taz

taz zahl ich

Ethischer Hacker über Gesundheitskonten

„Wir hatten theoretisch Zugriff auf alle Patientenakten“

Martin Tschirsich von Chaos Computer Club hält die neue elektronische Patientenakte nicht für sicher. Angreifer könnten gebrauchte Lesegeräte kaufen.

8.1.2025 18:00 Uhr teilen

Ein gebrauchtes Lesegerät ist schnell besorgt und schon kann es losgehen mit dem Hacken Foto: Fabian Sommer/dpa

Interview von **Kaija Kutter**

taz: Herr Tschirsich, Hamburg führt ab 15. Januar als Modellregion die elektronische Patientenakte (EPA) ein. Wieso ist die nicht sicher?

Martin Tschirsich: Das Bundesgesundheitsministerium verspricht, dass diese Akte die sicherste in Europa sei und diese Daten nicht gehackt

würden, weil es sie gar nicht an einer zentralen Stelle gibt. Das ist auch die ethische Voraussetzung für den Plan, dass sie jeder bekommt.

taz: Sofern er nicht widerspricht.

Tschirsich: Genau. Das Prinzip heißt „Opt out“: Tue ich nichts, bekomme ich als gesetzlich Versicherter eine Akte. Darin werden meine Gesundheitsdaten aus allen Institutionen des Gesundheitswesens lebenslänglich abgelegt und im Klartext verarbeitet. Und sofern die Daten pseudonymisierbar sind, stellt man sie auch zur Forschung IT-Konzernen zur Verfügung.

taz: Wo befindet diese Akte?

Tschirsich: Die ist zentral. Es gibt zwei Betreiber, IBM und Rise. Die betreiben diese Akten im Auftrag der jeweiligen Krankenkasse. Die Daten werden dort zentral in einem Rechenzentrum geführt und auch im Klartext verarbeitet.

taz: Auch Leberwerte vom Hausarzt-Check-up?

Tschirsich: Ja. Auch alle Rezepte und Abrechnungsdiagnosen der Kassen fließen dort hinein, letztere auch rückwirkend, nicht erst ab 2025. Und zwar von allen Leistungserbringern, von Ärzten und Kliniken bis zu medizinischer Fußpflege oder Logopädie. Durch das Einstecken ihrer Gesundheitskarte sind Versicherte dazu angehalten, eine Zugangsmöglichkeit auf diese EPA zu schaffen, damit Unterlagen aus der aktuellen Behandlung wie Arztbriefe und Laborergebnisse dort eingestellt werden.

taz: Sie und eine Kollegin vom Chaos Computer Club (CCC) schafften es, auf diese Akten zuzugreifen?

Tschirsich: Diese Akte gibt es ja in der ersten Version schon seit 2020. Da wiesen wir schon Mängel nach. Aber damals galt noch das „Opt in“-Prinzip. Man entschied sich für die Akte. Und es gab eine Pin für die EPA. Für potenzielle Angreifer interessant sind die Zugangsschlüssel der Leistungserbringer, also der Praxen und Kliniken. Und die sind leicht zu beschaffen.

taz: Wie denn?

Tschirsich: Die Herausgeber dieser Schlüssel lassen sich austricksen. Auch kann ein Angreifer sich gegenüber Arztpraxen als IT-Support-Dienstleister ausgeben. Das haben wir auf Gesuche hin gemacht, um zu zeigen, dass Dienstleister ein Einfallstor für Angriffe sind. Wir hätten dort Voll-Zugriff auf den Schlüssel der Institution gehabt.

taz: Beim CCC-Kongress zeigten sie ein Kartenlesegerät, das Sie über Ebay erwarben?

Tschirsich: Kleinanzeigenportale im Netz sind ein weiteres Einfallstor. Mit vier Stunden Zeiteinsatz gelangten wir darüber in Besitz eines Praxisausweises mitsamt der weiteren Zugangstechnik. Wir konnten dort Zugangsschlüssel gebraucht kaufen. Das kann offenbar passieren, wenn eine Praxis aufgelöst wird.

taz: Sie kauften ein Lesegerät und passende Schlüssel?

Tschirsich: Richtig. Das Lesegerät, in das die Gesundheitskarte gesteckt wird, hat an der Seite Schlitze, darin stecken weitere Schlüssel. Unter anderen der für die jeweilige Praxis und ihren Zugriff auf das Aktensystem.

taz: Was kann man da lesen?

