse verfügt und die Installation selbst durchgeführt hatte.

Nur eine echte Firewall kann das „Hacken" einer Arztpraxis verhindern.

der Augenarzt: Was ist denn das Problem beim Anschluss des Konnektors und des Routers beziehungsweise der Firewall? Einen Router bekommt man doch oft von der Telefonfirma – mit bereits integrierter Firewall.

J. Ernst: Ein Router ist keine Firewall. Sein Paketfilter kann keine professionelle Firewall ersetzen, da er nur Angriffe von außen abwehren kann. Von innen nach außen ist alles offen. Mit einer einfachen Malware kann ich mir beispielsweise über den DNS-Verkehr am Port 53 alle Daten senden lassen, ohne dass der Router eingreifen würde. Dies ist nur ein Beispiel, ich möchte hier ja keine Anleitung zum Datenstehlen geben. Hinzu kommt, dass Router oft über Jahre nicht aktualisiert werden und enorme Sicherheitslücken aufweisen. Diese Lücken sind bekannt und können ausgenutzt werden, da sie oft über Jahre nicht geschlossen werden. Nur zwei Beispiele: Denken Sie an das Jahr 2016, wo zehntausende Speedport-Router DDoS-Attacken gegen die Telekom durchgeführt haben. Die Lücke war bereits seit 2014 bekannt. Das Risiko wurde jedoch als zu gering erachtet, als dass man etwas dagegen hätte tun müssen. Im zweiten Fall gab es eine Lücke, bei der allein der Besuch einer kompromittierten Webseite ausreichte, um die Kontrolle über den Router zu übernehmen und so alle im Netzwerk befindlichen Daten abzufischen. Dies sind nur zwei Beispiele, ich könnte noch viele nennen.

der Augenarzt: Ist es aber auch nicht riskant, wenn man solche Probleme an die Öffentlichkeit bringt? Bei einem gravierenden Problem eines Softwareanbieters oder eines Internetdienstes wird die breitere Öffentlichkeit auch erst informiert, wenn das Sicherheitsupdate bereit ist und vom Nutzer installiert werden kann?

Ärzte sollten aus Sicherheitsgründen den Stecker aus der Internetdose ziehen.

J. Ernst: Ja, deswegen habe ich zuerst auch nur die gematik sowie die zuständigen Firmen informiert. Als die sich zwei Wochen lang nicht rührten, habe ich die Behörden des Bundes- und Landesdatenschutzes eingeschaltet. Zwei Monate später war immer noch nichts geschehen. Was sollte ich tun? Nur der Druck aus der Öffentlichkeit kann offensichtlich etwas verändern. Mir ging es primär darum, die Ärzte zu informieren, damit diese nicht unwissentlich haftbar werden und von hohen Strafzahlungen und Kosten bedroht sind. Darum haben wir ausschließlich in Fachzeitungen unsere Informationen verbreitet. Nur haben die Ärzte leider auch nicht reagiert. Ich hätte erwartet, dass jeder Arzt sofort den Stecker aus der Internetdose zieht – ich hätte das getan.

Dann haben uns Ärzte darüber informiert, dass sie nach unseren Veröffentlichungen über Sicherheitslücken einen sicheren seriellen Anschluss haben wollten, diesen jedoch durch die DVO verweigert bekamen. Ihnen wurde mitgeteilt, entweder sie unterschreiben, dass die TI ordnungsgemäß funktioniere oder es gebe 1 % Honorarabzug. Auch beim Berufsverband Psychosoziale Berufe, an den sich ein betroffener Arzt wandte, teilte man auf Anfrage mit, dass man auf Grund der Vertragsfreiheit keinen Dienstleister zwingen könne, eine selbst gewählte Installation durchzuführen. Der Anbieter biete ausschließlich die parallele und damit sicherheitstechnisch problematische Methode an.

Arztpraxen melden aus Angst Attacken von Hackern oftmals nicht.

Weiter wurde mir nach der Sendung Kontrovers (www.youtube.com/watch?v=sPgE3a7HCbQ) von mehreren Systemadministratoren persönlich mitgeteilt, dass in deren Betreuung befindliche Arztpraxen – nach der Anbindung an die TI – gehackt wurden. Diese meldeten die Vorfälle jedoch nicht, sondern vertuschten sie, da die Strafen die Existenz der Praxen bedrohen. Die Dunkelziffer ist hoch. Also muss ich zum Schutz der Patientendaten, die mir wichtig sind, eine breite Öffentlichkeit ansprechen.

der Augenarzt: Wie viele Beispielfälle mussten Sie zusammentragen, bis eine Reaktion kam, beziehungsweise wer hat Sie denn überhaupt ernst genommen?

