Deutscher Bundestag **Drucksache 21/2845**

21. Wahlperiode 17.11.2025

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Tobias Matthias Peterka, Peter Bohnhof, Ulrich von Zons, weiterer Abgeordneter und der Fraktion der AfD – Drucksache 21/2421 –

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

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/).

Das Bundesministerium für Arbeit und Soziales (BMAS) arbeitet mit großen Mengen personenbezogener Daten. Insbesondere beim sog. Bürgergeld ist ein hohes Maß an IT-Sicherheit erforderlich, um Missbrauch, Manipulation oder Datenabfluss zu verhindern. Angriffe auf die IT-Infrastruktur des BMAS oder auf Schnittstellen zwischen Bundesministerium, Jobcentern und Leistungsempfängern können die Auszahlung existenzsichernder Leistungen gefährden. Durch gezielte Cyberangriffe können Datenbestände verändert, Leistungsansprüche verfälscht oder Zahlungen an unberechtigte Empfänger umgeleitet werden. Die Möglichkeit, interne Abläufe des BMAS oder bei seinen nachgeordneten Behörden gezielt zu stören oder zu missbrauchen, eröffnet ein erhebliches Schadenspotenzial für die öffentliche Hand.

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

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

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. Advanced Persistent Threat-Gruppen (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 sol-

chen 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 (Entscheidungen des Bundesverfassungsgerichts (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, 12 und 14 bis 15 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 Arbeit und Soziales (BMAS) 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 BMAS eingesetzten Schutzmaßnahmen zu erhalten.

Unter Kenntnis der durch das BMAS 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 ließen 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 BMAS zeigen.

Mit der Beantwortung würde offengelegt, wie sich das BMAS 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 BMAS 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 BMAS zum Schutz der Infrastrukturen der Informations- und Kommunikationstechnologien 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 BMAS 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 BMAS 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 Analy-

se 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 BMAS und seinen Geschäftsbereich 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.

1. Über wie viele Rechenzentren verfügt das BMAS 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 (vgl. Frage 1) verfügen über eine funktionsfähige Notstromversorgung, die auch längerfristige (über mehrere Stunden oder Tage) Krisenlagen abdecken kann?

Alle Rechenzentren des BMAS verfügen über eine längerfristige Notstromversorgung unter Beachtung der Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik und der Nutzerpflichten der Netze des Bundes (NdB-Nutzerpflichten).

3. An welchen Standorten des BMAS 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 BMAS in den Jahren von 2022 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 BMAS in den vergangenen fünf Jahren 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 des Sicherheitsüberprüfungsgesetzes 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 BMAS (z. B. eigenes Computer Emergency Response Team [CERT], IT-Sicherheitsreferate, Zusammenarbeit mit dem BSI)?

Das Informationssicherheitsmanagement im BMAS wird im Referat Zb5 „IT-Steuerung“ wahrgenommen. Dort ist auch der Ressort-IT-Sicherheitsbeauftragte organisatorisch angesiedelt. Er berät die IT-Beauftragte in allen grundsätzlichen Belangen der Informationssicherheit und verfügt über ein direktes Vortragsrecht gegenüber der Hausleitung. Das operative IT-Sicherheitsmanagement wird im Referat Zb4 „IT-Betrieb“ wahrgenommen. Hier ist ebenfalls das Security Operations Center (SOC) angesiedelt. Das BMAS arbeitet eng mit dem Bundes Security Operations Center (BSOC) und dem Bundes-CERT im Bundesamt für Sicherheit in der Informationssicherheit zusammen. Weitere organisatorische Zuständigkeiten können dem Organigramm des BMAS entnommen werden.

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

Es werden alle geforderten Aufgaben des BSI IT-Grundschutzes im BMAS wahrgenommen. Hierzu zählen u. a. Informationssicherheitsmanagement, Netzwerksicherheit, Kryptografie, Incident Response, Schutz kritischer Infrastrukturen.

8. Welche Maßnahmen hat das BMAS seit 2020 ergriffen, um auf die Kritikpunkte des Bundesrechnungshofes im Bereich IT-Sicherheit zu reagieren (vgl. Vorbemerkung der Fragesteller)?

Das BMAS betreibt ein Managementsystem für Informationssicherheit (ISMS) unter Beachtung der BSI-Standards 200-x. Das IT-Sicherheitsniveau wird durch einen kontinuierlichen Verbesserungsprozess aufrechterhalten und an neue Gefährdungslagen angepasst. Die Kritikpunkte des Bundesrechnungshofes werden in diesem Prozess ebenso berücksichtigt, wie der technologische Wandel, neue Angriffstechniken und sonstige sicherheitsrelevante Rahmenbedingungen.

