Gemeinsame Pressemitteilung

Ärzteverbände warnen: Patientendaten für Hacker zugänglich

Berlin, 27. Juni 2019 – Die Ärzteverbände MEDI GENO Deutschland, Freie Ärzteschaft und Freier Verband Deutscher Zahnärzte warnen vor Sicherheitslücken in der Telematikinfrastruktur (TI). Die TI ist die gesetzlich vorgeschriebene Vernetzungsplattform des deutschen Gesundheitssystems. Alle deutschen Praxen müssen bis zum 30.06.2019 einen Zugang zur TI installiert oder zumindest bestellt haben – ansonsten fallen Honorarabzüge an. Versichertenstammdaten werden bereits in der TI abgeglichen. Künftig sollen Patientenakten in der TI platziert und möglicherweise auch gespeichert werden. MEDI GENO Deutschland und weitere Ärzteverbände reichen Klage ein.

Der Gesetzgeber zwingt alle Praxen in Deutschland, einen TI-Konnektor zu installieren und sich darüber mit der Telematikinfrastruktur (TI) zu verbinden. Ziel ist die Vernetzung aller, die an der Patientenversorgung beteiligt sind. Wegen Sicherheitsbedenken haben sich viele Ärzte und Psychotherapeuten gegen die Installation des TI-Konnektors entschieden. Für ihre Verweigerung nehmen die Praxisinhaber einen Honorarabzug in Kauf. Der Gesetzgeber will den Druck auf die Praxen erhöhen und die Honorarstrafe nächstes Jahr von einem auf 2,5 Prozent anheben.

Baumgärtner: TI-Konnektor schützt nicht gegen Hackerangriffe auf Praxissysteme
Dr. Werner Baumgärtner, Vorstandsvorsitzender von MEDI Baden-Württemberg und MEDI GENO Deutschland, hatte Zweifel an der Sicherheit der TI. Deshalb hat der MEDI Verbund IT-Experten beauftragt, die Technologie zu prüfen. Die Informatiker haben die Schutzprofile, nach denen die TI-Konnektoren zertifiziert werden, eingehend untersucht. “Bei der Prüfung der Schutzprofile fanden die Experten verschiedene ungeklärte Fragen zur Sicherheit des TI-Konnektors. Insbesondere schützt der Konnektor selbst bei ordnungsgemäßer Installation nicht zuverlässig gegen Angriffe in die Praxissysteme, obwohl das von Seiten der Kassenärztlichen Bundesvereinigung (KBV) gegenüber den Ärzten behauptet wird“, sagt Baumgärtner.

Auf Kritik keine Reaktion – auf Fragen keine Antwort
Mit den Ergebnissen der Gutachten wandte sich Baumgärtner an das Bundesamt für Sicherheit in der Informationstechnik (BSI), die KBV und die gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH), den Anbieter der TI und der zugehörigen Konnektoren, zu deren Gesellschaftern auch das Bundesministerium für Gesundheit zählt. „Auch schriftliche Anfragen brachten keine Antwort auf die Kernfrage, was der Konnektor als Firewall wirklich leistet und wie er die Arztinformationssoftware vor Angriffen aus der TI schützt. In der letzten Antwort der KBV, die sich auf Aussagen der gematik stützt, wurde aus einem Schutzprofil zitiert, das gar nicht auf die aktuellen Konnektoren zur Anwendung gekommen ist“, berichtet Baumgärtner.