J. Ernst: Mir haben meine Kunden genügt, um Alarm zu schlagen. Bis heute möchte niemand eine Erhebung dazu durchführen, wie viele parallele Anschlüsse gelegt wurden.

Erst vor kurzem hat die KVB einen entsprechenden Antrag auf Erhebung abgelehnt. Ich bin der Meinung, dass bis auf ganz wenige Ausnahmen alle Anschlüsse unsicher angelegt wurden, beweisen kann ich das jedoch nicht.
Wer mich ernst genommen hat? Ganz einfach: Die großen Namen können Sie alle direkt streichen. Die IG Med war die Erste, die mich angerufen und nach unserem Telefonat meine Angaben geprüft hat. Sowohl der Bundesdatenschutz als auch der Landesdatenschutz haben mich besucht, und wir haben gemeinsam verschiedene Arztpraxen besucht, darunter auch eine Praxis, die nicht zu meinen Kunden zählt. Man hat sich davon überzeugt, dass das Problem real ist. Passiert ist jedoch bis heute nichts. Alle – die Datenschützer, die gematik, das Bundesgesundheitsministerium – haben den gleichen Standpunkt und den verschweigen sie auch nicht.

der Augenarzt: Welchen Standpunkt?

Rechtlich trägt der Arzt und nicht der Techniker die volle Verantwortung.

J. Ernst: Verantwortlich für sein Netz und damit voll haftbar ist ausschließlich der Arzt. Tritt ein Datenverlust oder Hackerangriff ein und der parallele Anschluss ist so schlecht aufgebaut wie in unseren Beispielen, dann ist das fahrlässig bis vorsätzlich, da die Software unter Windows selbst auf die Lücke hinweist. Alle Beteiligten nehmen das scheinbar billigend in Kauf – und der Arzt wird mit aller Härte des Gesetzes bestraft. Übrigens: Keine Cyberpolice deckt Fahrlässigkeit ab.

Aus diesem Grund droht jedem Arzt nach § 203 StGB eine Geld- oder Gefängnisstrafe. Es gibt beispielsweise eine Praxis, der aufgrund eines Datenverlustes eine Geldbuße von 250 000 Euro sowie drei Monate Berufsverbot auferlegt wurde, wie uns ein Mitglied des C-Netz e.V. im Zusammenhang mit unserer Kampagne vertraulich mitgeteilt hat. Zusätzlich droht gemäß DSGVO eine Geldbuße bis zu 4 % des Jahresumsatzes der Praxis. Auch hier gibt es bereits einen Fall aus Baden-Württemberg: Eine Praxis musste 80 000 Euro Geldbuße wegen Verstoßes gegen die DSGVO bezahlen. In diesem Fall gelangten aufgrund unzureichender Sicherheit Gesundheitsdaten ins Internet [1].
Hinzu kommt, dass jeder Patient schriftlich per Post über das Datenleck informiert werden muss. Mit Anwaltskosten und Portokosten kommen da auch schnell 50 000 Euro zusammen. Zudem drohen natürlich auch Schadensersatzforderungen und ein Imageverlust. Wenn ein Patient beispielsweise aufgrund des Datenlecks einen Risikozuschlag zu seiner Versicherung zahlen muss, dann muss die Arztpraxis diesen Zuschlag für den Rest seines Lebens übernehmen.
Die Verantwortlichen, namentlich die gematik, das Bundesgesundheitsministerium und die Datenschutzbehörden, weisen jede Schuld von sich. Doch die TI-Geschädigten werden weiterhin bestraft, es besteht kein Interesse an Qualitätsmanagement oder Prävention. Das ist alles, was die „Großen“ wie die gematik, das Bundesgesundheitsministerium und die Datenschutzbehörden bei der Schuldfrage hinterher interessiert – sie sind raus. Jetzt vorbeugend etwas gegen das Problem unternehmen möchte offenbar niemand. Viel zu heiß das Thema, vermutlich wegen der politischen Agenda.

