Deutscher Bundestag **Drucksache 21/2698**

21. Wahlperiode 11.11.2025

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 21/2409 –

Cybersicherheit und Stellenabbau im Bereich IT-Sicherheit im Geschäftsbereich des Bundesministeriums des Innern

Vorbemerkung der Fragesteller

Cybersicherheit ist eine zentrale Zukunftsaufgabe, die gesamtstaatlich gedacht und umgesetzt werden muss. Nach aktuellen Berichten wurden im Geschäftsbereich des Bundesministeriums des Innern (BMI) rund 344 Stellen im Bereich IT-Sicherheit gestrichen, betroffen sind damit auch zentrale Behörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) und möglicherweise weitere nachgeordnete Behörden (www.security-insider.de/bund-reduziert-it-sicherheitsstellen-a-508f57e078fd32fa7cd1a915db00c76e/).

Angesichts der von der ehemaligen Bundesregierung selbst als „besorgniserregend“ beschriebenen Cybersicherheitslage erscheint dieser Stellenabbau den Fragestellern widersinnig (s. o.).

Der Stellenabbau im Geschäftsbereich des BMI erscheint ihnen widersprüchlich, weil gerade das BMI eine Kernverantwortung für die zivile Cybersicherheit, den Schutz kritischer Infrastrukturen sowie die Koordinierung der gesamtstaatlichen Abwehrmaßnahmen trägt. Im Hinblick auf die zunehmende Bedrohungslage durch Cyberoperationen staatlicher und nichtstaatlicher Akteure (www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html#:~:text=2.,verwundbar%20waren%20zudem%20Android%2DSysteme) ist ein Abbau von Ressourcen in diesem sicherheitskritischen Bereich nach Auffassung der Fragesteller erklärungsbedürftig.

Auch mit Blick auf die Warnung des Bundesrechnungshofes 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) ist der Stellenabbau in den Augen der Fragesteller fragwürdig. 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 sei und dass kritische IT-Dienste oft nicht georedundant verfügbar seien (s. o.).

Die Sicherheitsbehörden des Bundesministeriums des Innern – darunter das Bundesamt für Sicherheit in der Informationstechnik, das Bundeskriminalamt (BKA), das Bundesamt für Verfassungsschutz (BfV), die Bundespolizei sowie

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 10. November 2025 übermittelt.

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

die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) – sind in besonderem Maße mit der Abwehr, Aufklärung und Bekämpfung von Cyberangriffen sowie mit der Absicherung der eigenen Informations- und Kommunikationssysteme befasst.

Vor diesem Hintergrund ist es in den Augen der Fragesteller von besonderem Interesse, wie das BMI organisatorisch, personell und technisch aufgestellt ist, um solchen Bedrohungen wirksam zu begegnen zu können. Gleichzeitig stellen sich den Fragestellern Fragen nach der Prioritätensetzung und der strategischen Ausrichtung der Bundesregierung.

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. Diese Cybersicherheitsarchitektur muss unbedingt funktionsfähig bleiben.

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. Die APT-Gruppen 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 erwartet die Bevölkerung zu Recht einen auch mit IT funktionierenden Rechtsstaat und einen Fortschritt der Digitalisierung der öffentlichen Verwaltung.

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 potenziell 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 17 bis 19 und 24 bis 26 sowie teilweise Fragen 10, 21, 27 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 des Innern (BMI) 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 Bundesministerium des Innern eingesetzten Schutzmaßnahmen zu erhalten.

Unter Kenntnis der durch das BMI 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 BMI zeigen.

