Bundesrechnungshof

Bericht nach § 88 Absatz 2 BHO

an den Haushaltsausschuss des Deutschen Bundestages

Vorhaben der Cybersicherheit

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

Gz.: VII 4 - 0000583/III

16. Oktober 2024

Die Prüfungsergebnisse auf einen Blick

Cybersicherheit unkoordiniert und nicht bedarfsgerecht finanziert

Trotz der erheblichen Bedrohungen im Cyberraum koordiniert die Bundesregierung ihre Cybersicherheitsmaßnahmen ressortübergreifend unzureichend. Bislang ist weder für das Jahr 2025 noch in der mittelfristigen Finanzplanung die vom Haushaltsausschuss des Deutschen Bundestages (Haushaltsausschuss) geforderte auskömmliche Finanzierung im Bundeshaushalt sichergestellt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentrale Cybersicherheitsbehörde Deutschlands ist nicht bedarfsgerecht aufgestellt.

Worum geht es?

Cybersicherheit ist eine ressortübergreifende Aufgabe. Die Bundesregierung hat sich deshalb u. a. in der Nationalen Sicherheits- und der Cybersicherheitsstrategie zum Ziel gesetzt, diese zu stärken. Der Haushaltsentwurf für das Jahr 2025 und die mittelfristige Finanzplanung berücksichtigen hoch priorisierte Maßnahmen der Cybersicherheit nicht. Das Bundesministerium des Innern und für Heimat (BMI) hat zudem die Cybersicherheitsmaßnahmen nicht ressortübergreifend koordiniert. Die Ressorts agieren weiterhin isoliert, anstatt ihre Aktivitäten zu bündeln.

Was ist zu tun?

Die Bundesregierung muss die aus ihren strategischen Zielen resultierenden Cybersicherheitsmaßnahmen bewerten und priorisieren. Sie muss klar zwischen den Maßnahmen unterscheiden, die einzelne Ressorts alleine verantworten und solchen, die die Cybersicherheit aller Ressorts betreffen. Alle für die Cybersicherheit hoch priorisierten Maßnahmen sollten wie vom Haushaltsausschuss gefordert auskömmlich finanziert sein. Für übergreifende Maßnahmen sollte sie ein zentrales von allen Ressorts anteilig bereitgestelltes Budget einrichten. Zudem sollte sie alle Maßnahmen stringent koordinieren und stetig kontrollieren. Weicht eine ressortspezifische oder ressortübergreifende Maßnahme von den Zielen ab, muss die Bundesregierung gegensteuern. Nur so kann sie das Verbundrisiko minimieren. Das BSI muss begonnene Aktivitäten vorantreiben, um die Bundesverwaltung stärker bei ihrer Eigensicherung zu unterstützen und zu kontrollieren.

Was ist das Ziel?

Die Cybersicherheit wird sowohl zentral als auch dezentral gewährleistet. Die dafür erforderlichen Maßnahmen sind auskömmlich finanziert und es findet eine übergreifende Planung, Steuerung und Kontrolle statt. Das BSI ist bedarfsgerecht aufgestellt.

Inhaltsverzeichnis

Abkürzungsverzeichnis

B

BHO *Bundeshaushaltsordnung*
BMBF *Bundesministerium für Bildung und Forschung*
BMF *Bundesministerium der Finanzen*
BMI *Bundesministerium des Innern und für Heimat*
BOS *Behörden und Organisationen mit Sicherheitsaufgaben*
BSI *Bundesamt für Sicherheit in der Informationstechnik*
BSIG *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*
BSOC *Bundes Security Operation Center*

C

Cyber-AZ *Nationales Cyber-Abwehrzentrum*

H

Haushaltsausschuss *Haushaltsausschuss des Deutschen Bundestages*
HRB *Haushaltstechnische Richtlinien des Bundes*

I

IT-SiG 2.0 *Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT -Sicherheitsgesetz 2.0)*

K

KoSi *Kompetenzzentrum operative Sicherheitsberatung Bund*
KRITIS *Kritische Infrastrukturen*

M

MIRT *Mobile Incident Response Team*

N

NIS2UmsuCG *Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)*

R

Rechnungsprüfungsausschuss *Rechnungsprüfungsausschuss des Haushaltsausschusses des Deutschen Bundestages*
R-VSK *Ressortübergreifende Verschlusssachen-Kommunikation*

0 Zusammenfassung

In einer Zeit geopolitischer Spannungen mit Bedrohungen im Cyberraum ist die Informations- und Cybersicherheit von herausragender Bedeutung. Daher hat der Haushaltsausschuss das BMI am 16. November 2023 aufgefordert,

- mit den übrigen Ressorts spätestens für das Haushaltsjahr 2025 eine auskömmliche Finanzierung der prioritären Cybersicherheitsvorhaben der Nationalen Sicherheitsstrategie, der Cybersicherheitsstrategie und der Cybersicherheitsagenda zu konzipieren,
- gemeinsam mit den übrigen Ressorts ein zentrales Budget für Maßnahmen der Informations- und Cybersicherheit zu prüfen und
- das BSI organisatorisch, personell und finanziell so aufzustellen, dass es seine Unterstützungs- und Kontrollaufgaben gegenüber den Behörden und Rechenzentren der Bundesverwaltung vollumfänglich wahrnehmen kann.

Diese Maßgaben ergänzen den Beschluss des Haushaltsausschusses vom 10. November 2022, in dem er das BMI u. a. aufgefordert hatte,

- die Behördenleitungen durch das BSI über Mängel ihrer geprüften Rechenzentren zu informieren,
- der Bundesverwaltung Maßnahmen zur Informations- und Cybersicherheit zu empfehlen und
- ein übergreifendes IT-Sicherheitscontrolling in der Bundesverwaltung einzurichten.

Das BMI hat dem Haushaltsausschuss am 4. Juli 2024 einen Bericht vorgelegt. Der Bundesrechnungshof stellt hierzu im Wesentlichen fest:

0.1 Der Haushaltsentwurf für das Jahr 2025 und der Finanzplan bis zum Jahr 2028 berücksichtigen weder alle hoch priorisierten Cybersicherheitsvorhaben der Nationalen Sicherheitsstrategie noch der Cybersicherheitsstrategie. Das BMI hatte als das für die Informations- und Cybersicherheit federführende Ressort die Haushaltsanmeldungen der Bundesregierung für entsprechende Vorhaben nicht koordiniert. Ihm war nicht bekannt, welche Vorhaben die übrigen Ressorts eingebracht hatten oder welche davon die Bundesregierung im Haushaltsentwurf berücksichtigt hatte. Von 48 Maßnahmen seiner Cybersicherheitsagenda hat das BMI bislang weniger als 10 % abgeschlossen. 67 % befinden sich noch in Umsetzung. Das BMI gibt an, dass vor allem fehlende Haushaltsmittel dafür verantwortlich seien, dass es Maßnahmen zurückgestellt habe oder sie nur verzögert umsetze.

Ein ressortübergreifendes Controlling zu Maßnahmen der Informations- und Cybersicherheit gibt es weiterhin nicht.

Das BMI sollte gemeinsam mit den übrigen Ressorts den Finanzbedarf der hoch prioritären Maßnahmen zur Informations- und Cybersicherheit ermitteln. Hierfür sollten entsprechend der Maßgabe des Haushaltsausschusses auskömmliche Haushaltsmittel

bereitgestellt werden. Zudem sollte das BMI zügig ein Finanz- und Umsetzungscontrolling für die von der Bundesregierung initiierten Maßnahmen der Informations- und Cybersicherheit etablieren. (Tz. 2)

0.2 Das BMI und die übrigen Ressorts haben nicht mit dem gebotenen Nachdruck ein zentrales Budget für ressortübergreifende Vorhaben der Cybersicherheit geprüft. Auch die dafür erforderlichen Steuerungsstrukturen haben sie nicht erörtert.

Das BMI sollte spätestens bis zum Haushaltsaufstellungsverfahren für das Jahr 2026 sachgerechte Einsatzbereiche und Finanzierungsmodelle für ein solches zentrales Budget ausarbeiten und mit den Ressorts, insbesondere aber mit dem Bundesministerium der Finanzen (BMF), abstimmen. Die Bundesregierung sollte geeignete Steuerungsstrukturen schaffen, die es ihr ermöglichen, knappe Haushaltsmittel effektiv für die Informations- und Cybersicherheit einzusetzen. (Tz. 3)

0.3 Das BSI hat sich zum 1. Juli 2024 umorganisiert. Ziel ist es, die Bundesverwaltung stärker bei der Informations- und Cybersicherheit unterstützen und kontrollieren zu können. Das BMI erwartet dazu nach sechs Monaten eine Erfolgskontrolle. Vor der Umorganisation hatte das BSI weder den Ist- noch den Soll-Zustand seiner Aufgaben geeignet qualitativ und quantitativ definiert und keine Aufgabenkritik durchgeführt. Zudem hatte es die Wirtschaftlichkeit der Umorganisation nicht untersucht. Daher fehlen ihm derzeit die Voraussetzungen, um den Erfolg seiner neuen Organisation nachweisen zu können.