Politiker sehen keinen Handlungsbedarf, da der zertifizierte Testaufbau der gematik sicher ist.

der Augenarzt: Also keiner ist verantwortlich – und am Ende haften die Ärzte?

J. Ernst: Die „gematiker“ haben bei der Zertifizierung alles richtig gemacht, sagen sie. Darum müssen sie jetzt auch nicht tätig werden. Wenn die TI nicht so aufgebaut wird, wie in der Zertifizierung vorgeschrieben, dann ist der Arzt schuld. Mir gegenüber haben natürlich alle erklärt, man nehme das Problem sehr ernst. Da sich nach nun fast drei Monaten nichts getan hat, kann ich nur darüber spekulieren, wie ernst das Problem tatsächlich genommen wird. Vermutlich verweist jeder auf einen anderen, der sich darum kümmern soll. Herr Spahn hat, statt die Probleme erst einmal zu erkennen, anzupacken und zu klären, bereits die nächste Runde eingeläutet. Die Sicherheit soll weiter herabgesetzt werden, damit jeder mit seinem Smartphone auf seine Akte zugreifen kann.

Fast alle überprüften Praxisnetze sind unsicher.

Bei unseren exemplarischen gemeinsamen Besuchen mit den Datenschützern in einer von uns betreuten und in einer fremden Praxis (die vorher noch nie am Netz angeschlossen war), wurden alle meine Bedenken bestätigt. Mein eigener Zahnarzt wurde ebenfalls parallel angeschlossen. Dabei wurden die Daten sogar durch die Änderung des Standardgateways an der Firewall direkt zum Router vorbeigeschleust, zusätzlich wurden die der Windows-Firewall und der Virenschutz ausgeschaltet. Besucht haben uns ein Vertreter des Bundesdatenschutzes,

1. https://www.handelsblatt.com/politik/deutschland/datenschutzgrundverordnung-behoerden-verhaengen-erste-bussgelder-wegen-verstoessen-gegen-dsgvo/23872806.html?ticket=ST-8911-DufLrjzOoh5qE0IHPMAN-ap6

der Landesdatenschutzbeauftragte NRW selbst, ein technisch versierter Fachmann und eine Juristin des Landesdatenschutzbeauftragten NRW.

Um die Schwachstellen aufzudecken, sollte man öffentlich zu „freundlichem Hacken" aufrufen und dies finanziell belohnen.

Unsere Nachfrage nach „Whitehacking"-Tests (freundliches Hacken, um Schwachstellen zu finden und zu schließen) und Netzwerkmitschnitten, um eventuelle weitere Probleme aufzuzeigen, wurden abgelehnt. Für eine solche verantwortungsvolle Technik, bei der mit den Gesundheitsdaten gearbeitet wird, halte ich „Whitehacking"-Tests für unverzichtbar. Ich würde mir ein „Bug-Bounty"*-Programm wünschen. So machen das alle großen Konzerne, wie beispielsweise Apple und Google, die Wert auf Sicherheit legen.

der Augenarzt: Was sagen denn die Datenschützer? Die TI ist doch gesetzlich gewünscht und zertifiziert. Der Arzt kann ja fast nicht anders, als die Installation zuzulassen und der Technologie zu vertrauen? Wer sich nicht anbindet, bekommt Ärger.

J. Ernst: Das ist ganz einfach. Es hört sich verrückt an, ist aber real so: Der Bundesdatenschutzbeauftragte hat in seinem Tätigkeitsbericht klar gemacht, 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 deshalb an mich gewandt."

Ärzte sollten sich erst dann an die TI anschließen, wenn die gematik eine Datenschutz-Folgenabschätzung vorlegt.

Das bedeutet: Jeder Arzt ist gesetzlich dazu verpflichtet, eine DSFA anzufertigen. Da sich 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. Er muss sich nun an den Bundesdatenschutzbeauftragten wenden und dort die weitere Vorgehensweise erfragen. Der Arzt kann auch nach dem Anschluss der TI und den Veröffentlichungen der Probleme zu der Erkenntnis kommen, dass er womöglich gegen die DSGVO verstößt. Also erst einmal den Stecker ziehen und den Bundesdatenschutzbeauftragten fragen, wie weiter verfahren werden soll. Erst wenn diesem die DSFA der gematik vorliegt oder die Verantwortung juristisch geregelt wird, kann der Stecker wieder eingesteckt werden.

