Deutscher Bundestag **Drucksache 21/2681**

21. Wahlperiode 07.11.2025

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 21/2403 –

Cybersicherheit und Stellenentwicklung im Bereich IT-Sicherheit im Geschäftsbereich des Bundesministeriums für Landwirtschaft, Ernährung und Heimat

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%).

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/).

Die Landwirtschaft und die Ernährungswirtschaft stehen im Zuge der Digitalisierung vor tiefgreifenden Veränderungen. Systeme des Smart Farmings, digitale Plattformen für Agrar- und Ernährungsdaten, automatisierte Produktionsprozesse in der Lebensmittelwirtschaft sowie komplexe Liefer- und Logistikketten sind zunehmend digital gesteuert.

Damit steigt auch die Anfälligkeit gegenüber Cyberangriffen: Manipulationen an Agrardaten, Unterbrechungen von Lieferketten oder Angriffe auf Steuerungssysteme könnten nicht nur wirtschaftliche Schäden verursachen, sondern auch die Versorgungssicherheit mit Lebensmitteln beeinträchtigen. Besonders in Krisenlagen wie Pandemien und Naturkatastrophen kann eine zusätzliche Gefährdung durch Cyberangriffe gravierende Folgen haben.

Das Bundesministerium für Landwirtschaft, Ernährung und Heimat (BMLEH) trägt die Verantwortung für die Stabilität der landwirtschaftlichen Produktion,

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Landwirtschaft, Ernährung und Heimat vom 7. November 2025 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

die Sicherheit der Lebensmittelversorgung sowie die Stärkung der ländlichen Räume.

Vor diesem Hintergrund stellt sich den Fragestellern die Frage, inwieweit Cybersicherheitsaspekte in den Verantwortungsbereich des BMLEH 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. 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 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, in Teilen 5, 7, 9, 13, in Teilen 14 und 15 sowie in Teilen 17 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 BMLEH und dessen Geschäftsbereichsbehörden 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 BMLEH eingesetzten Schutzmaßnahmen zu erhalten.

Unter Kenntnis, der durch das BMLEH eingesetzten Produkte könnten Angreifer Schwachstellen ausmachen und diese gezielt ausnutzen. Vor allem in der Zusammenschau mit den Antworten der Bundesregierung auf die Kleinen Anfragen der Fraktion der CDU/CSU auf Bundestagsdrucksachen 20/8707 und 20/14887 ließe sich durch Aggregation und direkten Vergleich detaillierte Erkenntnisse ableiten, die die Entwicklung des Einsatzes und der Beschaffung von IT-Sicherheitsprodukten und der zukünftigen konkreten IT-Sicherheitsstrategie in der Bundesverwaltung und im BMLEH zeigen.

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

3. An welchen Standorten des BMLEH 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 BMLEH in den Jahren von 2020 bis 2025 konkret für den Ausbau und die Absicherung seiner IT-Infrastruktur (einschließlich Rechenzentren, Netze, Cloudlösungen) getätigt?

IT-Sicherheit ist IT-Betriebsziel, sodass alle Investitionen in den IT-Betrieb grundsätzlich in den Ausbau und die Absicherung der IT-Infrastruktur fließen.

5. In welchem Umfang hat das BMLEH 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 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 BMLEH (z. B. eigenes Computer Emergency Response Team [CERT], IT-Sicherheitsreferate, Zusammenarbeit mit dem BSI)?

Organisatorische Zuständigkeiten sind dem Organigramm des BMLEH zu entnehmen.

7. Welche spezifischen Zuständigkeiten bestehen im Geschäftsbereich des BMLEH für die Abwehr von Cyberangriffen auf digitale Systeme des Smart Farmings, der Produktions- und Verarbeitungseinrichtungen der Ernährungswirtschaft, Liefer- und Logistikketten, Datenplattformen im Bereich Agrar- und Lebensmittelwirtschaft sowie kritischen Infrastrukturen der Lebensmittelversorgung?

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.

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

Das IT-Sicherheitsniveau im BMLEH 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 BMLEH registriert, und wie wurde jeweils darauf reagiert (bitte nach Jahr und Anzahl der Zwischenfälle 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 Lebensmittelversorgungsketten und Agrar- bzw. Ernährungsdaten liegen dem BMLEH vor, und wie fließen diese in die Praxis der IT-Sicherheit ein?

Dem BMLEH liegen aktuell keine Bedrohungsanalysen zu Cyberangriffen auf Lebensmittelversorgungsketten und Agrar- bzw. Ernährungsdaten vor. Nach dem BSI-Gesetz sind die wesentlichen Aufgaben des Informationssicherheitsmanagements dem BSI übertragen.

11. Welche technischen und organisatorischen Maßnahmen wurden seit 2018 ergriffen, um Cyberangriffe auf digitale Systeme der Lebensmittel- und Agrarwirtschaft sowie auf Lieferketten abzuwehren?

