Deutscher Bundestag **Drucksache 21/2693**

21. Wahlperiode 10.11.2025

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 21/2408 –

Cybersicherheit und Stellenentwicklung im Bereich IT-Sicherheit im Geschäftsbereich des Bundesministeriums für Forschung, Technologie und Raumfahrt

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/).

Angriffe auf interne IT-Infrastrukturen des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) könnten nicht nur vertrauliche Forschungs- und Entwicklungsdaten gefährden, sondern auch sicherheitsrelevante Auswirkungen auf strategische Zukunftstechnologien und die Raumfahrt haben. Gleichzeitig ist der Schutz im Austausch mit Unternehmen, Hochschulen, internationalen Partnern und Raumfahrtorganisationen essenziell, um Datenabflüsse und Manipulationen zu verhindern.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Forschung, Technologie und Raumfahrt vom 10. 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 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 1, 3, 5 (in Teilen), 11, 12, 15, 17, 18, 20 und 21 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 Regie-

rungsfunktion 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 BMFTR eingesetzten IT-Sicherheitsprodukten, 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 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 BMFTR eingesetzten Schutzmaßnahmen zu erhalten.

Unter Kenntnis der durch das BMFTR 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 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 BMFTR zeigen.

Mit der Beantwortung würde offengelegt, wie sich das BMFTR 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 BMFTR 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, 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 im BMFTR 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 BMFTR 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 BMFTR 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 BMFTR 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 BMFTR 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 des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) verfügen über eine funktionsfähige Notstromversorgung.

3. An welchen Standorten des BMFTR 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 BMFTR 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 BMFTR 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 be-

rühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

6. Wie wird die Europäische Weltraumorganisation (ESA) in die Cybersicherheitsstrategie des BMFTR eingebunden?

Die Integration erfolgt im Zuge der Zuständigkeitsübertragung des Themas Raumfahrt in das BMFTR entsprechend dem Organisationserlass des Bundeskanzlers vom 6. Mai 2025.

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

Die zentrale Zuständigkeit für Informationssicherheit wird durch den Informationssicherheitsbeauftragten und seine Mitarbeiterinnen und Mitarbeiter abgebildet. Nach BSI-Grundschutz-Baustein ISMS. 1.A1 trägt die Hausleitung die Gesamtverantwortung für die Informationssicherheit im BMFTR und gestaltet den Sicherheitsprozess mit.

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

Die Informationssicherheit im BMFTR umschließt ein ganzheitliches Konzept, um eine breite Informationssicherheit sicherzustellen.

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

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

10. In welcher Form arbeitet das BMFTR mit nationalen und internationalen Partnern im Bereich Forschung, Technologie und Raumfahrt zusammen, um gemeinsame Sicherheitsstandards gegen Cyberbedrohungen zu etablieren?

Das Forschungsrahmenprogramm der Bundesregierung für IT-Sicherheit „Digital. Sicher. Souverän.“ leistet einen zentralen Beitrag zur Etablierung gemeinsamer Sicherheitsstandards gegen Cyberbedrohungen, indem es ressortübergreifend die Aktivitäten der IT-Sicherheitsforschung bündelt und gezielt die Entwicklung innovativer IT-Lösungen fördert. Ziel ist die Förderung technologischer Souveränität Deutschlands und Europas sowie die Schaffung eines robusten Schutzes vor Cyberbedrohungen über nationale Grenzen hinweg. Das BMFTR fördert auch Vorhaben, in denen die Forschungspartner durch gemeinsame Forschungsanstrengungen sowie Beteiligung an politischen und fachlichen Normierungsprozessen einen aktiven Beitrag zur Schaffung international anschlussfähiger, praxistauglicher Cybersicherheits-Standards leisten.

Das derzeit laufende EU-Rahmenprogramm für Forschung und Innovation „Horizont Europa“ räumt der zivilen Sicherheitsforschung einen eigenen Bereich (Cluster) innerhalb der zweiten Säule „Globale Herausforderungen und industrielle Wettbewerbsfähigkeit Europas“ ein. Unter der Überschrift „Zivile Sicherheit für die Gesellschaft“ unterstützt dieser Cluster die europäische Forschungszusammenarbeit u. a. in der Cybersicherheit, Katastrophenvorsorge und Resilienz.

11. Welche Verfahren bestehen, um den vertraulichen Austausch mit Hochschulen, Forschungsinstituten, Technologieunternehmen und Raumfahrtorganisationen vor Cyberangriffen zu schützen?

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.

12. Wie viele Sicherheitsvorfälle oder Cyberangriffe wurden in den letzten fünf Jahren im Zuständigkeitsbereich des BMFTR 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 Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

13. Wie bewertet die Bundesregierung die aktuelle Gefährdungslage durch Cyberangriffe auf das BMFTR, insbesondere in Bezug auf hochsensible Forschungs- und Raumfahrtdaten?

Es wird auf die allgemeine Lageeinschätzung des BSI verwiesen.

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

Die Beschäftigten des BMFTR nehmen regelmäßig Angebote für Schulungen und Fortbildungen wahr.

15. Welche konkreten Schritte plant das BMFTR, 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.

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

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

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

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. Wurden in den Jahren 2022, 2023 und 2024 Stellen im Bereich IT-Sicherheit im Geschäftsbereich des BMFTR 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.

19. Wie viele dieser möglichen Stellen (vgl. Frage 18) sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?

Derzeit sind keine Stellen unbesetzt. Über den Durchschnitt der Vakanzen kann keine Aussage getroffen werden, da diese nicht zentral erfasst werden.

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

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.

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

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.

22. Welche Maßnahmen ergreift das BMFTR ggf., 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).

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

Nein.

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