Mit der Beantwortung würde offengelegt, wie sich das BMI vor Cyberangriffen schützt. Dies würde potenziellen Angreifern wichtige Hinweise für etwaige Angriffe liefern. Dies gefährdet die Arbeitsfähigkeit und damit unmittelbar die Erfüllung des gesetzlichen Auftrags. Aufgrund der Vernetzung des BMI mit anderen Behörden hätte ein solche Ausnutzung einer Schwachstelle potenziell 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 BMI 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 BMI 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 BMI den Cybergefahren begegnet, welche Angriffe es erkannt hat, wie viele Personen welche IT-Sicherheitsaufgaben 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 potenzielle Angreifer detaillierte Kenntnis über vorgenannte Informationen erhalten, wäre ein Angriff auf das BMI 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.

Im Geschäftsbereich des BMI wurden seit 2022 keine Stellen im Bereich IT-Sicherheit abgebaut. Der von der Fraktion der AfD genannte Abbau von 344 Stellen ist auf eine fehlerhafte Meldung zur jährlichen Schriftlichen Frage 35 der Abgeordneten Anke Domscheit-Berg für das Jahr 2024 siehe Bundestagsdrucksache 20/10170 zurückzuführen. Der Fehler fiel auf, nachdem für 2025 wieder die korrekte Zahl gemeldet wurde. Die fehlerhafte Zulieferung wurde gegenüber der Abgeordneten Anke Domscheit-Berg in der Antwort der Bundesregierung auf ihre Schriftliche Frage 25 auf Bundestagsdrucksache 20/14639 korrigiert.

1. Wie viele Stellen im Bereich IT-Sicherheit wurden seit 2022 im Geschäftsbereich des BMI abgebaut – aufgeschlüsselt nach Behörde, Jahr und Funktion?

2. Welche Behörden (z. B. BSI, BfV oder spezifische Referate im BMI) sind vom Stellenabbau besonders betroffen?

3. In welcher Relation stehen diese Abbauzahlen zur durchschnittlichen Personalausstattung in vergleichbaren Haushaltsjahren?

4. Welche konkreten Gründe lagen dem BMI für die Entscheidung über den Abbau zugrunde (z. B. Haushaltseinsparungen, Prioritätenverschiebung, Umstrukturierung)?

5. Welche Kriterien und Prozesse wurden angewendet, um zu entscheiden, welche Stellen gestrichen werden?

6. Wurden fachlich besonders qualifizierte oder schwer zu ersetzende Positionen bevorzugt verschont, und wenn ja, wie wurde das methodisch sichergestellt?

7. Welche Auswirkungen erwartet die Bundesregierung im BMI-Fachbereich für IT-Sicherheit (z. B. beim BSI) durch den Stellenabbau konkret für Aufgaben wie Abwehr, Monitoring, Krisenreaktion, Prävention?

8. Gibt es interne Risikoanalysen oder Szenarien, in denen durch Stellenabbau Fähigkeiten eingeschränkt werden könnten (z. B. bei größeren Cybervorfällen)?

9. Wurden durch das BMI bereits konkrete Leistungseinbußen gegenüber Dritten (Bundesministerien, nachgeordnete Behörden, KRITIS-Betreiber [KRITIS = kritische Infrastrukturen]) festgestellt und diagnostiziert?

Fragen 1 bis 9 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet:

Im Geschäftsbereich des BMI wurden seit 2022 keine Stellen im Bereich IT-Sicherheit abgebaut. Auf die Vorbemerkung der Bundesregierung wird verwiesen.

10. Wie viele unbesetzte Stellen im Bereich IT-Sicherheit (nach Eingruppierung) existieren aktuell im Geschäftsbereich des BMI?

Aktuell sind im Geschäftsbereich des BMI etwa 300 Stellen unbesetzt.

Im Übrigen wird auf die Beantwortungen der jährlichen Anfragen der Abgeordneten Anke Domscheit-Berg nach besetzten und unbesetzten IT-Sicherheitsstellen in den Bundesministerien und deren nachgeordneten Behörden auf ihre Schriftliche Frage 25 auf Bundestagsdrucksache 20/14639 verwiesen.

Hinsichtlich der Eingruppierung der Stellen wird auf die Vorbemerkung der Bundesregierung verwiesen.

