BUNDES
RECHNUNGS
HOF

Bericht nach § 88 Absatz 2 BHO
an den Haushaltsausschuss des Deutschen Bundestages

Cybersicherheit

Effektiver Ressourceneinsatz durch bessere Steuerung

12. August 2026

Geschäftszeichen: VII 4 - 0000583-5

Dieser Bericht enthält das vom Bundesrechnungshof abschließend im Sinne des § 96 Absatz 4 BHO festgestellte Prüfungsergebnis. Er ist auf www.bundesrechnungshof.de veröffentlicht.

Dieser Bericht des Bundesrechnungshofes ist urheberrechtlich geschützt.

Auf einen Blick

Cybersicherheit: Bundesregierung muss Mittel effektiver steuern und kontrollieren

Mangelnde Transparenz und Steuerung gefährden die Cybersicherheit des Bundes. Die Bundesregierung hat bisher kein Informationssicherheitscontrolling (IS-Controlling) aufgebaut. Ihr fehlt so ein Überblick über den Stand der Cybersicherheit. Um Ausgaben für die Cybersicherheit priorisiert zu finanzieren, nutzt sie die im Grundgesetz verankerte Bereichsausnahme zum Schutz informationstechnischer Systeme nur unzureichend und nicht immer gesetzeskonform.

→ Worum geht es?

Der Haushaltsausschuss des Deutschen Bundestages hat gefordert, dass die Bundesregierung Maßnahmen zur Cybersicherheit mittels eines zentralen IS-Controllings über die Bereichsausnahme effektiv finanziert. Ressorts haben die Bereichsausnahme aber teilweise nicht, unzureichend oder nicht gesetzeskonform genutzt. Das geforderte IS-Controlling ist noch nicht etabliert und das Bundesamt für Sicherheit in der Informationstechnik (BSI) kann dazu kaum Erkenntnisse beisteuern. Nachweise der Bundesverwaltung zur Cybersicherheit liegen ebenfalls nicht vor. Die Bundesregierung hat damit insgesamt keinen belastbaren Überblick zum Stand der Cybersicherheit.

→ Was ist zu tun?

Die Bundesregierung muss die Cybersicherheit ressortübergreifend stärken. Hierzu muss das federführende Bundesministerium für Digitales und Staatsmodernisierung (BMDS) Maßnahmen zur Cybersicherheit konsequent steuern und ein geeignetes IS-Controlling mit belastbaren und steuerungsrelevanten Daten etablieren. Die Kontrollen des BSI und Nachweise der Einrichtungen der Bundesverwaltung bilden dessen Grundlage. Ressorts dürfen nur Personal- und Sachmittel in der Bereichsausnahme veranschlagen, die unmittelbar dem Schutz informationstechnischer Systeme dienen.

→ Was ist das Ziel?

Das BMDS hat ein IS-Controlling auf Grundlage aktueller Daten aus flächendeckenden Kontrollen des BSI und Nachweisen der Bundesverwaltung zur Cybersicherheit eingeführt. Auch mit Hilfe des IS-Controllings kann die Bundesregierung gezielt Personal- und Sachmittel aus der Bereichsausnahme zum Schutz informationstechnischer Systeme einsetzen und so die Cybersicherheit effektiv steuern und verbessern.

Inhaltsverzeichnis

0 Zusammenfassung 6

1 Aktuelle Lage im Cyberraum 9

2 Bereichsausnahme 10

2.1 Zweckfremde Ausgaben in der Bereichsausnahme 11

2.2 Kriterien für die Zuordnung von Ausgaben in die Bereichsausnahme 16

3 IS-Controlling 21

3.1 Kontrollen nach § 7 BSI-Gesetz 22

3.2 Nachweise nach § 43 Absatz 1 BSI-Gesetz 26

3.3 Aufbau des IS-Controllings 29

Abkürzungsverzeichnis

B

BKAmt *Bundeskanzleramt*

BMDS *Bundesministerium für Digitales und Staatsmodernisierung*

BMF *Bundesministerium der Finanzen*

BMFTR Bundesministerium für Forschung, Technologie und Raumfahrt

BMI *Bundesministerium des Innern*

BMVg *Bundesministerium der Verteidigung*

BSI *Bundesamt für Sicherheit in der Informationstechnik*

H

Haushaltsausschuss *Haushaltsausschuss des Deutschen Bundestages*

I

IS-Controlling *Informationssicherheitscontrolling*

K

KI *Künstliche Intelligenz*

KPI *Key Performance Indicators, englischer Begriff für steuerungsrelevante Kennzahlen*

0 Zusammenfassung

Die Bedrohungslage im Cyberraum ist infolge der geopolitischen Lage sowie des rasanten technischen Fortschritts hoch. Im Jahr 2025 registrierte das Bundeskriminalamt rund 334 000 Fälle von Cybercrime im engeren Sinne[1]. Der Schaden allein für die deutsche Wirtschaft lag bei 202,4 Mrd. Euro.[2] Auch die Bundesverwaltung ist von dieser Entwicklung mit gravierenden Konsequenzen für deren Cybersicherheit betroffen.

Die Bereichsausnahme gemäß Artikel 109 und 115 Grundgesetz ermöglicht es, die für die Schuldenregel relevanten Krediteinnahmen u. a. um Ausgaben für den Schutz informationstechnischer Systeme zu bereinigen. Im Ergebnis können damit Mehrausgaben außerhalb der Schuldenregel für die Cybersicherheit geleistet werden.

Im November 2025 hat der Haushaltsausschuss des Deutschen Bundestages (Haushaltsausschuss) in seinem Maßgabebeschluss die Bundesregierung aufgefordert, die Haushaltsmittel für Cybersicherheitsmaßnahmen in der Bundesverwaltung zentral unter Federführung des BMDS zu planen, zu steuern und zu überwachen. Der Haushaltsausschuss erwartet, dass die Bundesregierung die Bereichsausnahme zum Schutz informationstechnischer Systeme nutzt. Dadurch soll sie die Resilienz und Funktionsfähigkeit der Bundesverwaltung erhöhen und so einen wirksamen Beitrag zur Verteidigungsfähigkeit Deutschlands und zur Aufrechterhaltung zentraler Staatsfunktionen leisten. Das BSI soll seine Kontrollbefugnisse nutzen, um belastbare Informationen zum Stand der Cybersicherheit zu erheben und bereitzustellen. Diese sollen über ein ressortübergreifendes IS-Controlling dazu beitragen, die Haushaltsmittel im Bereich der Cybersicherheit effizient einzusetzen und Maßnahmen effektiv zu steuern. Der Haushaltsausschuss hat den Bundesrechnungshof gebeten, prüfend zu begleiten, wie die Bundesregierung seine Maßgaben umsetzt.

Der Bundesrechnungshof hat demgemäß ressortübergreifend seit Dezember 2025 untersucht,

- *wie die Bundesregierung die im Grundgesetz verankerte Bereichsausnahme zum Schutz informationstechnischer Systeme nutzt und*
- *wie der Umsetzungsstand des IS-Controllings in der Bundesverwaltung ist.*

Hierzu hat er beim Bundesministerium der Finanzen (BMF) dessen Vorgaben zur Bereichsausnahme analysiert und beim Auswärtigen Amt, dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium für Landwirtschaft, Ernährung und Heimat, dem Bundesministerium für Arbeit und Soziales sowie dem Bundesministerium für

[1] Cybercrime im engeren Sinne sind Straftaten, die sich direkt gegen IT-Systeme, Netzwerke oder deren Daten richten (z. B. Hacking, Schadsoftware).
[2] Bundeslagebild Cybercrime 2025, Bundeskriminalamt, Stand Mai 2026.

Forschung, Technologie und Raumfahrt (BMFTR) geprüft, wie diese die Vorgaben zur Bereichsausnahme angewendet haben.

Für die Bundesregierung hat das BMDS eine Stellungnahme mit Beiträgen des BMF und des BMFTR abgestimmt. Seine bisherigen Erkenntnisse unter Einbeziehung der Stellungnahme fasst der Bundesrechnungshof in diesem Bericht zusammen.

0.1

Die Bundesregierung hat keine Kriterien formuliert, welche Mittel der Bereichsausnahme zum Schutz informationstechnischer Systeme zuzuordnen sind. Zudem hat sie für die Jahre 2025 und 2026 insgesamt mindestens 1,2 Mrd. Euro in diese Bereichsausnahme verlagert, die nicht dem Schutz informationstechnischer Systeme dienen.

In der Folge war die Berechnung der maximal möglichen Nettokreditaufnahme zu hoch. Gleichzeitig wurden die vom Gesetzgeber vorgesehenen weiteren Ausgaben für die Cybersicherheit nicht zweckentsprechend eingesetzt, um diese zu stärken.

Der Bundesrechnungshof hat der Bundesregierung empfohlen, sicherzustellen, dass sie nur Haushaltsmittel der Bereichsausnahme zuordnet, die dem Schutz informationstechnischer Systeme dienen. Hierzu muss sie verbindliche Kriterien entwickeln und diese ressortübergreifend einheitlich anwenden. Bei der Definition der Kriterien sollte das federführende BMDS mit seiner Expertise unterstützen.

Die Bundesregierung hat darauf hingewiesen, dass die Gesetzesmaterialien die Grundgesetzänderung nicht weiter konkretisieren. Auch die angegebenen 1,2 Mrd. Euro dienten unmittelbar dem Schutz informationstechnischer Systeme. Der Schutz sei nur möglich, wenn man die gesamte Architektur solcher Systeme im Sinne technologischer Souveränität beherrsche.

Die Bereichsausnahme stellt eine privilegierte Ausnahme innerhalb der Schuldenregel dar. Ausgaben zum Schutz informationstechnischer Systeme sind von den übrigen IT-Ausgaben zu trennen. Solche zur technologischen Souveränität pauschal der Bereichsausnahme zuzuordnen, wird dem Ausnahmecharakter der Bereichsausnahme dagegen nicht gerecht.

