ZEIT ONLINE

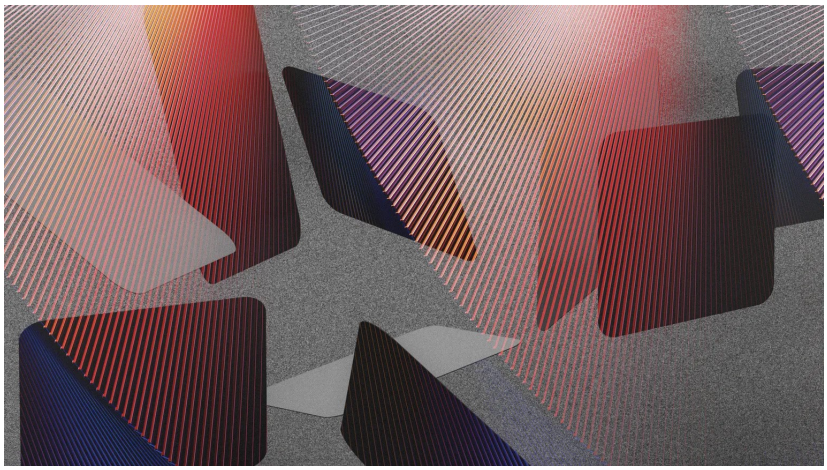
Z+ Elektronische Patientenakte

Geheimdienste? "Nicht relevant"

Die digitale Patientenakte wurde nicht darauf geprüft, ob Geheimdienste sie knacken können. Hoch fragwürdig, sagen Experten. Denn mit den Daten kann man Leute erpressen.

Von Eva Wolfangel

23. Dezember 2024, 17:44 Uhr



Ab 2025 liegen die Gesundheitsdaten von Menschen standardmäßig auch digital vor. Nur wer der elektronischen Patientenakte aktiv widerspricht, bekommt sie nicht. © [M] Alexander Hoepfner/ZEIT ONLINE; verw. Bild: Dim Gunger/Unsplash

Wie sicher ist die elektronische Patientenakte? Das ist gerade eine zentrale Frage für alle Menschen in Deutschland. Denn ab spätestens Februar 2025 bekommt jede Person, die einer Einrichtung nicht aktiv widerspricht, eine digitale Akte mit Diagnosen, Laborberichten, Röntgenbildern angelegt. Doch eine Recherche von ZEIT ONLINE zeigt: Es gibt Zweifel daran, wie gut das System wirklich vor digitalen Angriffen geschützt ist.

In einem aktuellen Sicherheitsgutachten [https://www.gematik.de/media/gematik/Medien/ePA_fuer_alle/Abschlussbericht_Sicherheitsanalyse_ePA_fuer_alle_Frauenhofer_SIT.pdf] der elektronischen Patientenakte, in Auftrag gegeben von der verantwortlichen Agentur Gematik und erstellt vom Fraunhofer-Institut für Sichere Informationstechnologie (SIT), heißt es nämlich, dass das System nicht auf Angriffe ausländischer Regierungen getestet wurde. Diese seien "nicht

relevant". Eine Formulierung, über die man sich wundern darf. Schließlich haben Geheimdienste aus vielen Ländern gezeigt, wie sehr sie sich für die Daten von Deutschen interessieren – von US-amerikanischen über chinesische bis hin zu russischen.

Nun mag sich manch einer denken: Ach, na ja, was soll ein Geheimdienst schon mit meinen Daten anfangen? Aber Gesundheitsdaten sind besonders sensible Daten. In der elektronischen Patientenakte kann Unfruchtbarkeit künftig genauso erfasst sein wie eine Depression – also Diagnosen, die man vielleicht nicht unbedingt mit der Öffentlichkeit teilen möchte. Und aus diesem Grund lässt sich mit solchen Informationen aus Sicht von Geheimdiensten viel anfangen: Man kann mehr über die Lebensgewohnheiten von Personen erfahren. Man kann solche Daten veröffentlichen, um beispielsweise Politikerinnen, Journalisten oder Menschen des öffentlichen Lebens zu diskreditieren. Man kann aber auch Menschen damit erpressen und versuchen, sie dazu zu bringen, Dinge zu tun, die sie eigentlich nicht tun wollen.

Elektronische Patientenakte

Thema

Z+ Gesundheitswesen
Elektronische Patientenakte – will ich das wirklich?
[https://www.zeit.de/digital/datenschutz/2024-10/elektronische-patientenakte-datenschutz-dokumente-krankenkasse-faq]

Klingt nach James Bond? Ist aber eine durchaus übliche Praxis im hybriden Krieg, wie ZEIT ONLINE von Geheimdienstexperten erfuhr. Warum also hat die Gematik darauf verzichtet, die Sicherheit der elektronischen Patientenakte auf genau diesen Punkt testen zu lassen?

