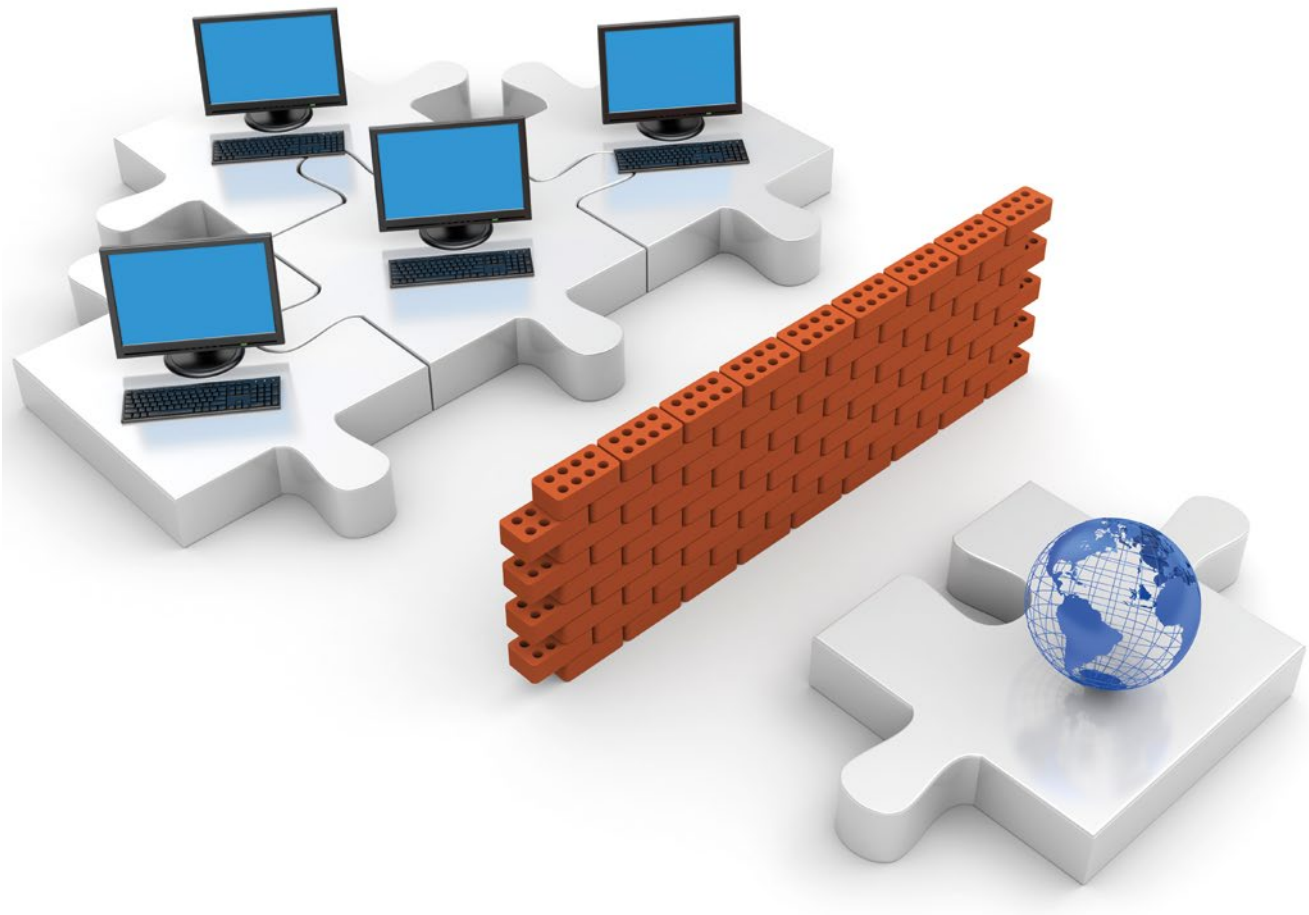


Feuerfest trotz TI

Abwehr gegen Hacker. Praxen mit TI-Anschluss sind häufig nur unzureichend vor Angriffen geschützt. Gematik und die Politik schieben den Schwarzen Peter den Ärzten und Zahnärzten zu, die Rechtslage ist undurchsichtig. Umso wichtiger, dass jeder seine Praxis so gut wie möglich selbst sichert. Die gute Nachricht: Schon wenige Maßnahmen erhöhen das Level erheblich – und sie sind nicht einmal kompliziert.

AUTOR: MAX HOPPENSTEDT

AB MÄRZ 2020 DROHEN 2,5 PROZENT GEBÜHRENABZUG FÜR

Zahnärzte, die sich noch nicht an die neue Telematik-Infrastruktur (TI) angeschlossen haben, um darüber das Versichertenstammdatenmanagement (VSDM) zu betreiben. In jüngster Zeit mehren sich jedoch die Berichte darüber, dass das TI-System ein IT-Risiko sein könnte. Vor allem einer sorgte für Unruhe: Laut einem vertraulichen Papier der Gematik weisen mehr als 90 Prozent der Arztpraxen in Deutschland, die bis Mai 2019 an die TI angeschlossen wurden, Sicherheitsrisiken auf. Das berichteten *NDR* und *Süddeutsche Zeitung* Mitte November.
In die gleiche Richtung weist eine Stichprobe des Frauenhofer-Forschers Prof. Dr. Harald Mathis. Er hatte im Auftrag des Bayerischen Facharztverbands die IT-Sicherheit von TI-Anschlüssen in 30 Praxen untersucht und ebenfalls dem *NDR* und der *SZ* von seinen Ergebnissen berichtet. Sein Fazit: Zwei Drittel der untersuchten Praxen seien nicht sicher angeschlossen und „in einem beklagenswerten Zustand" gewesen.