Das BSI muss zunächst die Voraussetzungen schaffen, um wie vom BMI erwartet eine Erfolgskontrolle durchführen zu können. Dabei muss es nachweisen, wie die neue Organisation die Informations- und Cybersicherheit der Bundesverwaltung stärken kann. (Tz. 4)

0.4 Das BSI nimmt seine Kontrollbefugnisse nach § 4a des Gesetzes über das BSI (BSIG) nicht in dem vorgesehenen und erforderlichen Umfang wahr. Die geplante flächendeckende Kontrolle der Bundesverwaltung bezeichnet das BMI daher als „nicht realistisch“. Damit ist auch das IT-Sicherheitscontrolling gefährdet, das der Haushaltsausschuss bereits im Jahr 2022 gefordert und das BMI dem Rechnungsprüfungsausschuss des Haushaltsausschusses (Rechnungsprüfungsausschuss) bis Ende des Jahres 2025 zugesagt hatte. Während weiterhin eine erhebliche Anzahl von Stellen beim BSI unbesetzt ist, führt es zur Begründung fehlendes Personal an. Des Weiteren hat das BSI die Bundesbehörden, deren Rechenzentren es schon vor geraumer Zeit geprüft hatte, noch nicht – wie vom Haushaltsausschuss gefordert – über die Mängel informiert und zur Informations- und Cybersicherheit beraten. Es plant, dies nachzuholen. Erst jetzt hat es begonnen, Mängel und deren Behebung systematisch nachzuhalten.

Das BSI muss seine freien Stellen zügig besetzen und darüber hinaus bestehenden Bedarf nachweisen. Dabei sollte es die für seine Kontrollbefugnisse nach § 4a BSIG benötigten Ressourcen höher priorisieren. (Tz. 5)

0.5 Das BSI hat bisher keinen Zeitplan vorgelegt, bis wann es den IT-Grundschutz reformieren wird. Seine Vorhaben zu dessen Maschinenverarbeitbarkeit sowie zur Definition von Messgrößen, Leistungszahlen und Zielgrößen für Informations- und Cybersicherheit befinden sich in einem frühen Stadium. Hierfür setzt es nur wenig Personal ein. Seine Handreichung für die Bundesverwaltung zur Personalbedarfsbemessung für den Bereich Informations- und Cybersicherheit sieht es für Ende 2024 vor.

Die Planungen des BSI zur Reform des IT-Grundschutzes sowie zu den Hilfsmitteln für die Bundesverwaltung sind unzureichend. Insbesondere fehlt ein verbindlicher Zeit- und Ressourcenplan. Auch ist nicht gewährleistet, dass das BSI tatsächlich eine mit den fachlichen Stellen abgestimmte und erprobte Handreichung zur Personalbedarfsbemessung für den Bereich Informations- und Cybersicherheit bis Ende 2024 vorlegen wird.

Das BSI sollte seine Reform des IT-Grundschutzes genau planen und terminieren. Maßnahmen zur Automatisierung der Informations- und Cybersicherheit wie etwa die Maschinenverarbeitbarkeit des IT-Grundschutzes oder die Definition von Messgrößen, Leistungszahlen und Zielgrößen sollte es höher priorisieren. Seine Handreichung zur Personalbedarfsbemessung kann eine wichtige Hilfe für die Ressorts darstellen und helfen, ihre Informations- und Cybersicherheit an ein für die Bundesverwaltung angemessenes Niveau anzugleichen. Das BSI sollte eine abgestimmte und erprobte Fassung Ende 2024 vorlegen. (Tz. 6)

0.6 Zusammenfassend ist festzustellen, dass Vorhaben der Cybersicherheit derzeit nicht bedarfsgerecht finanziert sind. Auch eine gemeinsame Finanzierung durch die Ressorts ist nicht sichergestellt. Das BMI hat diese nicht mit dem nötigen Nachdruck angestrebt. Die Transparenz über die Lastenverteilung innerhalb der Bundesregierung und über die Wirkung der Maßnahmen ist ungenügend. Es fehlt ein geeignetes Controlling.

Die vorhandenen Ressourcen des BSI reichen derzeit nicht aus, um die erforderlichen Unterstützungs- und Kontrollaufgaben wahrzunehmen. Inwieweit die Umorganisation des BSI die gesetzten Ziele erreicht, ist offen.

Der Bundesrechnungshof hat dem BMI die Gelegenheit gegeben, zu den Feststellungen, Würdigungen und Empfehlungen Stellung zu nehmen. Das BMI hat mitgeteilt, dass es von einer Stellungnahme absehe.

Der Bundesrechnungshof hält es für erforderlich, dass das BMI

- als federführendes Ressort die Maßnahmen zur Informations- und Cybersicherheit mit ressortübergreifender Relevanz hinreichend koordiniert,
- für diese ein geeignetes Finanzierungsmodell für ein auskömmliches zentrales Budget ausarbeitet,

- ein Finanz- und Umsetzungscontrolling für Maßnahmen der Informations- und Cybersicherheit als Teil des IT-Sicherheitscontrollings etabliert,
- das BSI anhält, seine offenen Stellen zeitnah zu besetzen,
- darüber hinaus bestehenden nachgewiesenen Bedarf des BSI durch Stellenzuweisungen deckt und
- für die erforderliche Transparenz, Steuerung und Kontrolle im Bereich der Informations- und Cybersicherheit sorgt. (Tzn. 7 und 8)

1 Einleitung

Krisenfeste resiliente IT-Systeme sind eine Grundvoraussetzung, um die Staats- und Regierungsfunktionen jederzeit aufrechterhalten zu können.

Angesichts zunehmender geopolitischer Spannungen und zuletzt sehr großer Bedrohungen im Cyberraum hat die Bundesregierung zur Informations- und Cybersicherheit weitgehende Ziele u. a. in der Nationalen Sicherheitsstrategie[1] und der Cybersicherheitsstrategie[2] definiert.

Die **Nationale Sicherheitsstrategie** als Dachstrategie aus dem Jahr 2023 sieht vor, die Fähigkeiten Deutschlands im Cyberraum auszubauen. Sie setzt u. a. die Ziele,

- die Cybersicherheitsstrategie weiterzuentwickeln,
- die Cybersicherheitsanforderungen an Kritische Infrastrukturen (KRITIS) anzupassen,
- gesetzliche Grundlagen für das Nationale Cyber-Abwehrzentrum (Cyber-AZ) zu schaffen,
- das BSI zur Zentralstelle im Bereich der IT-Sicherheit auszubauen und es unabhängiger aufzustellen sowie
- Handlungsempfehlungen für Unternehmen zu entwickeln.

Die **Cybersicherheitsstrategie** bildet den ressortübergreifenden strategischen Rahmen im Bereich Cybersicherheit bis zum Jahr 2026 und definiert die langfristige Ausrichtung der Cybersicherheitspolitik der Bundesregierung. Sie enthält insgesamt 44 Ziele, die die Bundesregierung in den Handlungsfeldern

- Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung,
- Gemeinsamer Auftrag von Staat und Wirtschaft,
- Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur und
- Aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik

erreichen will.

Neben diesen Strategien der Bundesregierung verfolgt das BMI als für die Informations- und Cybersicherheit federführendes Ressort seine **Cybersicherheitsagenda**[3]. Damit will es in seinem Zuständigkeitsbereich

- die Cybersicherheitsarchitektur modernisieren und harmonisieren,

---

1 Nationale Sicherheitsstrategie – Wehrhaft. Resilient. Nachhaltig. – Integrierte Sicherheit für Deutschland, Juni 2023.

2 Die Bundesregierung der 19. Wahlperiode hat am 8. September 2021 die Cybersicherheitsstrategie für Deutschland 2021 beschlossen.

3 Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat, Juni 2022.

- die Cyberfähigkeiten und digitale Souveränität der Sicherheitsbehörden stärken,
- Cybercrime und strafbare Inhalte im Internet bekämpfen,
- die Cybersicherheit der Behörden des Bundes stärken,
- die Cyber-Resilienz Kritischer Infrastrukturen stärken,
- zivile Infrastrukturen vor Cyberangriffen schützen,
- die digitale Souveränität in der Cybersicherheit stärken und
- krisenfeste Kommunikationsfähigkeit schaffen und Sicherheit der Netze ausbauen.

Die Bundesregierung hat nicht ermittelt, welcher Ausgaben- und Personalbedarf entsteht, um die Ziele der Strategien zu erreichen. Für die aus den Strategien resultierenden Maßnahmen sind keine zusätzlichen Haushaltsmittel vorgesehen; vielmehr müssen die Behörden diese aus dem laufenden Haushalt (zusätzlich) finanzieren.

Der Bundesrechnungshof hat in seinem Bericht[4] an den Haushaltsausschuss empfohlen, dass die Bundesregierung ihre Prioritäten und ihren Ressourceneinsatz zugunsten der Cybersicherheit neu ausrichten sollte. Gemeinsam mit den übrigen Ressorts sollte das BMI prüfen, ob ein zentrales Budget eine wirksame Handlungsoption darstellt, um Vorhaben der Cybersicherheit ressortübergreifend zu finanzieren. Denn diese kommen letztlich in einer stark vernetzten Bundesverwaltung allen Ressorts gemeinsam zu gute.