Ärzte: Patientendaten müssen geschützt werden
„Wir Ärzte kritisieren eine unsichere Zwangsvernetzung aller Daten im deutschen Gesundheitswesen, welche die Potenz hat, die ärztliche Schweigepflicht auszuhebeln“, sagt Dr. Silke Lüder, stellvertretende Bundesvorsitzende der Freien Ärzteschaft. Im Datenschutz und in der ärztlichen Schweigepflicht sieht sie eine wichtige Grundlage für das Vertrauensverhältnis zwischen Behandlern und Patienten: „Wenn mein Patient in der Sprechstunde nicht mehr darauf vertrauen kann, dass das, was er mir über seine gesundheitlichen Probleme berichtet, in meinem Sprechzimmer bleibt, kann ich nicht mehr für ihn arbeiten. Mein Patient wird mir vieles nicht mehr erzählen und ich kann dadurch keine aufschlussreichen Anamnesen mehr erheben und keine richtigen Diagnosen stellen“.
Wie verheerend Gesundheitsdaten in den falschen Händen sein könnten, zeigt sie anhand der Konsequenzen auf: „Wenn die genetische Diagnose eines Bewerbers für ein politisches Amt oder einen Managerposten auslesbar wäre, wäre das Erpressungspotenzial eminent.“

Baumgärtner betont, dass Patientendaten unbedingt geschützt werden müssen: „Patientendaten sind sensibler als Bankdaten. Gerade deshalb sind wir gegen jede zentrale Speicherung von Patientendaten. Eine solche ist als nächster Schritt auf der Basis einer unsicheren TI geplant.“

„Nicht hinnehmbar“: Bei Datenschutzpannen haften die Praxisinhaber
Für etwaige Folgen von Sicherheitslücken der staatlich aufgezwungenen TI-Konnektoren müssen die Praxisinhaber haften. Baumgärtner findet das inakzeptabel: „Die Praxen werden unter Strafe in eine TI gezwungen, deren Sicherheit nicht ausreichend geprüft ist und zu der entscheidende Fragen der Sicherheit nicht beantwortet sind. Die Haftung bei Datenverlust durch Hacking liegt gemäß der DSVGO bei den Praxen und die Patientendaten sind nicht so sicher, wie dies notwendig wäre.“ MEDI GENO Deutschland geht gerichtlich gegen die staatlich erzwungene Vernetzung vor.
Es sei nicht hinnehmbar, dass das Sozialgesetzbuch Arztpraxen dazu zwingt, sich an eine Telematikinfrastruktur anzuschließen, bei der ungeklärte Fragen der Sicherheit der Patientendaten bestehen, urteilt Frank Hofmann, Justitiar und Vorstand der MEDIVERBUND AG. „Wir halten deshalb den Zwang, einen TI-Konnektor zu installieren, für rechtlich unzulässig und lassen die Rechtmäßigkeit der Honorarabzüge gerichtlich prüfen“, sagt Hofmann, der die Musterklagen koordiniert. „Unser Ziel ist es, auf dem Rechtsweg die Honorarstrafe abzuschaffen. Dann können sich Arzt- und Psychotherapiepraxen gegen den TI-Konnektor und für eine sicherere Vernetzungstechnologie entscheiden – ohne finanzielle Einbußen hinnehmen zu müssen“, erklärt er.

Man behalte sich auch vor, Musterklagen gegen die Verantwortlichen des Zwangs zum Konnektoranschlusses zu führen, wenn Praxen, die an die TI angeschlossen sind gehackt werden. „Wir können die betroffenen Praxen an der Stelle nicht alleine lassen und werden deshalb im Sinne einer geteilten Verantwortlichkeit gemäß der DSVGO die Praxen bei Klagen unterstützen – sowohl gegen die Verantwortlichen für die TI-Zwangsinstallation, als auch gegen diejenigen, die nicht korrekt installiert haben“, ergänzt Hofmann.