90 PROZENT IM PARALLELBETRIEB ANGESCHLOSSEN

Damit bestätigt sich offenkundig, wovor der FVDZ seit Jahren warnt: Die Digitalisierung des Gesundheitswesens kann den Schutz der Patientendaten aushöhlen. Auch die Reaktion der Gematik auf die Medienberichte wirkt nicht gerade vertrauensbildend: Nach dem Bericht von *SZ* und *NDR* veröffentlichte die Organisation ein Statement, in dem es hieß: „Die Telematikinfrastruktur ist sicher." Das ist technisch grundsätzlich richtig, doch es hilft nichts, wenn die TI nicht richtig angeschlossen wird. Sowohl die Gematik selbst als auch unabhängige Experten empfehlen den Anschluss im seriellen Betrieb. Laut dem internen Papier sind aber mehr als 90 Prozent der Praxen im Parallelbetrieb angeschlossen. Dazu erklärten Gematik und Gesundheitsministerium auf Anfrage der *SZ* nur lapidar, die sichere Installation sei Aufgabe der Praxen.
Für Zahnärzte stellt sich nun die Frage: Kann meine Praxis durch die neue Telematikinfrastruktur gehackt werden? Und worauf sollte ich achten, wenn ich die Daten meiner Patienten schützen will? Um die Sicherheitsrisiken besser zu verstehen, lohnt sich ein genauerer Blick darauf, wie die TI funktioniert und wie Hacker eine Praxis angreifen können. Um es vorwegzunehmen: Das Thema IT-Sicherheit ist weniger kompliziert, als es auf den ersten Blick scheint, und auch Zahnärzte ohne besondere IT-Kenntnisse können mit einigen konkreten Maßnahmen ihre Praxis deutlich sicherer machen.
Und das ist oft auch dringend nötig, wie Jens Ernst erläutert. Ernst arbeitet als IT-Fachmann für Ärzte und hat schon Einblicke in die IT-Systeme zahlreicher Praxen genommen. „Die Hälfte der Praxen, in denen ich als Techniker war, sind oder waren bereits mit Schadsoftware infiziert", sagt Ernst. In einer Zahnarztpraxis, die er beraten hat, hatte sich ein Schadprogramm eingeschleust, das auf das Stehlen von Daten programmiert war. Wie gefährlich solche Schadsoftware auch in Praxen sein kann, die bereits an das TI-System angeschlossen sind, hat Ernst selbst mit einem Angriff vorgeführt: Dazu

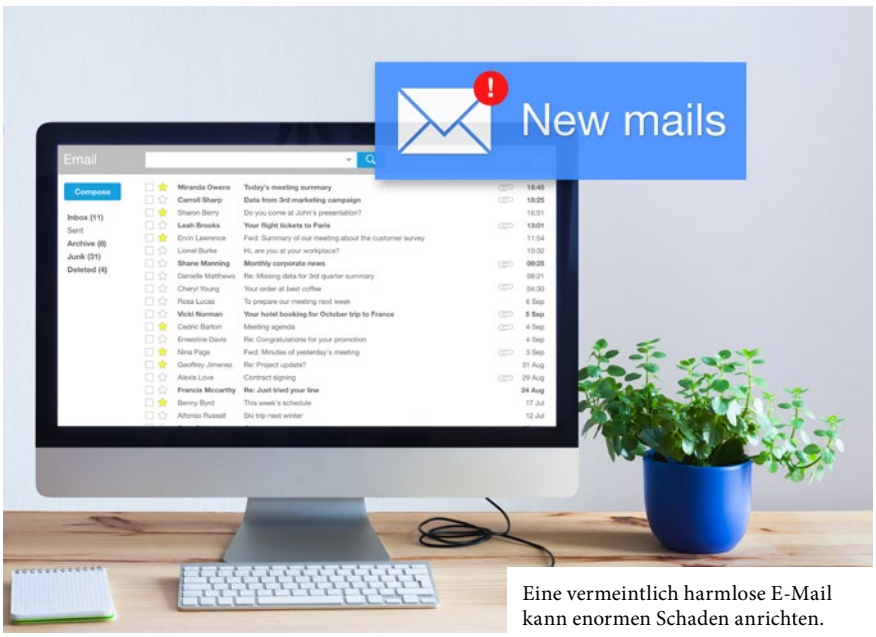
infizierte er die Praxis mit einer Schadsoftware durch eine harmlose E-Mail.

AUF EINMAL ANGREIFBAR

Sein Schadprogramm richtete dann automatisch eine neue Route ein, durch die Daten durch den Konnektor und den eigentlich vor Angriffen geschützten SIS-Tunnel zu einem von ihm kontrollierten Server geleitet werden. Anschließend könnte das Schadprogramm dafür sorgen, dass ihm automatisch die Daten geschickt werden, die er sehen will: „Ich kann mir auf die Weise jede beliebige Datei senden lassen, auch Datenbanken, die meist nicht verschlüsselt sind."
Ausgangspunkt der meisten Angriffe ist oft ein E-Mail-Anhang. Wenn ein Mitarbeiter einer Praxis den Anhang öffnet, lädt sich automatisch die Schadsoftware auf den Rechner, so auch bei dem Angriff von Jens Ernst. Dieses Risiko bestand bereits vor der Installation der Telematikinfrastruktur in den Praxen. Allerdings verschärft die Einführung der TI die Gefahr. Denn die Installation der TI-Systeme kann dazu führen, dass Praxen, die bisher nicht mit dem Internet verbunden waren, nun mit dem Netz verbunden und so theoretisch angreifbar werden.
Ärzte können sich gegen diese Angriffe allerdings schützen, wenn sie wissen, mit welchen Tricks Kriminelle versuchen, ihnen Schadprogramme unterzujubeln. Besonders beliebt ist es, eine Schadsoftware im Anhang von einer Bewerbung zu tarnen. Der Anhang trägt dann unauffällige Namen wie zum Beispiel Lebenslauf oder CV. Eine andere Masche kann es sein, dass ein Absender vorgibt, ein Arzt aus der Umgebung zu sein, der einen Befund schicken möchte – obwohl dieser Befund so niemals angefordert wurde. Praxishelfer sollten in solchen Fällen immer kurz den Arzt fragen, bevor sie den Anhang öffnen.