11. Wie haben sich offene Positionen (inklusive langdauernde Vakanz) im IT-Sicherheitsbereich über die Jahre von 2022 bis 2025 entwickelt?

Die Vakanzen haben sich im Geschäftsbereich des BMI unterschiedlich entwickelt. Teilweise waren die Stellen durchgehend besetzt, teilweise ergab sich durch eine nicht nahtlose Nachbesetzung eine vorübergehende Vakanz. Zudem können sich Vakanzen ergeben haben, wenn neue IT-Sicherheitsstellen dazugekommen sind. Im Übrigen wird auf die Beantwortungen der jährlichen Anfragen der Abgeordneten Anke Domscheit-Berg nach besetzten und unbesetzten IT-Sicherheitsstellen in den Bundesministerien und deren nachgeordneten Behörden auf ihre Schriftliche Frage 25 auf Bundestagsdrucksache 20/14639 verwiesen.

12. Welche Maßnahmen unternimmt das BMI, um Fachkräfte für IT-Sicherheit zu gewinnen, zu binden und ggf. neu aufzubauen?

Die Bundesregierung verbessert mit zahlreichen Maßnahmen die Attraktivität des öffentlichen Dienstes in der Bundesverwaltung. Vor allem auch vor dem Hintergrund des Personalbedarfs bei IT-Fachkräften hat der Bund bereits mit verschiedenen Maßnahmen reagiert. So sind in den letzten Jahren – in enger Abstimmung mit den Bedarfsträgern aus der Praxis – vielfältige Instrumente zur Gewinnung und Bindung von Fachkräften weiterentwickelt oder neue eingeführt worden.

Im Hinblick auf die von den Fragestellern benannten Fachkräfte für IT-Sicherheit sind insbesondere die folgenden Instrumente hervorzuheben:

Im Beamtenbereich:

- Einstellung von Fachkräften relevanter Fachrichtungen in höher bezahlte Besoldungsgruppen;
- neu konzipierte, praxisorientiert und flexibel einsetzbare Personalgewinnungs- und Personalbindungsprämie;
- die verbesserte Anerkennung von beruflichen Erfahrungszeiten bei der Stufenzuordnung.

Im Tarifbereich:

- dauerhaft deutliche Anhebung des Entgeltniveaus insbesondere in den fachkräfterelevanten höheren Entgeltgruppen;
- verschiedene Zulagen mit vielfältigen Kombinationsmöglichkeiten für die Gewinnung und Bindung von Fachkräften;
- Erleichterung bei der Gewinnung von Quereinsteigerinnen und -einsteigern.

Zudem wurden speziell für die Gewinnung von IT-Fachkräften neue Vorbereitungsdienste eingerichtet, um mit den veränderten Aufgaben und Anforderungen in diesem Bereich Schritt zu halten (z. B. „Vorbereitungsdienst für den gehobenen nichttechnischen Verwaltungsdienst des Bundes – Fachrichtung digitale Verwaltung und Cyber-Sicherheit“ sowie „Vorbereitungsdienst für den gehobenen technischen Verwaltungsdienst im Informationstechnikzentrum Bund“).

Auch das Laufbahnrecht wurde an die veränderten Anforderungen angepasst. So ist beispielsweise der Zugang zum höheren Dienst bereits mit einjährigem Master-Abschluss möglich.

13. Verfolgt das BMI einen mittelfristigen Personalplan, um den Rückgang im IT-Sicherheitsbereich zu stoppen oder umzukehren, insbesondere wenn die Bedrohungslage zunimmt?

Auf die Antwort zu den Fragen 1 bis 9 wird verwiesen.

14. Gibt es Szenarien oder Triggerpunkte (z. B. bei bestimmten Cybervorfällen, Bedrohungsindizes), bei denen das BMI personalpolitisch reagiert (z. B. Rückbaustopp, Neueinstellungen)?