Der Haushaltsausschuss hat daraufhin das BMI mit Beschluss vom 16. November 2023[5] aufgefordert,

1. für die prioritären, insbesondere für die in der Nationalen Sicherheitsstrategie, der Cybersicherheitsstrategie und der Cybersicherheitsagenda genannten Vorhaben der Cybersicherheit eine auskömmliche Finanzierung gemeinsam mit den Ressorts zu konzipieren, damit hierfür spätestens im Haushaltsjahr 2025 ausreichend Haushaltsmittel zur Verfügung stehen,
2. in diesem Zusammenhang die Einrichtung eines zentralen Budgets im Einzelplan 60 zu prüfen, das sich aus anteiligen, beispielsweise prozentual an den jeweiligen IT-Ausgaben orientierten Beiträgen aller Ressorts zusammensetzt und
3. darauf hinzuwirken, dass das BSI organisatorisch, personell und finanziell so aufgestellt ist, dass es seine Unterstützungs- und Kontrollaufgaben gegenüber den Behörden und Rechenzentren der Bundesverwaltung vollumfänglich wahrnehmen kann.

Das BMI sollte hierzu bis spätestens 30. Juni 2024 berichten.

Dieser Maßgabebeschluss ergänzt einen früheren Maßgabebeschluss[6] vom 10. November 2022. Darin hatte der Haushaltsausschuss das BMI u. a. dazu aufgefordert,

---

[4] Bericht des Bundesrechnungshofes nach § 88 Absatz 2 BHO an den Haushaltsausschuss vom 26. Oktober 2023, Ausschuss-Drucksache 20(8)4853.

[5] Ausschuss-Drucksache 20(8)5419.

[6] Ausschuss-Drucksache 20(8)2851.

- die Behördenleitungen und die Ressort-Informationssicherheitsbeauftragten über die Ergebnisse zu den in ihrem Zuständigkeitsbereich geprüften Rechenzentren detailliert zu informieren,
- darauf hinzuwirken, dass die geprüften Bundesbehörden für die Beseitigung der festgestellten Mängel einen verbindlichen Umsetzungsplan erstellen und dem BSI mindestens jährlich Informationen zum Stand der Umsetzung übermitteln,
- auf Grundlage der Prüfungserkenntnisse diese und darauf basierende Handlungsempfehlungen in geeigneter Weise der Bundesverwaltung zur Verfügung zu stellen,
- ein übergreifendes IT-Sicherheitscontrolling als Teil eines IT-Controlling Bund zu etablieren, um einen belastbaren, 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 und -schemata und seine neuen Kontrollbefugnisse aus dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0) zeitnah in einem neuen umfassenden Revisionsansatz für die Bundesverwaltung zusammenführt.

Der Haushaltsausschuss bat den Bundesrechnungshof, die Umsetzung beider Beschlüsse zu begleiten.

Das BMI hat dem Haushaltsausschuss am 4. Juli 2024 zur Thematik berichtet.[7] Der Bundesrechnungshof stellt hierzu Nachfolgendes fest:

2 Vorhaben der Cybersicherheit im Haushaltsentwurf 2025 und im Finanzplan bis 2028

Sachverhalt

Das BMI hat in seinem Bericht betont, dass die in der Nationalen Sicherheitsstrategie, der Cybersicherheitsstrategie und seiner Cybersicherheitsagenda genannten Vorhaben der Cybersicherheit angesichts der sehr hohen Bedrohungen im Cyberraum weiterhin „höchste Priorität“ hätten. Für diese Vorhaben habe es die „aus seiner Sicht erforderlichen Mittel für den Haushalt 2025 angemeldet“. Auf Nachfrage des Bundesrechnungshofes machte das BMI zum Bedarf für „kostenintensive Maßnahmen im Bereich der IT- und Cybersicherheit“ bis zum Jahr 2028 zudem folgende Angaben:

[7] Ausschuss-Drucksache 20(8)6375.

Tabelle 1

Soll-Ansätze für kostenintensive Vorhaben der Cybersicherheit liegen unter den Bedarfsmeldungen

Für die vom BMI benannten kostenintensiven Maßnahmen im Bereich der Informations- und Cybersicherheit (ohne IT-SiG 2.0) beträgt die Differenz zwischen Bedarfsmeldung und Soll-Ansätzen für den Haushalt 2025 rund 50 Mio. Euro. Für die Jahre 2026 bis 2028 steigt diese Differenz auf über 350 Mio. Euro an.

Maßnahme[8]	**2025**			**2026 bis 2028**		
	Bedarfs-meldung[a]	Ansatz im Reg.-Entwurf[a]	Differenz	Bedarfs-meldung[a] (kumuliert)	Ansatz im Finanzplan[a] (kumuliert)	Differenz (kumuliert)
KoSi Bund[9]	21 000	-	21 000	91 200	-	91 200
Cyberagentur	50 000	19 000[10]	31 000	150 000	119 600	30 400
Neue Aufgaben aus dem NIS2UmsuCG[11]	-	-		237 134	-[12]	237 134
Neue Aufgaben aus dem IT-SiG 2.0	129 000	nicht exakt bezifferbar[13]		387 000	nicht exakt bezifferbar	
Summe			**52 000**			**358 734**

Erläuterung: [a] Alle Angaben in Tsd. Euro.

Quelle: Angaben des Haushaltsreferates BMI; Haushaltsentwurf 2025; Finanzplan 2024 bis 2028.

---

8 Zusätzlich benannte das BMI auch den Digitalfunk sowie die Netze des Bundes als prioritäre Vorhaben der Cybersicherheit. Im Regierungsentwurf für den Haushalt 2025 sind in Kapitel 0602 (Titelgruppen 02 und 05) hierfür Haushaltsmittel von insgesamt über eine Mrd. Euro veranschlagt. Als Basisvorhaben für die Kommunikationsinfrastruktur der Bundesverwaltung sowie der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) tragen diese mittelbar zur Cybersicherheit bei, indem sie beispielsweise Daten auf dem Transportweg verschlüsseln. Als eigenständige Vorhaben der Cybersicherheit können sie jedoch nicht betrachtet werden. Entsprechend enthält die Cybersicherheitsagenda hierzu lediglich abgegrenzte Teilprojekte zur
- Modernisierung der Weitverkehrsnetze gemäß der „Netzstrategie 2030 für die öffentliche Verwaltung“,
- zentralen Unterstützung der Behörden bei der Einführung von IPv6,
- Einführung eines zentralen Videokonferenzsystems für die Bundesverwaltung,
- Modernisierung des Digitalfunknetzes für BOS (Sprachkommunikation) und zur
- Erweiterung des Digitalfunknetzes für BOS (Datenkommunikation).

Keines dieser Teilprojekte hat das BMI in seine Übersicht der kostenintensiven Vorhaben aufgenommen.

9 Kompetenzzentrum operative Sicherheitsberatung Bund (KoSi).

10 Kapitel 0602 Titel 544 02.

11 Das Bundeskabinett hat am 24. Juli 2024 den Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, NIS2UmsuCG) beschlossen. Der Bundesrechnungshof hat hierzu einen eigenen Bericht nach § 88 Absatz 2 BHO an den Haushaltsausschuss gerichtet. (Drs. 20(8)6487 vom 17. September 2024).

12 Gemäß Gesetzesbegründung zum Entwurf des NIS2UmsuCG soll der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

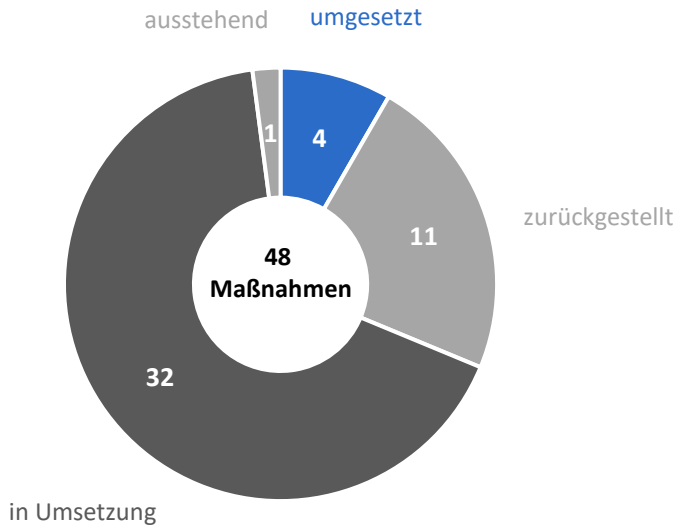
13 Die zusätzlichen Haushaltsmittel, mit denen das IT-SiG 2.0 aus dem Jahr 2021 umgesetzt werden soll, verteilen sich auf mehrere Titel, vorrangig im Kapitel 0623 (BSI). Angesichts eines Haushaltsvolumens für das BSI von insgesamt 238 Mio. Euro dürfte nur ein Bruchteil, auf jeden Fall deutlich weniger als 129 Mio. Euro, auf die zusätzlichen Aufgaben aus dem IT-SiG 2.0 entfallen.

Zu den Vorhaben der Cybersicherheitsagenda hat das BMI folgenden Sachstand mitgeteilt: Von den insgesamt 48 Maßnahmen seien vier erledigt, elf zurückgestellt, 32 in Umsetzung und eine ausstehend.