Weil die Gesetzesmaterialien den Begriff Schutz informationstechnischer Systeme nicht konkretisieren, hätte das BMF den Begriff operationalisieren und so auf ein gemeinsames Verständnis hinwirken müssen. Indem das BMF keine Vorgabe macht, verlagert es diese Aufgabe an jedes einzelne Ressort. Dies erhöht das Risiko, dass einzelne Ressorts den grundgesetzlichen Begriff der Ausgaben zum Schutz informationstechnischer Systeme zu

eng oder zu weit auslegen. Insbesondere wenden sie den Begriff uneinheitlich an. Der Bundesrechnungshof bekräftigt daher seine Empfehlungen. (Tz. 2)

0.2

Im November 2025 forderte der Haushaltsausschuss das zuständige BMDS auf, mithilfe des IS-Controllings die Haushaltsmittel für Cybersicherheit effektiv einzusetzen. Das BMDS will das IS-Controlling nunmehr bis zum Jahr 2027 funktionsfähig etablieren.

Das BSI hat seit über vier Jahren die Befugnis[3], die Sicherheit der Kommunikationstechnik zu kontrollieren. Bisher hat es in zwei Jahren bei 15 Einrichtungen des Bundes den grundlegenden Stand der Cybersicherheit geprüft sowie zehn weitere Kontrollen für das Jahr 2026 eingeplant. Das Verfahren, wie die Bundesverwaltung ihre Nachweise zu erbringen hat, hat das BSI bisher weder konzipiert noch pilotiert.

Aufgrund der unzureichenden Anzahl an Kontrollen des BSI wird dieses bei unverändertem Vorgehen mehr als 20 Jahre benötigen, um alle Einrichtungen des Bundes einmal zu kontrollieren. Nachweise der Bundesverwaltung, die als Datenbasis für das IS-Controlling dienen sollen, liegen nicht vor und sind erst ab Dezember 2030 verpflichtend. Dies ist aufgrund der zunehmenden Bedrohungslage nicht haltbar. Ohne ein wirksames IS-Controlling wird das BMDS die Cybersicherheit nicht zielgerichtet ressortübergreifend verbessern können.

Der Bundesrechnungshof hat empfohlen, das BSI solle

→ umgehend seine Vor-Ort-Kontrollen in der Bundesverwaltung deutlich ausweiten,
→ die Nachweiserbringung der Bundesverwaltung konzipieren und erproben und
→ Selbstauskünfte von Einrichtungen des Bundes zeitnah validieren.

Das BMDS sollte das IS-Controlling bereits bis Ende 2026 in der gesamten Bundesverwaltung etablieren, um darauf aufbauend ab dem Jahr 2027 den Einsatz von Haushaltsmitteln für Cybersicherheit ressortübergreifend zu planen, zu steuern und zu überwachen.

Das BMDS hat entgegnet, dem BSI fehle für weitere Kontrollen das Personal. Es wende daher eine dreistufige Prüfungsmethodik an, um vorliegende Selbstauskünfte zu validieren und für das IS-Controlling zu nutzen. Das BMDS will an seinem bisherigen Zeitplan für das IS-Controlling festhalten und sieht hierzu bis Ende 2026 eine Grundversion vor.

Den wesentlichen Empfehlungen des Bundesrechnungshofes will das BMDS nicht folgen. Ohne ausreichende, zeitnahe Vor-Ort-Kontrollen des BSI und Nachweise der Einrichtungen des Bundes ist eine valide Datengrundlage für ein IS-Controlling nicht gegeben. Somit werden dem BMDS notwendige Informationen für das Haushaltsaufstellungsverfahren fehlen. Der Bundesrechnungshof bleibt daher bei seinen Empfehlungen. (Tz. 3)

[3] Seit dem Jahr 2021 gemäß § 4a BSI-Gesetz und seit der Novellierung 2025 nunmehr § 7 BSI-Gesetz.

1 Aktuelle Lage im Cyberraum

Durch die geopolitischen Entwicklungen hat sich die Bedrohungslage im Cyberraum weiter verschärft. Die Lage der Cybersicherheit[4] in Deutschland ist weiterhin angespannt.[5] Laut BSI geht diese Bedrohung sowohl von staatlichen Akteuren als auch organisierten Cybercrime-Gruppen aus. Deren Aktivitäten und Ressourcen umfassen gezielte Aufklärungstätigkeiten zur Vorbereitung von Cyberangriffen, ein täglich wachsendes Arsenal an Schadsoftware sowie eine professionelle Angriffsinfrastruktur. Das Bundeskriminalamt hat rund 334 000 Cybercrime-Delikte im Jahr 2025 erfasst, von denen rund 208 000 aus dem Ausland verübt wurden.[6] Trotz dieser Bedrohungslage muss die Digitalisierung in Deutschland beschleunigt werden, um den Anforderungen einer modernen Gesellschaft und eines leistungsfähigen Wirtschaftsstandorts gerecht zu werden.

Die am 5. Dezember 2025 in Deutschland in Kraft getretene NIS-2-Richtlinie schafft einen EU-weit einheitlichen Rechtsrahmen, um ein hohes Sicherheitsniveau der Netz- und Informationssysteme zu gewährleisten. Die NIS-2-Richtlinie weitet Anforderungen zur Cybersicherheit, zum Risikomanagement und zu Meldepflichten deutlich aus und schafft ein einheitliches Regelungsregime. Rund 29 500 Unternehmen und Organisationen in Deutschland sind nun zu verbindlichen Sicherheitsmaßnahmen verpflichtet. Anforderungen der NIS-2-Richtlinie gelten auch für die Einrichtungen der Bundesverwaltung und führen zu Erfüllungsaufwänden.

Die Bundesregierung schätzte allein die Haushaltsausgaben ohne Erfüllungsaufwand für die NIS-2-Richtlinie auf rund 906 Mio. Euro bis zum Jahr 2029. Den initialen Erfüllungsaufwand berechnete sie mit 63 Mio. Euro und den jährlichen Erfüllungsaufwand mit 119 Mio. Euro. Die hierzu erforderlichen Personal- und Sachmittel muss die Bundesregierung in den Bundeshaushalt einbringen.

Der Gesetzgeber hat die Aufsichts- und Ordnungsrolle des BSI erheblich gestärkt, indem er dem BSI neue Befugnisse und Sanktionsmöglichkeiten eingeräumt hat.

[4] **Informationssicherheit** umfasst den ganzheitlichen Schutz aller Informationen einer Einrichtung – unabhängig davon, ob sie digital, physisch oder personell vorliegen – mit dem Ziel, Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen.
IT-Sicherheit ist ein Teilbereich davon und fokussiert sich auf den Schutz von IT-Systemen, Anwendungen und digitalen Daten.
Cybersicherheit konzentriert sich speziell auf die Abwehr von Bedrohungen aus dem Cyberraum, also auf Angriffe auf vernetzte Systeme und Infrastrukturen.
Behandlung im Text: Da der Cyberraum sich auf immer weitere Lebensbereiche ausdehnt und auch Bereiche erfasst, die bisher nicht von vernetzten IT-Systemen betroffen waren, werden die Begriffe Informationssicherheit und Cybersicherheit immer häufiger trotz der vorgenannten Differenzierung bedeutungsgleich genutzt. Im vorliegenden Bericht verwenden wir daher vorrangig den Begriff Cybersicherheit, es sei denn gesetzliche Regelungen oder andere Vorgaben sprechen explizit von Informationssicherheit oder IT-Sicherheit.

[5] BSI-Bericht „DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2025“, Stand November 2025, S. 2.

[6] Bundeslagebild Cybercrime 2025, Bundeskriminalamt, Stand Mai 2026.

Auf der Basis der NIS-2-Richtlinie hat der Haushaltsausschuss in seinem Maßgabebeschluss vom November 2025 die Bundesregierung aufgefordert, die Haushaltsmittel für Cybersicherheitsmaßnahmen in der Bundesverwaltung zentral unter Federführung des BMDS zu planen, zu steuern und zu überwachen. Er sieht hierfür ein zentrales Controlling der IT des Bundes als notwendig an. Teil des Controllings soll auch ein IS-Controlling sein. Vom BSI erwartet der Haushaltsausschuss, dass es seine Kontrollbefugnisse nutzt, um dazu belastbare Informationen zum Stand der Cybersicherheit in der Bundesverwaltung bereitzustellen.

Die Bundesregierung hat so die Resilienz und Funktionsfähigkeit der Bundesverwaltung zu erhöhen und die Verteidigungsfähigkeit Deutschlands sowie die Aufrechterhaltung zentraler Staatsfunktionen sicherzustellen.

Der Haushaltsausschuss hat den Bundesrechnungshof gebeten, die Umsetzung durch die Bundesregierung prüfend zu begleiten. Hierzu hat der Bundesrechnungshof untersucht,

→ wie die Bundesregierung die im Grundgesetz verankerte Bereichsausnahme zum Schutz informationstechnischer Systeme nutzt und
→ wie der Umsetzungsstand des IS-Controllings in der Bundesverwaltung ist.

Das BMDS hat eine mit dem BMF und dem BMFTR abgestimmte Stellungnahme abgegeben. Diese ist im Bericht berücksichtigt.

2 Bereichsausnahme

Artikel 115 Absatz 2 Grundgesetz sieht vor, dass der Bund die für die Schuldenregel relevanten Krediteinnahmen um Ausgaben folgender Bereichsausnahmekategorien bereinigt, soweit sie 1 % des nominalen Bruttoinlandsprodukts übersteigen:

→ Verteidigung,
→ Zivil- und Bevölkerungsschutz,
→ Nachrichtendienste,
→ Schutz der informationstechnischen Systeme und
→ Hilfe für völkerrechtswidrig angegriffene Staaten.

Ausgaben zum Schutz informationstechnischer Systeme kann die Bundesregierung damit der Bereichsausnahme zuordnen. Dies erlaubt ihr, bestehende Defizite in der Cybersicherheit priorisiert zu beheben und auch bei einer angespannten Haushaltslage zu finanzieren.