Arztpraxen müssen übrigens 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. Wichtig: Der Grundschutzkatalog ist kein Gesetz. Man kann vom Aufbau abweichen, muss dies aber begründen können, und die Sicherheit darf dabei nicht beeinträchtigt werden. Da Ärzte in der Regel nicht genügend IT-Wissen haben, sollten sie nicht vom geforderten Aufbau abweichen. Jeder Richter und jeder Sachverständige wird prüfen, ob die Regeln des BSI eingehalten wurden. Wurden diese nicht eingehalten, und der Arzt kann das nicht begründen, ist er haftbar.

der Augenarzt: Angenommen, ein Arzt hat einen Konnektor und stellt fest, dass nur ein Kabel angeschlossen ist – was würden Sie ihm raten?

Das Praxissystem läuft auch ohne Verbindung zum Internet weiter.

J. Ernst: Ich bin kein Jurist, darum kann ich keine Ratschläge erteilen. Wenn ich Arzt wäre, dann gäbe es für mich nur eines: Sofort den Stecker ziehen und die Verbindung zum Internet kappen. Das System geht dann in den Offline-Betrieb – nach dem Ziehen des Steckers läuft meiner Erfahrung nach alles komplett offline weiter. Das Einlesen der Karte in die Praxissoftware ist nicht beeinträchtigt. Dann würde ich den Bundesdatenschutzbeauftragten darüber informieren, dass meine DSFA in der aktuellen Situation ergeben hat, dass ich den TI-Anschluss in der derzeitigen Form nicht verwenden darf, ohne gegen die DSGVO zu verstoßen. Ich würde um Rat fragen, wie ich mich weiter verhalten soll und um eine DSFA der TI bitten. Bis ei-

* Ein „Bug-Bounty"-Programm bezeichnet eine Initiative zur Aufdeckung, Behebung und Veröffentlichung von Fehlern in Software, die von Unternehmen, Interessenverbänden, Privatpersonen oder Regierungsstellen betrieben wird. In der Regel wird hierfür ein Sach- oder Geldpreis ausgeschrieben.

ne Antwort vorliegt, könnte mich niemand dazu bewegen, den Stecker wieder in die Dose zu stecken. Vor einem Honorarabzug hätte ich keine Angst: Da ich mich gesetzeskonform verhalten habe, kann kein Richter der Welt guten Gewissens einen Honorarabzug durchsetzen. Dafür würde ich sogar bis zum Europäischen Gerichtshof gehen, denn die DSGVO ist eine nationale Umsetzung einer europäischen Verordnung und der EU Datenschutzbeauftragte ist ebenfalls informiert worden.

der Augenarzt: Im Moment würde der Ablauf in den Praxen durch das De-Konnektieren nicht beeinträchtigt; kein Arzt und kein Patient hätten einen Nachteil. Wer einen Stammdatenabgleich seiner Patienten durchgeführt hat, hätte sogar die Vorgabe erfüllt und dürfte wohl eher nicht belangt werden. Aber wie geht es dann weiter?

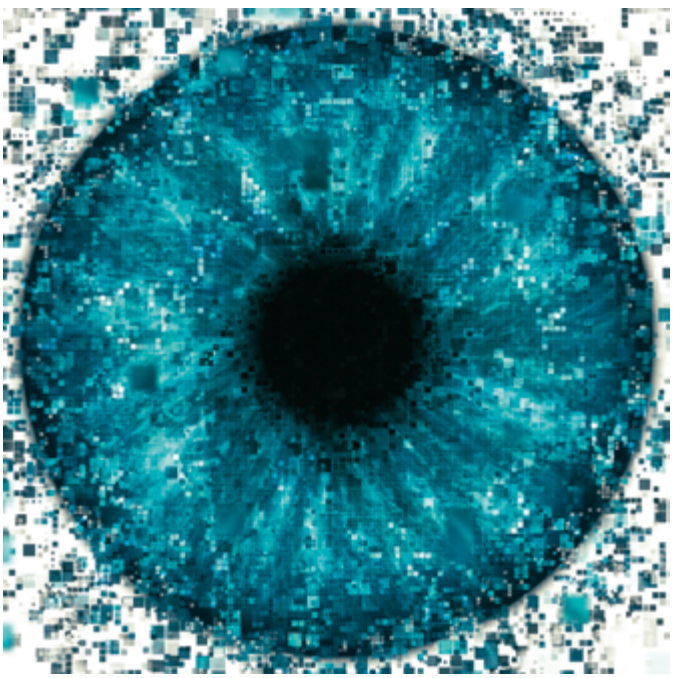
J. Ernst: Ich sehe in den falsch umgesetzten Anschlüssen die Bestätigung der Bedenken der Zweifler: Kleinste Fehler können zu katastrophalen Problemen führen. Es müssen dringend Diskussionen über Ethik und Moral sowie über Sicherheitsaspekte und mögliche Bedrohungen geführt werden – und das nicht von Medizinern oder Politikern, sondern von IT-Experten. Auch eine Bedrohung von Innen muss bedacht werden. Wesentliche Schutzprofile wurden nicht behandelt, da man diese nicht für relevant hält – aber gerade diese können relevant sein.

