Deutscher Bundestag **Drucksache 20/14939**

20. Wahlperiode 11.02.2025

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Christina Baum, Martin Sichert, Thomas Dietz, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 20/14668 –

Sicherheitsbedenken bezüglich der elektronischen Patientenakte

Vorbemerkung der Fragesteller

Die elektronische Patientenakte (ePA) soll ab Februar 2025 für alle gesetzlich Versicherten eingeführt werden. Ziel der ePA ist es, sämtliche Gesundheitsinformationen der Versicherten zu speichern und den berechtigten Akteuren im Gesundheitswesen zugänglich zu machen.

Der Chaos Computer Club (CCC) kritisierte aktuell aus seiner Sicht bestehende Sicherheitsmängel der elektronischen Patientenakte seit ihrer Einführung. Angeblich könnten unberechtigte Personen einfach auf Gesundheitsdaten von über 70 Millionen Versicherten zugreifen. Studien zeigten angeblich erhebliche Sicherheitslücken bei der Ausgabe von Praxisausweisen und Zugangstoken. Ein Gutachten, das die Sicherheit der ePA bestätigt, wird vom CCC infrage gestellt (www.ccc.de/en/updates/2024/ende-der-epa-experimente).

Die gematik GmbH hat schnell auf diese Kritik reagiert und mitgeteilt: Obwohl die vom CCC aufgezeigten Angriffsszenarien technisch möglich seien, würden sie in der Praxis als unwahrscheinlich gelten. Gründe hierfür seien die Notwendigkeit komplexer Voraussetzungen wie die illegale Beschaffung eines Institutionsausweises und anderer Zugangsdaten. Unberechtigte Zugriffe seien strafbar. Die gematik GmbH arbeitete intensiv mit Sicherheitsbehörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) an Maßnahmen zur Abwehr dieser Angriffe. Schutzmaßnahmen umfassten die Stärkung der Sicherheitsinfrastruktur und weitere Verschlüsselungen. Während der Pilotphase könnten nur ausgewählte Leistungserbringer auf die ePA zugreifen. Bedeutende Sicherungsmaßnahmen seien bereits in Arbeit, um die Telematikinfrastruktur (TI) noch besser zu schützen. Die Sicherheit der ePA werde permanent geprüft und weiterentwickelt (www.gematik.de/newsroom/news-detail/aktuelles-stellungnahme-zum-ccc-vortrag-zur-epa-fuer-alle).

Laut gematik GmbH sind „technische Lösungen zum Unterbinden der Angriffsszenarien bereits konzipiert und in der Umsetzung“ (ebd.). Die Telematikinfrastruktur sei insgesamt „mit höchsten und modernsten Sicherheitsstandards“ gebaut (ebd.). Darüber hinaus kündigt die gematik GmbH die „Ausweitung der Überwachungsmaßnahmen wie Monitoring und Anomalie-Erkennung“ an (ebd.). „Sicherheits- und Datenschutzbehörden“ sowie externe Experten seien involviert (ebd.).

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Gesundheit vom 10. Februar 2025 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Die Fragesteller möchten Klarheit über die Maßnahmen erhalten, die zur Sicherung der sensiblen Gesundheitsdaten der Bürger getroffen wurden und noch werden. Im Rahmen dessen dienen diese Fragen dazu, zu gewährleisten, dass alle Bedenken berücksichtigt werden und maximale Transparenz über die implementierten Sicherheitsmaßnahmen besteht. Eine gründliche Überprüfung der Sicherheit der ePA ist essenziell, um das Vertrauen der Öffentlichkeit zu gewinnen und mögliche Risiken zu minimieren.

1. Gibt es detaillierte Belege oder Berichte darüber, wie die identifizierten, von der gematik GmbH selbst als technisch möglich bewerteten Schwachstellen konkret behoben wurden, um sicherzustellen, dass die ePA wirklich gegen solche Angriffe geschützt ist (wenn ja, bitte darlegen)?