Was die elektronische Patientenakte so attraktiv für Geheimdienste macht

Die elektronische Patientenakte – kurz ePA – soll für einen besseren Datenaustausch [https://www.zeit.de/digital/datenschutz/2024-10/elektronische-patientenakte-datenschutz-dokumente-krankenkasse-faq#wie-sind-meine-daten-in-der-epa-gesichert] zwischen behandelnden Ärztinnen und Therapeuten sorgen. Es steht außer Frage, dass dies in der Regel für Patienten ebenso wie für das Gesundheitssystem von Vorteil ist. Für Patientinnen bedeutet das, dass sie nicht mehr jede Diagnose von irgendeinem Arzt hin zum nächsten schleppen müssen. Im Notfall kann es sogar lebensrettend sein, etwa wenn eine Ärztin in

der Notaufnahme sieht, auf welche Medikamente jemand allergisch ist, und entsprechend ein anderes Mittel einsetzen kann.

Zur Wahrheit gehört aber auch, dass Daten im Netz nie hundertprozentig sicher sind. Eine Sicherheitslücke oder ein schlecht aufgesetzter Server reichen, und schon können auch Fremde auf sensible Informationen zugreifen. Genau deshalb prüft man Systeme üblicherweise auf alle möglichen Einfallstore, bevor man sie für die Öffentlichkeit freischaltet.

Verantwortlich dafür ist im Fall der elektronischen Patientenakte die Gematik, die Nationale Agentur für digitale Medizin. Der größte Gesellschafter ist das Bundesgesundheitsministerium [https://www.zeit.de/thema/bundesministerium-fuer-gesundheit]. Die Gematik baut die sogenannte Telematikinfrastruktur, eine digitale Plattform, über die alle gesundheitlichen Anliegen zwischen Ärztinnen, Krankenhäusern, Psychotherapeuten und Patienten laufen sollen. Die elektronische Patientenakte ist eine Anwendung, die diese Infrastruktur verwendet, die Daten selbst sind bei zwei anderen Anbietern gespeichert.

Auf der Website der Gematik heißt es, das Bundesamt für Sicherheit in der Informationstechnik (BSI) lege "Vorgaben und Maßnahmen" für einzelne Komponenten der Telematikinfrastruktur fest. Und dass alle Dienste ein mehrstufiges Prüfverfahren durchlaufen müssten. Dazu zählen laut Website eine Sicherheitsevaluation beziehungsweise ein Gutachten.

Um die Sicherheit der elektronischen Patientenakte zu prüfen, hat die Gematik entsprechend ein Gutachten beim Fraunhofer SIT in Auftrag gegeben. Darin geht es auch um staatliche Akteure. Doch im Gutachten des Fraunhofer SIT wird zwar beschrieben, dass Regierungsorganisationen daran interessiert seien, "vertrauliche Informationen über Bürger zu sammeln, die Infrastruktur anderer Staaten anzugreifen oder nachrichtendienstliche Informationen zu gewinnen" und auch, dass diese über erhebliche Ressourcen sowie "hoch qualifiziertes Fachpersonal" verfügten und nicht wirtschaftlich motiviert seien. Aber dann folgt ein widersprüchlicher Satz: "In Bezug auf das ePA-System wurde nach Absprache mit der gematik festgelegt, dass Angriffe durch Regierungsorganisationen nicht relevant sind."

Dabei hat das Konzept der elektronischen Patientenakte mindestens zwei zentrale Säulen, die sie gerade für potente staatliche Angreifer vulnerabel macht: Das ist erstens die zentrale Datenspeicherung. Weil alle Daten an wenigen Punkten zusammenlaufen, lohnt es sich eher, viel Aufwand zu investieren – denn bei Erfolg hat man gleich Zugriff auf viele Informationen. Zwar sind die Daten verschlüsselt, aber wie die Erfahrung zeigt, ist nicht jede Verschlüsselung robust gegen alle Arten von Angreifern. Auch die Pseudonymisierung der Daten, wie sie bei der elektronischen Patientenakte bei Freigabe für Forschungszwecke vorgesehen ist, bringt nicht unbedingt etwas [h

ttps://www.zeit.de/2023/13/elektronische-patientenakte-datenschutz-karl-lauterbach/komplettansicht], weil Menschen einzigartig sind und schon wenige Datenpunkte reichen, um Diagnosen oder Laborberichte doch konkret einer Person zuzuordnen.