WIE MAN MAIL-ABSENDER UND LINKS PRÜFT

Im Sommer warnte die Techniker Krankenkasse (TK) vor einer anderen Angriffsvariante: Unbekannte Kriminelle hatten per E-Mail im Namen der TK an Ärzte und Apotheken angeblich angeforderte Patientendaten geschickt. Doch die Adresse des Absenders hatte die Endung @tkk-versicherung.com und nicht die eigentliche Endung von E-Mails der TK. Im Anhang waren keine Patientendaten, sondern eine Schadsoftware. Mitarbeiter sollten also immer genau auf die Adresse des Absenders achten. Wenn das E-Mail-Programm nur einen Namen und nicht die eigentliche Adresse anzeigt, hilft oft ein Rechtsklick auf den Absender, um die vollständige Adresse anzeigen zu lassen.
„Wenn in einer Mail steht, dass Sie wieder einen Millionenbetrag gewonnen haben, dann freuen Sie sich nicht über den Gewinn, sondern löschen das einfach", sagt Jens Ernst. Besonders in der Eile des Arbeitsalltags werden gefährliche Anhänge aber leichter übersehen, warnt er: „Hektik und Stress führen zu einer um 80 Prozent höheren Fehlerquote."
Eine andere Angriffsmethode sind Links in E-Mails oder heruntergeladenen Dokumenten, welche die Opfer auf Websites führen, die von den Angreifern kontrolliert werden. Entweder werden sie auf den oft täuschend echt aussehenden Seiten aufgefordert, persönliche Daten einzugeben, oder die Seite lädt heimlich Schadsoftware auf ihren Rechner. Gegen solche Angriffe hilft eine praktische Funktion, die fast alle Programme anbieten: Statt einfach mit einem Klick den Link zu öffnen, fahren Sie zuerst mit der Maus nur über den Link oder klicken mit der rechten Maustaste darauf. Dann wird Ihnen die Website angezeigt, zu der dieser Link führt. Wenn diese verdächtig ist, sollten Sie den Link in keinem Fall anklicken.
IT-Fachmann Ernst empfiehlt außerdem die Seite https://www.virustotal.com/. Hier lassen sich Anhänge und Links online darauf überprüfen, ob sie einen Virus auf Ihren Rechner spielen könnten.



Eine vermeintlich harmlose E-Mail kann enormen Schaden anrichten.

FIREWALL: WAS DAS BSI EMPFIEHLT

Zu jeder TI gehört auch eine Firewall, die vor Angriffen schützen soll. Doch eine Firewall bietet nur dann Schutz, wenn sie auch richtig installiert wird. Jens Ernst empfiehlt, die Firewall immer mit der Einstellung „All Deny" zu installieren. Auch das Bundesamt für Sicherheit in der Informationstechnologie (BSI) empfiehlt diese Einstellung. Sie bedeutet, dass alle Ports und Adressen, über die eine Verbindung aus dem Praxisnetz nach außen hergestellt werden könnte, erst einmal geschlossen sind.
Kein Gerät oder Computer kann sich jetzt mit dem Internet verbinden. Dann fügen die IT-Techniker Ausnahmegenehmigungen für alle für den Praxis-

betrieb notwendigen Komponenten hinzu, die sich mit dem Internet verbinden müssen. Das Lesegerät für die Gesundheitskarten bekommt dann genauso einen eigenen Zugang zur Außenwelt freigeschaltet wie die Abrechnungssoftware oder andere Geräte wie Röntgen oder Sonor.
Die Unternehmen, die die TI anschließen, konfigurieren die Firewall offenbar eher selten nach diesem Modell. Das zumindest ist die Erfahrung von Jens Ernst: „Ich habe noch nie in einer Praxis eine von einem TI-Dienstleistungsunternehmen eingerichtete Firewall gesehen, die auf All Deny konfiguriert war." Es habe durchaus schon Fälle gegeben, in denen zumindest ein Großteil der Verbindungen durch die Firewall geblockt wurde. Allerdings habe er auch Fälle gesehen, in denen sogar der häufig für das unbefugte Ausleiten von Daten genutzte Port 449 geöffnet war.

KONNEKTOR: DAS PASSWORT GEHÖRT IHNEN!

Ernst empfiehlt Ärzten daher, nach der Installation der TI, die Einstellungen der Firewall genau zu überprüfen. Das jedoch ist nicht immer ohne weiteres möglich: So berichteten ihm Ärzte, dass die TI-Dienstleister ihnen nicht immer die dafür notwendigen Passwörter überlassen hätten. Jeder Zahnarzt und jede Zahnärztin sollte nach der Installation im Besitz des Passworts für die Firewall und der beiden wichtigen Passwörter für den Konnektor sein. Hier gibt es sowohl ein Admin- als auch ein Praxis-Passwort. Mit Hilfe dieser Passwörter kann man überprüfen, ob die Firewall wirklich nur die notwendigen Verbindungen zulässt. „Die Ärzte haben die Geräte gekauft und sind Eigentümer der Geräte", sagt Ernst. „Sie haften auch für die Einstellungen in den Geräten. Darum müssen sie die Einstellungen auch kontrollieren."
Eine wichtige Entscheidung, vor der Zahnärzte beim Betrieb der TI stehen, ist die Frage, ob sie ihr Praxisnetzwerk parallel oder seriell anschließen lassen. Im seriellen Betrieb, der auch als Reihenbetrieb bezeichnet wird, wird der Konnektor direkt hinter dem Router, der die Praxis mit dem Internet verbindet, angeschlossen. Erst danach folgen in dieser Reihe alle anderen Geräte der Praxis, was dazu führt, dass die Daten aller Geräte der Praxis stets durch den Konnektor fließen, der dadurch auch als Firewall fungiert.
Im Parallelbetrieb sind parallel zum Konnektor noch Computer der Praxis direkt mit dem Router und somit mit dem Internet verbunden. Dieser parallele Zugang ist zwar leichter anzuschließen für die IT-Dienstleister, kann aber zu einem höheren Sicherheitsrisiko führen, da ein Praxisrechner schlechter geschützt mit dem Netz verbunden ist.

GEMATIK IN DER VERANTWORTUNG

FVDZ-Bundesvorstand drs. (NL) Hub van Rijt kritisiert, dass die Ärzte mit der Haftung für die Sicherheitsrisiken weitgehend alleine gelassen werden. „Das Problem ist: Ich kriege eine Box hingestellt, ich weiß nicht genau, was das ist, und ich kann da nicht ran, aber trotzdem muss ich dafür haften", sagt van Rijt. „Die Gematik sollte auch hier die Verantwortung übernehmen und die Haftung übernehmen." Ein weiterer

Schwachpunkt sei, dass es bisher keine Zertifizierung der Dienstleister durch das Gesundheitsministerium gibt. „Das Problem ist: Sie müssen sich als Arzt auf die IT-Fachleute verlassen." Doch dieser Schritt sei durch den Zeitdruck durch den Bundesgesundheitsminister hintenangestellt worden. Aufgrund der Sicherheitsrisiken plädiert van Rijt dafür, dass es Zahnärzten weiterhin erlaubt sein sollte, auch ohne Konnektor abzurechnen. „Es sollte zumindest möglich sein, weiterhin auch per CD oder per Stick oder auf Papier seine Abrechnungen zu machen. Meinetwegen kann man dafür einen gewissen Mehrpreis zahlen, aber es muss zumindest eine Option sein."

GUT ZU WISSEN

Auf der Seite https://www.virustotal.com/ kann man Mail-Anhänge und Links online darauf überprüfen, ob sie einen Virus auf ihren Rechner spielen könnten.

