Deutscher Bundestag **Drucksache 21/2378**

21. Wahlperiode 22.10.2025

Kleine Anfrage

der Abgeordneten Tobias Matthias Peterka, Ulrich von Zons, Lukas Rehm, Manfred Schiller, Tobias Teich, Gerold Otten, Dr. Rainer Kraft, Jan Wenzel Schmidt, Thomas Korell, Dr. Paul Schmidt, Robin Jünger, Dr. Malte Kaufmann, Dr. Daniel Zerbin, Mirko Hanker, Dr. Christina Baum, Reinhard Mixl, Dr. Dr. Michael Blos, Dr. Maximilian Krah, Carolin Bachmann, Stefan Keuter, Knuth Meyer-Soltau, Claudia Weiss, Julian Schmidt, Achim Köhler, Edgar Naujok, Kay-Uwe Ziegler, Joachim Bloch, Udo Theodor Hemmelgarn, Stefan Henze, Uwe Schulz, Sascha Lensing, Marc Bernhard, Rocco Kever, Volker Scheurell, Otto Strauß, Tobias Ebenberger und der Fraktion der AfD

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

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 (https://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 Kanzleramtes 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.

Wir fragen die Bundesregierung:

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?
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 Bundesministeriums für besondere Aufgaben bzw. des Bundeskanzleramtes sind kritische IT-Dienste georedundant verfügbar, und wie wird die Ausfallsicherheit regelmäßig überprüft?
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?
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?
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)?
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?
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?
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?

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)?
11. Welche Bedrohungsanalysen liegen dem Bundesministerium für besondere Aufgaben bzw. dem Bundeskanzleramt hinsichtlich gezielter Cyberangriffe auf seine Systeme in Krisenlagen vor?
12. Welche Bedrohungsanalysen liegen dem Bundesministerium für besondere Aufgaben bzw. dem Bundeskanzleramt hinsichtlich gezielter Cyberangriffe auf das Lagezentrum und die Kommunikationssysteme vor?
13. Welche Gefahren sieht die Bundesregierung für die Funktionsfähigkeit des Kanzleramtes, wenn zentrale IT-Systeme oder Kommunikationsinfrastrukturen während einer Krise durch Cyberangriffe gestört werden?
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?
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?
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?
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)?
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)?
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?
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)?
21. Wie viele dieser Stellen sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?
22. Welche spezifischen Qualifikationen (z. B. Krisen-IT, Kommunikationssicherheit, Schutz kritischer Infrastrukturen) werden bei der Besetzung von Stellen gefordert oder bevorzugt berücksichtigt?
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)?

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

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?

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

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?

Berlin, den 30. Oktober 2025

Dr. Alice Weidel, Tino Chrupalla und Fraktion

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