Um die vom Chaos Computer Club (CCC) aufgezeigten möglichen Angriffsszenarien auf die elektronische Patientenakte (ePA) zu unterbinden, werden kurzfristig zusätzliche Sicherheitsmaßnahmen in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) umgesetzt. Demnach ist der Zugriff auf das Aktensystem während der Pilotphase ausschließlich auf die in den Modell- und Pilotregionen teilnehmenden und verifizierten Leistungserbringer beschränkt. Vor dem bundesweiten Rollout bei allen Leistungserbringern werden zudem weitere technische und organisatorische Lösungen zur Erhöhung der Sicherheit umgesetzt und abgeschlossen sein. Die gematik hat hierzu mit dem BSI einen umfangreichen Maßnahmenplan erarbeitet, wie der Start der neuen ePA, die Pilotierungsphase und der sich daran anschließende bundesweite Rollout so mit Sicherheitsmaßnahmen flankiert wird, dass zu jederzeit ein angemessenes Sicherheitsniveau erhalten bleibt.

2. Wie wurde die von der gematik GmbH festgestellte Unwahrscheinlichkeit („in der Realität nicht sehr wahrscheinlich“) des Erfolgs möglicher Angriffsszenarien plausibilisiert (vgl. Vorbemerkung der Fragesteller)?

Die gematik und das BSI haben das Risiko möglicher Angriffsszenarien bewertet. Dementsprechend wäre ein Angriff zwar „möglich“, ist in der Realität aber eher unwahrscheinlich. In der Praxis bedeutet dies, dass ein hoher technischer Aufwand betrieben werden und ein Identitätsdiebstahl erfolgen müsste, um die erforderlichen Mittel zu erlangen. Dazu kommen das potentielle Entdeckungsrisiko und die Strafbarkeit der Handlung.

3. Welche spezifischen Sicherheitsmechanismen zur Abwehr möglicher Angriffsszenarien wurden bereits integriert, welche sind in der Umsetzung, welche in der Konzeption?

Die Bundesregierung nimmt die durch den CCC veröffentlichten Hinweise zur Sicherheit der elektronischen Patientenakte ePA sehr ernst. Die vom CCC beschriebenen Probleme sind bekannt und werden gelöst. Darüber hat sich das Bundesministerium für Gesundheit (BMG) auch vor dem 38. Chaos Communication Congress (38C3) mit dem CCC ausgetauscht. Das BMG und die gematik stehen insbesondere im intensiven Austausch mit den zuständigen Sicherheitsbehörden wie dem BSI und es wurden bereits technische Lösungen zum Unterbinden der Angriffsszenarien konzipiert, deren Umsetzung jeweils rechtzeitig abgeschlossen sein wird. Für die am 15. Januar 2025 gestartete Pilotphase bedeutet dies, dass zunächst nur die in der Modellregion teilnehmenden und explizit gelisteten Leistungserbringer („Whitelisting“) auf die ePA der Versicherten zugreifen können.

Vor dem bundesweiten Rollout bei den Leistungserbringern werden weitere technische Lösungen umgesetzt und abgeschlossen sein. Dazu gehört insbesondere, dass organisatorisch sowohl die Prozesse zur Herausgabe als auch zur Sperrung von Karten sowie technisch das VSDM++-Verfahren nachgeschärft werden. Gleichzeitig werden zusätzliche Überwachungsmaßnahmen wie Monitoring und Anomalie-Erkennung implementiert. Somit steht weder der kontrollierten Inbetriebnahme in den Modellregionen noch dem bundesweiten Rollout nach Umsetzung der Maßnahmen etwas entgegen. Die ePA für alle kann sicher von Praxen, Krankenhäusern, Apotheken sowie Patientinnen und Patienten genutzt werden.

4. Haben unabhängige Sicherheitsexperten die Risikoeinschätzung der gematik GmbH bestätigt, welche unabhängigen Sicherheitsprüfungen wurden und werden ggf. durchgeführt, um die Sicherheit der ePA zu gewährleisten, welche Ergebnisse haben diese Prüfungen erbracht, und inwieweit wurden die Empfehlungen der durchgeführten Sicherheitsprüfungen umgesetzt?

