Deutscher Bundestag **Drucksache 21/2528**

21. Wahlperiode 04.11.2025

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 21/2378 –

Cybersicherheit und Stellenentwicklung im Bereich IT-Sicherheit im Geschäftsbereich des Bundesministers für besondere Aufgaben

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 (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/).

Das Bundeskanzleramt nimmt als Bundesministerium für besondere Aufgaben und in der Funktion des Chefs des Bundeskanzleramtes eine Schlüsselrolle in der Steuerung und Koordinierung der Bundesregierung ein. Besonders in Krisenlagen – etwa während der COVID-19-Pandemie, im Rahmen der Energieversorgungskrise oder im Zusammenhang mit sicherheitspolitischen Herausforderungen wie dem Krieg in der Ukraine – fungiert das Kanzleramt als zentrale Schaltstelle für Krisenstäbe, ressortübergreifende Koordination und internationale Abstimmung. Eine besondere Bedeutung kommt dabei dem Lagezentrum des Bundeskanzleramtes zu, das als zentrale Schnittstelle für Informationen, Analysen und Kommunikationsprozesse zwischen den Ressorts und gegenüber internationalen Partnern dient.

Gerade in solchen Ausnahmesituationen kommt der Zuverlässigkeit und Sicherheit der IT-Systeme und Kommunikationsinfrastrukturen des Kanzleram-

---

Die Antwort wurde mit Schreiben des Bundeskanzleramtes vom 31. Oktober 2025 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

tes eine herausragende Bedeutung zu. Cyberangriffe auf das Kanzleramt könnten die Handlungsfähigkeit der Bundesregierung massiv beeinträchtigen – sei es durch Unterbrechung oder Manipulation von Kommunikationswegen zwischen Ressorts und Krisenstäben, Einschränkung der internationalen Abstimmung mit EU- und NATO-Partnern, Verfälschung oder Blockade krisenrelevanter Daten, Störung interner Entscheidungs- und Informationsprozesse im Lagezentrum des Kanzleramtes.

Vor diesem Hintergrund ist es für die Fragesteller von besonderem Interesse, wie das Bundeskanzleramt organisatorisch, personell und technisch aufgestellt ist, um solchen Bedrohungen wirksam zu begegnen.

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, 10 bis 12 und 14 bis 16, 18 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 Bundeskanzleramt 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 Bundeskanzleramt eingesetzten Schutzmaßnahmen zu erhalten.

Unter Kenntnis der durch das Bundeskanzleramt 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 Bundeskanzleramt zeigen.

Mit der Beantwortung würde offengelegt, wie sich das Bundeskanzleramt 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 Bundeskanzleramts 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 Bundeskanzleramt 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 Bundeskanzleramts 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 Bundeskanzleramt 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 Bundeskanzleramt 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 Bundesministerium für besondere Aufgaben bzw. das Bundeskanzleramt 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 Bundesministeriums für besondere Aufgaben bzw. des Bundeskanzleramtes 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 Bundesministerium für besondere Aufgaben bzw. das Bundeskanzleramt in den Jahren 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 Bundesministerium für besondere Aufgaben bzw. das Bundeskanzleramt in den vergangenen fünf Jahren Sicherheitsüberprüfungen (z. B. durch das BSI oder 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 Bundesministeriums für besondere Aufgaben bzw. des Bundeskanzleramtes (z. B. eigenes CERT (Community Emergency Response Team), IT-Sicherheitsreferate, Zusammenarbeit mit dem BSI)?

Organisatorische Zuständigkeiten sind dem Organigramm des Bundeskanzleramtes zu entnehmen.

7. Welche organisatorischen Schnittstellen bestehen zum Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie zu den Nachrichtendiensten (Bundesnachrichtendienst (BND), Bundesamt für Verfassungsschutz (BfV), Militärischer Abschirmdienst (MAD)), um die Cybersicherheit des Kanzleramtes in Krisenlagen sicherzustellen?

Die Koordination der Nachrichtendienste des Bundes gehört zu den Aufgaben des Bundeskanzleramtes. Schnittstellen zu den genannten Behörden bestehen insbesondere in den für die Koordinierung der Nachrichtendienste des Bundes sowie für die Innen- und Rechtspolitik zuständigen Fachabteilungen im Bundeskanzleramt.

8. In welchem Umfang ist das Bundesministerium für besondere Aufgaben bzw. das Bundeskanzleramt in die ressortübergreifende Steuerung der nationalen Cybersicherheitsstrategie eingebunden, insbesondere mit Blick auf Krisenbewältigung?

Bei der Nationalen Cybersicherheitsstrategie handelt es sich um eine Strategie der Bundesregierung, die unter Beteiligung aller Ressorts in Federführung des Bundesministeriums des Innern erarbeitet wurde. Die Strategie wurde im August dieses Jahres evaluiert. Derzeit wird an der Weiterentwicklung gearbei-

tet. Auch das Bundeskanzleramt ist daran im Rahmen seiner ihm in der Kompetenzordnung des Grundgesetzes zugewiesenen Aufgaben und Funktionen eingebunden.

9. Welche Maßnahmen hat das Bundesministerium für besondere Aufgaben bzw. das Bundeskanzleramt seit 2020 ergriffen, um auf die Kritikpunkte des Bundesrechnungshofes im Bereich IT-Sicherheit zu reagieren?

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

10. Wie viele Sicherheitsvorfälle oder Cyberangriffe wurden in den letzten fünf Jahren im Zuständigkeitsbereich des Bundesministeriums für besondere Aufgaben bzw. des Bundeskanzleramtes registriert, und wie wurde jeweils darauf reagiert (bitte nach Jahr, 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.

