Bleibtreustraße 24
10707 Berlin (Deutschland)
Telefon (030) 887 086-36
Telefax (030) 887 086-37

E-Mail info@medi-geno-deutschland.de
www.medi-geno-deutschland.de

MEDI GENO Deutschland e.V. ● Bleibtreustr. 24 ● 10707 Berlin

Kassenärztliche Bundesvereinigung
Herrn
Dr. Thomas Kriedel
Mitglied des Vorstandes
Herbert-Lewin-Platz 2
10623 Berlin

Berlin, 21. März 2019

Weitere offene Fragen zum TI-Konnektor – Kostenerstattung, Haftung und Sicherheit

Sehr geehrter Herr Dr. Kriedel,

da in der Berichterstattung bezüglich unserer Diskussion in der KBV-Vertreterversammlung am Freitag der Eindruck entstanden ist, dass Sie meine Einwände zum TI-Konnektor beantwortet oder entkräftet hätten, antworte ich heute mit einem Brief, den wir auf unserer Webseite veröffentlichen.

Ich möchte vorab noch einmal klarstellen, dass ich kein Gegner der Vernetzung oder Digitalisierung bin. Aber ich setze mich für eine Telematikinfrastruktur in den Praxen ein, bei der alle Kosten übernommen werden und die auf einer Technik basiert, die weder die Praxis-AIS langsamer macht, noch in vielen Praxen technische Probleme bringt. Besonders schlimm finde ich, dass die Politik, die Gematik oder die KVen nicht die vollständige Haftung für die den Praxen aufgezwungene, technisch veraltete Telematikinfrastruktur übernehmen – nur bis zum Konnektor. Ganz abgesehen von der Frage, warum wir uns so einen Eingriff in unsere Praxisorganisation überhaupt gefallen lassen müssen. Sie, Herr Dr. Kriedel, motivieren dennoch zur Installation – und „motivieren“ ist noch vorsichtig ausgedrückt.

Nun zu unserem Mailverkehr vor der KBV-Vertreterversammmlung, in der Sie – laut einer Meldung von facharzt.de – meine Vorbehalte alle entkräften konnten. Ich war da wohl in einer anderen Veranstaltung. Fakt ist doch, der TI-Konnektor ist eine Tür in das Praxis-AIS und wird mit Entstehung dieser riesigen Infrastruktur natürlich ein interessantes Objekt für Hacker.

***Meine erste Frage war:* Der Konnektor ist eine weitere Tür in das Praxis-AIS, manchmal die erste Tür! *Wer* die Haftung für alle Schäden übernimmt, die z.B. bei einem Hacker-Angriff für die Praxen entstehen, ist aus unserer Sicht ungeklärt. Technische Kosten, Kosten für die Information der Patienten und ggf. Kosten juristischer Auseinandersetzungen. Durch die neuen Vorgaben der EU-DSGVO hat sich die Rechtslage doch geändert und ist verschärft worden. Also können *Sie* mir schriftlich bestätigen, dass erstens die Praxen nicht haften und zweitens: Wer haftet ggf. konkret?**

***Ihre Antwort (Teilauszug):* Bei der Konzeption der TI und den damit verbunden Fachanwendungen wurde stets sehr hoher Wert auf die Themen Datensicherheit und Datenschutz in den Arztpraxen gelegt. Die Gematik als verantwortliche Organisation für die TI arbeitet in diesem Rahmen eng mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zusammen. Nach schriftlicher Auskunft des BfDI endet die datenschutzrechtliche Verantwortung des Arztes am Konnektor. Der Arzt ist somit, wie bisher auch, nur für die Systeme innerhalb der Praxis verantwortlich, die er auch unmittelbar beeinflussen kann.**

Wir möchten gerne unsere Fragen ergänzen:

- Wofür haften die Gematik und das BSI und die Anbieter der TI-Konnektoren?
- Wo endet die datenschutzrechtliche Verantwortung der Vorgenannten für IT-Sicherheitsvorfälle und Datenlecks, die aus dem Konnektor oder der TI oder den Bestandsnetzen heraus ausgelöst werden und die in die Praxen hinein wirken?
- Entsteht hier – da doch regelmäßig die Ursachenfeststellung bei IT-Sicherheitsvorfällen und Datenlecks äußerst schwierig ist – eine grundsätzliche Mithaftung der Vorgenannten, wenn Patientendaten in Umlauf geraten und – wie meist – nicht festgestellt werden kann, welcher Sicherheitsmangel ursächlich war?

Wir erwarten die Antworten mit Spannung.