Zweitens könnten die weitgehenden Nutzungsrechte für das behandelnde Personal ein Problem sein: So hat nicht nur ein Arzt in einer Klinik beispielsweise Zugriff, sondern viele der dort Beschäftigten – und zwar für jeweils drei Monate. Möglicherweise reicht es für einen Geheimdienst, eine Krankenschwester zu überzeugen, regelmäßig Daten abzuziehen. Auch wenn Zugriffe protokolliert werden: Sind die Daten einmal weg, lassen sie sich nicht zurückholen.

Warum die Gematik staatliche Angreifer nicht so wichtig findet

Fragt man die Gematik, warum man staatliche Angriffe nicht prüfen ließ, dann bekommt man ein recht allgemeines Statement zurück: Die elektronische Patientenakte werde "mit höchsten und modernsten Sicherheitsstandards gebaut, die wir zusammen mit den obersten Sicherheits- und Datenschutzbehörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) entwickeln und abstimmen". Man schütze die Telematikinfrastruktur (TI) "mit einem mehrstufigen Sicherheitskonzept" und bereite sich "auf Angriffe aller Akteure vor". Dabei würden auch staatliche Stellen mit in Betracht gezogen. Die ePA schließe damit potenzielle Einfallstore, die durch die bisherige Nutzung anderer Kanäle entstünden.

Steven Arzt, Leiter der Abteilung Secure Software Engineering, der das Gutachten beim Fraunhofer SIT betreut hat, betont, dass die Sicherheit des Systems "grundsätzlich geprüft" wurde. Dabei würde jeweils abgeschätzt, welche Relevanz welche Art von Angreifern haben. "Der Auftraggeber kann, abhängig von seiner eigenen Aufgabendefinition, bestimmte Angreifer als nicht relevant markieren." So wie es die Gematik getan hat. "Dies wird in der weiteren Analyse berücksichtigt und entsprechend dokumentiert", sagt Arzt.

Das Bundesgesundheitsministerium als Gesellschafter der Gematik sagte auf Anfrage, dass es "grundsätzlich" gelte, "jegliche Angriffe gegen die Systeme der elektronischen Patientenakte für alle zu unterbinden". Der Urheber eines solchen Angriffs sei aus IT-Sicherheitssicht nicht relevant. "Die Grundarchitektur der ePA bietet einen umfangreichen Schutz gegen viele potenzielle und relevante Bedrohungen." Ein Sprecher ließ offen, ob "viele" auch mächtige Angreifer wie Staaten beinhaltet, und wollte Nachfragen nicht weiter kommentieren. Die Akte sei aber "nicht zuletzt unter Einbeziehung der obersten Sicherheits- und Datenschutzbehörden konzipiert" worden.

Höchste Cybersicherheitsbehörde hält Entscheidung der Gematik für "nicht angebracht"

ZEIT ONLINE hat bei den besagten Behörden nachgefragt. Tatsächlich stößt die Ansicht der Gematik, laut der Angriffe ausländischer Regierungen nicht relevant seien, größtenteils auf Kritik.

Besonders bei sensiblen Daten wie jenen, die in der elektronischen Patientenakte gespeichert werden, sei "ein ganzheitlicher Sicherheitsansatz notwendig, der alle Bedrohungsakteure – einschließlich staatlicher Akteure – berücksichtigt", sagt eine BSI-Sprecherin auf Nachfrage. Das BSI ist die Aufsichtsbehörde für kritische Infrastrukturen im Gesundheitswesen und damit auch für die elektronische Patientenakte zuständig. Aus Sicht der Behörde sei der Schutz vor allen denkbaren Bedrohungen erforderlich, und es sei "nicht angebracht, potenzielle Angriffe ausländischer Regierungsorganisationen auszuschließen". Die elektronische Patientenakte enthalte hochsensible persönliche Daten, die besonders geschützt werden müssten.

Dies könne "im Rahmen der Gesamtbedrohungsanalyse mit sinnvollen Maßnahmen gegen andere Bedrohungen abgedeckt" sein. Möglicherweise wirkten also Schutzmaßnahmen gegen klassische "Hacker", wie sie im Verlauf des Gutachtens erörtert werden, auch gegen staatliche Akteure. Allerdings ergänzt die Sprecherin, "dass staatliche Organisationen über erhebliche Ressourcen und Expertise verfügen, um gezielt Informationen zu sammeln oder Infrastrukturen zu kompromittieren".