Hierzu hat der Bundesrechnungshof beim BMF dessen Vorgaben zur Bereichsausnahme analysiert und beim

→ Auswärtigen Amt,
→ dem Bundesministerium für Wirtschaft und Energie,
→ dem Bundesministerium für Landwirtschaft, Ernährung und Heimat,
→ dem Bundesministerium für Arbeit und Soziales,
→ sowie dem BMFTR

geprüft, wie diese die Vorgaben zur Bereichsausnahme angewendet haben. Für alle wesentlichen IT-Ausgaben der unmittelbaren Bundesverwaltung hat der Bundeskanzler mit Organisationserlass vom 6. Mai 2025 dem BMDS einen Zustimmungsvorbehalt eingeräumt.[7] Mit einer Verwaltungsvereinbarung haben BMDS, BMF und Bundeskanzleramt (BKAmt) den Zustimmungsvorbehalt konkretisiert. Danach umfassen IT-Ausgaben sämtliche Investitions- und Sachmittel für IT-Infrastruktur, IT-Services und Digitalisierungsvorhaben, IT-Betrieb, IT-Hard- und -Software sowie -Dienstleistungen (z. B. Schulungen oder externe Unterstützungsleistungen). Als wesentlich gelten Ausgaben, die entweder einen bestimmten Schwellenwert[8] überschreiten oder strategischen Aufgaben dienen. Eine strategische Aufgabe ist es, die Cybersicherheit in der Bundesverwaltung zu gewährleisten und zu stärken.[9] Die damit verbundenen Ausgaben fallen somit unabhängig von ihrer Höhe unter den Zustimmungsvorbehalt. Sowohl den Schwellenwert als auch die strategischen Aufgaben legt das BMDS fest. Das BMF gibt diese im Haushaltsaufstellungsrundschreiben bekannt.[10] Es berücksichtigt entsprechende Anmeldungen der Ressorts nur, sofern das BMDS diese nicht abgelehnt hat.

2.1 Zweckfremde Ausgaben in der Bereichsausnahme

Sachverhalt

Für die Bereichsausnahme „Ausgaben zum Schutz informationstechnischer Systeme“ gab das BMF vor, dass diese ausschließlich solche Ausgaben umfassen darf, die unmittelbar der Bereichsausnahmekategorie zuzuordnen sind. Sie darf keine mittelbaren Ausgaben wie sogenannte Overhead-Ausgaben für die Personalverwaltung enthalten.[11]

[7] Organisationserlass des Bundeskanzlers vom 6. Mai 2025, Nummer XIII: Ausgenommen sind der Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg), die Sicherheits- und Polizeiaufgaben im Geschäftsbereich des BMI, der Bundesnachrichtendienst und die Steuerverwaltung im Geschäftsbereich des Bundesministeriums der Finanzen.
[8] Für den Haushalt 2027 beträgt der Schwellenwert gemäß Haushaltsaufstellungsschreiben des BMF vom 26. Januar 2026, Gz. II A 1 – H1105/00054/001/004, für Finanzmittel zur Prüfung von IT- und Digitalisierungsvorhaben 500 000 EUR in einem Haushaltsjahr oder mit einem Gesamtvolumen von 3 000 000 EUR.
[9] Haushaltsaufstellungsrundschreiben des BMF, Gz. II A 1 – H 1105/00054/001/004 vom 26. Januar 2026, S. 15.
[10] „Vereinbarung entsprechend Organisationserlass des Bundeskanzlers gem. § 9 der GO der Bundesregierung vom 06. Mai 2025, Ziffer XIII“ zwischen BKAmt, BMDS und BMF vom 27. November 2025.
[11] Haushaltsaufstellungsrundschreiben des BMF, Gz. II A 1 – H 1105/00050/001/054 vom 19. Mai 2025, S. 6 f.

In den Bundeshaushalten der Jahre 2025 und 2026 sind Ausgaben von insgesamt 4,5 Mrd. Euro dieser Bereichsausnahmekategorie zugeordnet. Die zugehörigen Titelgruppen waren entsprechend den Vorgaben des BMF jeweils mit folgendem Haushaltsvermerk versehen:[12]

> „Aus den Titeln dieser Titelgruppe dürfen nur Ausgaben geleistet werden, die dem Schutz der informationstechnischen Systeme im Sinne des Artikel 115 Absatz 2 Satz 4 des Grundgesetzes dienen.“[13]

Der Haushaltsgrundsatz der sachlichen Bindung (§ 45 Absatz 1 BHO) sichert das Budgetrecht des Parlaments, indem Ausgaben nur zu dem im Haushaltsplan bezeichneten Zweck geleistet werden dürfen.

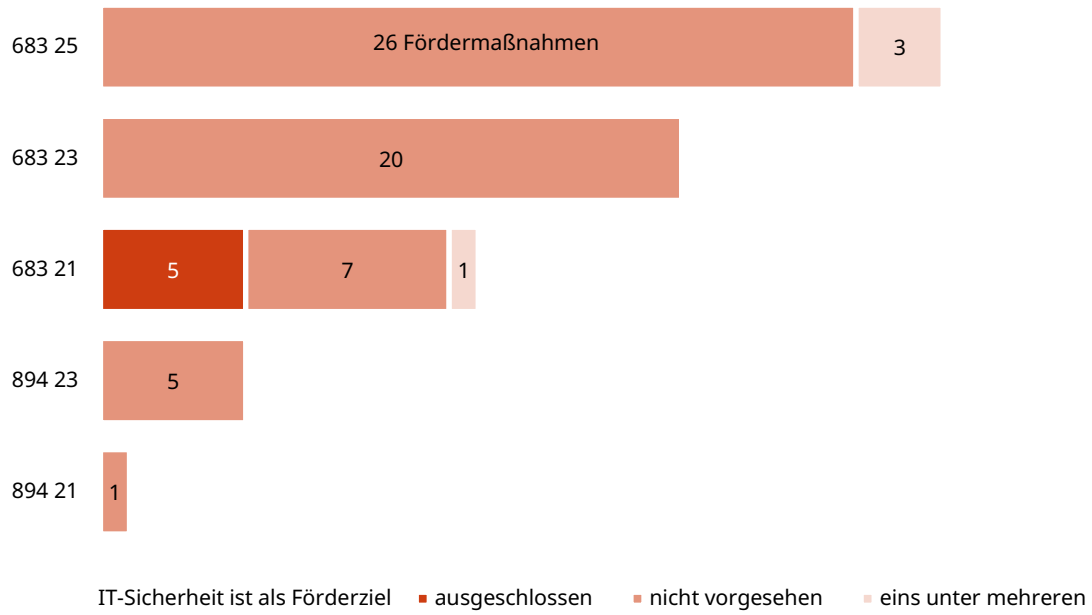
Die Bundesregierung veranschlagte in der Bereichsausnahme zum Schutz informationstechnischer Systeme auch Ausgaben der Forschungsförderung. Zugehörige Titel ordnete sie teilweise der Bereichsausnahme vollständig zu. Bei fünf Titeln[14] mit einem Finanzvolumen von insgesamt mehr als 1,2 Mrd. Euro in den Haushaltsjahren 2025 und 2026 benannte keine der zugehörigen Förderrichtlinien den Schutz informationstechnischer Systeme als primären Förderzweck.[15] Explizit schlossen sogar 5 von 68 Förderrichtlinien IT-Sicherheit als Forschungsgegenstand aus.[16]

[12] Haushaltsaufstellungsrundschreiben des BMF, Gz. II A 1 – H 1105/00050/001/054 vom 19. Mai 2025, S. 7.
[13] Haushaltsplan für den Bundeshaushalt 2026.
[14] Kapitel 3004 Titel 683 21, 683 23, 683 25, 894 21 und 894 23.
[15] Bewertung beruht auf einer Analyse der Förderrichtlinien. Hierbei geht der Bundesrechnungshof davon aus, dass sich dieser Tatbestand auf die Förderprogramme oder -maßnahmen übertragen lässt.
[16] Folgende Richtlinien schließen IT-Sicherheit als Forschungsgegenstand aus: Richtlinie zur Förderung von Forschungsprojekten mit Taiwan zum Thema Forschungs- und Innovationszusammenarbeit auf dem Gebiet der Künstlichen Intelligenz; Richtlinie zur Förderung von Forschungsprojekten zum Thema „Flexible, resiliente und effiziente Machine-Learning-Modelle“; Richtlinie zur Förderung von KI-Nachwuchswissenschaftlerinnen; Richtlinie zur Förderung von Ideennachwuchs: Forschungsvorhaben von KI-Nachwuchsgruppen; Richtlinie zur Förderung von wissenschaftlichen Nachwuchsgruppen unter Leitung von Frauen im Bereich der Künstlichen Intelligenz.

Abbildung 1

Schutz informationstechnischer Systeme nicht als Förderziel oder Förderzweck ausgewiesen

Im Kapitel 3004 hat die Bundesregierung mindestens fünf Titel der Bereichsausnahme zugeordnet, deren Ausgaben nicht dem Schutz informationstechnischer Systeme dienen. Aus diesen Titeln werden Fördermaßnahmen finanziert, in denen IT-Sicherheit als Forschungsgegenstand ausgeschlossen ist oder der Schutz informationstechnischer Systeme im Förderziel oder Förderzweck nicht oder nur als eines von mehreren Themen adressiert wird.



Grafik: Bundesrechnungshof. Quelle: Auswertung der Förderrichtlinien des BMFTR.

Im Jahr 2025 verausgabte die Bundesregierung aus diesen Titeln mehr als 600 Mio. Euro.[17] Sie förderte damit unter anderem die Bereitstellung von Rechenzeit, Methoden der Künstliche Intelligenz (KI) sowie Forschung zu Robotik. Geförderte Projekte entwickelten unter anderem eine Applikation zur Erkennung von Vogelstimmen sowie Verfahren zur Messung der Füllstände von Wertstoffcontainern oder Röntgenstrahlquellen.

Würdigung

Forschungsförderung kann grundsätzlich dem Schutz informationstechnischer Systeme dienen und entsprechende Ausgaben können dann der Bereichsausnahme

[17] Auswertung der HKR-Daten zum Haushaltsjahr 2025.

zugeordnet werden. Die vom Grundgesetz vorgegebene Anforderung erfüllen Fördermaßnahmen jedoch nicht, deren Förderziel und Förderzweck nicht auf den Schutz informationstechnischer Systeme ausgerichtet sind oder dies sogar ausschließen. Sofern es innerhalb einer Fördermaßnahme vereinzelt Projekte gab, die dem Schutz informationstechnischer Systeme dienten, hätte die Bundesregierung explizit nur deren Ausgaben der Bereichsausnahme zuordnen dürfen. In allen 68 Förderrichtlinien der genannten fünf Titel ist aber kein oder nur ein geringer Bezug zum Schutz informationstechnischer Systeme erkennbar. Somit hat die Bundesregierung Ausgaben in Höhe von 1,2 Mrd. Euro unzutreffend der Bereichsausnahme zugeordnet. Die Folge sind verfassungs- und haushaltsrechtliche Verstöße sowie das Verfehlen der politischen Zielvorgabe:

→ Indem sie die Haushaltsmittel im Jahr 2025 entgegen der Maßgabe des Haushaltsvermerks verausgabte, hat sie gegen den Willen des Haushaltsgesetzgebers gehandelt und Haushaltsmittel zweckwidrig eingesetzt.
→ Als weitere Folge kam es vor allem im Jahr 2025 zu einer höheren Nettokreditaufnahme als dies nach der Schuldenregel zulässig ist.
→ Zudem erreicht die Bundesregierung so nicht das Ziel, die Cybersicherheit und damit die Verteidigungsfähigkeit zu stärken.