Abbildung 1

Von 48 Maßnahmen bisher nur 4 umgesetzt

Zwei Jahre nach ihrer Veröffentlichung hat das BMI vier Maßnahmen aus der Cybersicherheitsagenda abgeschlossen. Zwei Drittel befinden sich in der Umsetzung.



Grafik: Bundesrechnungshof. Quelle: BMI.

Das BMI erläuterte, dass für neun der elf zurückgestellten Maßnahmen fehlende Haushaltsmittel ursächlich seien. Gleiches gelte für die Mehrzahl der Maßnahmen, die es noch umsetze. Diese könne es wegen unzureichender Mittel und Stellen nicht bis Ende 2024 abschließen.

Als Maßnahme der Cybersicherheitsagenda hatte das BSI für den Haushalt 2024 u. a. den Sondertatbestand „Sabotage-Resilienz für Staat und Wirtschaft stärken“ mit einem Mittelbedarf von 93 Mio. Euro über vier Jahre angemeldet. Anlass waren der russische Angriffskrieg gegen die Ukraine, die Zunahme von erfolgreichen Cyberangriffen sowie die steigende Anzahl von Anschlägen gegen physische Infrastrukturen. Diese zeigten, wie verwundbar IT-Infrastrukturen, beispielsweise die Rechenzentren oder die Kommunikationsstrukturen des Bundes, und wie sehr Staat und Gesellschaft auf deren störungsfreien Betrieb angewiesen sind. Daher wollte es mit diesen Mitteln die Resilienz der bestehenden IT-Infrastrukturen erhöhen. Weder im Haushaltsentwurf für das Jahr 2024 noch in dem für das Jahr 2025 fand der Bedarf Berücksichtigung.

Das Kompetenzzentrum operative Sicherungsberatung (KoSi) Bund ist sowohl Bestandteil der Cybersicherheitsagenda als auch der Cybersicherheitsstrategie. Dieses soll die Ressorts unterstützen, Informations- und Cybersicherheitsmaßnahmen umzusetzen. Mit Hilfe von KoSi Bund sollen die Bundeseinrichtungen ihre gravierendsten Umsetzungsdefizite forciert

beheben. Gleichzeitig soll KoSi Bund die Abhängigkeit von externen Beratungsleistungen bei der operativen Unterstützung von Bundesbehörden reduzieren. Der Rechnungsprüfungsausschuss hat das BMI erst kürzlich aufgefordert, eine auskömmliche Finanzierung des Betriebes des KoSi Bund mit dessen Bedarfsträgern zu vereinbaren.[14] Haushaltsmittel für das KoSi Bund hat das BMI weder in den Regierungsentwurf noch in den Finanzplan aufgenommen (vgl. Tabelle 1). Ausweislich des Sachstandsberichts zum Digitalprogramm[15] des BMI ist die Maßnahme KoSi Bund derzeit zurückgestellt.[16]

Das BMI geht in seinem Bericht an den Haushaltsausschuss weiterhin davon aus, dass die anderen Ressorts die erforderlichen Mittel für Vorhaben der Cybersicherheit im Haushalt 2025 ebenfalls angemeldet hätten. Auf Nachfrage erklärte das BMI, dass

- ihm die Haushaltsanmeldungen anderer Ressorts für prioritäre Maßnahmen der Informations- und Cybersicherheit nicht bekannt seien,
- es mit den anderen Ressorts nicht abgestimmt habe, welche Vorhaben der Cybersicherheit im Voranschlag zu berücksichtigen sind, und
- ihm nicht bekannt sei, welche der Vorhaben der Cybersicherheit der übrigen Ressorts im Regierungsentwurf in welchem Umfang berücksichtigt wurden.

Das vom Haushaltsausschuss in seinem Beschluss aus dem Jahr 2022 geforderte ressortübergreifende IT-Sicherheitscontrolling existiert noch nicht. Steuerungsrelevante Daten zur Informations- und Cybersicherheit in der Bundesverwaltung hat die Bundesregierung noch nicht festgelegt, erhoben, analysiert und bewertet.

Würdigung

Entgegen den Vorgaben des Maßgabebeschlusses des Haushaltsausschusses aus dem Jahr 2023 hat das BMI noch kein Finanzierungskonzept für Vorhaben der Cybersicherheit erarbeitet. Somit hat es weiterhin keinen Überblick darüber, in welcher Höhe und für welche Vorhaben der Cybersicherheit die Ressorts Mittel in den Regierungsentwurf aufgenommen haben. Infolgedessen weiß es nicht,

- welche Parallelentwicklungen stattfinden,
- wo andere Ressorts redundant an ähnlichen Fragestellungen arbeiten und
- welche Ausgabenschwerpunkte diese im Bereich der Cybersicherheit setzen.

---

[14] 20. Sitzung des Rechnungsprüfungsausschusses vom 15. März 2024, Beschluss zu TOP 8 („Bundesbehörden bei Informationssicherheit zentral unterstützen und IT-Personal entlasten“).

[15] Digitales Deutschland – Souverän. Sicher. Bürgerzentriert. Digitalpolitische Ziele und Maßnahmen bis 2025 des Bundesministeriums des Innern und für Heimat, April 2022.

[16] https://www.cio.bund.de/Webs/CIO/DE/cio-bund/digitalprogramm/sachstandsinformation_digitalprogrammBMI/sachstandsinformation_digitalprogrammBMI-node.html#doc21231288bodyText4, abgerufen am 30. August 2024: „Der Aufbau des KoSi Bund musste zurückgestellt werden.“

Es hat versäumt, sich hierzu mit den Ressorts abzustimmen. Da es trotz der Aufforderung des Haushaltsausschusses unverändert an einem ressortübergreifenden Controlling mangelt, überrascht es nicht, dass das BMI weiterhin keine Kenntnis über den Stand der Finanzierung hat. Dabei ist diese für das federführende Ressort, das innerhalb der Bundesregierung die Angelegenheiten der Informations- und Cybersicherheit verantwortet, unabdingbar. Wie es so der Vorgabe des Haushaltsausschusses nachkommen will, prioritäre Maßnahmen der Informations- und Cybersicherheit gemeinsam mit den übrigen Ressorts auskömmlich zu finanzieren, bleibt unbeantwortet.

Auch die Haushaltsplanungen für seinen eigenen Einzelplan werfen Fragen auf. So sind selbst die wenigen, vom BMI als kostenintensiv ausgewiesenen Vorhaben der Cybersicherheit für das Jahr 2025 und für den gesamten Finanzplanungszeitraum nicht am Bedarf ausgerichtet finanziert. Zu zahlreichen weiteren Vorhaben u. a. aus der Cybersicherheitsagenda, die aus Sicht des BMI allesamt höchste Priorität haben, fehlen ohne erkennbaren Grund entsprechende Haushaltsansätze. Auch der Beschluss des Rechnungsprüfungsausschusses, das KoSi Bund auskömmlich zu finanzieren, bleibt sowohl für den Regierungsentwurf des Bundeshaushalts 2025 als auch im Finanzplan bis 2028 unberücksichtigt.

Das BMI kann von den 48 Maßnahmen seiner eigenen Cybersicherheitsagenda nach eigenen Angaben deutlich über die Hälfte mangels Haushaltsmittel nicht oder allenfalls sehr verzögert umsetzen. Die gravierenden Bedrohungen im Cyberraum hätten erwarten lassen, dass sich diese Maßnahmen im Entwurf des Haushalts 2025 wiederfinden. Dies gilt sowohl für den Sabotageschutz exponierter IT-Infrastrukturen als auch für die operative Unterstützung der Ressorts. Beides hat nicht an Bedeutung verloren – eher im Gegenteil.

Insofern bleibt das BMI einen Beleg für seine Darstellung schuldig, es habe die für diese Vorhaben erforderlichen Mittel für den Haushalt 2025 angemeldet.

Empfehlung

Das BMI sollte die Maßnahmen zur Informations- und Cybersicherheit mit den Ressorts abstimmen. Nur so kann es sich einen Überblick darüber verschaffen, für welche Vorhaben diese in welcher Höhe Haushaltsmittel in ihren Einzelplänen veranschlagt haben. Es muss analysieren,

- welche Schwerpunkte einzelne Ressorts für Informations- und Cybersicherheit setzen und welche Ausgaben sie dafür vorsehen,
- welche Stellen der Bundesverwaltung redundant an ähnlichen Fragestellungen arbeiten und
- wo Parallelentwicklungen drohen.

Im Ergebnis sollte das BMI dann gemeinsam mit den Ressorts ermitteln, wie hoch der Finanzbedarf ist, um die für die Informations- und Cybersicherheit unabdingbaren

Maßnahmen der Nationalen Sicherheitsstrategie und der Cybersicherheitsstrategie sowie der Cybersicherheitsagenda umzusetzen. Erst auf Grundlage dieser Angaben wird es möglich sein,

- den Bedarf mit den vorhandenen Mitteln abzugleichen,
- einen möglichen Mehrbedarf zu identifizieren und
- Priorisierungen und eventuell Umschichtungen zu anderen Aufgabenfeldern vorzunehmen.

Darüber hinaus sollte das BMI zügig ein Finanz- und Umsetzungscontrolling für die Maßnahmen der Informations- und Cybersicherheit als Teil des IT-Sicherheitscontrollings etablieren. In dem Fall wäre es jederzeit auskunftsfähig und könnte etwaigen Nachsteuerungsbedarf frühzeitig selber identifizieren.

