Deutscher Bundestag **Drucksache 21/2846**

21. Wahlperiode 18.11.2025

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Tobias Matthias Peterka, Ulrich von Zons, Lukas Rehm, weiterer Abgeordneter und der Fraktion der AfD – Drucksache 21/2417 –

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

Vorbemerkung der Fragesteller

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

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Gesundheit vom 17. November 2025 übermittelt.

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

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.

Vorbemerkung der Bundesregierung

Cyberkriminelle und staatliche Akteure professionalisieren ihre Arbeitsweise. Sie sind technisch auf dem neuesten Stand und agieren aggressiv. Längst haben sie Strukturen für ihre kriminellen Dienstleistungen etabliert. Deutschland setzt der Bedrohung eine tragfähige Cybersicherheitsarchitektur entgegen. Die Funktionsfähigkeit der Cybersicherheitsarchitektur ist unbedingt zu schützen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet die Sicherheitslage in den fünf Dimensionen Bedrohung, Angriffsfläche, Gefährdung, Schadwirkung und Resilienz, wobei die Resilienz den vier anderen Dimensionen positiv entgegenwirkt (vgl. www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html).

Cyberbedrohungen gingen im vergangenen Jahr von diversen Angreifergruppen aus. APT-Gruppen („Advanced Persistent Threats“) betrieben beispielsweise Cyberspionage und starteten Angriffe auf Behörden der auswärtigen Angelegenheiten, der Verteidigung und der öffentlichen Sicherheit und Ordnung. Auch Unternehmen und Institutionen, die in diesen Bereichen tätig sind, waren betroffen. Darüber hinaus wurde die arbeitsteilige cyberkriminelle Schattenwirtschaft weiterhin professioneller: Sogenannte Access Broker handelten mit erbeuteten Zugangsdaten. Andere Cybercrime-Gruppen nutzten Zero-Day-Schwachstellen (d. h. Schwachstellen, die dem Hersteller noch nicht bekannt sind) zum Datendiebstahl. Auch die Angriffsflächen vergrößerten sich mit der weiter fortschreitenden Digitalisierung.

Über alle Arten von Cyberbedrohungen nehmen die Gefährdungen stetig weiter zu. Von einem Ransomware-Angriff auf einen kommunalen IT-Dienstleister Ende Oktober 2023 waren beispielsweise 72 kommunale Kunden mit rund 20.000 kommunalen Arbeitsplätzen betroffen. Die Folge waren teils monatelange Ausfallzeiten. Eine weitere Folge erfolgreicher Cyberangriffe sind exorbitante „Lösegeldzahlungen“ für durch Ransomware-Angriffe verschlüsselte Daten. Für gestohlene exfiltrierte Daten wurde dabei im Schnitt fast dreimal so viel gezahlt wie für erbeutete verschlüsselte Daten.

In allen Dimensionen hat sich die IT-Sicherheitslage deutlich verschärft: Zum einen führt der russische Angriffskrieg auf die Ukraine zu vermehrten Angriffen auf Verbündete der Ukraine (u. a. Deutschland) durch russlandfreundliche Cybergruppierungen oder mutmaßlich staatliche Stellen. Dabei müssen auch Sekundäreffekte zur Zerstörung von IT-Infrastruktur berücksichtigt werden.

Die stetig wachsende Komplexität der IT-Landschaft mit zunehmender Vernetzung von Behörden untereinander, mit Unternehmen, Bürgern sowie Cloud-Diensten erweitert die Wirkungsbreite von Angriffen auf einzelne Institutionen. Gleichzeitig ist der berechtigten Erwartung der Bevölkerung auf einen auch mit IT funktionierenden Rechtsstaat und einen Fortschritt der Digitalisierung der öffentlichen Verwaltung zu genügen.

Mit der Expertise des BSI, der Strafverfolgungsbehörden und den Verantwortlichen für Informationssicherheit in der Bundesverwaltung wird der oben dargestellten Gefährdungslage effektiv entgegengewirkt.

Durch die Veröffentlichung sensibler Informationen wäre die in langjährigen Prozessen erarbeitete Resilienz der Informationstechnik des Bundes erheblich gefährdet.

Der Aufbau von Expertise, IT-Sicherheitsinfrastruktur, Prozessen und Resilienzfaktoren beansprucht umfangreiche Ressourcen und insbesondere Zeit. Der Wiederaufbau nach einem erfolgreichen Cyberangriff könnte aber einen solchen Schaden anrichten, dessen Behebung potentiell ein Vielfaches davon kosten würde.

