Deutscher Bundestag **Drucksache 21/2647**

21. Wahlperiode 05.11.2025

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 21/2380 –

Cybersicherheit und Stellenentwicklung im Bereich IT-Sicherheit im Geschäftsbereich des Bundesministeriums für Wohnen, Stadtentwicklung und Bauwesen

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 Prozent22angespannt,f%C3 ProzentBCr%20Cyberangriffe%20durch%20Transparenz%20sch%C3 ProzentA4rfen%20und%20Cyber).

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

Mit der Digitalisierung von Verwaltungsverfahren im Bau- und Wohnungswesen entstehen für Bund, Länder und Kommunen neue Chancen, aber auch erhebliche Risiken. Digitale Bauantragsverfahren, die Wohnraumförderungsdatenbank, Building Information Modeling (BIM) in Planungs- und Bauprozessen sowie die internen Kommunikations- und Verwaltungsplattformen des Bundesministeriums für Wohnen, Stadtentwicklung und Bauwesen (BMWSB) sind zunehmend integraler Bestandteil staatlicher Kernaufgaben. Diese Verfahren haben bereits heute eine Schlüsselfunktion für die Umsetzung zentraler politischer Ziele – vom sozialen Wohnungsbau über Stadtentwicklungsprogramme bis hin zu Planungsprozessen für große Infrastrukturprojekte. Sie müssen daher im weiteren Sinne als Teil der kritischen Infrastruktur betrachtet werden. Ein erfolgreicher Cyberangriff auf diese Systeme könnte schwerwiegende Folgen haben: Blockaden oder Verzögerungen bei Bauanträgen könnten

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Wohnen, Stadtentwicklung und Bauwesen vom 5. November 2025 übermittelt.

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

die Umsetzung von Bauvorhaben erheblich verzögern, Manipulationen an der Wohnraumförderungsdatenbank könnten Förderentscheidungen verfälschen und das Vertrauen in staatliche Programme untergraben, Angriffe auf BIM-Verfahren könnten Bau- und Infrastrukturprojekte stören oder Fehlplanungen verursachen, Störungen in internen Verwaltungs- und Kommunikationssystemen könnten den Behördenbetrieb erheblich einschränken und die Zusammenarbeit mit Ländern und Kommunen gefährden.

Vor diesem Hintergrund stellt sich den Fragestellern die Frage, inwieweit Cybersicherheitsaspekte in den Verantwortungsbereich des Bundesministeriums für Wohnen, Stadtentwicklung und Bauwesen 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. 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 (vergleiche www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html).

Cyberbedrohungen gingen im vergangenen Jahr von diversen Angreifergruppen aus. Advanced Persistent Threat (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 (das heißt 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 (unter anderem 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 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 (vergleiche unter anderem 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 (Die 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 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 BMWSB 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 BMWSB eingesetzten Schutzmaßnahmen zu erhalten.

Unter Kenntnis der durch das BMWSB eingesetzten Produkte könnten Angreifer Schwachstellen ausmachen und diese gezielt ausnutzen. Vor allem in der Zusammenschau mit den Antworten der Bundesregierung auf die Kleinen Anfragen Bundestagsdrucksache 20/8707 und 20/14226 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 BMWSB zeigen.

Mit der Beantwortung würde offengelegt, wie sich das BMWSB 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 BMWSB 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 BMWSB zum Schutz der IKT-Infrastrukturen und darin verarbeiteten Daten aktuell eingesetzt werden beziehungsweise 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 BMWSB nicht ausreichend Rechnung tragen, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vergleiche BVerfGE 124, 78 [139]). Schon die Angabe, wie das BMWSB 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 potentielle Angreifer detaillierte Kenntnis über vorgenannte Informationen erhalten, wäre ein Angriff auf das BMWSB 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 BMWSB aktuell, und wie viele davon erfüllen nachweislich die geltenden Mindeststandards für IT-Sicherheit?

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

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

Die Fragen 1 bis 3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Das BMWSB ist eine vollkonsolidierte Behörde und besitzt keine eigenen Rechenzentren.

4. Welche Investitionen hat das BMWSB in den Jahren 2020 bis 2025 konkret für den Ausbau und die Absicherung seiner IT-Infrastruktur (einschließlich Rechenzentren, Netze, Cloudlösungen) getätigt?

Grundsätzlich bezieht das BMWSB Dienste der IT-Konsolidierung über die IT-Dienstleister des Bundes.

5. In welchem Umfang hat das BMWSB in den vergangenen fünf Jahren Sicherheitsüberprüfungen (z. B. durch das BSI oder unabhängige Dienstleister) durchführen lassen, und mit welchen Ergebnissen?