3 Zentrales Budget für Cybersicherheit im Bundeshaushalt

Sachverhalt

Der Haushaltsausschuss hat das BMI aufgefordert, zu prüfen, inwieweit ein zentrales Budget im Einzelplan 60 eingerichtet werden kann. Dieses sollte sich aus anteiligen – beispielsweise prozentual an den jeweiligen IT-Ausgaben orientierten – Beiträgen aller Ressorts zusammensetzen. In seinem Bericht weist das BMI darauf hin, dass es eine ressortübergreifende Aufgabe sei, die Sicherheit der IT-Infrastruktur des Bundes herzustellen und zu gewährleisten. Einem zentralen Budget müssten jedoch je nach Ausgestaltung alle Ressorts zustimmen. Ein allgemein zustimmungsfähiges Modell habe sich bislang noch nicht abgezeichnet.

Auf Nachfrage konnte das BMI nicht näher erläutern, welche Modelle es hierzu im Ressortkreis diskutiert hat. Ein zentrales Budget für Cybersicherheit ist weder im Regierungsentwurf für den Bundeshaushalt 2025 noch im Finanzplan bis 2028 vorgesehen.

Der Bundesrechnungshof hat im Regierungsentwurf ergänzend ausgewertet, über welche Ausgabetitel die Bundesregierung – ausweislich der Zweckbestimmung – explizit (auch) Vorhaben der Cyber-, IT- oder Informationssicherheit finanzieren will (vgl. Tabelle 2).

Tabelle 2

Der Haushaltsentwurf für das Jahr 2025 enthält acht Titel mit Ausgabemitteln für Zwecke der IT- oder Cybersicherheit

Haushaltstitel, die in der Zweckbestimmung oder in den Erläuterungen den expliziten Einsatz (auch) für Zwecke der IT- oder Cybersicherheit vorsehen, enthält der Regierungsentwurf nur sehr vereinzelt und über sechs Einzelpläne verteilt. Ein Titel, aus dem ressortübergreifende Maßnahmen finanziert werden können, gehört nicht hierzu.

Haushaltsstelle	Zweckbestimmung	Ansatz (in Tsd. Euro)
0501 687 27[17]	Maßnahmen der Abrüstung, Rüstungskontrolle sowie Zusammenarbeit zu Nichtverbreitung, **Cybersicherheit** und digitalen Technologien (wie K.I.)	40 000
0602 544 02	Disruptive Innovationen in der **Cybersicherheit** und Schlüsseltechnologien	19 000
0602 831 01	Erwerb von Beteiligungen im Bereich **Cybersicherheit**	-
0602 532 17	**IT- und Cybersicherheit**	2 482
0901 686 22	Mittelstand Digital; Erläuterung: **IT-Sicherheit** in der Wirtschaft	5 000
1016 812 02	Erwerb von Anlagen, Geräten, Ausstattungs- und Ausrüstungsgegenständen sowie Software im Bereich Informationstechnik; Erläuterung: **IT-Sicherheit**	49
1404 551 04	Disruptive Innovationen in **Cybersicherheit** und Schlüsseltechnologien	40 000
3004 683 20	Kommunikationssysteme, **IT-Sicherheit**; Erläuterungen: **Cyber- und IT-Sicherheit**, künftige Technologien (u. a. Quantenkommunikation), Anwendungen sowie gesellschaftliche Implikationen wie Schutz von Privatheit und Gefährdung durch Desinformation; im Deutschen Aufbau- und Resilienzplan enthaltene Maßnahme Forschungsnetzwerk Anonymisierung "**IT-Sicherheit** (Anonymisierung)“	106 440 20 000

Quelle: Haushaltsentwurf 2025.

Hinzu kommen die Ansätze für das BSI (Kapitel 0623) sowie Zuwendungen aus dem Haushalt des Bundesministeriums für Bildung und Forschung (BMBF) (Kapitel 3004) an das Helmholtz-Zentrum für Informationssicherheit CISPA[18] und das Nationale Forschungszentrum für Angewandte Cybersicherheit ATHENE[19].

[17] Die Zweckbestimmung des Titels soll im Haushaltsplan 2025 um den Begriff „Cybersicherheit“ ergänzt werden.

[18] Center for IT-Security, Privacy and Accountability (Kurzform: CISPA) wurde im Oktober 2011 als ein nationales BMBF-gefördertes Kompetenzzentrum für IT-Sicherheit und Datenschutz an der Universität des Saarlandes gegründet.

[19] ATHENE ist das größte Forschungszentrum für Cybersicherheit und Privatsphärenschutz in Europa; es ist eine Forschungseinrichtung der Fraunhofer-Gesellschaft mit diversen Beteiligungen anderer Forschungseinrichtungen.

Für ressortübergreifende Maßnahmen im Bereich der Cybersicherheit stehen im Regierungsentwurf keine Haushaltsmittel zur Verfügung. Einzig der Titel 532 17 im Kapitel 0602 dient dem BMI seit einigen Jahren dazu, gewisse Aktivitäten im Bereich der Cybersicherheit zu finanzieren, die eine Relevanz über das BMI hinaus haben. Im Jahr 2023 waren dies Ausgaben von insgesamt 386 Tsd. Euro, u. a. für die Weiterentwicklung der Cybersicherheitsstrategie und die Ausrichtung des ersten Berliner Cybersicherheitsgipfels des Nationalen Cybersicherheitsrates. Von den im Jahr 2024 verfügbaren Mitteln wies das BMI einen Großteil dem BSI für dessen Projekte zu.[20]

Nach den Haushaltstechnischen Richtlinien des Bundes (HRB) werden Ausgaben für Cybersicherheit im Haushaltsplan nicht separat veranschlagt. Sie sind Teil der Ausgaben für IT-Vorhaben, die grundsätzlich bei den Festtiteln 532 .1 und 812 .2 sowie im Übrigen anteilig bei den weiteren einschlägigen Festtiteln (zum Beispiel 511 .1, 518 .1, 525 .1) zu veranschlagen sind.[21] Für den Titel 812 .2 sehen die HRB sogenannte Standarderläuterungen vor, mit denen der Soll-Ansatz näher differenziert werden kann. Von der Möglichkeit eines separaten Ausweises der geplanten Ausgaben für IT-Sicherheit hat im Regierungsentwurf nur das Johann Heinrich von Thünen-Institut (Kapitel 1016) Gebrauch gemacht (vgl. Tabelle 2).

Würdigung

Das BMI ist dem Prüfauftrag des Haushaltsausschusses bisher nicht mit der gebotenen Intensität nachgekommen. Welche Modelle eines zentralen Budgets für Vorhaben der Cybersicherheit es mit den Ressorts erörtert hat und wie es diese ausgestalten wollte, konnte es nicht darlegen. Inwieweit es den Prüfauftrag des Haushaltsausschusses erfüllt hat, ist daher offen. Es kann somit kaum verwundern, dass sich die Ressorts bislang auch nicht auf ein Konzept verständigen konnten, einen Teil ihrer Haushaltsmittel in ein zentrales Budget zu verlagern. Zudem hätte das BMI, gegebenenfalls unterstützt vom BMF, den Ressorts den Mehrwert eines zentralen Budgets aufzeigen müssen.

Dafür hätte das BMI ermitteln sollen, ob und gegebenenfalls in welchem Umfang die Ressorts einzelne Vorhaben der Cybersicherheit dezentral aus (IT-)Titeln mit einer allgemeinen Zweckbestimmung mitfinanzieren. Dann hätte es allen Beteiligten die Vorteile einer Bündelung angesichts eng begrenzter Haushaltsmittel begründen können. Synergie- und Skaleneffekte, die durch eine Steuerung und Finanzierung von Maßnahmen an zentraler Stelle eröffnet werden würden, sind derzeit unbestimmt und nicht bezifferbar.

[20] Bundestagsdrucksache 20/11250, Antwort der Parlamentarischen Staatssekretärin Schwarzelühr-Sutter vom 30. April 2024 auf Frage 34.

[21] HRB, Ziffer 13.1.

Ein wichtiger Schritt wäre daher, die geplanten Ausgaben für Vorhaben der Cybersicherheit im Bundeshaushalt sichtbarer zu machen. Das Vorgehen des Heinrich von Thünen-Instituts[22], die für Zwecke der IT-Sicherheit vorgesehenen Ausgaben in einer Erläuterung konkret zu beziffern, kann hierzu ein pragmatischer Ansatz sein, ohne neue Titel in den Haushaltsplan aufnehmen zu müssen.

Für Maßnahmen, die von ressortübergreifender Bedeutung sind, wie beispielsweise

- die Einrichtung des KoSi Bund,
- der Betrieb und die Weiterentwicklung des Cyber-AZ[23] oder
- die Weiterentwicklung des Projekts zur ressortübergreifenden Verschlusssachen-Kommunikation (R-VSK)[24]

hätte das BMI gemeinsam mit den Ressorts dagegen prüfen sollen, ein zentrales Budget vorzusehen. Denn diese Vorhaben kommen allen Ressorts zugute. Um eine dauerhafte Finanzierung sicherzustellen, hätte die Bundesregierung ressortübergreifende Vorhaben aus den Einzelplänen herauslösen sollen. Schließlich besteht immer die Gefahr, dass deren Priorität gegenüber einzelplanspezifischen Fachaufgaben herabgestuft wird. Ein zentrales Budget würde auch die erforderliche Transparenz über den Ressourceneinsatz für Informations- und Cybersicherheit verbessern. Perspektivisch könnte die Bundesregierung darüber auch Angebote bereitstellen und finanzieren, die das BSI zentral für alle Bundesbehörden anbietet, z. B. das BSOC[25] oder die MIRT[26].