Das BMI richtet sein Personalmanagement im Rahmen der jeweils geltenden haushälterischen Rahmenbedingungen grundsätzlich anhand der bestehenden Bedarfslagen aus.

15. Welche Rolle spielen externe Kooperationen (z. B. mit Ländern, EU, Privatwirtschaft) zur Kompensation von Personaldefiziten im Bereich IT-Sicherheit, in welchem Umfang greifen das BMI und die genannten Sicherheitsbehörden auf externe Dienstleister im Bereich IT-Sicherheit zurück, und welche Risiken sieht die Bundesregierung dabei ggf. für die Vertraulichkeit, Integrität und Sicherheit der Arbeitsprozesse?

Das BMI und die genannten Sicherheitsbehörden setzen für hoheitliche Sicherheitsaufgaben im Sinne der Arbeitnehmerüberlassung keine externen Dienstleister ein.

16. Wie hat das BMI gegenüber anderen Ressorts, Behörden und externen Akteuren (z. B. KRITIS-Betreiber, IT-Dienstleister) den Stellenabbau begründet und kommuniziert?

Auf die Antwort zu den Fragen 1 bis 9 wird verwiesen.

17. Über wie viele Rechenzentren verfügt das BMI 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 Frage 17 nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

18. Welche dieser Rechenzentren (vgl. Frage 17) verfügen über eine funktionsfähige Notstromversorgung, die auch längerfristige (über mehrere Stunden oder Tage) Krisenlagen abdecken kann?

Alle Rechenzentren verfügen über eine funktionsfähige Notstromversorgung.

19. An welchen Standorten des BMI 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 Frage 19 nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

20. Welche Investitionen hat das BMI 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.

21. In welchem Umfang hat das BMI in den vergangenen fünf Jahren Sicherheitsüberprüfungen (z. B. durch das BSI oder 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 Numer 1 Gesetz 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 des Sicherheitsüberprüfungsgesetzes (SÜG) gegen die Kenntnisnahme durch Unbefugte gemäß § 3 Absatz 1 Satz 2 Nummer 9 BSIG statt.

Im Übrigen wird hinsichtlich der Frage nach konkreten Ergebnissen von Sicherheitsüberprüfungen 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.

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

Organisatorische Zuständigkeiten sind dem Organigramm des BMI zu entnehmen.

23. Welche Maßnahmen hat das BMI seit 2020 ggf. ergriffen, um auf die Kritikpunkte des Bundesrechnungshofes im Bereich IT-Sicherheit zu reagieren?

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

24. Wie viele Sicherheitsvorfälle oder Cyberangriffe wurden in den letzten fünf Jahren im Zuständigkeitsbereich des BMI registriert, und wie wurde jeweils darauf reagiert (bitte nach Jahr, Anzahl der Zwischenfälle, Behörde und Art der Angriffe differenzieren)?

25. Welche Bedrohungsanalysen zu Cyberangriffen auf die genannten Sicherheitsbehörden des BMI liegen dem BMI vor?

26. Welche technischen und organisatorischen Maßnahmen wurden seit 2018 ergriffen, um das BMI und seine Sicherheitsbehörden gegen Cyberangriffe abzusichern?

Aufgrund des Sachzusammenhangs werden die Fragen 24 bis 26 zusammen beantwortet.

Es wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Fragen 24 bis 26 nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

27. Welche konkreten Schritte plant das BMI ggf., um bis spätestens 2030 die vollständige Einhaltung der vom Bundesrechnungshof geforderten Mindeststandards (inklusive Notstromversorgung und georedundanter Systeme) sicherzustellen?

Die vom Bundesrechnungshof geforderte Einhaltung der Mindeststandards (inklusive Notstromversorgung und georedundanter Systeme sicherzustellen) wird im Rahmen des kontinuierlichen Verbesserungsprozesses angestrebt.

Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Frage 27 nach konkreten Schritten nicht erfolgen kann, weil die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

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