Das BMWSB wurde in 2021 aufgrund eines Erlasses des damaligen Bundeskanzlers errichtet. Als vollkonsolidierte Einrichtung (siehe Antwort zu Frage 1) betreibt es keine eigene Infrastruktur. Losgelöst davon prüft und berät das BSI

(und gegebenenfalls beauftragte Dritte) auf Basis seiner Zuständigkeiten das Haus hinsichtlich der Umsetzung einer angemessenen Sicherheit. Die so ermittelten Erkenntnisse und identifiziertes Optimierungspotential fließen in die fortwährende Verbesserung bestehender Sicherheitsmaßnahmen ein. Die rechtliche Grundlage hierfür ergibt sich aus § 3 Abs. 1 S. 2 Nr. 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 gegen die Kenntnisnahme durch Unbefugte gemäß § 3 Abs. 1 S. 2 Nr. 9 BSIG.

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

Innerhalb des BMWSB bestehen Organisationsstrukturen mit Verantwortlichkeiten für Informationssicherheit im Sinne der Regelungsvorgaben des BSI (Standard 200-1/200-2 und 200-3). Im Übrigen wird auf die Antwort zu Frage 1 verwiesen.

7. Welche spezifischen Zuständigkeiten bestehen im Geschäftsbereich des BMWSB für die Sicherung der digitalen Bauantragsverfahren, Wohnraumförderungsdatenbank, BIM-Verfahren und internen Kommunikations- und Verwaltungsplattformen?

Für die angemessene Umsetzung der notwendigen Sicherheit digitaler Bauantragsverfahren, sonstiger Verfahren und interner Plattformen liegen, wie üblich, jeweils konkrete spezifische organisatorische und fachliche Zuständigkeiten vor. Hierbei verantwortet die jeweils fachverantwortliche Seite auch die Betrachtung der sicherheitsrelevanten Aspekte im Rahmen einer jeweiligen Sicherheitskonzeption. Diese wiederum ist Teil der Gesamtsicherheitskonzeption des Ressorts und wird durch die Informationssicherheit gesteuert.

Eine Wohnraumförderdatenbank ist hier nicht bekannt.

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

Das BMWSB hat im Zuge eines der Gründung 2021 erfolgenden Aufbaus die Vorgaben des BSI sowie des Umsetzungsplan(UP) Bundes berücksichtigt. Bereits in 06/2022 wurde eine Stabsstelle Informationssicherheit etabliert, um die bestehenden Anforderungen zu berücksichtigen. Es wurden Maßnahmen eingeleitet, um eine angemessene Informationssicherheit in der Organisation zu etablieren und so den Hinweisen des Bundesrechnungshofes Rechnung zu tragen. Das Sicherheitsniveau im Ressort wird durch einen kontinuierlichen Verbesserungsprozess aufrechterhalten und stetig optimiert. Die Kritikpunkte des Bundesrechnungshofes werden in diesem Prozess berücksichtigt.

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

Auf festgestellte Sicherheitsvorfälle wurde durch das BMWSB sowie der zum Einsatz kommenden Dienstleister stets angemessen reagiert. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

10. Welche Bedrohungsanalysen zu Cyberangriffen auf die genannten digitalen Verfahren liegen dem BMWSB vor?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

11. Welche spezifischen Gefahren bestehen für die Verfügbarkeit und Integrität der Wohnraumförderungsdatenbank, Sicherheit der digitalen Bauantragsverfahren, Manipulationssicherheit bei BIM-Prozessen, interne Kommunikation und Datenverwaltung im BMWSB?

Für die Verfügbarkeit, Integrität und Sicherheit der digitalen Bauantragsverfahren und Building Information Modeling (BIM)-Verfahren existieren diverse Gefahren, die fortlaufend bewertet werden. Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

12. Welche technischen und organisatorischen Maßnahmen wurden seit 2018 ergriffen, um die genannten Verfahren gegen Cyberangriffe abzusichern?

Technische und organisatorische Maßnahmen zur Absicherung der eigenen Informationsverbünde werden seit Gründung stets geprüft und iterativ angemessen an aktuelle Entwicklungen angepasst. Auf die Vorbemerkung der Bundesregierung wird verwiesen.

13. Welche zusätzlichen Maßnahmen sind in Planung, um die digitale Bauverwaltung als kritische Infrastruktur künftig zu stärken bzw. zu erhöhen?

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

14. Welche konkreten Schritte plant das BMWSB, um bis spätestens 2030 die vollständige Einhaltung der vom Bundesrechnungshof geforderten Mindeststandards (inklusive Notstromversorgung und georedundanten Systemen) sicherzustellen?

Das BMWSB plant bis 2030 die Einhaltung aller relevanten Mindeststandards anzustreben. Konkrete Planungsschritte, um dieses Ziel mit den verfügbaren Ressourcen zu erreichen, wurden dafür identifiziert. Auf weiterführende Details wird aufgrund der gegebenen Kritikalität nicht eingegangen.

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

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

16. Wie hat sich die Zahl der IT-Sicherheitsstellen im BMWSB seit 2018 entwickelt (bitte jährlich angeben und nach Behörden differenzieren sowie nach Besoldungs- bzw. Entgeltgruppe aufschlüsseln)?