Mit Blick auf die in kurzen Abständen auftretenden kritischen Sicherheitslücken, den Zeitbedarf für das Patchen dieser Lücken und vor dem Hintergrund einer unbekannten Menge an möglichen Zero-Day-Exploits ist jederzeit mit Angriffen zu rechnen. Sollte mit absehbar verfügbaren Mitteln derzeit kein Angriff durchführbar sein, führt dies angesichts der schnellen technologischen Entwicklung zu keiner Reduzierung der Gefährdungslage, denn einmal veröffentlichte Informationen zur Sicherheitsarchitektur und deren Änderung lassen sich über die Zeit aggregieren und analysieren und mit zukünftig verfügbaren technischen Möglichkeiten für einen erfolgreichen Cyberangriff auf die IT der Bundesverwaltung ausnutzen. Dies bezieht sich auch auf Anzahl, Ort und Ausstattung von Rechenzentren, Ergebnisse technischer Sicherheitsüberprüfungen, Anzahl registrierter Sicherheitsvorfälle oder Cyberangriffe, zugrundeliegender Bedrohungsanalysen, ergriffener und in Planung befindlicher technischer und organisatorischer Maßnahmen gegen Cyberangriffe, der Anzahl von Stellen in der IT-Sicherheit und deren Entwicklung und weiterer Resilienzmaßnahmen wie Krisenstäben und konkreten Angaben zu internationaler Kooperation und Krisenlagen. Im Bereich der Informationssicherheit kommt der strategischen Vorausschau daher eine überragende Bedeutung zu.

Bereits wenige Kenntnisse über mögliche Schwachstellen reichen Cyberkriminellen oder staatlichen Akteuren aus, um die gesamte IT-Infrastruktur von Behörden unbrauchbar zu machen (vgl. u. a. oben skizzierte Angriffe auf Kommunalverwaltungen, Angriff auf Berliner Kammergericht, Hackerangriff auf den Deutschen Bundestag).

Darüber hinaus spielen bedeutende technische Entwicklungen auch bösartigen Akteuren im digitalen Raum in die Karten. Beispielsweise kann heute in einer noch vor kurzer Zeit kaum absehbaren Qualität künstliche Intelligenz genutzt werden, um aus der (auch aggregierten) Darstellung von Sicherheitsprodukten, Angaben zu Investitionen, konkreten Ergebnissen aus technischen Sicherheitsüberprüfungen konkrete Angriffsvektoren abzuleiten. Dies gilt auch für die Offenlegung von Softwareentwicklungen. In der Folge würde sich die Lage in allen vier Dimensionen Bedrohung, Angriffsfläche, Gefährdung und Schadwirkung dramatisch verschlechtern.

Die Sicherstellung der Staats- und Regierungsfunktion wäre massiv gefährdet.

Die Bundesregierung beantwortet die im Rahmen des parlamentarischen Fragerechts angefragten Sachverhalte gegenüber dem Deutschen Bundestag grundsätzlich öffentlich, transparent und vollständig, um dem verfassungsrechtlich verbrieften Aufklärungs- und Informationsanspruch des Deutschen Bundestages zu entsprechen. Soweit erfragte Informationen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann, und gegebenenfalls alternative Formen der Informationsvermittlung zu suchen, die das Informationsinteresse des Parlaments unter Wahrung der berechtigen Geheimhaltungsinteressen der Regierung befriedigen (BVerfGE 124, 161,193).

Nach sorgfältiger Abwägung ist die Bundesregierung zu der Auffassung gelangt, dass die Beantwortung der Kleinen Anfrage nicht durchgängig vollständig erfolgen kann.

Die Fragen 1, 3, in Teilen 5, 9, 13, 15 bis 17 und 19 können nach sorgfältiger Prüfung und Abwägung auch in eingestufter Form nicht beantwortet werden.

Die IT-Infrastruktur der Bundesregierung ist jeden Tag einer Vielzahl unterschiedlicher Angriffe ausgesetzt. Zur Aufrechterhaltung der Staats- und Regierungsfunktion ist diese Infrastruktur angemessen zu schützen. Eine Beeinträchtigung oder sogar ein Ausfall aufgrund erfolgreicher Cyberangriffe muss auch in der Zukunft bestmöglich verhindert werden.