Die Gematik hat auf ihrer Webseite unter anderem eine „Checkliste Zahnarztpraxis" zur Installation der TI: http://bit.ly/2YHN9GB

In der *ZDF*-Doku „Der Gläserne Patient" führt Jens Ernst vor, wie eine Attacke mit Schadsoftware abläuft: https://www.zdf.de/dokumentation/zdfzoom/zdfzoom-der-glaeserne-patient---daten-in-gefahr-100.html

„Manche Praxen wurden schlecht beraten“

ABC der IT-Sicherheit. Prof. Dr. Harald Mathis von der Hochschule Hamm-Lippstadt ist Leiter des Fraunhofer-Anwendungszentrums SYMILA (wo er unter anderem zu Biomikrosystemtechnik forscht) und spricht über sichere Passwörter, wackelige Betriebssysteme und wie man einen seriösen IT-Dienstleister findet.

INTERVIEW: MAX HOPPENSTEDT

Was sollte ein Arzt tun, wenn er wissen will, ob seine Praxis vor Hacker-Angriffen sicher ist, nachdem sie an die Telematikinfrastruktur (TI) angeschlossen wurde?

Harald Mathis: Die Ärzte sollten zunächst einmal drei Dinge prüfen: ob ihre Firewall richtig funktioniert, ob ihr Viren-Scanner eingeschaltet ist, und ob das gesamte Personal in Sachen Datenschutz und Datensicherheit gut geschult ist.

Warum muss das Personal in einer Arztpraxis denn auch über Computerfähigkeiten verfügen? Was müssen die Mitarbeiter wissen?

Das größte Einfallstor für die meisten wirklich ernsten Sicherheitsvorfälle sind menschliche Fehler. Daher ist es so wichtig, dass jeder in der Praxis sich um Datensicherheit Gedanken macht. Sonst besteht die Gefahr, dass Mitarbeiter auf falsche Links in Phishing-Mails klicken und so Schadsoftware auf einen Praxiscomputer laden. Eine andere Gefahr ist, dass sich Praxismitarbeiter verquatschen und sensible Zugänge versehentlich verraten oder dass Mitarbeiter Zettel mit Passwörtern rumliegen lassen. Ich habe auch schon Praxen gesehen, die gar kein Passwort für ihren Computer haben.

Wie bitte? Sie meinen, der gesamte Rechner war gar nicht mit einem Kennwort geschützt?

Genau, sie haben den Computer angeschaltet, er ist hochgefahren, und schon erschien vor ihnen auf dem Bildschirm der Desktop. Normalerweise sollte jeder Rechner so eingestellt sein, dass Sie sich vorher mit einem Passwort anmelden müssen.

Worauf muss man denn achten, dass solch ein Passwort auch sicher ist?

Ein sicheres Passwort besteht nicht aus einem im Lexikon stehenden Begriff. Es darf auch nichts Naheliegendes sein, was man als Angreifer leicht erraten kann. Ein Passwort sollte

EIN PASSWORT NICHT IM LEXIKON SUCHEN

immer Sonderzeichen und Groß- und Kleinschreibung enthalten und mindestens acht Zeichen lang sein.

Sie haben gesagt, Ärzte und Mitarbeiter sollten sich in Sachen Datensicherheit weiterbilden. Welche Institutionen können Sie empfehlen? Worauf sollten Ärzte achten, wenn sie ihre Mitarbeiter schulen wollen?

Ärzte sollten sich für solche Schulungen an renommierte Institutionen und Schulen wenden. Man könnte in Zukunft auch mit Handbüchern arbeiten, die bei einer Sicherheitsschulung erstellt werden. Auch eLearning-Kurse wären für die Zukunft sicher eine gute Option.

Sie haben sich in 30 Arztpraxen angeschaut, wie gut geschützt diese sind, nachdem sie an die TI angeschlossen wurden. Dabei haben Sie festgestellt, dass ein Drittel der Praxen nicht sicher war. Sie haben auch davon gesprochen, dass einige Praxen in einem „beklagenswerten Zustand" seien. Was meinen Sie damit genau?

Damit meine ich, dass Praxen teilweise gar keine Firewall hatten oder dass der Viren-Scanner total veraltet oder dass das Betriebssystem extrem rückständig war. Ich habe Praxen mit Windows XP gesehen, und für das neuere Windows 7 läuft ja schon bald der offizielle Support von Microsoft aus. All sowas können erhebliche Sicherheitsrisiken sein. In einem Fall habe ich auf meine Nachfrage, ob der Viren-Scanner denn korrekt funktioniert als Antwort zu hören bekommen: Ach, wir haben überhaupt einen Viren-Scanner? Man muss allerdings auch dazu sagen, dass unsere Untersuchung der 30 Arztpraxen kein wissenschaftlich repräsentatives Bild sein kann. Dafür ist die Stichprobe viel zu klein.

Was würden Sie nach Ihren Einblicken in den Praxen sagen, wo genau das Problem liegt? Ist das TI-System grundsätzlich unsicher?

Ganz klar nein. Wir haben ja auch viele Praxen gesehen, in denen alles sicher und richtig angeschlossen war. Es geht bei der Debatte um die Sicherheit der TI-Systeme nicht nur darum, wie gut die Software oder Hardware ist, sondern auch darum, dass einige Ärzte sich nicht um das Thema Datensicherheit und Datenschutz gekümmert haben. Und es gibt auch Ärzte, die bei der Installation der TI und beim Schutz ihrer Praxis auf Dienstleister vertraut haben, die offensichtlich nicht gut gearbeitet haben. Ich habe zwar auch Praxen vorgefunden, bei denen externe Dienstleister sich um die Anschlüsse gekümmert haben und bei denen alles mustergültig funktioniert hat. Aber offenbar muss man auch konstatieren, dass unter den 30 von uns untersuchten Praxen auch viele darunter waren, die laut eigenem Bekunden nicht gut beraten wurden.

Woran erkenne ich als Arzt denn, welcher Dienstleister vertrauenswürdig ist und welcher nicht? Wie finde ich einen seriösen IT-Experten?

Normalerweise würde ich sagen, durch eine Zertifizierung der IT-Experten. Diese gibt es in entsprechender Form aber bislang kaum. Ich würde daher empfehlen, mir Rezensionen über die IT-Dienstleister im Netz anzuschauen und mir von den Unternehmen Referenzkunden nennen zu lassen. So etwas schafft Vertrauen.

Sollten sich Praxen im Parallelbetrieb oder seriell anschließen lassen?