Empfehlung

Das BMI sollte spätestens bis zum Haushaltsaufstellungsverfahren für das Jahr 2026 sachgerechte Einsatzbereiche und Finanzierungsmodelle für ein zentrales Budget für Vorhaben der Cybersicherheit ausarbeiten und mit den Ressorts abstimmen. Es sollte hierzu das BMF mit seiner Expertise und in seiner Gesamtverantwortung für den Bundeshaushalt frühzeitig

---

[22] Das Thünen-Institut ist eine bundesunmittelbare, nicht rechtsfähige Anstalt des öffentlichen Rechts und Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Ernährung und Landwirtschaft mit Hauptsitz in Braunschweig.

[23] Die Bundesregierung will das Cyber-AZ als zentrale Kooperations-, Kommunikations- und Koordinationsplattform der relevanten (Sicherheits-) Behörden in Abhängigkeit von der Entwicklung der Bedrohungslage fortentwickeln. (Cybersicherheitsstrategie, Ziffer 8.3.4). Es soll die für das ganzheitliche Cyberlagebild erforderliche Koordinierungsfunktion einnehmen (Nationale Sicherheitsstrategie, Seite 61).

[24] Die Bundesregierung will mit der Weiterentwicklung des Projekts R-VSK die digitale Souveränität, Cybersicherheit und Krisenresilienz in Form hochsicherer Kommunikation zum Schutz von Geheimnissen von Staat und Wirtschaft stärken. Damit will sie schnellere, virtuelle Abstimmungen zu sensiblen Themen ermöglichen (Digitalstrategie mit Stand vom 25. April 2023, Seite 49).

[25] Zum Schutz der Regierungsnetze und IT-Systeme des Bundes vor Cyber-Angriffen betreibt das BSI das „Bundes Security Operations Center“ (BSOC), das u. a. Dienstleistungen zur Erfassung und Auswertung von Protokollierungs- und Sensordaten sowie zur Erkennung und Abwehr von Schadsoftware umfasst.

[26] In Fällen besonders herausgehobener IT-Sicherheitsvorfälle in der Bundesverwaltung kann das BSI ein Mobile Incident Response Team (MIRT) zur Unterstützung vor Ort entsenden.

einbeziehen. Für die (gemeinsame) Bewirtschaftung des zentralen Budgets sind Regelungen vorzusehen, die den Ressorts eine angemessene Mitwirkung sichern. Als erster Schritt wäre beispielsweise denkbar, im Einzelplan 60 einen Leertitel vorzusehen, der es ermöglicht, unterjährige Mehrausgaben für übergreifende Maßnahmen der Informations- und Cybersicherheit gegen Einsparung in den Einzelplänen zu leisten, wobei für die Einsparung in den (verbindlichen) Erläuterungen ein Verteilungsschlüssel festgelegt wird.[27] Alternativ könnten Ausgaben auch aus den Einzelplänen herausgelöst und in einem Verstärkungstitel Cybersicherheit im Einzelplan 60 gebündelt werden.[28] Auf diesen dürften die Ressorts dann nur unter bestimmten Voraussetzungen (beispielsweise bei einer Cybersicherheitsmaßnahme mit ressortübergreifender Bedeutung oder zur Bewältigung eines schweren IT-Sicherheitsvorfalls) zugreifen.

Unabhängig davon sollte die Bundesregierung für mehr Transparenz bei verbleibenden dezentralen Ausgaben für Informations- und Cybersicherheit sorgen. Diese Planungen sollte sie mit dem Informations- und Steuerungsbedarf des zu etablierenden IT-Sicherheitscontrollings eng verzahnen. Insgesamt wird es darauf ankommen, dass die Bundesregierung geeignete Steuerungsstrukturen schafft, die es ihr ermöglichen, knappe Haushaltsmittel effektiv zu nutzen und bedarfsgerechte sichere zentrale IT-Leistungen zu entwickeln und bereitzustellen.

4 Organisatorische Aufstellung des BSI

Sachverhalt

Der Haushaltsausschuss hat das BMI aufgefordert, darauf hinzuwirken, dass das BSI seine Unterstützungs- und Kontrollaufgaben gegenüber den Behörden und Rechenzentren der Bundesverwaltung vollumfänglich wahrnimmt. Hierfür sollte es sich organisatorisch, personell und finanziell geeignet aufstellen.

Das BMI hat in seinem Bericht auf die interne Umorganisation des BSI zum 1. Juli 2024 hingewiesen. Unter anderem habe dies eine Abteilung zur Eigensicherung des Bundes eingerichtet. Damit wolle das BSI seine Unterstützungs- und Kontrollaufgaben stärken. Zudem wolle es „Synergieeffekte […] erschließen, um Effizienzpotentiale auszuschöpfen."

Das BSI hat keine quantitativen Angaben in Form von Kennzahlen oder Indikatoren zum Ist- und Soll-Zustand seiner Organisation für die Eigensicherung des Bundes wie z. B.

[27] Vgl. beispielsweise die Veranschlagungspraxis im Kapitel 6002 Titel 971 03 für „Aufwendungen deutscher Sicherheitskräfte im Zusammenhang mit internationalen Einsätzen".

[28] Vgl. beispielsweise die Veranschlagungspraxis im Kapitel 6002 Titelgruppe 01 „Verstärkung von Ausgaben im Personalsektor".

- zum Grad der Automatisierung von Prozessen,
- zu Durchlaufzeiten dieser Prozesse oder
- zum Aufwand je Produkt

bestimmt und festgelegt. Eine Aufgabenkritik hat es nicht durchgeführt.

Qualitativ gab das BSI auf Nachfrage an, seine neue Organisation werde es insgesamt auf ein wachsendes und komplexeres Aufgabenspektrum vorbereiten, auch wenn kein ausreichendes Personal und keine auskömmlichen Sachmittel zur Verfügung stünden.

Eine Wirtschaftlichkeitsuntersuchung, die Aufwand und Nutzen der Umorganisation qualitativ wie quantitativ gegenüberstellt, hatte es nicht durchgeführt. Das BSI ist vom BMI aufgefordert, den Erfolg der Umorganisation nach sechs Monaten nachzuweisen und dann erforderlichenfalls seine Strukturen nachzujustieren.

Würdigung

Angesichts der Bedrohungen im Cyberraum ist es erforderlich, dass das BSI die Eigensicherung des Bundes stärkt. Dazu muss es u. a. seine Unterstützungs- und Kontrollaufgaben gegenüber Bundeseinrichtungen vollumfänglich wahrnehmen und Effizienzpotentiale ausschöpfen.

Ohne den Ist- und Soll-Zustand für seine organisatorischen Ziele zu definieren, ist es dem BSI aber kaum möglich, den Erfolg seiner neuen Abteilung zur Eigensicherung des Bundes zu messen. Es hätte hierfür geeignete Kennzahlen oder Indikatoren entwickeln sollen, anhand derer es die Wirkung seiner Umorganisation bestimmen kann. Auch hätte es eine Aufgabenkritik durchführen müssen. Wenn das BSI nicht regelmäßig ermittelt, wie sich die veränderte Organisationsstruktur auf seine Leistung auswirkt, kann es seine Organisation nicht geeignet steuern und auf das gesetzte Ziel ausrichten. In welchem Umfang die neue Organisationsstruktur Synergieeffekte erschließt, damit das BSI sein wachsendes komplexes Aufgabenspektrum bei nach seiner Einschätzung unzureichenden Personal- und Sachmitteln erfüllen kann, hat es nicht dargelegt.

Das BMI war vom Haushaltsausschuss aufgefordert, „darauf hinzuwirken, dass das BSI organisatorisch, personell und finanziell so aufgestellt ist, dass es seine Unterstützungs- und Kontrollaufgaben […] vollumfänglich wahrnehmen kann.“ Dazu reicht es nicht aus, das BSI aufzufordern, nach sechs Monaten eine Erfolgskontrolle durchzuführen. Vielmehr hätte es bereits vor der Umorganisation eine Wirtschaftlichkeitsuntersuchung vom BSI verlangen sollen, bei der dieses Alternativen betrachtet und Kosten und Nutzen gegenüberstellt. Denn jede größere Umorganisation stellt eine finanzwirksame Maßnahme dar. Für diese sieht die Bundeshaushaltsordnung (BHO) zwingend vor, dass angemessene Wirtschaftlichkeitsuntersuchun-

gen durchzuführen sind.[29] Auch hätte das BSI Kennzahlen und Indikatoren definieren und dazu Werte ermitteln müssen. Diese fehlen ihm nun als Grundlage für eine sachgerechte Erfolgskontrolle.

