Deutscher Bundestag **Drucksache 21/9086**

21. Wahlperiode 11.11.2026

Vorabfassung - wird durch die lektorierte Version ersetzt.

Kleine Anfrage

der Abgeordneten Robin Jünger, Ruben Rupp, Alexander Arpaschi, Sebastian Maack, Tobias Ebenberger, Lars Haise, Edgar Naujok, Steffen Janich, Dr. Michael Kaufmann, Micha Fehre, Beatrix von Storch, Ronald Gläser, Peter Bohnhof, Thomas Ladzinski, Sascha Lensing und der Fraktion der AfD

Finanzierung, Beschaffung und Wirtschaftlichkeit der Cybersicherheit der Bundesverwaltung

Die Verbesserung der Cybersicherheit der Bundesverwaltung erfordert neben rechtlichen und organisatorischen Änderungen erhebliche personelle, technische und finanzielle Ressourcen. Die parlamentarische Kontrolle muss deshalb neben dem angestrebten Sicherheitsniveau auch den Mittelbedarf, die tatsächliche Mittelverwendung, die Beschaffungswege und die messbare Wirkung zusätzlicher Ausgaben erfassen. Die Bundesregierung hat das Programm „CyberGovSecure“ am 22. Juli 2026 beschlossen. Das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) erklärte zugleich, für das Programm zusätzliche Personal- und Sachmittel im Haushaltsaufstellungsverfahren 2027 angemeldet zu haben. Der Kabinettsbeschluss sieht vor, dass für die Durchführung des Programms zusätzliche Mittel und Stellen für den Haushalt 2027 und die mittelfristige Finanzplanung angemeldet werden. Bestehende Rahmenverträge sollen genutzt werden. Zugleich können eigene Haushaltsmittel der Ressorts erforderlich sein. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) kann bei der operativen Unterstützung auch Dritte beauftragen. Die vorgesehenen Handlungsfelder reichen von Systemhärtung, Asset- und Schwachstellenmanagement über Protokollierung und Detektion, Netzwerksegmentierung und Zero-Trust-Architektur bis zu zentralem Identitäts- und Berechtigungsmanagement und Multifaktorauthentisierung. Diese Breite macht eine Priorisierung erforderlich. Der Kabinettsbeschluss sieht daher vor, Zielwerte festzulegen und den Umsetzungsstand mit einem Berichtswesen nachzuverfolgen (https://bmds.bund.de/aktuelles/pressemitteilungen/detail/digitale-wehrhaftigkeit-des-staates-staerken).

Aus Sicht der Fragesteller ist insbesondere die Inanspruchnahme externer Leistungen von parlamentarischem Interesse. Cyberforensik, Penetrationstests, Sicherheitsberatung, technische Implementierung und Betrieb spezialisierter Sicherheitsprodukte können besondere Fachkenntnisse erfordern, die nicht jederzeit in der Bundesverwaltung verfügbar sind. Gleichzeitig können langfristige externe Abhängigkeiten Kosten erhöhen und eigenes Fachwissen in der Verwaltung schwächen.

Der Koalitionsvertrag von CDU, CSU und SPD für die 21. Wahlperiode sieht eine gesteuerte Aufgaben- und Ausgabenkritik sowie eine stärkere ressortübergreifende Zusammenarbeit vor. Zudem soll der Einsatz externer und kostenintensiver Berater durch bessere Steuerung auf das notwendige Maß begrenzt werden. Die Koalition verbindet Staatsmodernisierung mit dem Anspruch,

staatliche Aufgaben effizienter zu organisieren (www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf).

Für sicherheitskritische IT-Beschaffungen kommt darüber hinaus der digitalen Souveränität Bedeutung zu. Eine starke Abhängigkeit von einzelnen Herstellern kann Wechselkosten erhöhen und die Reaktionsfähigkeit bei Sicherheits- oder Lieferproblemen beeinflussen. Interoperabilität, offene Schnittstellen, Kontrollierbarkeit und realistische Ausstiegsmöglichkeiten können nach Ansicht der Fragesteller daher neben Preis und technischer Leistungsfähigkeit relevante Beschaffungskriterien sein. Nachvollziehbar sollte jedenfalls sein, welcher zusätzliche Mitteleinsatz welches messbare Sicherheitsziel erreichen soll. Andernfalls lässt sich nicht beurteilen, ob höhere Ausgaben tatsächlich zu einer besseren Detektionsfähigkeit, kürzeren Reaktionszeiten oder einer geringeren Zahl offener Sicherheitsdefizite führen.