Empfehlung

Der Bundesrechnungshof hat der Bundesregierung empfohlen, im Vollzug des Haushalts 2026 sicherzustellen, dass sie nur Haushaltsmittel in der Bereichsausnahme verausgabt, die unmittelbar dem Schutz informationstechnischer Systeme dienen. Dies gilt auch für künftige Haushalte. Bereits in der Haushaltsaufstellung darf sie nur solche Mittel, die den Zweck nach Artikel 115 Grundgesetz erfüllen, der Bereichsausnahme zuordnen.

Stellungnahme

Das BMDS hat zur Frage der Veranschlagung von Haushaltsmitteln der Forschungsförderung vom BMFTR eine Stellungnahme eingeholt. Das BMFTR hat angegeben, dass sämtliche Ausgaben, die es der Bereichsausnahme zugeordnet und entsprechend veranschlagt habe, unmittelbar dem Schutz informationstechnischer Systeme dienten. Der Schutz dürfe nicht ausschließlich auf operative IT-Sicherheitsmaßnahmen reduziert werden. Eine hinreichende technologische Souveränität sei eine Grundvoraussetzung, um die Ziele des Artikel 115 Grundgesetz erfüllen zu können. Man müsse insofern die gesamte Architektur im Sinne technologischer Souveränität beherrschen. Dies beinhalte die physikalische Ebene, die Informations- und Kommunikationsebene bis zu den darauf aufbauenden Softwaresystemen und Anwendungen. Insofern sollten die relevanten Ausgaben für Forschung und Entwicklung zu Design und Produktion,

Validierung und Qualifizierung, Standardisierung, Aufbau resilienter Innovationsökosysteme sowie Fachkräfteentwicklung dem Zweck des Artikel 115 Grundgesetz dienen. Ein besonderes Augenmerk liege darauf, die datenbasierten Wertschöpfungsökosysteme des 21. Jahrhunderts gegenüber feindlichen Einflussnahmen abzusichern.

Zu den einzelnen Förderrichtlinien, die die IT-Sicherheitsforschung als Fördergegenstand ausschließen, hat das BMFTR angegeben, dies vermeide Überschneidungen zu anderen Förderbereichen. Ziel und Zweck der Förderungen entsprächen aber dem Schutz informationstechnischer Systeme.

Das BMDS hat darauf hingewiesen, dass es die Zweckbestimmungen der Titel zulasse, daraus zu leistende Ausgaben dem Schutz der informationstechnischen Systeme zuzuordnen. Einzelfragen des Haushaltsvollzugs, wonach das BMFTR nicht sachgemäß einzelne Ausgaben dem Schutz informationstechnischer Systeme zugeordnet habe, ließen sich durch die Haushaltsaufstellung nicht ausschließen. Es sei missverständlich, wenn der Bundesrechnungshof pauschal auf die gesamte Veranschlagung bei den betroffenen Titeln oder auf alle Ausgaben aus diesen Titeln abstelle.

Abschließende Würdigung

Die Bereichsausnahme stellt eine privilegierte Ausnahme innerhalb der Schuldenregel dar. Das BMF unterstrich diesen Ausnahmecharakter durch seine Vorgabe, Ausgaben zum Schutz informationstechnischer Systeme von den übrigen IT-Ausgaben zu trennen.

Es ist zutreffend, dass Ausgaben zum Schutz informationstechnischer Systeme nicht ausschließlich auf operative IT-Sicherheitsmaßnahmen zu beschränken sind. Auch Maßnahmen zur Förderung von Forschung und Entwicklung entlang der gesamten Architektur können einen wichtigen Beitrag zum Schutz informationstechnischer Systeme leisten.

Dies gilt jedoch ausschließlich unter der Voraussetzung, dass für jede Fördermaßnahme das Förderziel und der Förderzweck vorrangig dem Schutz informationstechnischer Systeme dienen. Nur dann dürfen die betreffenden Ausgaben der Bereichsausnahme zugeordnet werden. Sämtliche Ausgaben für die Forschung an informationstechnischen Systemen pauschal zu verlagern, wird dem Ausnahmecharakter der Bereichsausnahme nicht gerecht.

Selbst wenn die Titel nach dem Wortlaut ihrer Zweckbestimmungen Ausgaben zum Schutz informationstechnischer Systeme enthalten könnten, hat die Auswertung der Förderrichtlinien gezeigt, dass Projekte finanziert werden sollen, die nicht dem Schutz informationstechnischer Systeme dienen. BMFTR und BMF haben es damit versäumt, diese von den übrigen Ausgaben zu separieren.

Die Beispiele, wie eine Applikation zur Erkennung von Vogelstimmen, veranschaulichen den fehlenden Bezug zum Schutz informationstechnischer Systeme. Diese Beispiele stellen keine isoliert herausgegriffenen Einzelfälle dar. Vielmehr adressiert keine der Förderrichtlinien in den fünf Titeln vorrangig den Schutz der informationstechnischen Systeme in Förderziel und Förderzweck. Daher hätte das BMFTR sämtliche Ausgaben hierfür nicht in die Bereichsausnahme verlagern dürfen.

Der Bundesrechnungshof hält daher seine Empfehlungen aufrecht.

2.2 Kriterien für die Zuordnung von Ausgaben in die Bereichsausnahme

Sachverhalt

Die Vorgaben zur Cybersicherheit in der Bundesverwaltung leiten sich aus dem Umsetzungsplan Bund ab. Dieser legt fest, dass die Ressorts die Regelungen eigenverantwortlich umsetzen müssen.[18] Seit dem 6. Dezember 2025 ist jede Leitung einer Einrichtung der Bundesverwaltung gesetzlich dafür verantwortlich, „[…] die Voraussetzungen zur Gewährleistung der Informationssicherheit zu schaffen".[19]

Das BMF forderte die Ressorts mit seinem Haushaltsaufstellungsrundschreiben zum zweiten Regierungsentwurf 2025 und zum Regierungsentwurf 2026 dazu auf, alle Ausgaben für den Schutz informationstechnischer Systeme des Bundes den Titeln der dafür definierten Bereichsausnahme zuzuordnen.[20] Als Beispiele für einschlägige Titel nannte es 511 .1[21], 532 .1[22] und 812 .2.[23] Im Gegensatz zum Titel 511 .1 enthalten die Titel 532 .1 und 812 .2 ausschließlich Ausgaben im Bereich Informationstechnik. Kriterien, wie Ausgaben zum Schutz informationstechnischer Systeme gegenüber übrigen IT-Ausgaben zu unterscheiden sind, definierte das BMF nicht. Zwar erkannte und formulierte es das Risiko, die Ressorts könnten ihre Ausgaben uneinheitlich veranschlagen. Allerdings bewertete es das BMF als schwerwiegender, dass jedwede Definition materiell anfechtbar wäre. Zur Begründung führte es an, dass eine solche Definition den von Artikel 115 Grundgesetz gesetzten Umfang der zulässigen Ausgaben einschränken und damit gegen die Verfassung verstoßen könnte.

Das BMF wies intern zur Veranschlagung des eigenen Einzelplans auf Folgendes hin:

[18] Umsetzungsplan Bund 2017 des Bundesministeriums des Innern.
[19] § 43 Absatz 1 BSI-Gesetz.
[20] Haushaltsaufstellungsrundschreiben des BMF vom 19. Mai 2025, Gz. II A 1 – H1105/00050/001/054.
[21] Geschäftsbedarf und Kommunikation sowie Geräte, Ausstattungs- und Ausrüstungsgegenstände, sonstige Gebrauchsgegenstände, Software, Wartung.
[22] Aufträge und Dienstleistungen im Bereich Informationstechnik.
[23] Erwerb von Anlagen, Geräten, Ausstattungs- und Ausrüstungsgegenständen sowie Software im Bereich Informationstechnik.

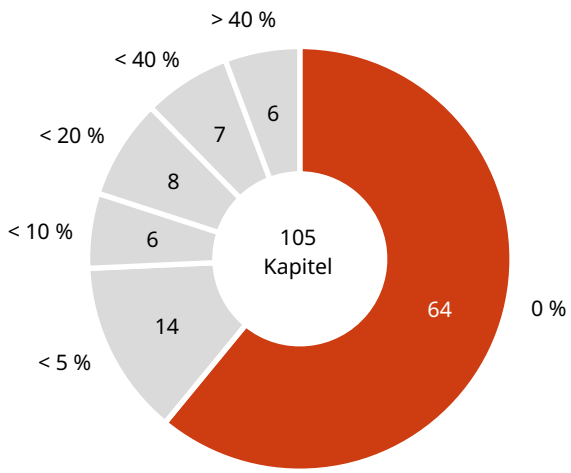
„Für künftige Haushaltsaufstellungsverfahren sollte unter Berücksichtigung der Erkenntnisse aus den Ressorts eine Präzisierung der Regelungen für die Bereichsausnahme „Schutz der informationstechnischen Systeme“ vorgenommen werden.“

Teilweise ordneten Ressorts keine Haushaltsmittel der Bereichsausnahme zu. In rund zwei Drittel der Kapitel, die IT-Ausgaben in den Titeln 532 .1 und 812 .2 enthielten und die nicht in eine der anderen Bereichsausnahmekategorien fielen,[24] wies der Bundeshaushalt 2026 keine IT-Ausgaben in der Bereichsausnahme aus.

Abbildung 2

Zwei Drittel der Kapitel mit IT-Ausgaben im Bundeshaushalt 2026 sehen keine IT-Ausgaben in der Bereichsausnahme vor.