Ärzte fordern sichere digitale Kommunikation im Medizinbetrieb
„Ärzte nutzen seit Langem digitalisierte Daten und wenden jede Form moderner Technik in Praxen und Kliniken an. Wir fordern eine sichere digitale Kommunikation im Medizinbetrieb:

Ende zu Ende verschlüsselt, ohne staatlichen Zugriff, ohne zentrale Speicherung – und jeder Patient bekommt wie auch jetzt schon seine medizinischen Daten ausgehändigt“, sagt Lüder. Minister Spahn sei die ursprüngliche Zielsetzung einer verbesserten digitalen Kommunikation im Gesundheitswesen völlig aus dem Blick geraten. Stattdessen werde jetzt populistisch eine unsichere Handykommunikation aufgebaut, mit der die Schweigepflicht nicht mehr gesichert werden könne. „Das neue Digitalgesetz aus dem Hause Spahn ist ein Zwangsgesetz zu Lasten von Patienten und Ärzten“, so die Allgemeinärztin.

Penetrations- und White-Hacking-Tests unter Strafandrohung verboten
Viele Sicherheitstests können nicht vorgenommen werden, weil eigene Tests der Ärzteschaft gesetzlich verboten sind. „Wir kritisieren auch, dass die Sicherheit des Anschlusses der Praxen an die TI nicht in einem Penetrationstest getestet wurde. Eigene Tests der Ärzteschaft sind gesetzlich verboten. Wir hätten den PEN-Test auf unsere Kosten durchgeführt“, erklärt Baumgärtner.

Penetrationstests gehören standardmäßig zu den sechs Testmethoden bei der Sicherheitsprüfung von Softwareprodukten und -systemen. Sie sind in der ISO 27034-1 festgeschrieben. „Jede dieser Methoden identifiziert andersartige Sicherheitslücken in Hardware und auch in jeder Art Software. Für die Nutzung freigegeben werden kann ein System oder ein Produkt erst nach einem erfolgreichen Security Test!“ erklärt Prof. Dr. Hartmut Pohl, Geschäftsführer der Cyber-Sicherheitsberatung softScheck GmbH. Deshalb schreibt die ISO-Norm vor, dass die Tests über den gesamten Prozess der Software-Entwicklung angewandt werden müssen. „Das bedeutet, dass der Security Testing Process mit allen sechs Methoden bei sicherheitsrelevanten Ergänzungen und Modifizierungen (Updates) erneut durchlaufen werden muss“, erklärt Pohl, der auch Sprecher des Präsidiumsarbeitskreises 'Datenschutz und IT-Sicherheit' der Gesellschaft für Informatik ist – der größten Informatikfachvertretung im deutschsprachigen Raum.

Sicherheitslücken nachgewiesen
„Patientendaten sind im Moment für Hacker leicht zugänglich. Und das, obwohl Gesundheitsdaten die langfristig schutzbedürftigsten Daten sind, die wir Menschen haben“, betont IT-Dienstleister Jens Ernst. Für seinen Kunden, eine Arztpraxis, hat er bei einer Sicherheitsprüfung auf verschiedene Arten das Testvirus EICAR über den ordnungsgemäß angeschlossenen TI-Konnektor ins Praxisnetzwerk eingeschleust. Nachgewiesen hat er auch, dass die integrierte Firewall die Kommunikation nicht kontrolliert und alle Ports ausgehend geöffnet sind. Der Test lässt auf unzureichenden Schutz der schließen.

Die gematik versichert im Informationsblatt zum TI-Konnektor: „Durch die integrierte Firewall des Konnektors und den optionalen und gegebenenfalls kostenpflichtigen Secure Internet Service (SIS) wird das LAN optimal vor unautorisierten Zugriffen von außen geschützt.“ Diesen Schutz zweifelt Jens Ernst an. Das Testvirus EICAR, das er für seinen Sicherheitstest verwendet hat, wird standardmäßig bei Virenschutztests verwendet. Entwickelt wurde es vom European Institute for Computer Anti-Virus Research(EICAR). Das EICAR Testvirus wird zum Prüfen von Virenscannern verwendet. Jeder Virenscanner muss diese Datei als Virus erkennen. Die TI und den Konnektor konnte das Testvirus passieren. Jens Ernst erklärt: „Das bedeutet, dass es keinen wirksamen Schutz gegen Malware – also Viren und Trojaner – durch die TI gibt.“