Elektronische Patientenakte noch immer nicht sicher

Berliner Thema

Die **ELEKTRONISCHE PATIENTENAKTE** zu hacken, ist deutlich komplizierter geworden, bleibt aber technisch möglich.

VON MATTHIAS SCHWARZER

BERLIN. Kurz vor dem Jahreswechsel 2024/25 war bei den Verantwortlichen der elektronischen Patientenakte (ePA) die besinnliche Stimmung vorbei: Hacker aus dem Umfeld des Chaos Computer Clubs (CCC) hatten auf der jährlichen Konferenz des Vereins gezeigt, wie man das neue digitale System hacken kann – und zwar so, dass potenziell ein Zugriff auf Millionen Akten möglich wäre. Die Folge: Die Einführung der ePA wurde zunächst verschoben, und rund fünf Prozent der Versicherten widersprachen der Nutzung zunächst.

Inzwischen ist die ePA offiziell eingeführt – seit dem 1. Oktober ist sie für Leistungserbringer auch verpflichtend. Und auch bei den Sicherheitsvorkehrungen hat sich in den vergangenen Monaten einiges getan: Gleich mehrfach besserte die Gematik, die bundeseigene Agentur für digitale Medizin, nach den Hinweisen des CCC nach. Die ePA zu hacken, ist heute schwieriger. Aber: Unmöglich ist es nicht.

Die IT-Fachleute des CCC bemängeln vor allem ein Detail, das das neu eingeführte Tool noch immer angreifbar macht. Eine Lösung ist laut Gematik in Aussicht – jedoch frühestens im Laufe des kommenden Jahres.

VIEL WISSEN REICHT FÜR EINEN EPA-HACK

Um das Problem zu erkennen, muss man verstehen, wie die ePA funktioniert. Wer auf eine Patientenakte zugreifen will, braucht derzeit einen Praxisausweis – und zweitens die vollständigen Daten des Versicherten. Konkret: die Kartennummer, die Krankenversicherungsnummer, die Adresse und den Versicherungsbeginn. Hier hat die Gematik bereits nachgebessert: Die bisherige Kombination aus Kartennummer und Krankenversicherungsnummer allein reicht jetzt für den Zugriff nicht mehr aus. Zudem reagierten die Entwickler nach der Kritik des CCC mit einer Beschränkung der möglichen Zugriffsmengen.

Die Hürden für einen Angriff sind also deutlich höher geworden, aber nicht unüberwindbar. Daten wie Adressen ließen sich möglicherweise durch Datenlecks herausfinden, andere durch Phishing. Die IT-Fachleute Bianca Kastl und Martin Tschirsich hatten auf der Jahreskonferenz des CCC auch gezeigt, wie sie mit Telefonanrufen bei Krankenkassen an Gesundheitskarten gelangt waren – und sogar über eine Sicherheitslücke an Praxisausweise. Im April demonstrierten die Hacker dann erneut, wie die ePA über das sogenannte Ersatzbescheinigungsverfahren angegriffen werden kann. Auch diese Sicherheitslücke stopfte die Gematik daraufhin.

Allerdings noch immer nicht zur vollständigen Zufriedenheit der Hacker: Der Umgang mit Sicherheitslücken bei der Behörde sei „klar ausbaufähig“, sagte Kastl dem RedaktionsNetzwerk Deutschland (RND). Um das Risiko wirksam zu minimieren, wünscht sich die IT-Expertin für die ePA ein ganz spezielles Verfahren.

DIGITALE SIGNATUR SICHERT PATIENTENAKTE AB

„Aktuell ist das Einzige, was für einen Zugriff auf eine ePA notwendig ist, eine Menge Wissen: Kartennummern, Krankenversicherungsnummern, Anschrift und Datum des Versicherungsbeginns“, erklärt Kastl. „Lösbar wäre das Problem dadurch, dass nur signierte, authentische Daten von der Gesundheitskarte gelesen werden. Damit ließe sich kryptografisch zweifellos nachweisen, dass auch wirklich eine von einer Krankenkasse ausgegebene Karte gelesen wird – eine sichere Technik existiert also schon länger, wurde aber bisher bei der ePA nicht angewendet.“

Genau so ein Verfahren ist nach Angaben der Gematik nun aber für das kommende Jahr geplant, wie die Behörde dem RND mitteilte. Geplant sei dann ein „Proof of Patient Presence“-Verfahren (Beweis, dass der Patient anwesend ist, kurz PoPP). Gefragt nach dem CCC-Vorschlag zur digitalen kryptografischen Signatur heißt es von der Agentur: „Ja, ein solches Verfahren ist mit PoPP geplant.“ Noch sei dieses allerdings in der Entwicklung, daher könne man keine Details nennen.