Informationen zu sämtlichen im Bundesministerium für Gesundheit (BMG) eingesetzten IT-Sicherheitsprodukten, Anzahl, Ort und Ausstattung von Rechenzentren, Ergebnisse technischer Sicherheitsüberprüfungen, Anzahl registrierter Sicherheitsvorfälle oder Cyberangriffe, zugrundeliegender Bedrohungsanalysen, ergriffener und in Planung befindlicher technischer und organisatorischer Maßnahmen gegen Cyberangriffe, der Anzahl von Stellen in der IT-Sicherheit und deren Entwicklung und weiterer Resilienzmaßnahmen wie Krisenstäben und konkreten Angaben zu internationaler Kooperation und Krisenlagen und Softwareentwicklungen beziehen sich unmittelbar auf die Fähigkeiten der Abwehr von Cybergefährdungen der Bundesbehörden. Ein Bekanntwerden der detaillierten Information würde das Staatswohl gefährden, denn damit würde es etwaigen Angreifern ermöglicht, konkrete Hinweise zu den im BMG eingesetzten Schutzmaßnahmen zu erhalten.

Unter Kenntnis der durch das BMG eingesetzten Produkte könnten Angreifer Schwachstellen ausmachen und diese gezielt ausnutzen. Vor allem in der Zusammenschau mit den Antworten der Bundesregierung auf die Kleinen Anfragen der Fraktion der CDU/CSU auf Bundestagsdrucksachen 20/8707 und 20/14887 ließe sich durch Aggregation und direkten Vergleich detaillierte Erkenntnisse ableiten, die die Entwicklung des Einsatzes und der Beschaffung von IT-Sicherheitsprodukten und der zukünftigen konkreten IT-Sicherheitsstrategie in der Bundesverwaltung und im BMG zeigen.

Mit der Beantwortung würde offengelegt, wie sich das BMG für Gesundheit vor Cyberangriffen schützt. Dies würde potentiellen Angreifern wichtige Hinweise für etwaige Angriffe liefern. Dies gefährdet die Arbeitsfähigkeit und damit unmittelbar die Erfüllung des gesetzlichen Auftrags. Aufgrund der Vernetzung des BMG mit anderen Behörden hätte ein solche Ausnutzung einer Schwachstelle potentiell erhebliche Auswirkungen auf die Informationssicherheit der gesamten Bundesverwaltung und könnte unmittelbar die Gewährleistung der Handlungsfähigkeit der Bundesverwaltung gefährden.

Es muss deshalb potentiellen Angreifern verborgen bleiben, welche IT-Sicherheitsprodukte, Anzahl, Ort und Ausstattung von Rechenzentren, Ergebnisse technischer Sicherheitsüberprüfungen, Anzahl registrierter Sicherheitsvorfälle oder Cyberangriffe, zugrundeliegender Bedrohungsanalysen, ergriffener und in Planung befindlicher technischer und organisatorischer Maßnahmen gegen Cyberangriffe, der Anzahl von Stellen in der IT-Sicherheit und deren Entwicklung und weiterer Resilienzmaßnahmen wie Krisenstäben und konkreten Angaben zu internationaler Kooperation und Krisenlagen im BMG zum Schutz der IKT-Infrastrukturen und darin verarbeiteten Daten aktuell eingesetzt werden bzw. der Arbeit zugrunde liegen.

Die Geheimhaltungsbedürftigkeit der Informationen ist sorgfältig abgewogen worden, eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Aufgabenerfüllung des BMG nicht ausreichend Rechnung tragen, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78 [139]). Schon die Angabe, wie das BMG den Cybergefahren begegnet, welche Angriffe es erkannt hat, wie viele Personen welche IT-Sicherheitsaufga-

ben ausführen, welche Bedrohungsszenarien es betrachtet und welche internationalen Kooperationen bestehen oder nicht bestehen, könnte zu einer Analyse der Verwundbarkeiten und Änderung des Angriffsverhaltens führen, die eine weitere Abwehr der Cybergefahren unmöglich machen würde. In diesem Fall wäre ein Ersatz durch andere Instrumente nicht möglich.

Würden potentielle Angreifer detaillierte Kenntnis über vorgenannte Informationen erhalten, wäre ein Angriff auf das BMG deutlich einfacher zu gestalten und mit höherer Erfolgsaussicht verbunden.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber der Pflicht zur Aufrechterhaltung der Staats- und Regierungsfunktion der Bundesrepublik Deutschland zurückstehen.

Vorgenannte Ausführungen und Abwägungen gelten auch für die Gewährleistung des sicheren Betriebs der Telematikinfrastruktur und ihrer Anwendungen und Systeme.