Die Zahl der Informationssicherheits-/IT-Sicherheitsstellen hat sich seit Gründung des Ressorts 2021 erhöht. Gegebene situative Veränderungen werden in diesem Kontext jährlich neu bewertet. Im Übrigen wird an dieser Stelle auf weitere Angaben aufgrund der gegebenen Kritikalität verzichtet und auf die Vorbemerkung der Bundesregierung verwiesen.

17. Wurden in den Jahren 2020 bis 2024 Stellen im Bereich IT-Sicherheit im Geschäftsbereich des BMWSB abgebaut, umgewidmet oder neu geschaffen, und wenn ja, in welchem Umfang?

In den Jahren 2021 bis 2024 gab es keinen Stellenabbau im Ressort. Erfolgte Neueinstellungen im Bereich Informationssicherheit/IT-Sicherheit führten zu einer längerfristig vorhandenen Personalstärke. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

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

Im BMWSB stellt die IT-Sicherheit eine Untermenge der Informationssicherheit dar. Die Betrachtung der Thematik unter den Aspekten des Managementsystems beinhaltet deutlich mehr als eine Reduzierung auf technische Aspekte. Aufgrund der Eigenschaft als vollkonsolidiertes Haus verfügt das BMWSB selbst über keine der in der Fragestellung benannten Infrastrukturen (siehe Antwort zu Frage 1).

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

Es sind aktuell keine Stellen unbesetzt.

20. Welche spezifischen Qualifikationen (z. B. IT-Sicherheit in Verwaltungsverfahren, Schutz kritischer Datenbanken, OT (Operational Technology)-Sicherheit in Bauprozessen) werden bei der Besetzung von Stellen gefordert oder bevorzugt berücksichtigt?

Bei der Besetzung von Informationssicherheits- und IT-Sicherheitsstellen werden fachliche Geeignetheit und vorhandenen Qualifikationen angestrebt. Hierbei spielt insbesondere eine fundierte Wissensbasis der relevanten Managementsysteme, aber auch Kenntnisse der Verwaltung des IT-Managements sowie der übergreifenden Aspekte eine Rolle. Bei fehlenden Kenntnissen wird nachgeschult. Die jeweils konkreten Anforderungen sind in den jeweiligen Ausschreibungen aufgeführt.

21. Welche Schulungen und Fortbildungen wurden für Beschäftigte des BMWSB und seiner nachgeordneten Behörden im Bereich IT-Sicherheit seit 2018 durchgeführt (bitte nach Jahr und Art der Fortbildung aufschlüsseln)?

Im BMWSB und seinen nachgeordneten Behörden werden verschiedene adressatengerechte Schulungen, auch durch Dritte, durchgeführt. Diese orientieren sich an den bestehenden aktuellen Bedarfen.

22. Welche Kooperationen bestehen mit anderen Ressorts, den Ländern, Kommunen oder internationalen Organisationen zur Stärkung der Resilienz gegen Cyberangriffe?

Das BMWSB pflegt im Rahmen der Zusammenarbeit Kooperationen mit anderen Ressorts, Ländern und internationalen Organisationen, um die eigene Resilienz gegen Cyberangriffe zu stärken.

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

Es werden organisatorische und technische Maßnahmen ergriffen, um die Resilienz besonders sensibler Systeme zu gewährleisten. Hierbei verfolgt das BMWSB insbesondere einen integrierten Management-Ansatz. Bei diesem werden, sofern möglich und sinnvoll, verschiedene Managementsysteme zusammengefasst. In Folge können die verfügbaren (personellen/monetären) Ressourcen bestmöglich eingesetzt und eine Doppelbelastung vermieden werden.

24. Plant die Bundesregierung, die IT-Sicherheitskapazitäten im BMWSB mittelfristig auszubauen, mit welchem zeitlichen Horizont?

Die Entwicklungen in diesem Bereich werden fortlaufend beobachtet; bei Bedarf wird über geeignete Maßnahmen entschieden.

25. Inwieweit bewertet die Bundesregierung die digitalen Verwaltungs- und Planungsverfahren des BMWSB als kritische Infrastruktur im Sinne des IT-Sicherheitsgesetzes, und welche Konsequenzen ergeben sich daraus für die Cybersicherheitsstrategie?

Digitale Verwaltungs- und Planungsverfahren werden vom BMWSB im jeweils konkreten Einzelfall bewertet. Hierzu wurden konkrete Schutzbedarfe entwickelt, anhand deren ein einheitliches und strukturiertes Vorgehen möglich ist. Konsequenzen für eine angemessene Cybersicherheitsstrategie ergeben sich entsprechend der rechtlichen Rahmenbedingungen und orientieren sich damit an den bestehenden Vorgaben (UP Bund, BSI etc.).

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