der Augenarzt: Laien nennen es Verschwörung und Paranoia, die den Traum von der digitalen Zukunft vermiesen sollen. An was denkt der Fachmann, wenn er über Bedrohung spricht?

J. Ernst: Stellen Sie sich beispielsweise vor, die Fern-Update-Funktion der Konnektoren würde wie 2016 bei der Speedport-Panne [Suchbegriff Mirai-Botnetz] genutzt werden, um einen gezielten Angriff auf das Gesundheitswesen zu führen. Angreifer könnten so, ab dem Jahr 2021 wenn alle Krankenhäuser, Apotheken, Ärzte und Pflegeeinrichtungen an der TI angeschlossen sind, das gesamte Gesundheitswesen deutschlandweit vollständig zum Erliegen bringen.
Diese äußerst wichtige Problemstelle ist zum Beispiel in den Schutzprofilen nicht berücksichtigt worden.

Es ist nur eine Frage der Zeit, bis ein IT-System gehackt wird.

Allein im Jahr 2018 sind mehr als 16500 Sicherheitslücken und andere Schwachstellen in Computersystemen- und Hardware registriert worden, was einer Steigerung gegenüber 2016 von mehr als dem 2,5-fachen entspricht. Das zeigt, dass selbst hochsichere IT-Systeme ein Ablaufdatum haben. Es ist also nicht die Frage ob, sondern nur wann ein IT-System geknackt werden wird. (Quelle: www.cvedetails.com/browse-by-date.php).
Auch ein Angriff auf die Ärzte aus der Telematik heraus ist nicht Bestandteil der Sicherheitsvorkehrungen. Man hält es nicht für nötig, sich mit diesem Szenario auseinanderzusetzten. Das innere geschlossene Netz der TI sei sicher. Denken wir an den Trojaner Locky, der 2016 das gesamte „sichere“ Bahnnetz befallen hat. Nur ein Fehler hat dazu geführt, dass das Bahnnetz verschlüsselt wurde. Ich halte ein solches Szenario für übertragbar: Da alle Praxen Tag und Nacht an der TI hängen, wären alle Patientendaten deutschlandweit innerhalb weniger Stunden verschlüsselt und die Ärzte damit nicht mehr arbeitsfähig. Was sagt der hippokratische Eid dazu? Entschuldigung, ich kann Ihnen nicht helfen, mein Computer läuft nicht?



Lebenswichtige medizinische Geräte mit Netzwerkanschluss würden erst nach Eingriff durch einen Systemtechniker wieder funktionieren. Da alle Geräte in Deutschland gleichzeitig betroffen wären, würde dies einen wochenlangen Ausfall bedeuten. 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 Angreifer ist auf diese Weise vollkommen problemlos möglich. Erst wenn all diese Dinge wirklich geklärt sind, und man immer noch ein derartiges Netz haben möchte, sollte wieder eine Inbetriebnahme erfolgen. Dann aber richtig, mit gesetzlichen Regelungen, die die Haftung betreffen und strengen Regeln, wie genau der Anschluss stattzufinden hat.

der Augenarzt: Ist das denn technisch möglich?

J. Ernst: Meiner Meinung nach gehört die Telematik in eine sogenannte „demilitarisierte Zone". So bezeichnet man ein extra an der Firewall angeschlossenes Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Geräte. Das bedeutet, man kann exakt steuern, welche Informationen ausgetauscht werden dürfen und wie diese Informationen auszusehen haben. Eine Verbreitung von Malware über und aus der TI in das Praxisnetz wird dadurch weitestgehend unterbunden.

der Augenarzt: Wenn man ein Türschloss und eine Alarmanlage kauft, prüft der Handwerker, ob alles funktioniert. Wie kann man prüfen, ob die TI sicher ist?