5. Gibt es unabhängige Prüfungen, um sicherzustellen, dass der Zugriff auf ePA-Daten in der Praxis sicher bleibt, und ggf. welche?

10. Inwiefern wird die Telematikinfrastruktur insgesamt kontinuierlichen Prüfungen von unabhängigen Experten unterzogen, um möglichst keine Schwachstellen zu übersehen, und um welche Prüfungen konkret handelt es sich dabei ggf.?

Die Fragen 4, 5 und 10 werden gemeinsam beantwortet.

Das BSI ist eine unabhängige und neutrale Stelle für Fragen zur Daten- und IT-Sicherheit. Generell wird und wurde die gematik jederzeit hinsichtlich ihrer sicherheitsrelevanten Bewertungen und Entscheidungen vom BSI als nationale Cyber-Sicherheitsbehörde begleitet. Darüber hinaus beauftragt die gematik regelmäßig externe Sicherheitsgutachten zum Design der Telematikinfrastruktur (TI) und ihrer Anwendungen. Im Kontext der ePA-Sicherheitsarchitektur sei an dieser Stelle auf die Gutachten der Technischen Universität Graz und des Fraunhofer-Instituts für Sichere Informationstechnologie verwiesen, die auf der Webseite der gematik veröffentlicht wurden. Außerdem wird die konkrete Implementierung der Produkte durch die Industrie vor ihrer Zulassung durch Gutachterinnen und Gutachter geprüft. Diese Prüfung wird von der gematik GmbH und (im Fall der ePA) zusätzlich vom BSI qualitätssichernd begleitet.

Darüber hinaus ist die gematik hinsichtlich des Sicherheitsdesigns der ePA und aller anderen Produkte der TI vollständig transparent und veröffentlicht kontinuierlich sämtliche Spezifikationen. Soweit die gematik selbst den Auftrag erteilt hat, wie z. B. im Fall des E-Rezeptes, wird zusätzlich der Quellcode der auf dieser Basis entwickelten Software veröffentlicht. Auf diese Weise können auch externe Sicherheitsforscherinnen und Sicherheitsforscher ohne Beauftragung Sicherheitslücken identifizieren.

Neben diesen Sicherheitsanalysen vor der Inbetriebsetzung werden im Auftrag der gematik regelmäßig Penetrationstests nach Start des Produktivbetriebs durchgeführt. Im Rahmen des von der gematik seit Oktober 2022 gestarteten Bug-Bounty-Programms („Coordinated Vulnerability Disclosure Program“) steht dies auch externen Sicherheitsforschenden offen.

Regelmäßig werden bei diesen Tests und Analysen Verbesserungspotentiale entdeckt, auf die hier nicht im Einzelnen eingegangen werden kann. Im Fall des „Coordinated Vulnerability Disclosure Program“ der gematik GmbH sind diese

aber z. B. bei Zustimmung der Sicherheitsforschenden auf der Webseite der gematik veröffentlicht.

6. Soll und ggf. wie soll sichergestellt werden, dass keine menschlichen Fehler zu Sicherheitslücken führen, und was wird nach Kenntnis der Bundesregierung konkret unternommen, um die Schulung von Nutzern und die Handhabung von sensiblen Ausweisen und Karten effektiv zu gestalten?

Fehler durch menschliches Versagen werden sich nie vollständig vermeiden lassen. Personen, die berufsmäßig dazu berechtigt sind, auf die betreffenden Daten zuzugreifen, müssen verantwortungsvoll damit umgehen. Im Fall der Praxisausweise hat die Gesellschafterversammlung der gematik aber beschlossen, dass zusätzliche Sensibilisierungsmaßnahmen ergriffen werden sollen, um den Ausweisinhaberinnen und -inhabern die Kritikalität der betreffenden Chipkarten zu verdeutlichen und auf den sensiblen Umgang mit der Karte und der dazugehörigen PIN hinzuwirken.

7. Wie wird sichergestellt, dass die Ausgabeprozesse für Heilberufs- und Praxisausweise sowie Gesundheitskarten manipulationssicher gestaltet sind?