Da kann man nichts eindeutig empfehlen. Im Zweifelsfall kann der serielle Anschluss aber sicherer sein, beziehungsweise er bietet weniger Gefahren für eine fehlerhafte Installation.

Was ist denn das Problem am Parallelbetrieb?

Da besteht die Gefahr, dass ich zusätzlich einen unsicheren Rechner angeschlossen habe. Im Zweifelsfall ist es ideal, überhaupt keinen Rechner im Internet anzuschließen.

Sollten Ärzte wirklich versuchen, in ihrer Praxis überhaupt gar keinen Rechner mit dem Internet zu verbinden, auf dem sensible Patientendaten und die Daten aus dem PVS sind?

Ja, das ist definitiv eine besonders sichere Option. Man kann auch die Rechner, die mit dem Internet verbunden sind und die Rechner mit den Patientendaten strikt voneinander trennen.

Würden Sie sagen, dass das Gesundheitsministerium das Ganze übereilt gemacht hat?

Das Gesundheitsministerium kann nicht alle Arztpraxen überprüfen. Wir haben 1,5 Milliarden Euro in die TI investiert, und ich finde es gut, die Digitalisierung im Gesundheitswesen voranzutreiben. Wir dürfen auch die vielen positiven Möglichkeiten dieser neuen Technik nicht vergessen. Wir müssen nun dafür sorgen, dass das System sicher eingeführt wird. Ich kann aber auch die Ärzte verstehen. Sie sind keine gelernten Informatiker, auch wenn einige von denen, die ich getroffen habe, durchaus IT-affin sind. Ich habe bei den 30 Praxen und den Ärzten, mit denen ich gesprochen habe, auch keinen erlebt, der das Thema nicht ernst genommen hat und sich nicht hat beraten lassen. Ich konnte bei meinen Beobachtungen auch keine allgemeine, pauschale TI-Skepsis feststellen. Ich weiß nicht, ob es ohne die Berichterstattung der letzten Monate ein solches Bewusstsein dafür gäbe, wie wichtig die IT-Sicherheit ist. Daher ist es gut, die Ärzte weiter darüber aufzuklären, was schieflaufen kann, und ihnen dann möglichst gute Hilfestellung und Beratung zur Seite zu stellen.

Beschneidung persönlicher Freiheitsrechte

Digitale Versorgung-Gesetz. Am 7. November 2019 wurde mit den Stimmen der Großen Koalition in 3. Lesung das Digitale Versorgung-Gesetz (DVG) mit den vom Gesundheitsausschuss vorgeschlagenen Änderungen (BT-Drs.: 19/14867) angenommen. Für die Zahnärzteschaft werden relevante gesetzliche Regelungen erläutert.

AUTOREN: RA MICHAEL LENNARTZ, RA MANFRED WEIGT
(EXTERNER ZERTIFIZIERTER DATENSCHUTZBEAUFTRAGTER)

Ziel des Gesetzes ist nach dem Gesetzentwurf und den Ausführungen von Bundesgesundheitsminister Jens Spahn, insbesondere die Digitalisierung im Gesundheitswesen voranzubringen. Um dieses Ziel zu erreichen enthält das Gesetz bereits einen wesentlichen Teil erforderlicher Regelungen. Da bereits das nächste Gesetz „DVG II" in der Pipeline ist und Anfang 2020 kommen soll (unter anderem mit Regelungen zur elektronischen Patientenakte), sind die Regelungen wohl nicht abschließend.

GESUNDHEITSAPPS

Gesetzlich versicherte Patienten haben Anspruch auf digitale Gesundheitsanwendungen, die dazu bestimmt sind, Krankheiten zu erkennen, zu überwachen, zu behandeln oder zu lindern oder auf digitale Gesundheitsanwendungen, die die Kompensation von Verletzungen oder Behinderungen unterstützen können (§ 33a SGB V).
Die digitalen Gesundheitsanwendungen können bei Nachweis medizinischer Indikation auch von Zahnärztinnen und Zahnärzten verordnet werden. Übersteigen die Kosten die festgelegten Vergütungsbeträge, müssen diese vom Versicherten selbst getragen werden.

VERZEICHNIS DIGITALER GESUNDHEITSANWENDUNGEN

Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) hat ein Verzeichnis entsprechender digitaler Gesundheitsanwendungen zu führen (§ 139e SGB V). Um in dieses Verzeichnis aufgenommen zu werden, hat der Hersteller bei der Beantragung der Aufnahme den Nachweis über Sicherheit, Funktionstauglichkeit, Qualität der Anwendung, Anforderungen des Datenschutzes und der Datensicherheit sowie positive Versorgungseffekte zu erbringen. Ist dem Hersteller der Nachweis

PATIENTEN DER GKV HABEN ANSPRUCH AUF DIGITALE ANWENDUNGEN

positiver Versorgungseffekte nicht möglich, kann er die Aufnahme in das Verzeichnis für bis zu zwölf Monate zur Erprobung beantragen.
Auch Krankenkassen sind befugt, Verträge mit den Herstellern von Gesundheitsapps zu schließen. Grundsätzlich ist vorgesehen, dass der GKV-Spitzenverband mit Wirkung für alle Krankenkassen mit den Herstellern von digitalen Gesundheitsanwendungen Vergütungsbeträge vereinbart. Verhandlungen und die Vorbereitung von Niederschriften hierüber sind dabei vertraulich (§ 134 SGB V).

TELEKONSILE UND VIDEOSPRECHSTUNDE

Im BMV-Z ist zu regeln, dass Konsilien in einem weiten Umfang in der vertragszahnärztlichen und in der sektorenübergreifenden Versorgung als telemedizinische Leistungen abgerechnet werden können, wenn bei ihnen sichere elektronische Informations- und Kommunikationstechnologien eingesetzt werden (§ 87 Abs. 2 SGB V). Die KBV/KZBV und der GKV-Spitzenverband haben ein Verfahren zur Authentifizierung, das im Rahmen der Videosprechstunde genutzt wird, festzulegen und zu vereinbaren (§ 291g SGB V).

INNOVATIONSFOND, FÖRDERUNG VON VERSORGUNGSINNOVATIONEN UND INVESTMENTVERMÖGEN

Krankenkassen bekommen die Möglichkeit, mit Herstellern von Medizinprodukten, Unternehmen aus dem Bereich der Informationstechnologie, Forschungseinrichtungen und Leistungserbringern sowie deren Gemeinschaften Modelle zur Verbesserung der Qualität und Wirtschaftlichkeit der Versorgung (Innovationsfond, § 68a SGB V) zu entwickeln. Zudem können Krankenkassen Versorgungsinnovationen fördern, soweit die Daten rechtmäßig erhoben und gespeichert wurden (§ 68b SGB V). Hier erfolgt der Rückgriff auf Abrechnungsdaten (§ 284 SGB V).