9. Wie viele Sicherheitsvorfälle oder Cyberangriffe wurden in den letzten fünf Jahren im Zuständigkeitsbereich des BMAS registriert, und wie wurde jeweils darauf reagiert (bitte nach Jahr und Anzahl der Vorfälle aufschlüsseln)?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen, nach der die Beantwortung der Fragen nicht erfolgen kann, weil die erbetenen Informatio-

nen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

10. Wie bewertet die Bundesregierung die aktuelle Gefährdungslage durch Cyberangriffe auf die IT-Systeme des BMAS und der mit dem Bürgergeld befassten Jobcenter?

Die Bundesregierung bewertet die IT-Sicherheitslage als sehr angespannt. Cyberkriminelle und staatliche Akteure professionalisieren zunehmend ihre Arbeitsweise. Die Bundesagentur für Arbeit (BA) und ihre dezentralen Lokationen sind jeden Tag ca. 1,3 Milliarden sicherheitsrelevanten Ereignissen ausgesetzt. Als KRITIS-Betreiberin gemäß § 8a Absatz 1 BSIG ist die BA dazu verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind. Die BA hat hierfür ein eigenes Computer Emergency Response Team (CERT), das aktiv über ein integriertes Security Operation Center (SOC) die digitale Sicherheit der BA überwacht und entsprechend Maßnahmen einleitet. Im Übrigen wird auf die Vorbemerkung der Bundesregierung und die Antwort zu Frage 6 verwiesen.

11. Welche Schulungs- und Sensibilisierungsmaßnahmen zum Thema Cybersicherheit wurden für Mitarbeiter des BMAS seit 2020 durchgeführt?

IT-Sicherheitsschulungen finden regelmäßig statt und sind fester Bestandteil der regulären IT-Schulungen.

12. Welche konkreten Schritte plant das BMAS, 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.

13. Wie viele Stellen im Bereich IT-Sicherheit existieren derzeit im Geschäftsbereich des BMAS (bitte nach Behörden und Besoldungsgruppen aufschlüsseln)?

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

14. Wie hat sich die Zahl der IT-Sicherheitsstellen im BMAS seit 2020 entwickelt (bitte jährlich angeben und nach Behörden differenzieren)?

15. Wurden in den Jahren 2022, 2023 und 2024 Stellen im Bereich IT-Sicherheit im Geschäftsbereich des BMAS abgebaut, umgewidmet oder neu geschaffen, und wenn ja, in welchem Umfang?

Die Fragen 14 und 15 werden gemeinsam beantwortet.

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 sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?

Derzeit ist eine Stelle unbesetzt. Ausgeschriebene Stellen bleiben zwischen sechs bis zwölf Monaten unbesetzt.

17. Welche besonderen Schwierigkeiten sieht die Bundesregierung bei der Gewinnung von IT-Sicherheitsfachkräften im Geschäftsbereich des BMAS, und welche Maßnahmen werden ergriffen, um diese Herausforderungen zu bewältigen?

Der allgemeine Fachkräftemangel insbesondere im Bereich der IT-Sicherheit und der Wettbewerb mit der Privatwirtschaft aufgrund der hohen Nachfrage sowie einem in Teilen besseren Gehaltsgefüges stellen besondere Herausforderungen bei der Personalgewinnung dar. Zudem erfordert die schnelle technologische Entwicklung eine ständige Fortbildung der IT-Fachkräfte. Neben Stellenausschreibungen setzen das BMAS und sein Geschäftsbereich auch auf Aus- und Weiterbildung und attraktive Arbeitsbedingungen um im Wettbewerb mit anderen Arbeitgebern bestehen zu können.

18. Welche Rolle spielt das Informationstechnikzentrum Bund (ITZBund) in Bezug auf die IT-Sicherheit für das BMAS, und wie entwickelt sich dort die Personalausstattung in diesem Bereich?

Das BMAS nimmt auch an der IT-Konsolidierung teil und verlagert IT-Services in die zentralen Rechenzentren im ITZ-Bund. Daher ist die Gewährleistung der Informationssicherheit im ITZ Bund auch für das BMAS von hoher Bedeutung.

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

Das BMAS nimmt ebenfalls an der IT-Konsolidierung teil. Maßnahmen ergeben sich aus dem Kabinettbeschluss zur IT-Konsolidierung und sind veröffentlicht. Im Übrigen gilt die Gemeinsame Geschäftsordnung der Bundesministerien (GGO).

20. Plant die Bundesregierung, die IT-Sicherheitskapazitäten im BMAS mittelfristig auszubauen, und wenn ja, mit welchem zeitlichen Horizont?

Das BMAS hat im Rahmen des NIS2-Umsetzungsgesetzes entsprechende Mehrbedarfe geltend gemacht, welche nach Inkrafttreten des Gesetzes und Bereitstellung der geforderten Stellen ausgeschrieben werden sollen.

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