Sie führen in Ihrer Antwort auf meine erste Frage (Teilauszug) weiter aus: Durch die Nutzung der TI entsteht somit generell kein höheres Risiko für die teilnehmenden Ärzte.

Wir halten diese Aussage für nicht nachvollziehbar:
Hat ein Arzt die Patientendaten tragenden AIS bisher vorsichtigerweise in einem isolierten, rein lokalen Netzwerk betrieben, stellt die erzwungene Vernetzung auf jeden Fall grundsätzlich eine Risikosteigerung dar.

Schlimmer noch:
Unsere Sicherheitsexperten versichern uns, nach ausführlicher und intensiver Lektüre der Schutzprofile für den Konnektor, keine einzige Maßnahme und keinen Schutzmechanismus gefunden zu haben, der die Praxis vor Angriffen mittels des Konnektors schützt!

Die folgende Abbildung aus dem Schutzprofil der aktuell zugelassenen Konnektoren (BSI-CC-PP-0047-2015, Seite 37, Abb. 4) sowie der ergänzende Text stellen die im Konnektor-Sicherheitsdesign berücksichtigten Angriffspfade dar.

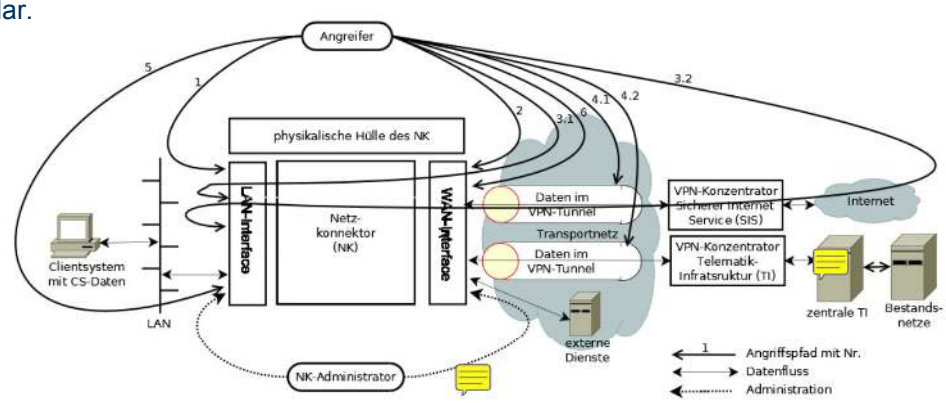

Abbildung 4: Externe Einheiten und Objekte im Zusammenhang, Angriffspfade

Zusätzlich zu den in Abbildung 4 visualisierten Angriffspfaden (Nr. 1 bis Nr. 6) bzw. den zugeordneten Bedrohungen könnte ein Angreifer

- unbemerkt ganze Konnektoren durch Nachbauten ersetzen (T.NK.counterfeit) oder
- die Kommunikation mit netzbasierten Diensten (Bezug von Sperrlisten für Gültigkeitsprüfung von Zertifikaten, Zeitsynchronisation, DNS) manipulieren (T.NK.Zert_Prüf, T.NK.TimeSync, T.NK.DNS).

Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0047ma1b_pdf.pdf?__blob=publicationFile&v=2

BSI-CC-PP-0047-2015, Seite 37, Abb. 4)

Interpretiert man die Abbildung, so wurden offenkundig Angriffspfade aus der TI oder den Bestandsnetzen genauso wenig betrachtet, wie Angriffe durch die (externen) Konnektor-Administratoren. Tatsächlich soll der vom Arzt nicht kontrollierbare Konnektor aber unmittelbar ohne weitere Schutzmaßnahmen im LAN der Arztpraxis agieren und direkt mit den AIS-Systemen intensiv und auf Ebene der Patientendaten interagieren.

Hier entstehen also ganz klar neue und zusätzliche Risiken, die im Konnektorsicherheitskonzept nicht adressiert wurden. Daher müsste der Konnektor nach dem Stand der IT-Sicherheitstechnik eigentlich durch eine eigene Firewall von den AIS isoliert werden.

Trotz wiederholten Anfragen erhalten wir aber weder von der Gematik noch dem BSI die notwendigen technischen Informationen. Vielleicht können Sie uns ja Auskunft geben?

Unabhängig davon bleibt natürlich die Frage, wer bezahlt zusätzliche Sicherheitsmaßnahmen, die durch Versäumnisse seitens des BSI und der Gematik notwendig geworden sind – zum Beispiel die Beschaffungs- und Betriebskosten.

Sie führen in Ihrer Antwort auf meine erste Frage (Teilauszug) weiter aus: In vielen Fällen ist das Sicherheitsniveau in der Praxis durch die Anbindung des Konnektors als zusätzliche Schutzmaßnahme gestiegen.

