Deutscher Bundestag **Drucksache 20/14668**

20. Wahlperiode 24.01.2025

Kleine Anfrage

der Abgeordneten Dr. Christina Baum, Martin Sichert, Thomas Dietz, Kay-Uwe Ziegler, Carolin Bachmann, Jörg Schneider, Jürgen Braun, Gereon Bollmann und der Fraktion der AfD

Sicherheitsbedenken bezüglich der elektronischen Patientenakte

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 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.

Wir fragen die Bundesregierung:

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)?
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)?
3. Welche spezifischen Sicherheitsmechanismen zur Abwehr möglicher Angriffsszenarien wurden bereits integriert, welche sind in der Umsetzung, welche in der Konzeption?
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?
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?
7. Wie wird sichergestellt, dass die Ausgabeprozesse für Heilberufs- und Praxisausweise sowie Gesundheitskarten manipulationssicher gestaltet sind?
8. Welche Maßnahmen werden unternommen, um den Missbrauch der Telematikinfrastruktur-Ausweise zu verhindern?
9. Sind bisher Vorfälle von unberechtigten Zugriffen auf die ePA bekannt geworden, welche sind dies ggf., und welche Konsequenzen wurden daraus ggf. gezogen?
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.?
11. Welche spezifischen Überwachungsmaßnahmen sollen zum Monitoring und zur Anomalie-Erkennung ausgeweitet werden, und wie werden diese Monitoring- und Anomalie-Detektionstechnologien konkret implementiert?

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?

Berlin, den 15. Januar 2025

Dr. Alice Weidel, Tino Chrupalla und Fraktion

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