Empfehlung

Das BMI sollte das BSI anweisen, die vorgesehene Erfolgskontrolle für seine Umorganisation nach den Vorgaben der Nummert 2.2 der Verwaltungsvorschriften zu § 7 BHO durchzuführen. Diese muss folgende Untersuchungen umfassen:

- Zielerreichungskontrolle
- Wirkungskontrolle
- Wirtschaftlichkeitskontrolle

Das BMI sollte hierfür mit dem BSI die Ziele der Umorganisation mittels Kennzahlen und Indikatoren messbar definieren.

5 Unterstützungs- und Kontrollaufgaben des BSI

Sachverhalt

Der Haushaltsausschuss hatte das BMI im Jahr 2022 aufgefordert, dafür Sorge zu tragen, dass das BSI seine bestehenden Prüfinstrumente und -schemata (u. a. die Sicherheitsanalysen von Rechenzentren) und seine neuen Kontrollbefugnisse aus dem IT-SiG 2.0 zeitnah in einem neuen umfassenden Revisionsansatz für die Bundesverwaltung zusammenführt. Hierzu stellt das BMI dar, das BSI habe zwischenzeitlich konzipiert, wie es seine seit dem 1. Dezember 2021 bestehenden Kontrollbefugnisse nach § 4a BSIG umsetzen wolle. Das Konzept aus dem Jahr 2023 sieht u. a. vor, innerhalb von drei Jahren, d. h. bis zum Jahr 2026, die Bundesverwaltung mit ihren 400 bis 500 Einrichtungen[30] flächendeckend zu prüfen. Das BSI will danach jede Bundeseinrichtung alle drei Jahre einer Revision unterziehen. Es müsste demnach pro Jahr zwischen 130 und 160 Bundeseinrichtungen prüfen. Die Ergebnisse der flächendeckenden Anwendung des § 4a BSIG sollen wesentliche Basis des künftigen IT-Sicherheitscontrollings der Bundesverwaltung sein.

Für die Kontrollaufgaben hat das BSI einen Personalbedarf von 64 Stellen geltend gemacht. Zudem wollte es sich hierfür durch externe Prüfer unterstützen lassen. Dem BSI stehen für

[29] § 7 Absatz 2 Satz 1 BHO.
[30] Davon nutzen ca. 120 Einrichtungen die Netze des Bundes.

die Prüfungen nach § 4a BSIG aktuell neun Stellen zur Verfügung. Von diesen konnte es zwei Stellen besetzen.

Im Jahr 2024 hat das BSI bisher drei Pilotprüfungen erfolgreich abgeschlossen. Im Sachstandsbericht zu seinem Digitalprogramm teilt das BMI mit, dass flächendeckende Prüfungen gemäß § 4a BSIG derzeit „nicht realistisch“ seien.[31]

Der Haushaltsausschuss hatte weiter gefordert, das BSI solle auf Grundlage seiner Prüfungserkenntnisse der Bundesverwaltung geeignete Handlungsempfehlungen bereitstellen. In seinem Konzept sieht das BSI vor, geprüfte Einrichtungen intensiv zu beraten, wie sie die festgestellten Mängel beseitigen können. Bei den Pilotprüfungen ist dies nicht erfolgt.

Zu zurückliegenden Sicherheitsanalysen der Rechenzentren teilte das BMI mit, das BSI bereite diese nach und werde dabei dem Beschluss des Haushaltsausschusses entsprechend die Behördenleitungen und Ressort-Informationssicherheitsbeauftragten über die Ergebnisse informieren. Darüber hinaus werde das BSI wie gefordert darauf hinwirken, dass die geprüften Bundesbehörden mindestens jährlich über den Sachstand zu den Mängeln berichten. Erstmals wende dieses einen sogenannten „Nachhalte-Mechanismus“ an. Diesen wolle das BSI auch für die Mängel nutzen, die es bei Prüfungen gemäß § 4a BSIG feststellt.

Auf Nachfrage des Bundesrechnungshofes informierte das BSI, dass es auch zu den bereits durchgeführten Pilotprüfungen die betroffenen Behördenleitungen noch beraten werde und es erwarte, dass ein größerer nachgelagerter Beratungsbedarf entstehe.

Würdigung

Das BMI hat den Maßgabebeschluss des Haushaltsausschusses aus dem Jahr 2022 in wichtigen Punkten noch nicht umgesetzt.

Zwar hat das BSI zwischenzeitlich konzipiert, wie es seine Kontrollbefugnisse nach § 4a BSIG wahrnehmen will, allerdings lässt sich dieses Konzept mit den bislang zur Verfügung stehenden Ressourcen nicht umsetzen. Dies ist besonders nachteilig, da die Kontrollbefugnisse nach § 4a BSIG erheblich dazu beitragen können, die Informationssicherheitsanforderungen in der Bundesverwaltung durchzusetzen. Angesichts eines vom BSI ermittelten Bedarfs von 64 Beschäftigten, um Prüfungen zu planen, durchzuführen und nachzubereiten, ist der Einsatz von lediglich zwei Personen unzureichend. Flächendeckende Prüfungen sind damit nicht nur – wie vom BMI dargestellt – nicht realistisch, sondern unmöglich. Nahezu drei Jahre nach Inkrafttreten der gesetzlichen Vorgaben ist dies ein Zustand, der der Bedeutung der neuen Kontrollaufgaben des BSI für die Cybersicherheit in der Bundesverwaltung nicht gerecht wird.

---

[31] https://www.cio.bund.de/Webs/CIO/DE/cio-bund/digitalprogramm/sachstandsinformation_digitalprogrammBMI/sachstandsinformation_digitalprogrammBMI-node.html#doc21231288bodyText4, abgerufen am 30. August 2024.

Solange das BSI die Kontrollen nicht in dem vom Gesetzgeber erwarteten Umfang durchführt, fehlen den IT-Steuerungsgremien wichtige Informationen. Sie können den aktuellen Sicherheitszustand der Bundesbehörden nicht vollständig erfassen. Insoweit besteht die Gefahr, dass sie Entscheidungen ohne valide Grundlage treffen. Bundesbehörden wiederum fehlt die erforderliche kompetente und neutrale Rückspiegelung ihrer Cybersicherheitssituation, damit sie Defizite erkennen und die bestehenden Anforderungen erfüllen können. Auch kann das BMI so seine Zusage an den Rechnungsprüfungsausschuss, bis Ende 2025 ein funktionierendes und aussagekräftiges IT-Sicherheitscontrolling aufzubauen, nicht einhalten. Ihm fehlt dafür eine solide, aus den Revisionsergebnissen des BSI gespeiste, Datenbasis.

Von Bedeutung ist auch, gerade diejenigen Einrichtungen des Bundes zu beraten, deren IT hinsichtlich der Informationssicherheit Mängel aufzeigt. Obwohl der Haushaltsausschuss bereits Ende des Jahres 2022 gefordert hatte, die Behördenleitungen und die Ressort-Informationssicherheitsbeauftragten über die Ergebnisse zu den in ihrem Zuständigkeitsbereich geprüften Rechenzentren detailliert zu informieren, hat das BSI bisher davon abgesehen. Solange es jedoch die Prüfungsergebnisse nicht für die geprüften Stellen aufbereitet und diesen übermittelt, können diese auch nicht angemessen auf Mängel reagieren. Mit zunehmendem Abstand zur Prüfung laufen solche Informationen Gefahr, nicht mehr aktuell und sachgerecht zu sein. Der Bundesrechnungshof geht davon aus, dass sich die Situation in den geprüften Rechenzentren seit der Prüfung durch das BSI erheblich verändert hat. Bei den Pilotprüfungen zum § 4a BSIG wiederholt das BSI nun diesen Fehler, wenn es die betroffenen Behördenleitungen nicht unmittelbar über die Ergebnisse informiert und umfassend berät. Im Ergebnis riskiert es, dass seine Kontrollen eine geringere Wirkung entfalten.

Das BSI hätte früher nachhalten müssen, wie Bundeseinrichtungen mit Mängeln umgehen und wann bzw. wie sie diese beheben. Ohne den Nachhalte-Mechanismus fehlte ihm ein Überblick über den Stand deren Informationssicherheit und Prozesse. Mit einem solchen Mechanismus hätte es stärker darauf drängen können, dass die Einrichtungen die Mängelbehebung hinreichend priorisieren. Das BSI hätte den Nachhalte-Mechanismus schon früher einsetzen können, um Erfahrungswissen für künftige Fälle zu schaffen.

Empfehlung

Das BMI muss den Maßgabebeschluss des Haushaltsausschusses aus dem Jahr 2022 vollständig umsetzen. Dafür muss das BSI die freien Stellen zügig besetzen. Der Deckung seines Ressourcenbedarfs für die Kontrollbefugnisse gemäß § 4a BSIG muss es besondere Priorität einräumen, da davon auch der Aufbau eines wirksamen IT-Sicherheitscontrollings abhängt.

Geprüfte Stellen muss das BSI zeitnah über die Ergebnisse seiner Kontrollen informieren. Den Nachhalte-Mechanismus sollte es umgehend etablieren und für seine Prüfungen gemäß § 4a BSIG stringent einsetzen. U. a. mit Hilfe dieser Datenbasis sollte es den Status der Informationssicherheit sowie die Wirkung seiner Kontrollen dokumentieren.