Für die Förderung der neuen Versorgungsformen und -forschung stehen von 2020 bis 2024 je 200 Millionen Euro zur Verfügung. Dabei ist für die Datenauswertung Pseudonymisierung ausreichend.

Für diese Förderung der neuen Versorgungsformen und -forschung stehen von 2020 bis 2024 je 200 Millionen Euro zur Verfügung. Dabei ist für die Datenauswertung eine Pseudonymisierung ausreichend. Eine Anonymisierung ist angeordnet, wenn die Auswertung auch mit anonymisierten Daten erfolgen kann. Individuelle Information können an den Versicherten gegeben werden, wenn dieser schriftlich oder elektronisch eingewilligt hat. Hierbei ist der Widerruf durch den Versicherten jederzeit möglich. Zudem können die Krankenkassen bis zu 2 % ihrer Finanzreserve zur Förderung der Entwicklung digitaler Innovationen anlegen (Investmentvermögen; § 263 SGB V).

TI-NUTZUNGSVERPFLICHTUNG, VERZEICHNISDIENST

Die TI muss für digitale Vordrucke genutzt werden, sobald diese zur Verfügung stehen (§ 87 SGB V). Zudem hat die Gesellschaft für Telematik einen elektronischen Verzeichnisdienst einzurichten (§ 75b SGB V). Dabei kann diese Aufgabe an Dritte delegiert werden. In diesem Verzeichnis werden Daten für die Suche, Identifikation und Adressierung von Leistungserbringern, organisatorischen Einheiten von Leistungserbringern oder anderen, die die Telematikinfrastruktur nutzen, gesammelt. Daten von Versicherten sollen nicht gesammelt werden.

RICHTLINIEN ZUR IT-SICHERHEIT UND SANKTION

Bis zum 20.6.2020 sind Richtlinien von der KBV/KZBV zur IT-Sicherheit festzulegen (§ 75b SGB V). Die Richtlinie hat auch Anforderungen an die sichere Installation und Wartung von Komponenten und Diensten der TI zu enthal-

ten und ist jährlich anzupassen. Wird die TI nicht eingeführt, erfolgt eine Kürzung der Vergütung ab dem 1. März 2020 um 2,5 Prozent (§ 291 Absatz 2b SGB V).

Haftung

Für die Frage der Haftung ist bei der TI wesentlich zu klären, wer Verantwortlicher im Sinn des Datenschutzes für die entsprechende Datenverarbeitung ist. Der Bundesdatenschutzbeauftragte stellt hierzu in seinem Tätigkeitsbericht zum Datenschutz 2017/2018 fest, dass die Frage, wer Verantwortlicher für die TI ist, noch nicht endgültig geklärt werden konnte.
Auch durch das DVG wird bezüglich der Haftungsfrage keine Klarheit geschaffen, sodass vorerst auf die Sichtweise der DSGVO und des Europäischen Gerichtshofes (EuGH) zurückzugreifen ist. Verantwortlicher ist demnach derjenige, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO). In seinem (ähnlich gelagerten) Urteil vom 5. Juni 2018 (Aktenzeichen C 210/16) hat der EuGH in Bezug auf Facebook-Fanpages festgestellt, dass dort eine gemeinsame Verantwortung von Facebook und dem Fanseitenbetreiber vorliegt. Daher ist nicht auszuschließen, dass bei der TI trotz gesetzlicher Anbindungsverpflichtung eine Mitverantwortung der Zahnärztin und des Zahnarztes statuiert wird, soweit es sich um die Datenverarbeitung mittels TI in der Praxis handelt (etwa das Einlesen der Gesundheitsdaten). Wenn aber die Daten über den Konnektor die Praxis verlassen und sich nicht mehr im Einflussbereich des Behandlers befinden, sollte dessen datenschutzrechtliche Verantwortlichkeit für die weitere Verarbeitung im Rahmen der TI nicht mehr gegeben sein.
Hierzu bleibt aber eine Entscheidung der zuständigen Gerichte oder eine entsprechende Stellungnahme der Datenschutzbehörden abzuwarten. Möglich ist auch, dass die Zahnärztinnen und Zahnärzte lediglich als datenschutzrechtliche Auftragsverarbeiter für die Gematik gesehen werden, da sie gerade keine Kompetenz haben, über die Zwecke der Verarbeitung zu entscheiden, sondern lediglich dazu verpflichtet sind, die Gesundheitsdaten im Auftrag der Gematik einzulesen.

DATENVERARBEITUNG, DATENZUSAMMENFÜHRUNG UND -ÜBERMITTLUNG

Die Krankenkassen haben an den GKV-Spitzenverband mit einem Versichertenpseudonym versehene Daten, auch solche über abgerechnete Leistungen, zu übermitteln (303b SGB V). Eine Vertrauensstelle ist dabei, quasi datentreuhänderisch zuständig für ein Verfahren zur Pseudonymisierung (§ 303c SGB V).

Durch Datentransfer wird umfangreichen Datensammlungen mit Analysen Tür und Tor geöffnet. Das birgt große Gefahren.

ELEKTRONISCHES REZEPT

Bis 31.03.2020 müssen notwendige Regelungen für die Verwendung von elektronischen Verordnungen durch KBV/KZBV und dem Spitzenverband der Krankenkassen erlassen werden (§ 86 SGB V).

BEWERTUNG

Sicherlich ist das Ansinnen legitim, die Digitalisierung voranzutreiben. Daten in sozialen Medien (Facebook, Twitter und Co) werden freiwillig preisgegeben. Bei den Daten beispielsweise im Rahmen der Gesundheitsapps handelt es sich regelmäßig um besonders sensible Gesundheitsdaten, die preisgegeben werden. Insbesondere ist mit der Datenübermittlung und den Handlungsoptionen (zum Beispiel Zuordnung zum versicherten Mitglied) Tür und Tor für umfangreiche Datensammlungen mit Analysen geöffnet. Damit ist die konkrete Gefahr verbunden, dass der Patient nicht mehr Souverän seiner Daten bleibt. Damit bleibt die Gefährdung des Datenschutzes ein Hauptkritikpunkt in der Welt der digitalen Gesundheitsanwendungen. Es bleibt die Chance des Gesetzgebers, mit den geplanten neuen Regelungen (DVG II) auch die Haftungssituation im Fall der TI klar und eindeutig zu regeln.
Zudem wird hier beispielsweise mit IT-Richtlinien, Verzeichnisdiensten et cetera ganz neue Bürokratie geschaffen. Man könnte es zum Beispiel bei den umfassenden Verpflichtungen der DSGVO belassen und Ausführungen zu umfassenden technischen und organisatorische Maßnahmen zur Einhaltung des Datenschutzes in den Praxen verlangen. Auf Sanktionen wie bei der TI-Anwendung zu setzen, wird die Akzeptanz der Digitalisierung mit Sicherheit nicht erhöhen.

