Deutscher Bundestag **Drucksache 21/2692**

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 21/2418 –

Cybersicherheit und Stellenentwicklung im Bereich IT-Sicherheit im Geschäftsbereich des Bundesministeriums für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit

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 Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit (BMUKN) trägt eine zentrale Verantwortung für die nukleare Sicherheit in Deutschland. Dazu gehört auch die Aufsicht über den sicheren Betrieb kerntechnischer Anlagen und die Umsetzung internationaler Verpflichtungen. Die Gewährleistung hoher Sicherheitsstandards im Bereich der nuklearen Sicherheit umfasst nicht nur den physischen Schutz kerntechnischer Anlagen, sondern zunehmend auch die Dimension der Cybersicherheit. Angriffe auf kritische Infrastrukturen haben in den vergangenen Jahren zugenommen (www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html#:~:text=Aktuelle%20Trends%20und%20Entwicklungen%20der,Gefahren%20Warnhinweise%20und%20Sonderauswertungen%20heraus), und auch im internationalen Kontext warnen Fachgremien wie die Internationale Atomenergie-Organisation (IAEO) vor steigenden Risiken im Bereich der IT- und Operational Technology (OT)-Sicherheit nuklearer Einrichtungen

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit vom 10. November 2025 übermittelt.

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

(www.heise.de/news/Atomenergie-Organisation-baut-Trainingslager-fuer-Kampf-gegen-Nuklearterrorismus-6135943.html). Neben diesem besonders sicherheitskritischen Bereich unterliegen jedoch auch weitere Zuständigkeiten des BMUKN – wie Umwelt- und Naturschutz – spezifischen Cyberrisiken. So sind etwa Mess- und Überwachungssysteme im Umweltbereich, digitale Infrastrukturen sowie Datenbanken und Verwaltungsprozesse im Naturschutz ebenfalls potenziellen Angriffen ausgesetzt.

Vor diesem Hintergrund stellt sich den Fragestellern die Frage, inwieweit Cybersicherheitsaspekte in den Verantwortungsbereich des BMUKN 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 BSI beobachtet die Sicherheitslage in den fünf Dimensionen Bedrohung, Angriffsfläche, Gefährdung, Schadwirkung und Resilienz, wobei die Resilienz den vier anderen Dimensionen positiv entgegenwirkt (vgl. https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html).

Cyberbedrohungen gingen im vergangenen Jahr von diversen Angreifergruppen aus. 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 funktionie-

renden 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, in Teilen 5, 9 bis 12 und 14, 16 und 19 können nach sorgfältiger Prüfung und Abwägung auch in eingestufter Form nicht beantwortet werden.

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

Informationen zu sämtlichen im BMUKN 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 BMUKN eingesetzten Schutzmaßnahmen zu erhalten.

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

Mit der Beantwortung würde offengelegt, wie sich das BMUKN 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 BMUKN 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 BMUKN 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 BMUKN 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 BMUKN 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 BMUKN 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 BMUKN 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 verfügen über eine funktionsfähige Notstromversorgung.

3. An welchen Standorten des BMUKN 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 BMUKN 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, so dass Investitionen in den IT-Betrieb grundsätzlich in den Ausbau und die Absicherung der IT-Infrastruktur fließen.

5. In welchem Umfang hat das BMUKN 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 Absart 1 Satz 2 Nummer 1 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 Summer 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 BMUKN (z. B. eigenes Computer Emergency Response Team [CERT], IT-Sicherheitsreferate, Zusammenarbeit mit dem BSI)?

Organisatorische Zuständigkeiten sind dem Organigramm des BMUKN zu entnehmen.

7. Welche spezifischen Zuständigkeiten bestehen im Geschäftsbereich des BMUKN für die Cybersicherheit kerntechnischer Anlagen?

Das BMUKN nimmt im Rahmen der Bundesauftragsverwaltung die Bundesaufsicht im Bereich der nuklearen Sicherheit gegenüber den Ländern wahr und ist in diesem Zusammenhang mit der Rechts- und Zweckmäßigkeitsaufsicht betraut, das schließt insbesondere die Cybersicherheit der kerntechnischen Anlagen mit ein.

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

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

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

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

10. Welche Bedrohungsanalysen zu Cyberangriffen auf kerntechnische Anlagen liegen dem BMUKN derzeit vor, und wie werden diese in die Aufsichtspraxis integriert?

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.