Das Bundesamt für Verfassungsschutz bestätigt auf Anfrage, dass fremde Nachrichtendienste "grundsätzlich auch ein Interesse an Daten deutscher Bürgerinnen und Bürger" hätten. "Cyberangriffe sind ein probates Mittel für fremde Nachrichtendienste, auch solche Daten zu erlangen", schreibt die Behörde. Solche Angriffe stellten "eine Bedrohung für die deutsche Politik, Wirtschaft, Wissenschaft sowie für kritische Infrastrukturen dar".

Die Behörde verweist in ihrer Antwort zudem auf den aktuellen Verfassungsschutzbericht 2023 [https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2024-06-18-verfassungsschutzbericht-2023.pdf?__blob=publicationFile&v=17], in dem sie auf mehreren Seiten explizit vor den Aktivitäten des russischen Geheimdienstes warnt. Die Gefährdung müsse "als hoch eingestuft werden". Mit allen Mitteln spioniere der Geheimdienst in Deutschland – sowohl mit Cyberangriffen als auch mit klassischer Informationsgewinnung. Im Fokus stünden Angehörige diplomatischer Vertretungen und anderer Behörden oder Firmen, aber auch Wissenschaftlerinnen und Wissenschaftler oder Studierende. "Sofern die gewonnenen Informationen die Zielpersonen kompromittieren können, scheuen die Dienste auch vor aggressiven

Anwerbungsversuchen nicht zurück", heißt es in dem Bericht. Gerade Deutschland sei auch aufgrund seiner Rolle in der Europäischen Union, der Nato und weiteren internationalen Organisationen für andere Staaten von besonderem Interesse und weiterhin ein zentrales Ziel von politischer Spionage.

Ein Sprecher der Bundesbeauftragten für den Datenschutz erklärt, dass die Bundesdatenschützerin nicht in das Gutachten eingebunden sei und "daher keine eigenen Kenntnisse darüber" habe, nach welchen Maßgaben der Gematik das Fraunhofer SIT seine Untersuchung durchgeführt habe. Die Aussage der Gematik, "dass Angriffe von Regierungsorganisationen nicht relevant sind", könne die BfDI daher nicht beurteilen.

Das Bundesverteidigungsministerium und der Bundesnachrichtendienst ließen Fragen von ZEIT ONLINE unbeantwortet.

"Vertrauen wird dann nicht entstehen"

Mitglieder des Parlamentarischen Kontrollgremiums, die den Bundesnachrichtendienst sowie den militärischen Abschirmdienst überprüfen und sich gut mit der üblichen Praxis von Geheimdiensten auskennen, lassen keine Zweifel daran, dass auch sie die Entscheidung der Gematik nicht nachvollziehen können.

"Selbstverständlich sind diese hochsensiblen Daten ein durchaus lohnendes Angriffsziel – auch und gerade für Organisationen, die im direkten Kontakt mit ausländischen Regierungen stehen", sagt Konstantin von Notz von den Grünen, Vorsitzender des Parlamentarischen Kontrollgremiums, dazu auf Anfrage von ZEIT ONLINE.

Die Aussage, dass in Bezug auf das ePA-System Angriffe durch Regierungsorganisationen als "nicht relevant" eingestuft werden, habe ihn gerade angesichts der Sensibilität der gespeicherten Daten "durchaus verblüfft". Gerade jetzt, wo es um die flächendeckende Einführung der elektronischen Patientenakte gehe, müsse die Sicherheit der Daten höchste Priorität haben. "Ist dies nicht der Fall, riskieren wir erfolgreiche Angriffe. Vertrauen wird dann nicht entstehen."

Auch sein Kollege im Parlamentarischen Kontrollgremium, der stellvertretende Vorsitzende und CDU-Abgeordnete Roderich Kiesewetter, zeigt sich erstaunt: Gerade für feindliche ausländische Regierungen sei es "im Rahmen hybrider Einflussnahme absolut relevant, an Gesundheitsdaten deutscher Bürger zu gelangen". Warum die Gematik die Relevanz möglicher Sicherheitsbedrohungen festlege und nicht die dafür zuständigen Nachrichtendienste oder Sicherheitsbehörden, halte er "für hoch fragwürdig".

"Im Rahmen transnationaler Repression lässt sich erkennen, dass relevante Personen häufig manipuliert und erpresst werden, indem Familienmitgliedern gedroht wird", sagt Kiesewetter. Geheimdienste ziehen sich dann nicht die Daten der Zielperson, sondern etwa des Ehemannes oder der Großmutter, und versuchen so beispielsweise eine verantwortliche Person im Bereich kritischer Infrastrukturen zu beeinflussen.