11. Welche Bedrohungsanalysen liegen dem Bundesministerium für besondere Aufgaben bzw. dem Bundeskanzleramt hinsichtlich gezielter Cyberangriffe auf seine Systeme in Krisenlagen 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 Bedrohungsanalysen liegen dem Bundesministerium für besondere Aufgaben bzw. dem Bundeskanzleramt hinsichtlich gezielter Cyberangriffe auf das Lagezentrum und die Kommunikationssysteme 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.

13. Welche Gefahren sieht die Bundesregierung für die Funktionsfähigkeit des Kanzleramtes, wenn zentrale IT-Systeme oder Kommunikationsinfrastrukturen während einer Krise durch Cyberangriffe gestört werden?

In einer Krise durch Cyberangriffe können Gefahren entstehen, die zu einem Ausfall von Systemen oder deren Teilen führen kann. Falls zentrale oder alle IT-Systeme oder Kommunikationsinfrastrukturen ausfallen, stehen diese nicht mehr zur Verfügung, was eine Gefahr für die Funktionsfähigkeit des Bundeskanzleramtes darstellt. Die für diese Fälle vorgesehenen redundanten Systeme sichern jedoch die Aufrechterhaltung der Funktionsfähigkeit des Bundeskanzleramtes.

14. Welche technischen und organisatorischen Maßnahmen wurden seit 2018 ergriffen, um das Lagezentrum und die IT-Infrastruktur des Bundesministeriums für besondere Aufgaben bzw. des Bundeskanzleramtes mit Blick auf Krisenstäbe und internationale Koordination abzusichern?

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. Welche zusätzlichen Maßnahmen sind in Planung, um die Widerstandsfähigkeit des Bundesministeriums für besondere Aufgaben bzw. des Bundeskanzleramtes gegen Cyberangriffe in künftigen Krisenlagen zu erhöhen?

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. Welche konkreten Schritte plant das Bundesministerium für besondere Aufgaben bzw. das Bundeskanzleramt, um bis spätestens 2030 die vollständige Einhaltung der vom Bundesrechnungshof geforderten Mindeststandards (inklusive Notstromversorgung und georedundanten Systemen) 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.

17. Wie viele Stellen im Bereich IT-Sicherheit existieren derzeit im Bundesministerium für besondere Aufgaben bzw. im Bundeskanzleramt (bitte nach Behörden und Besoldungs- bzw. Entgeltgruppen aufschlüsseln)?

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

18. Wie hat sich die Zahl der IT-Sicherheitsstellen im Bundesministerium für besondere Aufgaben bzw. im Bundeskanzleramt seit 2018 entwickelt (bitte jährlich angeben und nach Behörden differenzieren sowie nach Besoldungs- bzw. Entgeltgruppe 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.

19. Wurden in den Jahren 2020 bis 2024 Stellen im Bereich IT-Sicherheit im Bundesministerium für besondere Aufgaben bzw. im Bundeskanzleramt 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 Informatio-

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

20. Welche konkreten Aufgabenbereiche decken die IT-Sicherheitsstellen im Bundesministerium für besondere Aufgaben bzw. im Bundeskanzleramt ab (z. B. Netzwerksicherheit, Kryptografie, Incident Response, Schutz kritischer Infrastrukturen (KRITIS), IT-Forensik)?

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

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

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

22. Welche spezifischen Qualifikationen (z. B. Krisen-IT, Kommunikationssicherheit, Schutz kritischer Infrastrukturen) werden bei der Besetzung von Stellen gefordert oder bevorzugt berücksichtigt?

Spezifische Qualifikationen sind in Stellenausschreibungen öffentlich einsehbar.

23. Welche Schulungen und Fortbildungen wurden für Beschäftigte des Bundesministeriums für besondere Aufgaben bzw. des Bundeskanzleramtes und seiner nachgeordneten Behörden im Bereich IT-Sicherheit seit 2018 durchgeführt (bitte nach Jahr und Art der Fortbildung aufschlüsseln)?

Die Beschäftigten des Bundeskanzleramtes und dessen Geschäftsbereich nehmen regelmäßig Angebote für Schulungen und Fortbildungen wahr.

24. Welche Kooperationen bestehen mit internationalen Partnern, insbesondere im Rahmen von EU und NATO, zur Stärkung der Resilienz gegen Cyberangriffe?

Das Bundeskanzleramt steht im Rahmen seiner Aufgaben im regelmäßigen Austausch mit ausländischen Dienststellen zu verschiedenen sicherheitspolitischen Themen.

25. Welche Maßnahmen ergreift das Bundesministerium für besondere Aufgaben bzw. das Bundeskanzleramt, 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.

26. Plant die Bundesregierung, die IT-Sicherheitskapazitäten im Bundesministerium für besondere Aufgaben bzw. des Bundeskanzleramtes mittelfristig auszubauen, mit welchem zeitlichen Horizont?

Nein.

27. Inwieweit sieht die Bundesregierung eine Notwendigkeit, die IT-Systeme und Kommunikationsinfrastrukturen des Bundesministeriums für besondere Aufgaben bzw. des Bundeskanzleramtes im Sinne der KRITIS-Logik des IT-Sicherheitsgesetzes besonders zu schützen?

Die Bundesregierung sieht die Notwendigkeit, die IT-Systeme und Kommunikationsinfrastrukturen des Bundeskanzleramtes besonders zu schützen. Daher sieht unter anderem im Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung der Anwendungsbereich der öffentlichen Verwaltung das Bundeskanzleramt und die Bundesministerien vor.

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