Diese Behauptung können wir im Lichte der obigen Ausführungen beim besten Willen nicht nachvollziehen. Erläutern Sie bitte technisch detailliert, welche zusätzliche Schutzwirkung der Konnektor für eine Praxis erbringen soll, und wieso unsere Einschätzung, dass der Konnektor ein zusätzliches Risiko ist, falsch sein soll. An welcher Stelle in den Schutzprofilen wird Ihre Einschätzung bestätigt?

Auf Ihre Antworten zu meiner zweiten Frage gehe ich an anderer Stelle ein, da es sich um zukünftige Kosten handelt und nicht um ungeklärte Fragen der Technik und Sicherheit.

Meine dritte Frage war: PEN-Tests liegen nach unseren Informationen bisher nicht vor. Ist es Praxen, die installiert haben, erlaubt, einen solchen durchzuführen?

Ihre Antwort: Der Praxis ist es aus rechtlicher Sicht nicht verwehrt, Penetrationstests in Bezug auf die eigene IT-Infrastruktur durchzuführen. Eine zwingende rechtliche Verpflichtung, solche durchzuführen, ergibt sich aber insbesondere nicht aus der DSGVO.

Die Vergangenheit hat deutlich belegt, dass reine Zertifizierungen – egal auf welchem Niveau – keine verlässliche Gewähr für IT-Sicherheit sind. Das Hamburger Wahlstift-Debakel hatte es ja sogar in die Tagesmeldungen geschafft.

Dieses Debakel trat trotz einer vom BSI begleitenden Sicherheitszertifizierung ein – einer Sicherheitsprüfung nach genau demselben Regelwerk, wie es für die Konnektoren (und andere Gesundheitstelematik-Komponenten) zum Einsatz kommt.

Jedem, der im letzten Jahrzehnt die Tagespresse verfolgt hat, sollte klar sein, dass es in den Netzen großer Institutionen immer wieder zu schwerwiegenden IT-Sicherheitsvorfällen kommt – der Bundestag und verschiedene deutsche Krankenkassen sind sicherlich relevante Beispiele für unser Thema.

Trotz wiederholter Nachfragen bei BSI und Gematik haben wir bisher leider nicht in Erfahrung bringen können, ob im Rahmen der Zertifizierung und Zulassung der Konnektoren aktive Tests durch unabhängige, renommierte Sicherheitsspezialisten stattgefunden haben.

Solche sogenannten PEN-Tests sind Stand der Kunst, und gerade im Bereich der Sicherheit der höchstsensiblen Patientendaten unseres Erachtens ein Gebot der Sorgfaltspflicht des BSI, der Gematik sowie aller Protagonisten der zwangsweisen Einführung dieser Technologie.

Der Vortrag von Martin Tschirsich zur Sicherheit verschiedener “Gesundheits-Apps” hat zumindest uns die Notwendigkeit solcher Tests eindrücklich vor Augen geführt.

Wenn wir aber den erheblichen Aufwand und die Kosten in Kauf nehmen würden, um solche – absolut notwendigen – Untersuchungen selbst durchzuführen, dann stünden wir vor dem technischen Problem, dass für einen technisch aussagekräftigen Test eine Kooperation seitens der Gematik und des BSI notwendig ist. Deshalb die Frage: Ob Sie uns und einer Gruppe von niedergelassenen Ärztinnen und Ärzten, die den Konnektor installiert haben, erlauben, einen solchen PEN-Test von einer unabhängigen Stelle durchführen zu lassen?

Sehr geehrter Herr Dr. Kriedel,

Ihre Antworten haben mich in meiner bisherigen Haltung bestärkt.

Ich sehe natürlich den Druck, der von vielen Seiten auf die Praxen ausgeübt wird. Ich bin trotzdem davon überzeugt richtig zu handeln und auch davon, dass wir in den Praxen bessere Lösungen verdient haben – im Hinblick auf Kostenerstattung, Technik, Haftung und Datensicherheit. Zudem sollten wir die Praxen und die Patienten auch vor einer Abgabe der Patientendaten in zentrale Speicher schützen. Dies ist im Rahmen der elektronischen Patientenakte (ePA) ja schon geplant. Deshalb verweigere ich weiterhin die Installation des Konnektors in meiner Praxis, werde die Strafe erwarten und dann dagegen klagen.

Dennoch erwarte ich Ihre geschätzten Antworten mit großem Interesse.

Mit freundlichen Grüßen

Dr. Werner Baumgärtner
Vorstandsvorsitzender