1. Über wie viele Rechenzentren verfügt das BMG aktuell, und wie viele davon erfüllen nachweislich die geltenden Mindeststandards für IT-Sicherheit?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Fragen nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

2. Welche dieser Rechenzentren verfügen über eine funktionsfähige Notstromversorgung, die auch längerfristige (über mehrere Stunden oder Tage) Krisenlagen abdecken kann?

Alle Rechenzentren verfügen über eine funktionsfähige Notstromversorgung.

3. An welchen Standorten des BMG sind kritische IT-Dienste georedundant verfügbar, und wie wird die Ausfallsicherheit regelmäßig überprüft?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Fragen nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

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?

IT-Sicherheit ist IT-Betriebsziel, sodass alle Investitionen in den IT-Betrieb grundsätzlich in den Ausbau und die Absicherung der IT-Infrastruktur fließen.

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?

Es findet eine regelmäßige Beratung mit dem BSI auf Basis seiner Zuständigkeiten für die Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes gemäß § 3 Absatz 1 Satz 2 Nummer 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) sowie im Speziellen für die Durchführung von technischen Prüfungen zum Schutz amtlich geheim gehaltener Informationen nach § 4 Sicherheitsüberprüfungsgesetz gegen die Kenntnisnahme durch Unbefugte gemäß § 3 Absatz 1 Satz 2 Nummer 9 BSIG statt. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Frage nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

6. Welche organisatorischen Zuständigkeiten für Cybersicherheit bestehen innerhalb des BMG (z. B. eigenes Computer Emergency Response Team [CERT], IT-Sicherheitsreferate, Zusammenarbeit mit dem BSI)?

Organisatorische Zuständigkeiten sind dem Organigramm des BMG zu entnehmen.

7. Welche spezifischen Zuständigkeiten bestehen im Geschäftsbereich des BMG für den Schutz persönlicher Gesundheitsdaten, insbesondere im Zusammenhang mit der elektronischen Patientenakte und der Telematikinfrastruktur?

Organisatorische Zuständigkeiten sind den Organigrammen des BMG und der Geschäftsbereichsbehörden zu entnehmen.

Themen, die die Digitalisierung des Gesundheitswesens im Rahmen des Fünften Buches Sozialgesetzbuch betreffen, sind auf Seiten des BMG in einer Digitalisierungsabteilung gebündelt. Dies betrifft auch Themen zur Datensicherheit 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?

Das IT-Sicherheitsniveau im BMG wird durch einen kontinuierlichen Verbesserungsprozess aufrechterhalten. Die Kritikpunkte des Bundesrechnungshofes werden in diesem Prozess berücksichtigt.

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)?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Fragen nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

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?

Die Fragen 10 und 11 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Festlegungen und Maßnahmen zur Telematikinfrastruktur, die Fragen der Datensicherheit berühren, hat die gematik im Benehmen mit dem BSI zu treffen, Festlegungen und Maßnahmen, die Fragen des Datenschutzes berühren, im Benehmen mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI; vgl. § 311 Absatz 2 Satz 1 des Fünften Buches Sozialgesetzbuch – SGB V). Auf dieser Grundlage hat die gematik einen umfangreichen Rahmen geschaffen mit technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Telematikinfrastruktur und ihrer Anwendungen.

Alle relevanten Erkenntnisse fließen in diesem Rahmen in die Maßnahmen zur Gewährleistung der Sicherheit der Telematikinfrastruktur und ihrer Anwendungen und Systeme ein.

Der Schutz der durch die – zwischenzeitlich eingestellten – Corona-Warn-App (CWA), die CovPass- und die CovPassCheck-App verarbeiteten Daten war der Bundesregierung ein hohes Anliegen. Daher wurde bei der Entwicklung ein besonderes Augenmerk auf technische und organisatorische Maßnahmen der Datensicherheit und des Datenschutzes gelegt. Dazu zählte auch die frühzeitige und den ganzen Entwicklungs- bzw. Bereitstellungsprozess begleitende Beteiligung von BSI und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI).

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?

Die ressortübergreifende Cybersicherheitsarchitektur des Bundes obliegt in ihrer strategischen Ausrichtung und operativen Koordinierung dem Bundesministerium des Innern sowie dem Bundesministerium für Digitales und Staatsmodernisierung. Diese Ressorts tragen die Federführung für die Weiterentwicklung der Cybersicherheitsstrategie der Bundesregierung sowie für die Festlegung übergreifender Sicherheitsstandards.

Das BMG setzt im Rahmen seines Geschäftsbereichs die von den zuständigen Stellen entwickelten und koordinierten Sicherheitsmaßnahmen um. Die Umsetzung erfolgt dabei in enger Abstimmung mit dem BSI.