Tschirsich: Unser Lesegerät war schon mit allen Schlüsseln besteckt. Da steckte auch der Ausweis der Institution drin. Die Pin, die ich brauchte, um den freizuschalten, wurde auf nette Anfrage auch noch mitgeliefert. Dieses Lesegerät schließe ich dann an. Dafür brauche ich noch eine bestimmte Netzwerkverbindung zu diesen zentralen Rechenzentren. Der dafür nötige Konnektor, das ist eine kleine Hardwarebox, ist frei käuflich. Oder ich bestelle mir so einen Software-Konnektor im Internet. An diesen Zugang steckten wir unser Kartenlesegerät. Wir hätten, wenn es die EPA für alle schon gäbe, Zugang auf alle Patienten-Akten bekommen, die für diese Praxis freigegeben sind. Also alle, die diese Praxis in den letzten 90 Tagen besuchten und der Akte nicht widersprachen.

taz: Wie viele?

Tschirsich: Etwa 1.000 Stück. Aber wir hatten über dieses Lesegerät theoretisch Zugriff auf alle 70 Millionen Patientenakten. Das ist technisch möglich. Das wurde auch von der „Gematik“, der Nationalen Agentur für Digitale Medizin, die diesen Prozess betreut, bestätigt. Es gibt hier leider einen kleinen Fehler mit großer Wirkung. Das Digitalgesetz sieht vor, dass der Zugriff einer Praxis auf die Akte nur möglich ist, wenn auch zuvor die Karte des Versicherten gesteckt war. Wir konnten nachweisen, dass eine Arztpraxis auch ohne dies auf die Patientenakte zugreifen kann. Angreifer können vortäuschen, dass beliebige Gesundheitskarten gesteckt waren und dann auf diese Akten zugreifen.

taz: Wer hacken will, braucht also nur ein gebrauchtes Kartenlesegerät und das beschriebene Zubehör?

Tschirsich: Richtig. Denn ich benötige als Angreifer nur die Nummer einer Karte und nicht die echte Karte selbst. Diese Nummern sind einfach aufsteigend vergeben. Man zählt einfach von einer Karte noch eins, zwei, drei Nummern hoch, dann hat man schon den nächsten Versicherten. Das ist ein Mangel, auf den wir mehrfach hinwiesen.

taz: Was können denn Böswillige mit den Akten anstellen?

Tschirsich: Der Nachteil ist das mangelnde Vertrauen. Viele Menschen möchten ihre Gesundheitsinformationen nicht mit allen teilen, weil sie stigmatisierende Diagnosen haben. Sie könnten aber sehr von den Vorteilen einer elektronischen Akte profitieren. Diese Menschen werden von den Vorteilen abgeschnitten, weil das System schlecht gemacht ist.

taz: Ist die Karte sinnvoll?

Tschirsich: Viele Mediziner sagen, so eine elektronische Patientenakte können sie gut gebrauchen, damit zum Beispiel unbeabsichtigte Wechselwirkungen von Medikamenten der Vergangenheit angehören.

taz: Was muss passieren?

Tschirsich: Wir müssen an die Entwicklung dieser digitalen Infrastruktur anders herangehen. Wir brauchen eine unabhängige und belastbare Risikobewertung. Die Risiken, die wir auf dem Kongress in Hamburg demonstrierten, waren seit August bekannt. Aber erst mit dem praktischen Nachweis wird hektisch gehandelt. Wir wünschen uns, dass solche Risiken zuvor behandelt werden. Dazu braucht es eine unabhängige Einschätzung, zum Beispiel des Bundesdatenschutzbeauftragten, die auch publik gemacht wird. Damit wir alle eine informierte Entscheidung treffen können sollte.

taz: Sollte Hamburg als Modellregion denn jetzt mit der Akte starten?

Tschirsich: Nach Auskunft der zuständigen Ministerien wird das so sein. Zunächst gehen am 15. Januar 300 Praxen in Hamburg und in Franken mit den bekannten Mängeln an den Start. Und aus jeder dieser 300 Praxen besteht dann der Vollzugriff auf alle 70 Millionen Aktenkonten. Die werden nämlich schon parallel angelegt und bis zum 15. Februar mit Daten gefüllt. Das dauert ein paar Wochen. Ist diese Testphase abgeschlossen, soll – trotz grundsätzlich fortbestehender Mängel – die Nutzung deutschlandweit passieren.

taz: Können wir die Zustimmung noch zurückziehen?

Tschirsich: Jederzeit.

taz: Was tun Sie selbst?

Tschirsich: Das sage ich nicht. Jeder hat einen ganz unterschiedlichen medizinischen Bedarf. Und wenn ich jetzt aus privilegierter Position heraus sage, ich nehme so eine Akte, weil ich bisher mit keiner stigmatisierenden Diagnose durchs Leben gehe, gilt das für viele andere nicht.

taz: Geben Sie einen Rat?

Tschirsich: Das ist so ein bisschen wie beim Beipackzettel. Dort findet ja auch immer eine Risikoaufklärung statt. Wenn man nicht möchte, dass eine andere Person zum Telefon greift und sich in zehn Minuten