J. Ernst: Eine Sicherheitsprüfung ist äußerst kritisch, denn es gibt dabei mehrere Probleme. Erstens: Wenn die Daten unverschlüsselt im Praxisnetz gesendet werden, dann sieht man natürlich alle Daten im Klartext. Wenn es sich um echte Patientendaten handelt, ist das bereits ein meldepflichtiger Verstoß gegen die DSGVO. So aber arbeitet die TI derzeit offenbar überall.
Wenn man beispielsweise mit der Analysesoftware Wireshark® Netzwerk-Protokollmitschnitte anfertigt, kann einem vorgeworfen werden, die andere Seite – also die Telematik-Server – zu kompromittieren. Das ist strafbar. Ich gehe sogar davon aus, dass dies nicht unbemerkt bleiben würde, falls die Firewalls auf der anderen Seite so gut sind wie behauptet. Die IP-Adresse, die dann einen Scan in Richtung Telematik durchführt, landet dort auf einer Liste und kann zu jeder Zeit in eine echte Adresse mit Straße und Hausnummer umgewandelt werden. Davon rate ich ab. Ohne eine gesetzliche Regelung und ohne zulässige „Whitehacking"-Tests durch führende Experten muss man leider dem vertrauen, was man vorgesetzt bekommt und sich an die Regeln des BSI, der gematik und der KBV halten. Daran scheitert es aber in den meisten Praxen.

Ärzte sollten sich beim Anschluss schriftlich bescheinigen lassen, dass alle Regeln des Bundesamtes für Sicherheit in der Informationstechnik eingehalten werden.

Lassen Sie sich von Ihrem IT-Unternehmen schriftlich bescheinigen, dass alle Regeln der TI und des BSI eingehalten werden. Wird die Unterschrift verweigert, kann man davon ausgehen, dass man ein hohes Risiko eingeht. Eine zweite Meinung einzuholen, ist sicherlich nicht von Nachteil.

der Augenarzt: Unsere Leser sind Ärzte. Inwieweit müssen sie die Technik, die bei ihnen installiert wird, verstehen? Herr Kriedel von der KBV hat ja bekanntgegeben, man müsse sich das System vom Techniker erklären lassen.

J. Ernst: Das ist genau so, als würde ich Sie fragen, wie ich als ITler erkennen kann, dass mein Blinddarm entzündet ist. Ich kann im Internet recherchieren und abwägen, ob das zutreffen könnte, aber wenn ich sicher sein will, muss ich wohl einen Experten fragen.

Änderungen am System müssen immer protokolliert werden.

Da noch nicht einmal die Installateure, die die TI bei meinen Kunden aufgebaut haben, meinen Ausführungen aufgrund mangelndem Grundlagenwissens folgen konnten, wie soll denn der Praxisbetreiber dem Installateur folgen und was soll dieser erklären? Er hat schließlich selbst lediglich den Auftrag bekommen: „Steck das Kabel dort rein und wenn das nicht geht, ruf an." Mehr Information hatten die Techniker nicht. Es wurde auch kein Protokoll über die erfolgten Änderungen an der Infrastruktur angefertigt. Bisher konnte mir noch kein einziger Arzt bestätigen, ein solches Protokoll erhalten zu haben. Dies ist aber verpflichtend. Wie soll der IT-Dienstleister denn die Probleme erkennen, wenn er nicht weiß, welche Änderungen durchgeführt wurden? Dafür sind genau die Änderungsprotokolle da, um den Dienstleister zu informieren und natürlich auch den Praxisbetreiber. Wenn er das nicht versteht, dann muss er sich an seinen ITler wenden. Dieser muss dann die Sinnhaftigkeit prüfen und dem Praxisbetreiber erklären. Die Firma, welche die TI installiert hat, sollte unbedingt unterschreiben, dass alle Regeln des BSI eingehalten wurden.

der Augenarzt: Vielen Dank, dass Sie sich Zeit genommen haben unsere Fragen zu beantworten.

Die Fragen stellte
Dr. Stefan Bültmann