Unternehmen des Sektors Ernährung, die unter den Anwendungsbereich des BSI-Gesetzes fallen, sind zum Treffen geeigneter, wirksamer und verhältnismäßiger Risikomanagementmaßnahmen verpflichtet. Darunter fällt auch die Implementierung von geeigneten technischen und organisatorischen Maßnahmen (TOMs).

12. Welche besonderen Vorkehrungen bestehen beim BMLEH für Krisen- und Notlagen, in denen Cyberangriffe die Versorgungssicherheit zusätzlich gefährden könnten?

Unternehmen des Sektors Ernährung, die unter den Anwendungsbereich des BSI-Gesetzes fallen, werden zum Treffen besonderer Vorkehrungen zur Stärkung ihrer Resilienz gegenüber Cyberangriffen verpflichtet. Darüber hinaus ist das BSI für die Unterstützung zur Bewältigung von Cybersicherheitsvorfällen zuständig.

13. Welche konkreten Schritte plant das BMLEH ggf., 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.

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

Auf die Antwort der Bundesregierung auf die Schriftliche Frage 25 der Abgeordneten Anke Domscheit-Berg auf Bundestagdrucksache 20/14639 zu IT-Sicherheitsstellen wird verwiesen. Hinsichtlich der weiteren Aufschlüsselung 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 hat sich die Zahl der IT-Sicherheitsstellen im BMLEH seit 2018 entwickelt (bitte jährlich angeben und nach Behörden differenzieren sowie nach Besoldungs- bzw. Entgeltgruppe aufschlüsseln)?

Auf die Antwort der Bundesregierung auf die Schriftliche Frage 25 der Abgeordneten Anke Domscheit-Berg auf Bundestagdrucksache 20/14639 zu IT-Sicherheitsstellen wird verwiesen. Hinsichtlich der weiteren Aufschlüsselung 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 (vgl. Frage 15) entfallen unmittelbar auf Aufgaben zur Sicherung der Versorgungssicherheit und der Ernährungswirtschaft?

Keine dieser Stellen entfallen unmittelbar auf Aufgaben zur Sicherung der Versorgungssicherheit und der Ernährungswirtschaft. Die in der Frage angesprochenen Aufgabenbereiche werden von anderen Organisationseinheiten im Haus wahrgenommen.

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

Es fand ein Aufwuchs von sechs Stellen statt. Hinsichtlich der weiteren Aufschlüsselung 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. Wie viele dieser möglichen Stellen (vgl. Frage 17) sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?

Auf die Antwort der Bundesregierung auf die Schriftliche Frage 25 der Abgeordneten Anke Domscheit-Berg auf Bundestagdrucksache 20/14639 zu IT-Sicherheitsstellen wird verwiesen. Offene Stellen bleiben wenige Wochen vakant.

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

Alle für den grundsätzlich sicheren IT-Betrieb notwendigen Aufgaben werden abgedeckt.

20. Welche spezifischen Qualifikationen werden bei der Besetzung von Stellen mit Blick auf die Versorgungsketten- und Infrastruktursicherheit gefordert oder bevorzugt berücksichtigt?

Spezifische Qualifikationen sind in Stellenausschreibungen öffentlich einsehbar.

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

Die Beschäftigten des BMLEH und dessen Geschäftsbereich nehmen regelmäßig Angebote für Schulungen und Fortbildungen, u. a. zu den Themen Informationssicherheitsmanagement, Awareness, technische und operative Sicherheit, BCM etc. wahr.

22. Welche Kooperationen bestehen mit anderen Ressorts, insbesondere dem Bundesamt für Sicherheit in der Informationstechnik, sowie mit europäischen und internationalen Organisationen zur Stärkung der Resilienz von Versorgungsketten gegen Cyberangriffe?

Die Zusammenarbeit mit dem BSI und anderen Ressorts erfolgt aufgrund der einschlägigen gesetzlichen Regelungen und der Informationssicherheitsorganisation der Bundesverwaltung. Für darüberhinausgehende Sicherheitskooperationen im Bereich Cybersicherheit ist das BSI zuständig.

23. Welche Rolle spielen private Unternehmen der Ernährungswirtschaft, Agrarbetriebe und Verbände in den Sicherheitskooperationen des BMLEH?

Für Sicherheitskooperationen im Bereich Cybersicherheit ist das BSI zuständig. BMLEH nimmt an Veranstaltungen der „Unabhängigen Partnerschaft Kritischer Infrastrukturen (UP KRITIS)“ teil. Dies ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen. Das BSI betreibt die Geschäftsstelle des UP KRITIS.

24. Welche Maßnahmen ergreift das BMLEH 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 GGO.

25. Inwiefern beteiligt sich das BMLEH an europäischen oder internationalen Organisationen im Hinblick auf den Schutz von Patientendaten?

Es liegen keine Informationen zu einer Beteiligung vor.

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

Im Rahmen der Ausarbeitung von NIS2 ist ein mittelfristiger Ausbau der IT-Sicherheitskapazitäten geplant. Der zeitliche Horizont wird sich im Rahmen der Entwicklung des Gesetzentwurfs abzeichnen.

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