Deutscher Bundestag **Drucksache 21/2417**

21. Wahlperiode 27.10.2025

Kleine Anfrage

der Abgeordneten Tobias Matthias Peterka, Ulrich von Zons, Lukas Rehm, Manfred Schiller, Tobias Teich, Gerold Otten, Dr. Rainer Kraft, Jan Wenzel Schmidt, Thomas Korell, Dr. Paul Schmidt, Robin Jünger, Dr. Malte Kaufmann, Dr. Daniel Zerbin, Mirco Hanker, Dr. Christina Baum, Dr. Maximilian Krah, Reinhard Mixl, Dr. Michael Blos, Carolin Bachmann, Stefan Keuter, Marc Bernhard, Knuth Meyer-Soltau, Claudia Weiss, Julian Schmidt, Achim Köhler, Edgar Naujok, Kay-Uwe Ziegler, Joachim Bloch, Udo Theodor Hemmelgarn, Stefan Henze, Uwe Schulz, Sascha Lensing, Rocco Kever, Volker Scheurell, Otto Strauß, Tobias Ebenberger und der Fraktion der AfD

Cybersicherheit und Stellenentwicklung im Bereich IT-Sicherheit im Geschäftsbereich des Bundesministeriums für Gesundheit

Die Cybersicherheitslage in Deutschland wird von der Bundesregierung und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) regelmäßig als „angespannt bis kritisch“ beschrieben (www.tuev-verband.de/pressemitteilungen/angespannt-bis-kritisch-die-cybersicherheitslage-in-deutschland#:~:text=Lagebericht%20des%20BSI:%20Cybersicherheit%20in%20Deutschland%20).

Auch der Bundesrechnungshof warnt vor eklatanten Sicherheitslücken in den Rechenzentren und Netzen des Bundes (https://www.spiegel.de/politik/deutschland/cybersicherheit-rechnungshof-warnt-vor-mangelndem-schutz-der-bundes-it-a-6baacfe5-2e6b-4e8b-a64b-e10d9cf2585e). Unter anderem bemängelt der Bundesrechnungshof, dass weniger als 10 Prozent der mehr als 100 Bundesrechenzentren die Mindeststandards erfüllen, dass die Notstromversorgung in Krisenlagen vielfach unzureichend ist und dass kritische IT-Dienste oft nicht georedundant verfügbar sind (s. o.). Nach aktuellen Berichten hat die Bundesregierung im Bereich IT-Sicherheit Stellen abgebaut (https://www.security-insider.de/bund-reduziert-it-sicherheitsstellen-a-508f57e078fd32fa7cd1a915db00c76e/).

Die fortschreitende Digitalisierung des Gesundheitswesens, insbesondere durch die Einführung der elektronischen Patientenakte (ePA), das E-Rezept sowie die Nutzung der Telematikinfrastruktur, erhöht die Anforderungen an die IT-Sicherheit im Gesundheitsbereich erheblich. Persönliche Gesundheitsdaten zählen zu den besonders sensiblen Datenkategorien. Ihre Vertraulichkeit, Integrität und Verfügbarkeit sind von überragender Bedeutung für den Schutz der Patienten, das Vertrauen in das Gesundheitssystem sowie für die Erfüllung rechtlicher Verpflichtungen.

Darüber hinaus hat die COVID-19-Pandemie gezeigt, dass digitale Systeme im Gesundheitswesen in Krisenzeiten massiv belastet werden und gleichzeitig neue Angriffspunkte für Cyberattacken entstehen. Anwendungen wie die Corona-Warn-App, Impf- und Testdatenbanken oder digitale Meldeketten ver-

deutlichen die besondere Bedeutung resilienter IT-Sicherheitsarchitektur im Geschäftsbereich des Bundesministeriums für Gesundheit (BMG).

Vor diesem Hintergrund stellt sich den Fragestellern die Frage, inwieweit Cybersicherheitsaspekte in den Verantwortungsbereich des BMG integriert sind und wie sich die personelle Ausstattung in den letzten Jahren entwickelt hat.

Wir fragen die Bundesregierung:

1. Über wie viele Rechenzentren verfügt das BMG aktuell, und wie viele davon erfüllen nachweislich die geltenden Mindeststandards für IT-Sicherheit?
2. Welche dieser Rechenzentren verfügen über eine funktionsfähige Notstromversorgung, die auch längerfristige (über mehrere Stunden oder Tage) Krisenlagen abdecken kann?
3. An welchen Standorten des BMG sind kritische IT-Dienste georedundant verfügbar, und wie wird die Ausfallsicherheit regelmäßig überprüft?
4. Welche Investitionen hat das BMG in den Jahren von 2020 bis 2025 konkret für den Ausbau und die Absicherung seiner IT-Infrastruktur (einschließlich Rechenzentren, Netze, Cloudlösungen) getätigt?
5. In welchem Umfang hat das BMG in den vergangenen fünf Jahren ggf. Sicherheitsüberprüfungen (z. B. durch das BSI oder durch unabhängige Dienstleister) durchführen lassen, und mit welchen Ergebnissen?
6. Welche organisatorischen Zuständigkeiten für Cybersicherheit bestehen innerhalb des BMG (z. B. eigenes Computer Emergency Response Team [CERT], IT-Sicherheitsreferate, Zusammenarbeit mit dem BSI)?
7. Welche spezifischen Zuständigkeiten bestehen im Geschäftsbereich des BMG für den Schutz persönlicher Gesundheitsdaten, insbesondere im Zusammenhang mit der elektronischen Patientenakte und der Telematikinfrastruktur?
8. Welche Maßnahmen hat das BMG seit 2020 ergriffen, um auf die Kritikpunkte des Bundesrechnungshofes im Bereich IT-Sicherheit zu reagieren?
9. Wie viele Sicherheitsvorfälle oder Cyberangriffe wurden in den letzten fünf Jahren im Zuständigkeitsbereich des BMG registriert, und wie wurde jeweils darauf reagiert (bitte nach Jahr und Anzahl der Zwischenfälle aufschlüsseln)?
10. Welche Bedrohungsanalysen zu Cyberangriffen auf die Telematikinfrastruktur und die elektronische Patientenakte liegen dem BMG ggf. vor, und wie fließen diese in die Praxis der IT-Sicherheit ein?
11. Welche technischen und organisatorischen Maßnahmen wurden seit 2020 ggf. ergriffen, um den Schutz der elektronischen Patientenakte sowie anderer digitaler Gesundheitsanwendungen (z. B. E-Rezept, Corona-Warn-App) zu gewährleisten?
12. Welche Lehren haben die Bundesregierung und das BMG aus sicherheitsrelevanten Vorfällen oder Angriffen während der COVID-19-Pandemie (z. B. auf Impfregister, Meldeketten, Corona-Warn-App) gezogen?
13. Welche konkreten Schritte plant das BMG, um bis spätestens 2030 die vollständige Einhaltung der vom Bundesrechnungshof geforderten Mindeststandards (inklusive Notstromversorgung und georedundanter Systeme) sicherzustellen?

14. Wie viele Stellen im Bereich IT-Sicherheit existieren derzeit im Geschäftsbereich des BMG (bitte nach Behörden und Besoldungs- bzw. Entgeltgruppen aufschlüsseln)?
15. Wie hat sich die Zahl der IT-Sicherheitsstellen im BMG seit 2018 entwickelt (bitte jährlich angeben und nach Behörden differenzieren sowie nach Besoldungs- bzw. Entgeltgruppe aufschlüsseln)?
16. Wie viele dieser Stellen entfielen unmittelbar auf Aufgaben zur Sicherung personenbezogener Gesundheitsdaten?
17. Wurden in den Jahren von 2020 bis 2024 Stellen im Bereich IT-Sicherheit im Geschäftsbereich des BMG abgebaut, umgewidmet oder neu geschaffen, und wenn ja, in welchem Umfang?
18. Welche konkreten Aufgabenbereiche decken die IT-Sicherheitsstellen im BMG ab (z. B. Netzwerksicherheit, Kryptografie, Incident Response, Schutz kritischer Infrastrukturen, IT-Forensik)?
19. Wie viele dieser Stellen sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?
20. Welche spezifischen Qualifikationen im Bereich Datenschutz und Cybersicherheit werden bei der Besetzung von Stellen gefordert oder bevorzugt berücksichtigt?
21. Welche Schulungen und Fortbildungen wurden für Beschäftigte des BMG und seiner nachgeordneten Behörden im Bereich IT-Sicherheit und Datenschutz seit 2018 durchgeführt (bitte nach Jahr und Art der Fortbildung aufschlüsseln)?
22. Welche Kooperationen bestehen ggf. mit anderen Ressorts, insbesondere dem Bundesamt für Sicherheit in der Informationstechnik, sowie mit internationalen Organisationen im Hinblick auf den Schutz von Patientendaten?
23. Welche Maßnahmen ergreift das BMG, um die Resilienz seiner besonders sensiblen Systeme trotz möglicher Personalknappheit im Bereich IT-Sicherheit sicherzustellen?
24. Inwiefern beteiligt sich das BMG an europäischen oder internationalen Organisationen im Hinblick auf den Schutz von Patientendaten?
25. Plant die Bundesregierung, die IT-Sicherheitskapazitäten im BMG mittelfristig auszubauen, und mit welchem zeitlichen Horizont?

Berlin, den 22. Oktober 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