Der folgenden Abbildung ist zu entnehmen, wie hoch der prozentuale Anteil der IT-Ausgaben zum Schutz informationstechnischer Systeme im Verhältnis zu den gesamten IT-Ausgaben ist. Diese Ausgaben sind an den Titeln 532 .1 und 812 .2 gemessen. IT-Ausgaben sind insgesamt in 105 Kapiteln des Bundeshaushalts vorhanden. In 64 Kapiteln sind keine IT-Ausgaben zum Schutz informationstechnischer Systeme in der Bereichsausnahme veranschlagt. 41 Kapitel haben solche Ausgaben anteilig veranschlagt.



Grafik: Bundesrechnungshof. Quelle: Haushaltsgesetz 2026.

[24] Die Kapitel 0616, 0628, 0629, 1403 und 1413 haben Ausgaben in den Titeln 532 .1 und 812 .2 veranschlagt. Sie fallen aber vollständig unter eine andere Bereichsausnahmekategorie.

Kriterien, nach denen die Ressorts Mittel veranschlagten, hatten teilweise weder diese noch das BMF dokumentiert. Auch im Haushaltsaufstellungsrundschreiben zum Haushaltsjahr 2027 nannte das BMF keine weiteren Kriterien für eine Zuordnung zur Bereichsausnahme zum Schutz informationstechnischer Systeme.[25]

Das BMDS sah u. a. Ausgaben, die dem Ziel dienen, die Cybersicherheit der Bundesverwaltung zu gewährleisten oder zu stärken, unabhängig von ihrer Höhe als wesentliche IT-Ausgaben an.[26] Sie fallen somit unter seinen Zustimmungsvorbehalt.

Die Haushaltsmittel der Bereichsausnahmekategorie „Schutz der informationstechnischen Systeme“ soll im Haushalt 2027 gemäß dem Entwurf der Bundesregierung von 2,8 Mrd. Euro auf 3,9 Mrd. Euro steigen.[27]

Würdigung

Der Bundesrechnungshof erkennt an, dass es große sicherheitspolitische Nachholbedarfe gibt. Eine dauerhafte und unbegrenzte Öffnung der Schuldenregel, wie sie die Bereichsausnahme zur Behebung des sicherheitspolitischen „Notstands“ vorsieht, darf aber – vor allem mit Blick auf die erheblich steigenden Zinsausgaben – nicht zu einem künftigen finanziellen Notstand des Bundes führen.[28]

Dabei ist zu berücksichtigen, dass die Ressorts die Cybersicherheit ihrer IT selbst verantworten und dies bei der Mittelplanung berücksichtigen müssen. Veranschlagen sie IT-Ausgaben, haben sie gleichzeitig Haushaltsmittel für deren Cybersicherheit einzuplanen. Dass die Bundesregierung in zahlreichen Kapiteln zwar IT-Ausgaben veranschlagte, aber keine Haushaltsmittel für die Bereichsausnahme zum Schutz informationstechnischer Systeme anmeldete, ist daher nicht plausibel. Indem die Bundesregierung Ausgaben für Cybersicherheit teilweise gar nicht der Bereichsausnahme zuordnete, hat sie deren Intention unterlaufen. Dies ist angesichts der bestehenden Defizite und der aktuellen Bedrohungslage inakzeptabel. Zudem widerspricht das Vorgehen den Vorgaben des Haushaltsaufstellungsrundschreibens. Derzeit fehlt insgesamt ein einheitlicher Maßstab, wie Ausgaben zum „Schutz informationstechnischer Systeme“ von übrigen IT-Ausgaben abzugrenzen sind. Dieser muss für alle Ressorts klarstellen, wie sie einheitlich und zutreffend ihre Mittel zu veranschlagen haben.

Obwohl das BMF dieses Problem selbst erkannt hat, unterließ es im Haushaltsaufstellungsrundschreiben für den Haushalt 2027 entsprechende Änderungen. Dies ist angesichts der deutlichen Steigerung der Bereichsausnahme im Jahr 2027 auf 3,9 Mrd. Euro

[25] Haushaltsaufstellungsrundschreiben des BMF, Gz. II A 1 – H 1105/00054/001/004.
[26] Haushaltsaufstellungsrundschreiben des BMF, Gz. II A 1 – H 1105/00054/001/004.
[27] Eckwerte des Regierungsentwurfs zum Bundeshaushalt 2027 und des Finanzplans des Bundes 2026 bis 2030, Gz. II A 1 – H 1120/00442/001/002 vom 28. April 2026.
[28] Vgl. Tz. 6 der Stellungnahme des Bundesbeauftragten für Wirtschaftlichkeit in der Verwaltung, Eckwerte für den Bundeshaushalt 2027 und die Finanzplanung 2028 bis 2030, Verschuldungsdynamik eindämmen und Bundeshaushalt endlich strukturell konsolidieren, Gz. I 2 - 0003749 vom 20. April 2026.

nicht nachvollziehbar. Das BMF hätte durch Kriterien oder Vorgaben dafür Sorge tragen müssen, dass die Ressorts die in der Bereichsausnahme etatisierten Ausgaben eindeutig, nachvollziehbar und überprüfbar abgrenzen. Nur so kann es darauf hinwirken, dass die Ressorts zutreffend und einheitlich veranschlagen. Zudem könnte es im Einzelnen darauf hinwirken, Maßnahmen auf das von dem Gesetzgeber geforderte Maß zu begrenzen, mittel- bis langfristig die Ausgaben zu reduzieren und die Inanspruchnahme der Bereichsausnahme zurückzuführen.

Das BMF sollte hierbei auf die Expertise des BMDS zurückgreifen, um eine fachliche Abgrenzung vorzunehmen. Dieses muss für seinen Zustimmungsvorbehalt ohnehin Ausgaben identifizieren, „die dem Ziel dienen, die Cybersicherheit der Bundesverwaltung zu gewährleisten“. Das BMF könnte auf diese Analyse zurückgreifen.

Empfehlung

Der Bundesrechnungshof hat dem BMDS empfohlen, bei der Prüfung des Zustimmungsvorbehalts den Ressorts mitzuteilen, nach welchen Kriterien es Ausgaben identifiziert, die der Cybersicherheit zuzuordnen sind.

Für das Haushaltsaufstellungsrundschreiben sollte das BMF klarstellen, dass für den Schutz informationstechnischer Systeme Ausgaben nach diesen Kriterien in der Bereichsausnahme zu veranschlagen sind. Außerdem sollte das BMF die Haushaltsanmeldungen der Ressorts anhand der vom BMDS festgelegten Kriterien prüfen. Veranschlagt eine Behörde keine IT-Sicherheitsausgaben in der Bereichsausnahme, sollten BMF und BMDS die Gründe hierfür hinterfragen.

Mittelfristig müssen die verteidigungs- und sicherheitspolitischen Daueraufgaben als staatliche Kernaufgaben grundsätzlich ohne Bereichsausnahme von der Schuldenregel bestritten werden. Die Inanspruchnahme der Bereichsausnahme sollte daher sukzessive zurückgefahren werden.

Stellungnahme

Das BMDS hat mitgeteilt, das BMF habe die Veranschlagung in der Bereichsausnahme konkretisiert. Wie vom Bundesrechnungshof zutreffend dargestellt, habe dieses ausdrücklich vorgegeben, dass mittelbare Ausgaben nicht zu berücksichtigen sind. Den Gesetzesmaterialien zur Grundgesetzänderung seien keine weiteren Konkretisierungen zu entnehmen. Eigene weitere Konkretisierungen liefen damit Gefahr, die vom Gesetzgeber geschaffene Möglichkeit entweder zweckwidrig einzuschränken oder den grundgesetzlichen Begriff zu überdehnen. Dies gelte insbesondere, da die Cybersicherheit ein dynamisches, entwicklungsoffenes und technisch geprägtes Feld sei. Das BMF

habe zudem recherchiert, ob verbindliche Kriterien existieren, die den Begriff „Schutz informationstechnischer Systeme“ präzisieren, solche aber nicht auffinden können.

Der Interessenkonflikt, Defizite in der Cybersicherheit mit Hilfe der Bereichsausnahme zu beheben und Ausgaben zu reduzieren, sei offensichtlich. Es erscheine fraglich, ob dieser durch Kriterien oder Vorgaben aufzulösen sei.

Abschließende Würdigung

Die vom BMDS angeführten Konkretisierungen betrachten nicht, welche unmittelbaren Ausgaben die Ressorts für die Bereichsausnahme berücksichtigen sollen. Dennoch muss der Begriff „Ausgaben zum Schutz informationstechnischer Systeme“ operationalisiert werden. Indem das BMF keine Vorgabe macht, überlässt es diese Aufgabe den Ressorts und deren individueller Interpretation. Dies verstärkt das vom BMF identifizierte Risiko, wonach einzelne Ressorts den grundgesetzlichen Begriff der Ausgaben zum Schutz informationstechnischer Systeme zu eng oder zu weit auslegen. Insbesondere ergibt sich keine einheitliche Auslegung. Damit wird das BMF seiner zentralen Verantwortung für das Haushaltsaufstellungsverfahren nicht gerecht. Aufgrund der Dynamik der Cybersicherheit und ihres technischen Charakters sollte das BMF auf die Expertise des BMDS zurückgreifen.

Auch der Bundesrechnungshof sieht das Spannungsverhältnis zwischen der zu stärkenden Cybersicherheit und der dringenden signifikanten Rückführung der Neuverschuldung des Bundes. Abgestimmte Kriterien für Ausgaben zum Schutz informationstechnischer Systeme sind deshalb unerlässlich, um

- → zum einen transparent zu machen, welche Ausgaben von der Bundesregierung für den Schutz als vordringlich anzusehen sind und
- → zum anderen den durch die Bereichsausnahme ermöglichten Verschuldungsspielraum verfassungskonform festzustellen.

Es liegt dann in der Verantwortung der Bundesregierung und des Haushaltsgesetzgebers für die langfristige Tragfähigkeit der Bundesfinanzen, in welchem Ausmaß von höheren Verschuldungsmöglichkeiten tatsächlich Gebrauch gemacht wird.[29]

Das BMDS greift die Empfehlungen des Bundesrechnungshofes nicht auf. Der Bundesrechnungshof hält diese daher aufrecht.