Technisch dürfte das Verfahren so funktionieren: Der Patient oder die Patientin steckt wie bisher die Gesundheitskarte beim Arzt ins Gerät. Dann werden allerdings nicht einfach nur Daten von der Karte gelesen, sondern es läuft im Hintergrund ein „Challenge-Response-Verfahren“ ab. Der PoPP-Service – ein Teil des Sicherheitssystems – generiert eine Zufallszahl und sendet diese an die Gesundheitskarte. Diese verschlüsselt die Zahl und sendet das Ergebnis zurück. Nur wenn die Zufallszahl korrekt verschlüsselt wurde, ist die Karte echt und liegt physisch vor. Einen genauen Startzeitpunkt für 2026 nannte die Behörde zunächst nicht.

Bis dahin bleibt zumindest ein Restrisiko. IT-Fachleute verweisen immer wieder auf die Gefahren, die durch unzureichende Authentifizierungsmaßnahmen innerhalb der ePA entstehen können. Kastl nennt etwa einen Fall aus Singapur: „2018 wurden dort die Gesundheitsdaten von 1,5 Millionen Menschen abgegriffen. Ziel war dabei auch die Medikationsliste des Regierungspräsidenten.“ Daten dieser Sensibilität machten aus entsprechenden Leaks „ein Risiko für ganze Staaten“, weil sie Angriffe auf andere kritische Infrastrukturen oder Politikerinnen und Politiker ermöglichten, erklärt die Expertin.

Kastl führt als einen weiteren Fall den Cybereinbruch bei Bitmarck auf, einem IT-Dienstleister der gesetzlichen Krankenkassen und Anbieter der ePA im Jahr 2023. Dabei wurden Daten wie Namen, Geburtsdaten und die eindeutige Krankenaktennummer der Versichertenkarte von rund 300.000 Onlinekunden verschiedener Krankenkassen abgegriffen. Auch damals machten IT-Fachleute unter anderem unzureichende Authentifizierungsmaßnahmen als Grund aus.

Für Privatpersonen können Angriffe schwere Folgen haben. Im sehr viel digitaleren Dänemark hatten sich die Täter Zugang zu persönlichsten Informationen Zehntausender Patientinnen und Patienten über ein Konsortium von Arztpraxen verschafft, darunter auch Krankenakten. Allan Frank, IT-Sicherheitsspezialist bei der dänischen Datenschutzbehörde, sagte dem RND damals, dass solche intimen Daten für Erpressungsversuche genutzt werden könnten – schließlich dürften die wenigsten Betroffenen wollen, dass ihre Behandlungen öffentlich werden.

NUR FÜNF PROZENT HABEN WIDERSPROCHEN

In Deutschland fühlen sich die meisten Patientinnen und Patienten mit ihrer ePA offenbar – trotz deren Mängel – sicher genug. Vor einigen Wochen veröffentlichte die Gematik aktuelle Zahlen zur Nutzung. Diese seien während der ersten vier Wochen, in denen Praxen, Apotheken und Krankenhäuser die ePA für alle nutzen sollen, weiter angestiegen.

17,4 Millionen Abrufe von Medikationslisten seien in der letzten Oktoberwoche verzeichnet worden. In der letzten Septemberwoche seien es noch 12,6 Millionen gewesen. Auch die Befüllung der Patientenakten schreitet voran: Allein im Oktober habe es 10,6 Millionen Dokumenten-Uploads gegeben. Die Gesamtzahl seit dem Start der ePA liegt bei 37 Millionen.

Der Anteil derjenigen, die der ePA widersprochen haben, ist im Vergleich weiterhin gering. Wie der bundesweite Verband der Krankenkassen, der GKV-Spitzenverband, dem RND mitteilte, liegt die Widerspruchsquote weiterhin bei etwa fünf Prozent.

In der ePA sind sensible Gesundheitsdaten der Patientinnen und Patienten gespeichert. Symbolfoto: Vitaly Gariev / Unsplash