Konkrete sicherheitsrelevante Vorkommnisse und die hieraus resultierenden Erkenntnisse werden im Rahmen der etablierten Melde- und Kommunikationswege zwischen den beteiligten Behörden ausgewertet. Die Ableitung übergreifender Handlungsempfehlungen und strategischer Anpassungen liegt in der Federführung vorgenannter Stellen.

Während der Zeit der Bereitstellung der CWA, der CovPass- und der CovPassCheck-App sind keine Sicherheitslücken bekannt, die die Sicherheit oder den Schutz der mit der CWA, der CovPass- oder der CovPassCheck-App verarbeiteten Daten gefährdet hätten. Insofern zeigt dies, dass die Maßnahmen zur Sicherstellung von Datensicherheit und Datenschutz wirksam waren.

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?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Fragen nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

14. Wie viele Stellen im Bereich IT-Sicherheit existieren derzeit im Geschäftsbereich des BMG (bitte nach Behörden und Besoldungs- bzw. Entgeltgruppen aufschlüsseln)?

Alle Stellen im IT-Betrieb haben auch das Ziel IT-Sicherheit.

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)?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Fragen nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

16. Wie viele dieser Stellen entfielen unmittelbar auf Aufgaben zur Sicherung personenbezogener Gesundheitsdaten?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Fragen nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

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?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Fragen nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

18. Welche konkreten Aufgabenbereiche decken die IT-Sicherheitsstellen im BMG ab (z. B. Netzwerksicherheit, Kryptografie, Incident Response, Schutz kritischer Infrastrukturen, IT-Forensik)?

Alle für den grundsätzlich sicheren IT-Betrieb notwendigen Aufgaben werden abgedeckt.

19. Wie viele dieser Stellen sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Frage nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

20. Welche spezifischen Qualifikationen im Bereich Datenschutz und Cybersicherheit werden bei der Besetzung von Stellen gefordert oder bevorzugt berücksichtigt?

Spezifische Qualifikationen sind in Stellenausschreibungen öffentlich einsehbar.

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)?

Die Beschäftigten des BMG und dessen Geschäftsbereich nehmen regelmäßig Angebote für Schulungen und Fortbildungen wahr.

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?

Das BMG steht im Rahmen seiner Aufgaben im Austausch mit dem BSI und anderen Ressorts innerhalb der Bundesregierung ebenso wie mit ausländischen Dienststellen und internationalen Organisationen zu verschiedenen Themen, unter anderem auch zum Patientendatenschutz.

Festlegungen und Maßnahmen zur Telematikinfrastruktur, die Fragen der Datensicherheit berühren, hat die gematik im Benehmen mit dem BSI zu treffen, Festlegungen und Maßnahmen, die Fragen des Datenschutzes berühren, im Benehmen mit der BfDI (vgl. § 311 Absatz 2 Satz 1 SGB V).

23. Welche Maßnahmen ergreift das BMG, um die Resilienz seiner besonders sensiblen Systeme trotz möglicher Personalknappheit im Bereich IT-Sicherheit sicherzustellen?

Es ist bekannt, dass die IT-Konsolidierung begonnen wurde. Maßnahmen ergeben sich aus dem Kabinettbeschluss zur IT-Konsolidierung und sind veröffentlicht. Im Übrigen gilt die Gemeinsame Geschäftsordnung der Bundesministerien (GGO).

24. Inwiefern beteiligt sich das BMG an europäischen oder internationalen Organisationen im Hinblick auf den Schutz von Patientendaten?

Das BMG steht im Rahmen seiner Aufgaben auch zu diesem Thema im Austausch mit europäischen oder internationalen Organisationen.

25. Plant die Bundesregierung, die IT-Sicherheitskapazitäten im BMG mittelfristig auszubauen, und mit welchem zeitlichen Horizont?

Die Bundesregierung misst der IT-Sicherheit in allen Ressorts einen hohen Stellenwert bei. Die personelle und technische Ausstattung der Bundesministerien wird grundsätzlich im Rahmen der regulären Haushaltsverfahren sowie in Abstimmung mit den zuständigen Stellen fortlaufend evaluiert.

Im Geschäftsbereich des BMG werden die IT-Sicherheitskapazitäten entsprechend den sich wandelnden Anforderungen und Aufgabenstellungen angepasst. Unter anderem im Rahmen der Umsetzung europäischer Regelungen und Vorhaben – wie beispielsweise der NIS-2-Richtlinie – wird aktuell der Personalbedarf in verschiedenen Bereichen geprüft.

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