[29] Vgl. hierzu Tz. 6 der Stellungnahme des Bundesbeauftragten für Wirtschaftlichkeit in der Verwaltung, Eckwerte für den Bundeshaushalt 2027 und die Finanzplanung 2028 bis 2030, Verschuldungsdynamik eindämmen und Bundeshaushalt endlich strukturell konsolidieren, Gz. I 2 - 0003749 vom 20. April 2026.

3 IS-Controlling

Die Innovationszyklen in der IT haben sich drastisch verkürzt und betragen inzwischen nicht mehr Jahre, sondern oft nur noch wenige Monate. Im Zuge dieser Entwicklungen verändert sich fortlaufend, welche IT die Bundesverwaltung einsetzt und wie intensiv sie diese nutzt. Dies wirkt sich unmittelbar auf die Cybersicherheit der Bundesverwaltung aus, denn die Bundesverwaltung muss diese gegen die dynamische Entwicklung absichern und resilient aufstellen.

Ein IS-Controlling schafft die notwendige Grundlage, um die Cybersicherheit systematisch planen, steuern, überwachen und bewerten zu können. Hierbei gilt es, folgende im IT-Grundschutz festlegten Schutzziele zu erreichen:

→ Vertraulichkeit stellt sicher, dass nur befugte Personen auf Daten oder Kommunikationsinhalte zugreifen können,
→ Integrität stellt sicher, dass Unbefugte Daten in IT-Systemen nicht verändern oder manipulieren können, und
→ Verfügbarkeit stellt sicher, dass Nutzende auf die benötigten IT-Systeme unterbrechungsfrei zugreifen und mit diesen arbeiten können.

Zu diesem Zweck bedarf es Kennzahlen, an denen sich die Sicherheitsmaßnahmen von Einrichtungen messen lassen. Das IS-Controlling erhebt die dafür erforderlichen Daten, bereitet diese auf und ermittelt daraus die aktuellen Werte der Kennzahlen. Auf Basis der ermittelten Kennzahlen können Entscheidungsträger geeignete Maßnahmen ergreifen, um die Schutzziele wirtschaftlich, risikoorientiert und wirksam sicherzustellen.

Mit Beschluss vom November 2022 forderte der Haushaltsausschuss die Bundesregierung auf,

→ ein übergreifendes IT-Sicherheitscontrolling als Teil eines IT-Controlling Bund zu etablieren, um einen belastbaren und fortlaufend aktuellen Überblick über den Stand der IT-Sicherheit in der gesamten Bundesverwaltung zu erhalten, und
→ dafür Sorge zu tragen, dass das BSI seine bestehenden Prüfinstrumente/-schemata und seine neuen Kontrollbefugnisse aus dem IT-Sicherheitsgesetz 2.0 zeitnah in einem neuen umfassenden Revisionsansatz für die Bundesverwaltung zusammenführt.

Der Rechnungsprüfungsausschuss forderte in seiner Sitzung im Juni 2023 das Bundesministerium des Innern (BMI) auf, ein IS-Controlling für die Bundesverwaltung „bis zum Jahr 2025 aufzubauen“. Er gab vor, das IS-Controlling solle auch auf den Erkenntnissen des BSI aus

→ seinen Prüfungen nach § 7 BSI-Gesetz[30] sowie
→ entsprechenden Nachweispflichten[31] der Einrichtungen der Bundesverwaltung gemäß § 43 Absatz 1 BSI-Gesetz

beruhen.

In seiner Sitzung im Oktober 2025 forderte der Rechnungsprüfungsausschuss das BMI und das BMDS ergänzend auf, dafür Sorge zu tragen, dass das BSI sein Personal verstärkt in den Kontroll- und Beratungseinheiten einsetzt. Dieses soll die Angaben der Behörden zum Zustand ihrer Cybersicherheit im Wesentlichen aus Erkenntnissen seiner unabhängigen Prüfungen vor Ort und nicht aus ungeprüften Selbstauskünften beziehen. Darüber hinaus soll das BMDS die Planungen für das IS-Controlling des Bundes mit Nachdruck vorantreiben und frühzeitig mit dem zentralen IT-Controlling Bund verzahnen. Dies soll verhindern, dass es zu abweichenden Entwicklungen kommt.

Ergänzend hatte der Haushaltsausschuss die Bundesregierung im November 2025 aufgefordert, Haushaltsmittel für Maßnahmen der Cybersicherheit in der Bundesverwaltung auf Grundlage eines zentralen IS-Controllings unter der Federführung des BMDS effektiv zu planen, zu steuern und fortlaufend zu überwachen. Außerdem solle das BSI seine gesetzliche Kontrollbefugnis nutzen, um vollständige und valide Informationen für das IS-Controlling bereitzustellen.

3.1 Kontrollen nach § 7 BSI-Gesetz

Sachverhalt

Das BSI als nationale Cybersicherheitsbehörde konzipierte im September 2021, wie es seine ab Dezember 2021 geltenden neuen Befugnisse zur Kontrolle der Sicherheit der Kommunikationstechnik des Bundes umsetzt. Es sah vor,

→ mit einer **Standardrevision** vor Ort bei allen Einrichtungen im Drei-Jahres-Rhythmus allgemeine Sicherheitsaspekte zu erheben und diese Informationen durch
→ tiefergehende **Spezialprüfungen** zu einzelnen Themen sowie
→ speziell auf die Bedürfnisse von IT-Dienstleistern abgestimmte **Dienstleisterprüfungen** zu ergänzen.

[30] Der Gesetzgeber befugte mit § 4a BSI-Gesetz das BSI in Absatz 1 zur Kontrolle der Sicherheit der Kommunikationstechnik des Bundes. Der § 4a BSI-Gesetz trat zum 1. Dezember 2021 in Kraft. Mit dem reformierten BSI-Gesetz ersetzt seit dem 6. Dezember 2025 der § 7 den § 4a im BSI-Gesetz.

[31] Gemäß § 43 Absatz 1 BSI-Gesetz sind die Leitungen der Einrichtungen der Bundesverwaltung dafür verantwortlich, die Voraussetzungen zur Gewährleistung der Informationssicherheit zu schaffen. Die Einrichtungen müssen diese dem BSI spätestens zum 6. Dezember 2030 und anschließend regelmäßig nach dessen Vorgaben nachweisen.

Ab Januar 2024 pilotierte das BSI sein Vorgehen zur Standardrevision und passte es daraufhin noch zweimal erheblich an. Derzeit sieht es für die Standardrevision eine Interviewphase, eine Dokumentenprüfung und Vor-Ort-Begehungen vor.

Die Standardrevision will das BSI durch eine sich jährlich wiederholende Basisdatenerhebung „flankieren“. Diese soll ihm trotz begrenzt einsetzbarer Personalressourcen für Kontrollen vor Ort ermöglichen, einen vollständigen Überblick über den Stand der Cybersicherheit bei den Einrichtungen des Bundes zu erhalten. Stellt das BSI bei der Basisdatenerhebung Unstimmigkeiten fest, so könne es Basisdaten unterstützend erheben. Hierbei füllen BSI und die betroffene Einrichtung den Fragebogen der jährlichen Datenerhebung gemeinsam aus.

Im Jahr 2023 ging das BSI nach einer plausibilisierten Schätzung von 400 bis 500 zu kontrollierenden Einrichtungen aus. Im März 2025 senkte es die Anzahl auf etwa 200 Einrichtungen ab. Im Dezember 2025 erweiterte das reformierte BSI-Gesetz den Adressatenkreis der Kontrollen von Bundesbehörden auf alle Einrichtungen der Bundesverwaltung[32].

Das BSI kontrollierte mit der Standardrevision[33] die Sicherheit der Kommunikationstechnik in den Jahren 2024 bis 2025 bei insgesamt 15 Einrichtungen des Bundes vor Ort. Zehn weitere Kontrollen vor Ort plante es für das Jahr 2026 ein. Zudem beabsichtigte es, ab Mai 2026 die Basisdatenerhebung bei zwei Einrichtungen zu pilotieren.

Bis zum Jahr 2026 hatte das BSI nur für den „Mindeststandard des BSI zur Nutzung der ressortübergreifenden Kommunikationsnetze des Bundes („Nutzerpflichten NdB“)“ eine Spezialprüfung konzipiert und bei Einrichtungen durchgeführt. Zudem hatte es ausgewählte Themen bei einem Infrastrukturbetreiber geprüft. Sonstige, auf die Standardrevision abgestimmte Spezial- oder Dienstleisterprüfungen hat es bisher nicht erarbeitet. Dezentrale IT-Betriebe der Bundesverwaltung hat es auch nicht berücksichtigt.

Würdigung

Der Haushaltsausschuss und der Rechnungsprüfungsausschuss haben BMI und BMDS bei einer fortlaufend angespannten Bedrohungslage frühzeitig darauf hingewiesen, die

[32] Nicht vom BSI zu kontrollieren sind gemäß § 2 Nummer 21 und 37 Kommunikationstechnik des Bundesverfassungsgerichts, der Bundesgerichte, soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes, soweit sie ausschließlich in deren eigener Zuständigkeit betrieben wird. Zudem gilt gemäß § 29 Absatz 3 BSI-Gesetz, dass die Geschäftsbereiche des Auswärtigen Amts und des Bundesministeriums der Verteidigung sowie der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz von den Regelungen des § 7 Absatz 5 Satz 4, der §§ 10, 13 Absatz 1 Satz 1 Nummer 1 Buchstabe e sowie der §§ 30, 33 und 35 ausgenommen sind. Das Auswärtige Amt erlässt im Einvernehmen mit dem BMDS eine allgemeine Verwaltungsvorschrift, um die Ziele der NIS-2-Richtlinie im Geschäftsbereich des Auswärtigen Amts durch ergebnisäquivalente Maßnahmen umzusetzen.

[33] Die Kontrollen führte das BSI mittels der Standardrevision als freiwillige Pilotprüfungen sowie gemäß § 4a BSI-Gesetz in der Fassung vom Dezember 2021 bzw. § 7 BSI-Gesetz in der Fassung vom Dezember 2025 durch.

Cybersicherheit umfassend zu kontrollieren und zu steuern. Die Anforderung, auch Erkenntnisse des BSI aus den Kontrollen gemäß § 7 BSI-Gesetz und den Nachweispflichten gemäß § 43 Absatz 1 BSI-Gesetz in das IS-Controlling einfließen zu lassen, unterstützt zudem ein wirtschaftliches Vorgehen. Die Forderung, das BSI solle verstärkt vor Ort prüfen, sollte den – auch nach den Prüfungserkenntnissen des Bundesrechnungshofes – oft wenig kritischen Selbsteinschätzungen der Einrichtungen entgegenwirken. Dementsprechend sollten Experten des BSI den Stand der Cybersicherheit als neutrale Dritte bewerten.