6 Arbeitshilfen und Aufwandsreduzierung

Sachverhalt

Das BMI stellt in seinem Bericht an den Haushaltsausschuss dar, das BSI stelle Arbeitshilfen bereit und wolle den für Informationssicherheit entstehenden Aufwand in der Bundesverwaltung reduzieren. Auch entwickele das BSI eine Arbeitshilfe zur Personalbedarfsermittlung im Bereich der Informations- und Cybersicherheit. Diese solle Ende 2024 zur Verfügung stehen.

Den IT-Grundschutz will das BSI künftig automatisieren, in dem es diesen in ein von Maschinen verarbeitbares Regelwerk umwandelt und zudem messbare Zielgrößen als Metadaten und Leistungszahlen definiert. Zum jetzigen Zeitpunkt befinden sich die Konzepte zur Maschinenverarbeitbarkeit noch in einer frühen Phase der Entwicklung. Ein Whitepaper hierzu will es Ende des Jahres veröffentlichen. Eine stabile Version der Datenstruktur, die für die Maschinenverarbeitbarkeit notwendig ist, liege noch nicht vor. Hierzu führe das BSI Gespräche mit den Anwendern des IT-Grundschutzes und den Herstellern von IT-Grundschutz-Tools. Auch die Themen Messgrößen, Leistungszahlen und Zielgrößen entwickele es agil. Die Diskussionen hierzu seien noch nicht abgeschlossen. Inwieweit die Messgrößen, Leistungszahlen und Zielgrößen für die Bundesverwaltung geeignet seien, diskutierten die Beteiligten intensiv. Um dies abschließend beurteilen zu können, müsse der Reifegrad der entsprechenden Konzepte aber fortgeschrittener sein.

Für die beiden Themenkomplexe setze es derzeit jeweils zwei Beschäftigte ein. Zahlreiche Fachexpertinnen und Fachexperten des BSI würden diese zudem unterstützen.

Der Rechnungsprüfungsausschuss hatte das BMI erst im März 2024 aufgefordert,[32] mit Nachdruck darauf hinzuwirken, dass das BSI u. a. den IT-Grundschutz weiter vereinfacht und einen verbindlichen Zeitplan erstellt, bis wann es den reformierten Grundschutz veröffentlicht.

Würdigung

Eine Handreichung des BSI für die Personalbemessung im Bereich der Informations- und Cybersicherheit könnte dazu beitragen, dass alle Bundeseinrichtungen einheitliche Maßstäbe für die Personalbedarfsermittlung in diesem kritischen Bereich anwenden. Allerdings ist dies nur eine von vielen Arbeitshilfen des BSI. Dem BMI fehlt ein Überblick darüber, welche Arbeitshilfen das BSI bisher bereitgestellt hat und in welcher Weise diese den Aufwand für die Bundesverwaltung reduzieren. Insofern bleibt es in seinem Bericht unkonkret.

[32] 20. Sitzung des Rechnungsprüfungsausschusses vom 15. März 2024, Beschluss zu TOP 8.

Insgesamt steht das BSI mit der Reform des IT-Grundschutzes erst am Anfang eines langen, aufwändigen und komplexen Weges. Dies wird besonders an den geringen Fortschritten bei der Frage der Maschinenverarbeitbarkeit deutlich. Auch die Entwicklung von geeigneten Indikatoren, Messgrößen, Leistungszahlen und Zielgrößen[33] zur Informations- und Cybersicherheit ist noch nicht weit fortgeschritten. Bedauerlich ist, dass das BSI diese vielversprechende Entwicklung erst so spät begonnen hat und es voraussichtlich noch mehrere Jahre benötigen wird, um hierdurch die Informationssicherheit und deren Überwachung verstärkt automatisieren zu können. Ebenso vermisst der Bundesrechnungshof Erfolgskontrollen, mit denen das BSI nachhält, dass es seine Ziele wirtschaftlich erreicht. Angesichts der Einsparpotenziale, die eine stärkere Automatisierung des IT-Grundschutzes für die Bundesverwaltung verspricht, verwundert es, dass das BSI für diesen Ansatz nur vier Beschäftigte hauptamtlich einsetzt.

Das BMI hätte vom BSI zumindest einen Zeitplan für die geforderte Überarbeitung und Vereinfachung des IT-Grundschutzes einfordern und vorlegen sollen. Nun ist weiterhin unbestimmt, bis wann es die Reform des IT-Grundschutzes abschließen wird.

Empfehlung

Das BMI muss den IT-Grundschutz wie gefordert vereinfachen. Dazu sollte es einen verbindlichen Zeitplan vorlegen, bis wann das BSI den reformierten Grundschutz und dazu passende Arbeitshilfen veröffentlichen wird.

Wegen ihres großen Nutzens für die gesamte Bundesverwaltung sollte das BMI dafür Sorge tragen, dass das BSI die Handreichung zur Personalbedarfsbemessung im Bereich der Informations- und Cybersicherheit schnellstmöglich fertigstellt. Zudem sollte es sich einen Überblick über die vorhandenen Arbeitshilfen des BSI verschaffen.

Die Automatisierung des IT-Grundschutzes sollte das BSI mit Nachdruck vorantreiben und hierfür ausreichend Ressourcen bereitstellen. Das Regelwerk muss es in eine geeignete Datenstruktur überführen und messbare Zielgrößen festlegen. Durch Erfolgskontrollen muss das BSI sicherstellen, dass es das Ziel, den IT-Grundschutz zu vereinfachen und zu automatisieren, wirtschaftlich erreicht.

[33] Indikatoren zeigen Zustände oder Trends an.
Messgrößen liefern die konkreten Daten.
Leistungszahlen bewerten Effizienz oder Effektivität durch Verhältnisbildung.
Zielgrößen definieren angestrebte Ergebnisse oder Sollwerte.

7 Stellungnahme des BMI

Der Bundesrechnungshof hat dem BMI den Entwurf des Berichts zur Stellungnahme übersandt. Das BMI hat in seiner Antwort mitgeteilt, dass es von einer Stellungnahme absehe.

8 Fazit des Bundesrechnungshofes

Für die Vorhaben der Cybersicherheit ist weder für das Jahr 2025 noch in der mittelfristigen Finanzplanung die vom Haushaltsausschuss geforderte auskömmliche Finanzierung im Bundeshaushalt sichergestellt. Das BMI hat sich nicht mit dem nötigen Nachdruck dafür eingesetzt, dass die Ressorts Maßnahmen mit ressortübergreifender Bedeutung auch gemeinsam finanzieren. Insgesamt ist die Transparenz über die Lastenverteilung innerhalb der Bundesregierung und über die Wirkung der Cybersicherheitsmaßnahmen ungenügend. Hierfür fehlt ein geeignetes IT-Sicherheitscontrolling.

Die vorhandenen Ressourcen des BSI reichen derzeit nicht aus, um die erforderlichen Unterstützungs- und Kontrollaufgaben wahrzunehmen. Inwieweit die Umorganisation des BSI die gesetzten Ziele erreicht, ist offen.

Zusammenfassend hält es der Bundesrechnungshof für erforderlich, dass das BMI

- als federführendes Ressort die Maßnahmen zur Informations- und Cybersicherheit mit ressortübergreifender Relevanz hinreichend koordiniert,
- sich einen Überblick darüber verschafft, für welche Vorhaben der Cybersicherheit die Ressorts in welcher Höhe Haushaltsmittel in ihren Einzelplänen veranschlagt haben,
- auf dieser Grundlage gemeinsam mit den Ressorts ermittelt, wie hoch der etwaig verbleibende Finanzbedarf ist, um die für die Cybersicherheit prioritären Maßnahmen insbesondere der Nationalen Sicherheitsstrategie und der Cybersicherheitsstrategie sowie der Cybersicherheitsagenda umzusetzen,
- hierfür und für weitere Vorhaben von ressortübergreifender Relevanz ein Finanzierungsmodell für ein auskömmliches zentrales Budget ausarbeitet und unter Einbeziehung des BMF mit den Ressorts abstimmt und
- zügig ein Finanz- und Umsetzungscontrolling für die Maßnahmen der Informations- und Cybersicherheit als Teil des IT-Sicherheitscontrollings etabliert, um jederzeit zum Sachstand auskunftsfähig zu sein und etwaigen Nachsteuerungsbedarf frühzeitig selber identifizieren zu können.

Außerdem sollte das BMI darauf hinwirken, dass das BSI

- die begonnenen Maßnahmen im Bereich der Personalgewinnung, organisatorischen Neuaufstellung und fachlichen Stärkung der Eigensicherung der Bundesverwaltung vorantreibt und fortlaufend auf Anpassungsbedarf hin überprüft und

- die Maßgaben des Haushaltsausschusses vom 10. November 2022, insbesondere den Nachhalte-Mechanismus für die Mängel der geprüften Bundesbehörden, zügig und vollständig umsetzt.

Das BMI sollte den Haushaltsausschuss so rechtzeitig über den Sachstand zur Umsetzung dieser Maßgaben informieren, dass erforderlichenfalls ergänzende Maßgaben noch im Verfahren zur Aufstellung des Bundeshaushalts für das Jahr 2026 berücksichtigt werden können.

Essers Scherwa

Beglaubigt: Schmid, BPAss,
wegen elektronischer Bearbeitung ohne Unterschrift und Dienstsiegelabdruck.