Deutscher Bundestag **Drucksache 21/9379**

21. Wahlperiode 23.11.2026

Vorabfassung - wird durch die lektorierte Version ersetzt.

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Robin Jünger, Ruben Rupp, Alexander Arpaschi, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 21/9086 –

Finanzierung, Beschaffung und Wirtschaftlichkeit der Cybersicherheit der Bundesverwaltung

Vorbemerkung der Fragesteller

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.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Digitales und Staatsmodernisierung vom 23. November 2026 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Der Koalitionsvertrag zwischen 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 Bundesregierung 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.

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?

Die Mittel für das Programm CyberGovSecure wurden nicht über den Regierungsentwurf zum Bundeshaushalt 2027 angemeldet, sondern im parlamentarischen Verfahren eingebracht.

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?

Die explizit für Maßnahmen des Programms CyberGovSecure zur Verfügung stehenden Haushaltsmittel im Jahr 2026 belaufen sich auf 2.727,50 T Euro. Davon waren im September 2026 ein Betrag von 1.190 T Euro gebunden und insgesamt 150 T Euro verausgabt.

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?

Die zur Verfügung stehenden Haushaltsmittel werden den für das jeweilige Jahr priorisierten und beschlossenen CyberGovSecure-Maßnahmen bedarfsgerecht zugeordnet.

Nach sehr sorgfältiger Abwägung ist die Bundesregierung zu dem Schluss gekommen, dass eine weitergehende Aufschlüsselung der Mittel nach den genannten Handlungsfeldern aus Gründen der Informationssicherheit nicht möglich ist. Die Zuordnung könnte im Zusammenhang mit weiteren Informationen Rückschlüsse auf Schwerpunkte und Umfang geplanter Sicherheitsmaßnahmen ermöglichen. Diese Informationen könnten zur Vorbereitung gezielter Angriffe auf die Einrichtungen der Bundesverwaltung genutzt werden.

Vorabfassung - wird durch die lektorierte Version ersetzt.

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?

Das Programm CyberGovSecure wurde im Jahr 2026 mit einer Anschubfinanzierung erfolgreich gestartet. Damit konnten die Grundlagen für die Durchführung geschaffen und erste Maßnahmen, teils mit externer Unterstützung, angestoßen werden.

Nach sehr sorgfältiger Abwägung ist die Bundesregierung zu dem Schluss gekommen, dass eine weitergehende Darstellung der erfragten Leistungen aus Gründen der Informationssicherheit nicht möglich ist. Die gemeinsame Offenlegung von Auftragsgegenständen, Laufzeiten und Auftragswerten könnte Rückschlüsse auf Art, Umfang und zeitliche Einordnung sicherheitsrelevanter Prüf- und Unterstützungsleistungen ermöglichen. Diese Informationen könnten genutzt werden, um Schutzmaßnahmen gezielt zu umgehen und Angriffe auf die Einrichtungen der Bundesverwaltung vorzubereiten.

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?

Die Beauftragung von externen IT-Sicherheitsleistungen im Programm CyberGovSecure durch das BSI erfolgt unter Beachtung des geltenden Vergaberechts.

Nach sehr sorgfältiger Abwägung ist die Bundesregierung zu dem Schluss gekommen, dass eine Aufschlüsselung nach Vergabearten insoweit nicht erfolgen kann, da dadurch konkrete sicherheitsrelevante Beschaffungen identifizierbar würden. Dies könnte insbesondere durch einen Abgleich mit anderweitig verfügbaren Vergabeinformationen ermöglicht werden. Soweit sich daraus Rückschlüsse auf Umfang und Organisation von Sicherheitsmaßnahmen ergeben, könnten diese Angriffe auf die Einrichtungen der Bundesverwaltung erleichtern. In diesem Fall stehen einer weitergehenden Beantwortung Gründe der Informationssicherheit entgegen.

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?

Für die Umsetzung von CyberGovSecure werden im Wesentlichen bestehende zentrale Rahmenverträge genutzt. Sofern im Zuge der Programmdurchführung weitere Bedarfe identifiziert werden, wird der Abschluss zusätzlicher Rahmenverträge entsprechend geprüft. Die Feststellung der Wirtschaftlichkeit von Maßnahmenumsetzungen erfolgt anhand geeigneter Wirtschaftlichkeitsuntersuchungen gemäß § 7 BHO.