Wir fragen die Bundesregierung:

1. Welche zusätzlichen Personal- und Sachmittel hat das Bundesministerium für Digitales und Staatsmodernisierung für „CyberGovSecure“ im Regierungsentwurf des Bundeshaushalts 2027 und in der mittelfristigen Finanzplanung angemeldet, und welche Beträge entfallen jeweils auf Personal, Investitionen, laufenden Betrieb und externe Leistungen?
2. Welche Haushaltsmittel stehen für Maßnahmen von „CyberGovSecure“ im Jahr 2026 tatsächlich zur Verfügung, und welcher Betrag war davon im September 2026 jeweils verausgabt, rechtlich gebunden oder noch nicht gebunden?
3. Welche Mittel sind nach der gegenwärtigen Programmplanung den Handlungsfeldern Systemhärtung, Assetmanagement, Schwachstellenmanagement, Protokollierung und Detektion, Netzwerksicherheit, Informationssicherheitscontrolling, Daten- und Zugriffsschutz sowie Mobile-Device-Management zugeordnet?
4. Welche externen Beratungs-, Forensik-, Penetrationstest-, Implementierungs- oder sonstigen IT-Sicherheitsleistungen mit einem Auftragswert von jeweils mindestens 100 000 Euro wurden seit dem 1. Januar 2026 für ressortübergreifende Maßnahmen von „CyberGovSecure“ durch das Bundesministerium für Digitales und Staatsmodernisierung oder das Bundesamt für Sicherheit in der Informationstechnik beauftragt, und welche Auftragsgegenstände, Laufzeiten und Auftragswerte betreffen diese Leistungen?
5. Welches Gesamtauftragsvolumen der in Frage 4 genannten externen IT-Sicherheitsleistungen wurde im Wege eines offenen oder nicht offenen wettbewerblichen Verfahrens, über bestehende Rahmenverträge beziehungsweise ohne vorherigen Teilnahmewettbewerb vergeben?
6. Welche bestehenden zentralen Rahmenverträge werden für die Umsetzung von „CyberGovSecure“ genutzt, für welche Leistungsarten werden zusätzliche Rahmenverträge vorbereitet, und anhand welcher Wirtschaftlichkeitsuntersuchungen wurde entschieden, Leistungen zentral statt dezentral zu beschaffen?
7. Welche zusätzlichen Investitionen in Protokollierungs- und Detektionsinfrastruktur, Mehrfaktorauthentisierung, Identitäts- und Berechtigungsmanagement, Schwachstellenmanagement sowie Netzwerksegmentierung wurden seit dem Kabinettsbeschluss vom 22. Juli 2026 freigegeben oder zur haushalterischen Freigabe vorgelegt?

Vorabfassung - wird durch die lektorierte Version ersetzt.

8. Wie viele zusätzliche Stellen sind mit Stand des Haushaltsentwurfs 2027 für die Koordination und operative Umsetzung von „CyberGovSecure“ beim Bundesministerium für Digitales und Staatsmodernisierung und beim Bundesamt für Sicherheit in der Informationstechnik vorgesehen, und welche Aufgabenprofile sollen diese Stellen jeweils abdecken?
9. Welche Anforderungen an Interoperabilität, Datenportabilität, offene Schnittstellen, Herstellerwechsel und Vermeidung technisch oder wirtschaftlich schwer auflösbarer Anbieterabhängigkeiten gelten bei sicherheitskritischen Beschaffungen im Rahmen von „CyberGovSecure“?
10. Welche quantifizierten Wirkungskennzahlen ordnet die Bundesregierung den zusätzlichen Ausgaben für „CyberGovSecure“ zu, insbesondere hinsichtlich des Anteils vollständig erfüllter Sicherheitsvorgaben, der Zahl überfälliger kritischer Schwachstellen, der Abdeckung zentraler Detektionssysteme und der Dauer bis zur Erkennung und Eindämmung erheblicher Sicherheitsvorfälle?
11. Welche Wirtschaftlichkeitsuntersuchungen, Kosten-Nutzen-Bewertungen oder vergleichbaren Entscheidungsgrundlagen liegen der Bundesregierung für die im Rahmen von „CyberGovSecure“ vorgesehenen zentralen Sicherheitsmaßnahmen vor, insbesondere für Protokollierung und Detektion, Identitäts- und Berechtigungsmanagement, Netzwerksegmentierung sowie Schwachstellenmanagement, und anhand welcher quantifizierbaren Kriterien wird überprüft, ob der zusätzliche Mitteleinsatz tatsächlich zu einer Verringerung festgestellter Sicherheitsdefizite oder zu kürzeren Erkennungs- und Reaktionszeiten führt?
12. Welche vertraglich oder organisatorisch gesicherten Kapazitäten hält die Bundesregierung für den kurzfristigen Einsatz externer Cyberforensik-, Incident-Response- und Wiederherstellungsdienstleister bei einem schwerwiegenden Cyberangriff auf Einrichtungen des Bundes vor, welche maximalen Reaktionszeiten beziehungsweise Abruffristen sind hierfür vereinbart, und welche zusätzlichen Rahmenverträge oder Vorsorgemaßnahmen wurden seit dem Cyberangriff auf die Berliner Landesverwaltung geprüft, vorbereitet oder abgeschlossen?

Berlin, den 6. November 2026

Dr. Alice Weidel, Tino Chrupalla und Fraktion

Vorabfassung - wird durch die lektorierte Version ersetzt.

Vorabfassung - wird durch die lektorierte Version ersetzt.

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