Das BSI hat mehr als vier Jahre nach Inkrafttreten seiner Kontrollbefugnis die Sicherheit der Kommunikationstechnik des Bundes unzureichend geprüft. In zwei Jahren hat es lediglich 15 Kontrollen auf Basis der Standardrevision vor Ort durchgeführt. Geht man von der Mindestzahl von 200 zu prüfenden Einrichtungen aus, so wird das BSI bei unverändertem Vorgehen rund 20 Jahre benötigen, um die allgemeinen Sicherheitsaspekte bei allen Einrichtungen einmal zu kontrollieren. Zudem ist mit dem reformierten BSI-Gesetz die Anzahl der zu kontrollierenden Einrichtungen deutlich angestiegen.

Die jährliche flächendeckende Basisdatenerhebung soll aus Sicht des BSI die Standardrevision nur „flankieren“. Diese kann aber das Ergebnis weniger Kontrollen vor Ort verfälschen. Denn zehn Kontrollen stehen nun weit über 200 Selbstauskünften gegenüber. Deren Validität könnte das BSI nur dann beurteilen, wenn es sowohl die Methoden, Werkzeuge als auch die Prozesse zur Erhebung der Daten genau definiert und vorschreibt. Die Einrichtungen des Bundes müssten sodann auch genau diese Vorgaben einhalten, um vergleich- und belastbare Ergebnisse zu erzielen. Zudem müsste das BSI die Ergebnisse mittels ausreichender repräsentativer Kontrollen vor Ort validieren. Insgesamt erfüllt die derzeit geplante Praxis nicht die Anforderungen des Rechnungsprüfungsausschusses. Dieser erwartete ausdrücklich vom BSI, den Stand der Cybersicherheit im Wesentlichen auf Basis von Erkenntnissen aus unabhängigen Prüfungen vor Ort und gerade nicht aus ungeprüften Selbstauskünften zu ermitteln. Das BSI hätte demnach eine deutlich höhere Zahl von Kontrollen vorsehen müssen.

Auch hätte es fehlende Spezial- und Dienstleisterprüfungen konzipieren und auf die Standardrevision abstimmen müssen. Derzeit ist offen, wie das BSI durch Kontrollen die Umsetzung seiner Mindeststandards befördern und die besonderen Herausforderungen der IT-Dienstleister des Bundes in der Cybersicherheit dabei berücksichtigen will. Darüber hinaus muss es auch die dezentralen IT-Betriebe in der Bundesverwaltung betrachten und in seine Kontrollen integrieren.

Empfehlung

Der Bundesrechnungshof hat das BSI aufgefordert, seine Kontrollbefugnis im gebotenen Umfang und in erforderlicher Qualität auszuüben. Die Sicherheit muss es

flächendeckend vor Ort kontrollieren. Die Kontrollfolge hat es dabei risikoorientiert zu gestalten.

Es muss anstreben, jede Einrichtung alle drei Jahre und darüber hinaus auch anlassbezogen zu kontrollieren. Ein Anlass könnte z. B. sein, dass die Basisdatenerhebung eine ungünstige Entwicklung der Cybersicherheit aufzeigt. Um eine flächendeckende Kontrolle zu erreichen, muss es die Anzahl der Kontrollen deutlich erhöhen. Dafür sollte es u. a. Personal entsprechend der Forderung des Rechnungsprüfungsausschusses verstärkt in den Kontroll- und Beratungseinheiten einsetzen.

Die jährliche Basisdatenerhebung sollte es lediglich ergänzend zu seinen Kontrollen vor Ort heranziehen. Das BSI muss sicherstellen, dass es selbst einen unabhängigen repräsentativen Stand der Cybersicherheit in der Bundesverwaltung erhebt. Es muss so zu vermeiden, dass ungeprüfte Eigenauskünfte der Ressorts seine eigenen Erkenntnisse verfälschen.

Darüber hinaus muss es Spezialprüfungen für die Mindeststandards und Dienstleisterprüfungen konzipieren und mit der Standardrevision abstimmen. Die dezentralen IT-Betriebe der Bundesverwaltung hat es hierbei ebenfalls zu berücksichtigen.

Stellungnahme

Das BMDS hat angegeben, es werde vorhandene Erkenntnisse aus Kontrollen und Nachweispflichten in das IS-Controlling einfließen lassen. Datengrundlage und -lieferant sei primär die Basisdatenerhebung, die es als formular- und toolbasierte Selbstauskunft umsetze. Diese liefere den Ist-Zustand der Informationssicherheit für das IS-Controlling. Die Ergebnisse der Basisdatenerhebung werde das BSI heranziehen, um die Einrichtungen zu ermitteln, die es mittels Standardrevision zu prüfen plane.

Die fehlenden personellen Ressourcen limitierten weiterhin das Prüfwesen. Dies verhindere, die Standardrevision als ausschließliche Prüfung vor Ort quantitativ auszuweiten. Daher könne eine belastbare Übersicht, inwieweit die Bundesverwaltung das Informationssicherheitsmanagement umgesetzt habe, nicht allein auf Erkenntnissen von Kontrollen vor Ort basieren.

Die angepasste dreistufige Prüfmethodik[34] des BSI erlaube eine optimale Balance von Datenqualität und Aufwand. Mit ihr könne das BSI den Ist-Zustand der Cybersicherheit der Bundesverwaltung mit seinen vorhandenen Ressourcen ermitteln. Zudem werde das BSI die Angaben der Einrichtungen des Bundes bei der Basisdatenerhebung mit einer Standardrevision prüfen. Dies erhöhe den Druck auf die Einrichtungen, wahrheitsgemäß zu antworten. Darüber hinaus hat das BMDS mitgeteilt, es werde beim

[34] Diese bestehe aus der formular- und toolbasierten Basisdatenerhebung, der BSI unterstützte Selbstauskunft und den plausibilisierten Eingaben sowie der Kontrollen vor Ort.

übergreifenden Berichtswesen berücksichtigen, ob die Informationen aus der Basisdatenerhebung oder Standardrevision stammen. Ob das BSI die Kontrollen vor Ort deutlich ausweiten werde, hat es offengelassen.

Das BSI plane mittlerweile für das Jahr 2026, bei einem IT-Dienstleister der Bundesverwaltung auf der Standardrevision aufbauende Spezialprüfungen von IT-Diensten durchzuführen. Diese Planung stehe unter dem Vorbehalt ausreichender Prüfkapazitäten.

Abschließende Würdigung

Der Bundesrechnungshof hält es weiterhin nicht für sachgerecht, dass primär die Basisdatenerhebung als Selbstauskunft die Datengrundlage für das IS-Controlling bilden soll. Die dreistufige Prüfungsmethodik erfüllt nicht die Forderung des Rechnungsprüfungsausschusses, im Wesentlichen Erkenntnisse zur Cybersicherheit aus unabhängigen Prüfungen vor Ort zu erhalten. Selbstauskünfte liefern keine nach einheitlichen Maßstäben ermittelten objektiven Ergebnisse. Das BMDS und das BSI nehmen somit in Kauf, dass nicht vor Ort überprüfte Selbstauskünfte den Bericht zum Stand der Cybersicherheit verfälschen und dieser ein verzerrtes Bild zeichnet. Dagegen können Kontrollen von Experten des BSI vor Ort dazu beitragen, dass sich die Selbstauskünfte sukzessive verbessern. Durch sie wird für die Einrichtungen offenkundig, welche Schwachstellen sie im Detail besitzen. Dieser Lerneffekt wird sich aber nur dann einstellen, wenn das BSI die Anzahl der Prüfungen vor Ort signifikant erhöht.

Der allgemein und wiederholt vorgebrachte Verweis auf fehlende Ressourcen ist weder zielführend noch sachgerecht. Denn es obliegt dem BSI, seine über 1 700 Stellen so einzusetzen, dass es den größtmöglichen Sicherheitsgewinn erzielt. Einen Nachweis, dass seine dreistufige Prüfungsmethodik Aufwand und Sicherheitsgewinn im angemessenen Verhältnis setzt, hat es bisher nicht erbracht. Die bisherigen Erfahrungen mit Selbstauskünften lassen bezweifeln, dass es für diese Aufgabe sein Personal effektiv und effizient disponiert hat.

Der Bundesrechnungshof bekräftigt daher seine Empfehlungen.

3.2 Nachweise nach § 43 Absatz 1 BSI-Gesetz

Sachverhalt

Das reformierte BSI-Gesetz trat am 6. Dezember 2025 in Kraft und sieht in § 43 Absatz 1 vor:

„Die Leitung der Einrichtung der Bundesverwaltung ist dafür verantwortlich, unter Berücksichtigung der Belange des IT-Betriebs die Voraussetzungen zur Gewährleistung der Informationssicherheit zu schaffen. Die Einrichtungen der Bundesverwaltung weisen dem Bundesamt die Erfüllung der Anforderungen nach Satz 1 spätestens fünf Jahre nach Inkrafttreten dieses Gesetzes und anschließend regelmäßig nach seinen Vorgaben nach."

Das BSI beabsichtigt derzeit, die Nachweispflicht über die für die Kontrolle nach § 7 BSI-Gesetz vorgesehene Basisdatenerhebung als Selbstauskunft umzusetzen. Es legte hierzu nicht dar,

→ wie es die Nachweiserbringung in die Basisdatenerhebung integrieren und
→ wann es die Nachweisanforderung erstmals und in welchem Abstanden anschließend durchführen will.

Nach Abschluss der Pilotierung wollte es ab Juni 2026 die Basisdatenerhebung phasenweise in der restlichen Bundesverwaltung ausrollen. Abhängig von diesem Rollout will es nicht vor Herbst 2026 offizielle Informationen zur Nachweispflicht nach § 43 Absatz 1 Satz 2 BSI-Gesetz an die Einrichtungen der Bundesverwaltung herausgeben. Bei Bedarf werde es über die elektronischen Fragebögen hinaus weitere Arbeitshilfen zur Verfügung stellen. Aufgrund der gesetzlich vorgesehenen Übergangsfrist müssen Einrichtungen Nachweise verpflichtend erst zum 6. Dezember 2030 erbringen.