Nach sehr sorgfältiger Abwägung ist die Bundesregierung zu dem Schluss gekommen, dass eine weitergehende Beantwortung hinsichtlich sicherheitsrelevanter Einzelheiten der Rahmenverträge und ihrer Entscheidungsgrundlagen

Vorabfassung - wird durch die lektorierte Version ersetzt.

nicht möglich ist. Angaben zu bestehenden und vorbereiteten Leistungsangeboten könnten zusammen mit den zugrunde liegenden Wirtschaftlichkeitsuntersuchungen Rückschlüsse auf die Organisation zentraler Sicherheitsleistungen ermöglichen. Dadurch könnten die Verteilung von Schutzfunktionen und sicherheitsrelevante Abhängigkeiten erkennbar werden. Diese Informationen könnten zur Vorbereitung gezielter Angriffe auf die Einrichtungen der Bundesverwaltung genutzt werden.

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?

Nach sehr sorgfältiger Abwägung ist die Bundesregierung zu dem Schluss gekommen, dass eine Darstellung der freigegebenen oder zur Freigabe vorgelegten in der Frage genannten Investitionen aus Gründen der Informationssicherheit nicht möglich ist. Die Angaben könnten Rückschlüsse auf geplante Erweiterungen der Schutzmaßnahmen und deren Vorbereitung ermöglichen. In Verbindung mit weiteren Informationen könnten daraus sicherheitsrelevante Übergangsphasen abgeleitet und für die Vorbereitung gezielter Angriffe auf die Einrichtungen der Bundesverwaltung genutzt werden.

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?

Dem BSI sind als Ergebnis der Bereinigungssitzung für den Haushalt 2027 für die Themen „NIS2UmsuCG“ (151 Stellen) und „Schutz der informationstechnischen Systeme (u. a. Cyberdome, CISO Bund, ZEAM, NATO SAA)“ (100 Stellen) entsprechende Stellen zugewiesen worden. Das Thema „CyberGovSecure“ lässt sich in Verknüpfung mit der Rolle CISO Bund grundsätzlich beiden Stellenzuweisungen zuordnen. Die genaue Verteilung der Stellen, in Bezug auf den jeweiligen Zuweisungszweck, wird im Detail noch vorgenommen.

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“?

Die in der Frage angesprochenen Anforderungen sind im Zusammenhang mit dem jeweiligen Beschaffungsgegenstand zu betrachten. Neben den einschlägigen rechtlichen Rahmenbedingungen sind dabei der Schutzbedarf, der Stand der Technik und die konkreten Einsatzbedingungen von Bedeutung. Auch die verfügbaren marktüblichen Lösungen sind in diesen Zusammenhang einzuordnen. Die Bedeutung einzelner Anforderungen lässt sich daher nur unter Berücksichtigung der jeweiligen technischen, betrieblichen und wirtschaftlichen Rahmenbedingungen beurteilen. Die den einzelnen CyberGovSecure-Maßnahmen zugrundeliegenden übergreifenden Controls der Informationssicherheit leiten sich grundsätzlich aus den bestehenden Standards des BSI ab, die herstellerneutral sind.

Vorabfassung - wird durch die lektorierte Version ersetzt.

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?

Für CyberGovSecure sind übergreifende Controls der Informationssicherheit definiert. Bei der Bewertung der Wirkung sind die unterschiedlichen Ausgangslagen und die jeweiligen Umsetzungsbedingungen zu berücksichtigen. Die in der Frage angesprochenen Größen betreffen unterschiedliche Aspekte der Informationssicherheit. Ihre Entwicklung lässt sich nicht unabhängig von den technischen Rahmenbedingungen und der Bedrohungslage einordnen. Ein unmittelbarer Rückschluss auf die Wirkung einzelner Ausgaben setzt deshalb eine entsprechend belastbare Bewertungsgrundlage voraus.

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?

Vor einer externen Beauftragung zentraler Sicherheitsmaßnahmen durch das BSI werden angemessene Wirtschaftlichkeitsuntersuchungen gemäß § 7 BHO durchgeführt. Bei der fachlichen Einordnung von Sicherheitsmaßnahmen sind deren Zweck, die angestrebte Schutzwirkung und die jeweiligen Einsatzbedingungen zu berücksichtigen.

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?

Eine Darstellung der seitens der Bundesregierung vorgehaltenen Kapazitäten für den Einsatz bei schwerwiegenden Cyberangriffen auf Einrichtungen des Bundes ist aus Gründen der Informationssicherheit nicht möglich. Die Offenlegung der erbetenen Angaben würde konkrete Rückschlüsse auf Sicherheitsniveau und Schutzvorkehrungen der Bundesregierung und Einrichtungen der Bundesverwaltung zulassen. Diese Informationen könnten von potentiellen Angreifern genutzt werden und dadurch die Sicherheit der Einrichtungen der Bundesverwaltung gefährden.

Vorabfassung - wird durch die lektorierte Version ersetzt.

Vorabfassung - wird durch die lektorierte Version ersetzt.

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