Die Bundesregierung hat nach den Feststellungen des CCC im Jahr 2019 das Mandat für die Definition und Durchsetzung der Sicherheitsanforderungen der Herausgabeprozesse dieser Ausweise an die gematik übertragen. Seitdem wurden diese Prozesse verschärft, so dass aktuell weder ein Praxisausweis noch ein Heilberufsausweis ohne eine persönliche Identifikation auf dem eIDAS- (electronic IDentification, Authentication and trust Services) Vertrauensniveau „hoch“ ausgegeben werden kann. Seitdem sind der Bundesregierung keine Fälle von missbräuchlichem Erwerb einer solchen Karte durch Fehler im Herausgabeprozess bekannt geworden.

8. Welche Maßnahmen werden unternommen, um den Missbrauch der Telematikinfrastruktur-Ausweise zu verhindern?

Mit drei Maßnahmenkategorien soll der Missbrauch der Praxisausweise und der Heilberufsausweise verhindert werden:

Prävention:

– Sicherstellung im Rahmen der Ausgabeprozesse, dass nur berechtigte Personen diese Ausweise erhalten.
– In Planung: Sicherstellung, dass ein Praxisausweis nicht ohne manuelle Prüfung erneut zur Einrichtung eines VPN-Zugangs verwendet werden kann (potentieller Hinweis auf unberechtigte Weitergabe).
– Monitoring, ob eine Praxis tatsächlich alle ihr zugeordneten Praxisausweise besitzt (bei teilnehmenden Einrichtungen an der Pilotierung vollständig, bundesweit stichprobenartig).

Detektion:

– Protokollierung aller Zugriffe auf E-Rezept und ePA, so dass Versicherte im Rahmen der Datenschutzkontrolle alle erfolgten Zugriffe nachvollziehen können.

– In Umsetzung: Erkennung von missbräuchlicher Verwendung durch Erkennung von Sicherheitsproblemen oder Anomalien im Verhalten der Nutzenden beim Zugriff auf Dienste der TI.

Reaktion:

– In Umsetzung: Zugriffsverweigerung bei erkannten Sicherheitsproblemen (in Abhängigkeit der Faktenlage automatisch oder nach manueller Prüfung).

– Möglichkeit der Strafverfolgung im Rahmen des § 399 des Fünften Buches Sozialgesetzbuch (SGB V).

9. Sind bisher Vorfälle von unberechtigten Zugriffen auf die ePA bekannt geworden, welche sind dies ggf., und welche Konsequenzen wurden daraus ggf. gezogen?

Solche Fälle sind bisher nicht bekannt.

11. Welche spezifischen Überwachungsmaßnahmen sollen zum Monitoring und zur Anomalie-Erkennung ausgeweitet werden, und wie werden diese Monitoring- und Anomalie-Detektionstechnologien konkret implementiert?

Die Festlegung, welche Überwachungsmaßnahmen zum Monitoring und zur Anomalie-Erkennung zusätzlich getroffen werden, erfolgt in enger Abstimmung zwischen der gematik und dem BSI. Auch die Implementierung erfolgt in Abstimmung mit dem BSI.

12. Wie stellt die Bundesregierung angesichts einer sich ständig weiterentwickelnden Bedrohungslandschaft sicher, dass die Sicherheitsarchitektur der ePA auch in den kommenden Jahren auch gegen neue, noch unbekannte Bedrohungen gewappnet ist, gibt es einen klaren Plan für regelmäßige, weitreichende Sicherheitsaudits und Upgrades, und wie oft findet eine Sicherheitsüberprüfung der Telematikinfrastruktur statt?

Die Sicherheit der Anwendungen der TI wird generell auch mit Blick auf zukünftige potenzielle Bedrohungen stetig weiterentwickelt. So sind die kryptographischen Algorithmen in der ePA bereits heute gegen sogenannte „store now, decrypt later“-Angriffe gewappnet, die im Kontext der Quantenkryptographie relevant sind. Darüber hinaus führt die gematik regelmäßig Audits zur Betriebssicherheit und beauftragt Penetrationstests. Es werden pro Jahr zwischen 15 und 20 Audits und etwa 20 bis 25 Penetrationstests in der TI durchgeführt.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333