„Größte Gefahr geht von Benutzern aus“

TI-Anschluss: Horror oder Panikmache? Es gibt zahlreiche Meldungen über angeblich desaströse Zustände bei der TI-Installation in Arzt- und Zahnarztpraxen. Bei inzwischen über 100.000 Installationen unter Zeitdruck ist es nicht verwunderlich, dass auch mal Probleme auftreten. Für Außenstehende ist kaum zu beurteilen, ob es sich um vermeidbare Einzelfälle oder ein strukturelles Defizit handelt. Der *DFZ* hat mit dem Zahnarzt Dr. Holger Neumeyer gesprochen, der zugleich Anwender und Einrichter ist, weil er als lizenzierter Fachmann Konnektoren und Lesegeräte installiert und Praxen mit der TI verbunden hat.

INTERVIEW: DR. JOACHIM HÜTTMANN

DFZ: Herr Dr. Neumeyer, Sie sind Zahnarzt in Schleswig-Holstein, haben aber gleichzeitig in vielen Praxen als Dienstleister vor Ort (DvO) – wie es bei der Gematik heißt – die Installation der Telematik-Infrastruktur durchgeführt. Wie kam es dazu?

Dr. Neumeyer: Es gibt in Schleswig-Holstein seit 1999 eine körperschaftsunabhängige Organisation mit etwa 1.200 Mitgliedern, die Vertragsgemeinschaft freiberuflicher Zahnärztinnen und Zahnärzte, kurz VgfZ, deren Vorstand ich angehöre. Als es 2017 ernst wurde mit der TI und die technischen Rahmenbedingungen, die Anbieter, deren Preise und die Erstattungsbeträge der Krankenkassen bekannt wurden, haben wir beschlossen, mit Anbietern Kontakt aufzunehmen, um für unsere Mitglieder Sonderkonditionen zu erreichen. Unsere gemeinsamen Absichten wurden allerdings dadurch torpediert, dass die Gematik erst im Herbst 2018 und damit ein Jahr nach der ersten Zulassung eines Konnektors weitere Konnektoren zugelassen und damit Wettbewerb ermöglicht hat. Ich hatte mich während dieser Zeit intensiv mit der technischen Seite beschäftigt und dann auch in meiner Praxis die Installation selbst durchgeführt. Als ich darüber in der Bezirksgruppe und im Kreisverein berichtete, baten mich andere Praxen, auch bei ihnen die Installation der TI zu erledigen.

DAS THEMA SICHERHEIT NICHT VERNACHLÄSSIGT

Dann haben Sie auch einen guten Einblick in die EDV-Strukturen von Zahnarztpraxen erhalten. Man liest immer wieder von mangelnden Sicherheitsvorkehrungen der Praxis-EDV. Wie sind Ihre Erfahrungen?

Ich habe keine einzige Praxis getroffen, in der das Thema Sicherheit vernachlässigt worden wäre. Die meisten Praxen beschäftigen einen externen Administrator, der das Praxisnetzwerk konfiguriert und die erforderlichen

Sicherheitsstandards implementiert hat. In einigen Praxen sind die Praxisinhaber aufgrund eigenen EDV-Wissens selbst die Administratoren. Auch wenn die Hardware-Ausstattung der Praxen völlig unterschiedlich ist, sorgen die verwendeten modernen Router wie etwa die FritzBox bereits für eine sehr hohe Sicherheit. In allen Praxen kam zusätzlich eine aktuelle, softwarebasierte Firewall inklusive Virenschutz zum Einsatz. In einigen Praxen wurde sogar eine Hardware-Firewall eingesetzt.

Die Konnektoren und Lesegeräte sollen in den meisten Fällen von den DvOs ohne Rücksprache mit dem Praxisinhaber im sogenannten Parallelmodus installiert worden sein, obwohl es die Möglichkeit gibt, den Konnektor selbst als Firewall zu nutzen. Was sagen Sie dazu?

Wie dargelegt, sind die meisten Praxisnetzwerke durch entsprechende Konfiguration bereits auf einem sehr hohen Sicherheitslevel. Deshalb spricht überhaupt nichts dagegen, Konnektor und Kartenterminal durch Parallelinstallation in ein solchermaßen abgesichertes Netzwerk als weitere Komponenten hinzuzufügen. Anders verhält es sich mit Praxen, die bisher ihren Praxisrechner überhaupt nicht mit dem Internet verbunden hatten. Wenn der Praxisinhaber dies auch weiterhin so belassen will, ist es sinnvoll, die serielle Installation vorzunehmen. Das bedeutet, der gesamte Datenverkehr wird über den Konnektor geleitet, und die Firewall des Konnektors übernimmt den Schutz der Praxis-EDV.

In einigen Fällen sollen DvOs einfach vorhandene Firewalls ausgeschaltet haben, weil die Installation dann einfacher ist. Stimmt das?

Davon habe ich auch gehört. Hier stoßen wir auf ein Problem, das ganz offensichtlich viel mit dem Zeitdruck zu tun hat, den der Gesetzgeber durch einen viel zu engen Zeitrahmen in Kombination mit der Androhung von Strafmaßnahmen gegen die Ärzteschaft verursacht hat. Woher soll denn die benötigte Anzahl qualifizierter DvOs kommen, wenn innerhalb kürzester Zeit weit über 100.000 Institutionen an die TI angeschlossen werden sollen? Verschärfend kommt hinzu, dass die DvOs von den Anbietern der Konnektoren mit einer Zeitvorgabe von zwei Stunden pro Praxis losgeschickt wurden. Da scheint es für den einen oder anderen Installierenden einfacher gewesen zu sein, eine Firewall einfach auszuschalten, anstatt mit dem IT-Administrator der Praxis Kontakt aufzunehmen und gemeinsam mit diesem gegebenenfalls die für die Funktionsfähigkeit des Konnektors benötigten Ports freizuschalten. Aber dies sind nur Mutmaßungen. Die Kolleginnen und Kollegen in deren Praxen ich installiert habe, wussten es jedenfalls sehr zu schätzen, keinen Wildfremden an ihre Praxis-EDV lassen zu müssen. Gesetzgeber und Gematik haben in vielen Punkten die Sensibilität der Praxen mit Füßen getreten und wundern sich nun über mangelnde Akzeptanz.

