Deutscher Bundestag **Drucksache 21/2656**

21. Wahlperiode 06.11.2025

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 21/2422 –

Cybersicherheit und Stellenentwicklung im Bereich IT-Sicherheit im Geschäftsbereich des Bundesministeriums für Digitales und Staatsmodernisierung

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 Digitales und Staatsmodernisierung (BMDS) trägt eine Schlüsselrolle bei der Gestaltung und Umsetzung der digitalen Transformation in Deutschland. Seine Aufgaben umfassen die Modernisierung der Verwaltung, die Förderung digitaler Infrastrukturen sowie die Sicherstellung einer funktionierenden digitalen Daseinsvorsorge. Cyberangriffe auf das Bundesministerium könnten nicht nur die interne Arbeitsfähigkeit erheblich einschränken, sondern auch das Vertrauen der Bürger in die digitale Verwaltung und in staatliche Modernisierungsprojekte untergraben. Besonders kritisch ist dabei in den Augen der Fragesteller, dass das BMDS in enger Zusammenarbeit mit anderen Ressorts, Ländern, Kommunen und privaten Akteuren die Umsetzung zentraler Digitalisierungsmaßnahmen koordiniert. Sicherheitslücken in den behördeninternen IT-Systemen oder im Datenaustausch könnten unmittelbare Auswirkungen auf den Erfolg von Digitalisierungsprogrammen haben.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Digitales und Staatsmodernisierung vom 6. November 2025 übermittelt.

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

1. Über wie viele Rechenzentren verfügt das BMDS aktuell, und wie viele davon erfüllen nachweislich die geltenden Mindeststandards für IT-Sicherheit?

2. Welche dieser Rechenzentren (vgl. Frage 1) verfügen über eine funktionsfähige Notstromversorgung, die auch längerfristige (über mehrere Stunden oder Tage) Krisenlagen abdecken kann?

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

4. Welche Investitionen hat das BMDS in den Jahren von 2022 bis 2025 konkret für den Ausbau und die Absicherung seiner IT-Infrastruktur (einschließlich Rechenzentren, Netze, Cloudlösungen) getätigt?

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

8. Welche Maßnahmen hat das BMDS seit 2020 ergriffen, um auf die Kritikpunkte des Bundesrechnungshofes im Bereich IT-Sicherheit zu reagieren (vgl. Vorbemerkung der Fragesteller)?

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

10. Wie bewertet die Bundesregierung die aktuelle Gefährdungslage durch Cyberangriffe auf die IT-Systeme des BMDS und seine IT-Infrastruktur?

11. Welche internen Notfall- und Reaktionspläne bestehen im BMDS für den Fall von Cyberangriffen auf zentrale Verwaltungsprozesse?

12. Inwiefern sind Länder und Kommunen, die in föderalen Digitalisierungsprojekten mit dem BMDS zusammenarbeiten, in die Cybersicherheitsstrategie des Bundesministeriums eingebunden?

13. Welche Schulungs- und Sensibilisierungsmaßnahmen zum Thema Cybersicherheit wurden für Mitarbeiter des BMDS seit 2020 durchgeführt?

14. Welche konkreten Schritte plant das BMDS ggf., um bis spätestens 2030 die vollständige Einhaltung der vom Bundesrechnungshof geforderten Mindeststandards (inklusive Notstromversorgung und georedundanter Systeme) sicherzustellen?

15. Wie viele Stellen im Bereich IT-Sicherheit existieren derzeit im Geschäftsbereich des BMDS (bitte nach Behörden und Besoldungsgruppen aufschlüsseln)?

16. Wie hat sich die Zahl der IT-Sicherheitsstellen im BMDS seit 2020 entwickelt (bitte jährlich angeben und nach Behörden differenzieren)?

17. Wurden in den Jahren 2022, 2023 und 2024 Stellen im Bereich IT-Sicherheit im Geschäftsbereich des BMDS abgebaut, umgewidmet oder neu geschaffen, und wenn ja, in welchem Umfang?

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

Die Fragen 1–5 sowie 8–18 werden zusammen beantwortet.

Das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) existiert erst seit Inkrafttreten des Organisationserlasses des Bundeskanzlers vom 6. Mai 2025. Stellen aus anderen Bundesministerien gehen förmlich erst nach Abschluss der Verwaltungsvereinbarungen mit den anderen Ressorts und frühestens zum 1. Januar 2026 an das BMDS über. Zudem verfügt das BMDS noch über keine eigene IT-Infrastruktur. Sie befindet sich noch im Aufbau. Folglich befinden sich auch eigene, interne Notfall- und Reaktionspläne sowie Cybersicherheitsstrategien in der Ausarbeitung.

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

Organisatorische Zuständigkeiten sind dem Organigramm des BMDS zu entnehmen.

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

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

19. Welche besonderen Schwierigkeiten sieht die Bundesregierung ggf. bei der Gewinnung von IT-Sicherheitsfachkräften im Geschäftsbereich des BMDS, und welche Maßnahmen werden ggf. ergriffen, um diese Herausforderungen zu bewältigen?

Das BMDS verfügt noch über keinen eigenen Geschäftsbereich.

20. Welche Rolle spielt das Informationstechnikzentrum Bund (ITZBund) in Bezug auf die IT-Sicherheit für das BMDS, und wie entwickelt sich dort die Personalausstattung in diesem Bereich?

Das BMDS nimmt die Dienste des ITZBund im Rahmen der IT-Konsolidierung in Anspruch. Im Übrigen wird auf die Antwort zu Frage 19 verwiesen.

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

Maßnahmen ergeben sich aus dem Kabinettbeschluss zur IT-Konsolidierung. Im Übrigen gilt die GGO.

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

Nein.

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