11. Welche Bedrohungsanalysen zu Cyberangriffen in den Bereichen Umwelt- und Naturschutz, z. B. auf Messnetze, Dateninfrastrukturen oder Steuerungssysteme, liegen dem BMUKN derzeit vor?

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. Welche konkreten Schritte plant das BMUKN, 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 BMUKN (bitte nach Behörden und Besoldungs- bzw. Entgeltgruppen aufschlüsseln)?

Alle Stellen im IT-Betrieb haben auch das Ziel IT-bzw. Informationssicherheit. In der Zusammenarbeit des IT-Betriebs mit dem Informationssicherheitsbeauftragten wird die Informationssicherheit im BMUKN gewährleistet.

14. Wie hat sich die Zahl der IT-Sicherheitsstellen im BMUKN 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.

15. Wie viele Stellen mit Bezug zur IT- und Cybersicherheit waren seit 2020 im Geschäftsbereich des BMUKN vorhanden, die unmittelbar den sicheren Betrieb kerntechnischer Anlagen betreffen (bitte jeweils nach Jahr, Organisationseinheit und Besoldungs- bzw. Entgeltgruppe aufschlüsseln)?

Es wird auf die Antwort zu Frage 13 verwiesen.

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

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

Alle für den grundsätzlich sicheren IT-Betrieb notwendigen Aufgaben werden abgedeckt. Die Aufgabenbereiche orientieren sich dabei grundlegend an den Vorgaben und Standards des BSI.

18. Wie viele dieser Stellen (vgl. Frage 17) sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?

Keine Stelle ist derzeit unbesetzt, offene Stellen bleiben nur wenige Wochen vakant.

19. In welchen Abteilungen oder nachgeordneten Behörden des BMUKN werden Fragen der IT- und Cybersicherheit mit Bezug zur nuklearen Sicherheit bearbeitet?

Fragen der IT- und Cybersicherheit mit Bezug zur nuklearen Sicherheit werden im BMUKN in der Abteilung S „Nukleare Sicherheit, Strahlenschutz“ und im BASE bearbeitet.

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

Spezifische Qualifikationen sind in Stellenausschreibungen öffentlich einsehbar.

21. Welche Schulungen und Fortbildungen zur Abwehr von Cyberangriffen auf kerntechnische Anlagen wurden seit 2018 für Beschäftigte des BMUKN und seiner nachgeordneten Behörden durchgeführt (bitte nach Jahr und Art der Fortbildung aufschlüsseln)?

Die Beschäftigten des BMUKN und dessen Geschäftsbereich nehmen regelmäßig Angebote für Schulungen und Fortbildungen wahr und berücksichtigen die Handlungsempfehlungen des BSI.

22. In welchem Umfang bestehen Kooperationen mit anderen Ressorts und Behörden, insbesondere dem Bundesamt für Sicherheit in der Informationstechnik, sowie mit internationalen Organisationen wie der International Atomic Energy Agency [IAEO], der Organization for Economic Co-operation and Development/Nuclear Energy Agency (OECD/NEA) oder im Rahmen der EU im Bereich Cybersicherheit kerntechnischer Anlagen sowie in Umwelt- und Naturschutzbereichen?

Das BMUKN steht im Rahmen seiner Aufgaben im regelmäßigen Austausch mit dem BSI sowie etwaigen ausländischen Dienststellen und Organisationen zu verschiedenen sicherheitspolitischen Themen.

23. Welche konkreten Vorkehrungen wurden vom BMUKN und von der Bundesregierung getroffen, um Angriffe auf digitale Steuerungs- und Sicherheitssysteme kerntechnischer Anlagen zu verhindern?

Das BMUKN hat die Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT) und die Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und bei Tätigkeiten der Sicherungskategorie III sowie der umsichtigen Betriebsführung gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT SK III) erlassen. Beide Richtlinien sind als „VS-Nur für den Dienstgebrauch“ eingestuft.* Im Übrigen wird auf die Antwort zu Frage 7 und auf die Vorbemerkung der Bundesregierung verwiesen.

Im Übrigen werden alle für den grundsätzlich sicheren IT-Betrieb notwendigen Aufgaben abgedeckt. Die Aufgabenbereiche orientieren sich dabei an den Vorgaben und Standards des BSI.

24. Welche Maßnahmen ergreift das BMUKN, 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).

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

Der Bedarf wird permanent überprüft und bei Bedarf angepasst.

* Das Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit hat die Antwort als „VS-Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

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