Dann liefen die Installationen insgesamt wohl ziemlich reibungslos?

Für alle Beteiligten war die TI-Installation Neuland. Es gab unzählige theoretische Testläufe und Simulationen, aber Erfahrungen mit Installationen im realen Praxisleben hatte keiner. Wie Sie wissen, ist jede Praxis ein Individualbetrieb. Dementsprechend gab es in jeder Praxis ganz eigene Herausforderungen. Sei es die zu bestimmten Zeiten aktive Kindersicherung, die die Internetnutzung durch Mitarbeiterinnen reguliert, aber dann eben auch die VPN-Verbindung des Konnektors einfach ausschaltet. Natürlich hatten die Hersteller der Konnektoren versucht, alle Fallstricke vorher zu bedenken. In der realen Installationssituation tauchten aber anfangs dann teilweise doch erhebliche Probleme auf. Das betraf auch das Zusammenspiel zwischen der TI und den Praxisverwaltungssystemen. Hier mussten einige Softwarehäuser kräftig nacharbeiten. Inzwischen laufen die Systeme sehr zuverlässig.

Hat sich aus Ihrer Sicht durch die TI der Gematik das Sicherheitsrisiko für die Praxen erhöht?

Praxisnetzwerke, die bisher ausreichend geschützt gewesen waren, sind durch die Implementierung der TI nicht unsicherer geworden. Die größte Gefahr für die Sicherheit der Praxissysteme geht weiterhin von den befugten Benutzern selbst aus, also „menschliches Versagen“. Kriminelle nutzen immer wieder typische menschliche Schwächen aus. E-Mails werden mit Viren, Trojanern und anderen Scheußlichkeiten gespickt und der Empfänger durch verführerische Betreffzeilen, verlockende Angebote oder vermeintlich

harmlose Anhänge zum Öffnen von Phishing-Webseiten oder infizierten Anhängen verleitet. Hier gilt es, wachsam zu sein und auch das Praxispersonal immer wieder zu sensibilisieren. Besser noch ist es, den Mailverkehr über einen gesonderten Rechner laufen zu lassen, der in keiner Verbindung zum Praxisrechner steht. Das ist dann zwar unbequemer, aber eben deutlich sicherer. Den gezielten Hackerangriff auf eine einzelne Zahnarztpraxis zum Erbeuten von Daten wird es wohl eher nicht geben. Dazu sind die Daten in einer normalen Zahnarztpraxis einfach zu uninteressant. Es sind vielmehr die üblichen Erpressungsmethoden, die die Praxen bedrohen.

Die Kosten der TI-Erstausstattung sollten von den Krankenkassen mittels Pauschalen erstattet werden. Ist die Implementierung der Telematikinfrastruktur also für die Praxen kostenneutral gewesen?

Schön wär's! In der Realität lagen die Preise für Konnektor, Lesegerät und Installation von Beginn an exakt auf der Höhe der Erstattungspauschalen. Anders ausgedrückt: Das Geld der Krankenkassen wurde via KZV und Zahnarzt direkt an die Hersteller durchgeleitet. Für notwendige Hardware- und Softwareergänzungen an den bestehenden Praxisnetzwerken als Voraussetzung für die TI-Installation mussten die Praxen ganz allein aufkommen. Und dann muss jedem klar sein, dass sich diese Förderung auf die Erstausstattung der Praxen bezogen hat. Von einer Übernahme der Folgekosten ist nirgends die Rede. Dabei ist im TI-System aufgrund von Vorgaben durch das BSI eine maximale Nutzungszeit oder Haltbarkeit der Hardware von fünf Jahren fest verankert. Die in den Geräten verwendeten Sicherheitszertifikate laufen automatisch nach dieser Zeit ab. So ist das Sicherheitszertifikat im Konnektor in Form einer gSMC-K fest verbaut. Die Praxis SMC-B und die SMC-KT des Kartenterminals sind – zumindest theoretisch – auswechselbar. Bedenkt man, dass die ersten Konnektoren 2017 in Betrieb gingen, muss man kein Hellseher sein, um zu wissen, was ab 2022 passieren wird. Die Sicherheitszertifikate laufen von einem Tag auf den anderen ab, und aus ist es mit der Online-Anbindung der Praxis. Es sei denn, die Praxen schaffen rechtzeitig und definitiv auf eigene Kosten neue Hardware an. Dabei wird der Gesetzgeber mit neuen Sanktionsdrohungen sicherlich gern behilflich sein. Die Praxen haben ein solches Szenario mit den Lesegeräten bei der Ersteinführung der eGK ab 2004 schließlich genauso schon erlebt. Als die Geräte nach einigen Jahren kaputtgingen, mussten die Praxen auf eigene Rechnung neue Geräte anschaffen. Bei der TI ist jedenfalls „kaputt" schon fest eingebaut.

Den gezielten Hackerangriff auf eine einzelne Zahnarztpraxis zum Erbeuten von Daten wird es eher nicht geben. Dazu sind die Daten in einer normalen Zahnarztpraxis zu uninteressant. Es sind vielmehr die üblichen Erpressungsmethoden, die die Praxen bedrohen.

Sehen Sie als Zahnarzt denn wenigstens einen klaren Nutzen für die Praxen durch die TI-Anbindung?

Dieses gigantische Projekt hat bisher für die Zahnarztpraxis, man muss es so deutlich sagen, keinerlei Nutzen gebracht. Die einzige bis heute implementierte Anwendung ist der sogenannte Online-Stammdatenabgleich. Der ist für die Zahnarztpraxis selbst weitestgehend uninteressant, denn den Nutzen haben ausschließlich die Krankenkassen, die die eGK ihrer Versicherten mit Hilfe unserer Praxen aktualisieren oder ungültige Karten sperren können. Von den weiteren angekündigten Anwendungen der TI ist die Funktion „KOM-LE", also die „Kommunikation der Leistungserbringer" für die Zahnarztpraxis die einzig sinnvolle Erweiterung. Diese soll eine gesicherte Kommunikation aller Leistungserbringer im Gesundheitswesen untereinander ermöglichen. Das wäre ein Gewinn für unsere Praxen. Damit stünde eine sichere Möglichkeit zum elektronischen Versand von Arzt- oder Patientenbriefen und Röntgenbildern zur Verfügung.

Herr Dr. Neumeyer, wir danken Ihnen für dieses Gespräch.