Würdigung

Entgegen den Erwartungen des Rechnungsprüfungsausschusses ist nicht davon auszugehen, dass dem BSI vor Ende der gesetzlichen Übergangsfrist im Dezember 2030 hinreichende und vergleichbare Nachweise vorliegen, die verlässliche Informationen für das IS-Controlling bieten werden. Das BSI sieht nämlich nach heutigem Stand vor, die Daten für die Nachweise ebenfalls mit der Basisdatenerhebung – also einer Selbstauskunft – zu ermitteln. Auch für die Nachweise kann eine jährliche Selbstauskunft nur belastbare und vergleichbare Daten liefern, wenn sie auf standardisierten, automatisiert erhobenen und rein objektiv messbaren Eingaben beruht. Derzeit ist nicht erkennbar, wie das BSI dies mit dem geplanten Vorgehen sicherstellen will. Es ist zu befürchten, dass es mit viel Aufwand von den Einrichtungen des Bundes Daten zusammentragen lässt, die aufgrund der Art der Erhebung keine hinreichend verlässliche Grundlage für notwendige Entscheidungen zur Cybersicherheit der Bundesverwaltung bieten.

Empfehlung

Der Bundesrechnungshof hat empfohlen, dass das BSI umgehend ein Verfahren für die nach § 43 Absatz 1 BSI-Gesetz vorgesehenen Nachweise etablieren sollte. Hierzu sollte

es Nachweisformulare und Handreichungen mit Vorgaben zu Erhebungswerkzeugen, -prozessen und -methoden entwerfen, testen und veröffentlichen. Es kann so

→ den Einrichtungen des Bundes eine klare Struktur für die Nachweise vorgeben und
→ die Datenerhebung standardisieren, damit diese ihre Nachweise zielgerichtet und wirtschaftlich erbringen können.

Zur Basisdatenerhebung sollte das BSI daher untersuchen,

→ welche Werkzeuge, Prozesse und Methoden dafür erforderlich sind und
→ welche Ausgaben und welcher Aufwand dadurch entstehen.

Stellungnahme

Das BMDS beabsichtige, zu prüfen, inwieweit die bestehenden Abfragen die vorgesehenen Kennzahlen für das IS-Controlling liefern. Die Ergebnisse dieser Prüfung werden die Grundlage bilden, das Kennzahlsystem weiter auszugestalten. Das BSI halte daran fest, dass eine Nachweiserbringung über einen Fragenkatalog bei seinen unzureichenden Personalkapazitäten sinnvoll und ressourcenoptimiert sei. „Voraussetzungen zur Gewährleistung der Informationssicherheit“ seien maßgeblich organisatorischer Art. Deren Abweichungen werde das BSI mit der Standardrevision ermitteln.

Das BSI plane zudem, die Nachweise nach § 43 Absatz 1 BSI-Gesetz in die toolbasierte Basisdatenerhebung zu integrieren. Im Kern handele es sich bei einem solchen Nachweis immer nur um eine Selbstauskunft.

Abschließende Würdigung

Statt eines neutral gehaltenen Nachweisverfahrens – das auch auf den Ergebnissen unabhängiger Auditorinnen und Auditoren beruhen könnte – hält das BSI an Selbstauskünften als Datenbasis für das IS-Controlling fest. Das BSI plant, diese Selbstauskünfte in die Basisdatenerhebung zu integrieren. Diese hat es jedoch bislang weder konzipiert noch erprobt, und dazu auch keinen konkreten Zeitplan angeführt. Zu den unterstützenden Werkzeugen, Prozessen, Methoden, Aufwänden und Methoden hat das BMDS nicht Stellung genommen.

Der Bundesrechnungshof hält an seinen Empfehlungen fest.

3.3 Aufbau des IS-Controllings

Sachverhalt

Im Juli 2023 teilte das BMI dem Haushaltsausschuss mit, es plane, das geforderte übergreifende IS-Controlling aufzubauen. Dieses werde das Zusammenspiel aus Kontrollen des BSI und Selbsterklärungen/Nachweisen neu definieren. Ziel sei, einen belastbaren, fortlaufend aktuellen Überblick über die Cybersicherheit zu gewinnen und diese zielgerichtet zu steuern. Der Aufbau des IS-Controllings müsse u. a. die Umsetzung der Kontrollen des BSI gemäß BSI-Gesetz und das NIS-2-Umsetzungsgesetz[35] berücksichtigen.

Im Dezember 2024 hatte das BMI dem Rechnungsprüfungsausschuss zugesichert, bis Ende des Jahres 2025 ein IS-Controlling aufzubauen. Das nunmehr zuständige BMDS hat in einem Bericht an die Berichterstatter für den Einzelplan 24 erklärt, dass sich das IS-Controlling derzeit im Aufbau befinde. Es plane,

1. bis Ende des 2. Quartals 2026 die Rahmenbedingungen für das IS-Controlling zu schaffen. Hierzu will es Kennzahlen mit den Basisdatenerhebungen des BSI abgleichen und steuerungsrelevante Kennzahlen (KPI) entwickeln.
2. bis Ende des 4. Quartals 2026 die Definition der Key Performance Indicators (KPI) abzuschließen, standardisierte Prozesse zu entwickeln und zudem die Datenerhebung zu pilotieren.
3. im Jahr 2027 die Datenlage des IS-Controllings auszubauen und einen ersten Bericht mit fundierten und konsolidierten Daten zu erstellen.
4. für den Zeitraum über das Jahr 2027 hinaus das IS-Controlling unter Berücksichtigung der Steuerungsbedarfe kontinuierlich weiterzuentwickeln.

Vorbereitend hat das BSI bisher 18 KPI definiert. Die erforderlichen Daten dafür sollen die Einrichtungen des Bundes einmal jährlich liefern. Das BSI hat hierzu nicht ermittelt, inwieweit diese bereits mittels geeigneter Prozesse, Werkzeuge und Ressourcen in der Lage sind, die Daten mit angemessenem Aufwand zu erheben.

Würdigung

Entgegen der Aufforderung des Haushaltsausschusses und des Rechnungsprüfungsausschusses haben das BMI und später das BMDS noch kein IS-Controlling aufgesetzt. Erst mehr als dreieinhalb Jahre nach dem Beschluss des Haushaltsausschusses hat das BMDS nun begonnen, steuerungsrelevante Kennzahlen zu definieren, standardisierte Prozesse zu entwickeln und die Datenerhebung zu pilotieren. Dies sind allesamt wichtige vorbereitende Schritte für ein IS-Controlling. Trotz der zweijährigen Vorbereitung

[35] Novellierung des BSI-Gesetzes vom 2. Dezember 2025, um die NIS-2-Richtlinie (Sicherung von Netz- und Informationssystem) der Europäischen Union in nationales Recht zu überführen.

des BMI und der Übernahme der Aufgaben und des Personals, hat das BMDS diese erst im Jahr 2026 eingeleitet. Die jetzt begonnenen konzeptionellen Arbeiten hätten bereits abgeschlossen sein können.

Auch kann das BSI aufgrund

→ einer fehlenden vollständigen Konzeption,
→ der unzureichenden Kontrollen nach § 7 BSI-Gesetz und
→ fehlender verlässlicher Nachweise nach § 43 Absatz 1 BSI-Gesetz

in absehbarer Zeit – also auch nach dem Jahr 2027 – nur unzureichend repräsentative Erkenntnisse aus der Bundesverwaltung zum IS-Controlling beisteuern. Dies erschwert die verfügbare Datenlage für das IS-Controlling, das zwingend vollständige und belastbare KPI-Daten benötigt, noch mehr.

Entsprechend seiner Planung will das BMDS das IS-Controlling erst im Jahr 2027 und somit rund vier Jahre nach der ersten Aufforderung des Haushaltsausschusses in Grundzügen produktiv nutzen. Da es zu diesem Zeitpunkt über keine geeignete, repräsentative Datenlage verfügt, kann es die Cybersicherheit in der Bundesverwaltung nicht effektiv planen, steuern und fortlaufend überwachen.

Diese deutliche zeitliche Verzögerung wird der Bedrohungslage für die Cybersicherheit der Bundesverwaltung nicht gerecht.

Empfehlung

Der Bundesrechnungshof hat dem BMDS empfohlen, das IS-Controlling als Teil seiner künftigen Steuerungsinstrumente aufzubauen und in Betrieb zu nehmen. Hierfür muss es ermitteln,

→ welche KPI für eine effektive und effiziente Steuerung der Cybersicherheit notwendig sind und
→ welche Daten es dafür mit welchen Methoden und Mitteln erheben muss.

Für die KPI muss es anschließend die Ist-Werte ermitteln und mit den übrigen Ressorts Soll-Werte verbindlich festlegen.

Darüber hinaus muss es konzipieren, wie es die Erkenntnisse aus den Kontrollen des BSI gemäß § 7 BSI-Gesetz und aus den Nachweisen nach § 43 Absatz 1 BSI-Gesetz als Datenquellen für das IS-Controlling nutzt.

Das BMDS muss anstreben, bereits bis Ende des Jahres 2026 das IS-Controlling in der gesamten Bundesverwaltung zu etablieren, damit es bereits ab dem Jahr 2027 den

Einsatz von Haushaltsmitteln für Cybersicherheit ressortübergreifend planen, steuern und überwachen kann. Dafür muss es ein Vorgehen entwickeln.

Stellungnahme

Das BMDS hat auf den bisherigen an den Haushaltsausschuss berichteten Zeitplan verwiesen und diesen bestätigt. Demnach werde es eine erste Grundversion des IS-Controllings bis Ende des Jahres 2026 erstellen und anschließend iterativ erweitern.

Abschließende Würdigung

Das BMDS will unsere Empfehlungen grundsätzlich umsetzen, jedoch an seinem Zeitplan festhalten. Dies birgt das Risiko, dass notwendige Informationen für das Haushaltsaufstellungsverfahren und -gesetzgebung fehlen.

Das BMDS lässt offen, ob es verbindliche Soll-Werte für die KPI festlegt oder mit den Ressorts vereinbaren wird.

Essers Scherwa

Beglaubigt: Puzius, Tarifbeschäftigte
Wegen elektronischer Bearbeitung ohne Unterschrift und Dienstsiegelabdruck.