BUNDESRECHNUNGSHOF

Bericht nach § 88 Absatz 2 BHO
an den Haushaltsausschuss des Deutschen Bundestages, den Innenausschuss des Deutschen Bundestages und den Ausschuss für Digitales und Staatsmodernisierung des Deutschen Bundestages

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

15. September 2025

Geschäftszeichen: VII 4 - 0002698/1

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

Umsetzung der NIS-2-Richtlinie nutzen, um Cyberresilienz zu stärken

Der vorliegende Gesetzentwurf erschwert in Zeiten akuter Bedrohungen die Resilienz Deutschlands im Cyberraum. Überhöhte Haushaltsmittelforderungen einzelner Ressorts dürfen nicht zu uneinheitlichen und lückenhaften nationalen Sicherheitsmaßnahmen führen. Wenige Änderungen am Gesetzentwurf könnten das Informationssicherheitsniveau in der Bundesverwaltung deutlich erhöhen und lange bekannte Cyber-Defizite beseitigen.

→ Worum geht es?

Deutschland muss die NIS-2-Richtlinie der Europäischen Union (EU) vom 14. Dezember 2022 in nationales Recht überführen. Diese soll ein hohes gemeinsames Cybersicherheitsniveau gewährleisten. Der Gesetzentwurf der Bundesregierung bleibt in zentralen Punkten hinter diesem Ziel zurück. Statt das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentrale Stelle zu stärken, werden dessen Befugnisse zur Abwehr von Gefahren im Cyberraum durch Ausnahmeregelungen für Bundesbehörden beschnitten. Das neue Amt der Koordinatorin oder des Koordinators für Informationssicherheit (CISO Bund) bleibt ohne nähere Angaben im Gesetzestext inhaltsleer. Zudem sind finanzielle und personalwirtschaftliche Auswirkungen des Gesetzes nicht sachgerecht ermittelt.

→ Was ist zu tun?

Das Gesetz muss den IT-Grundschutz des BSI für alle Einrichtungen der Bundesverwaltung verbindlich vorschreiben. Diesen sollte das BSI durchgängig kontrollieren dürfen. Das BSI muss im Einzelfall vorgesehenen Ausnahmen vom Anwendungsbereich des Gesetzes zustimmen. Der CISO Bund sollte ressortübergreifende Steuerungsbefugnisse erhalten. Bedarfe der Ressorts zur Umsetzung des Gesetzes sind kritisch zu hinterfragen.

→ Was ist das Ziel?

Das Gesetz schafft den Rahmen für ein hinreichendes, einheitliches Informationssicherheitsniveau. Jede Einrichtung der Bundesverwaltung weist dieses nach drei Jahren erstmalig und danach regelmäßig nach. Während das BSI die federführende Aufsichtsbehörde für Informations- und Cybersicherheit ist, steuert ein CISO Bund diese ressortübergreifend. Die Ressorts erhalten die für eine wirtschaftliche und effektive Umsetzung des Gesetzes erforderlichen Ressourcen.

Inhaltsverzeichnis

0 Zusammenfassung 7

1 Einleitung 14

1.1 Lage der Informations- und Cybersicherheit in Verwaltung und Wirtschaft 14

1.2 BSI-Gesetz 15

1.3 NIS-2-Richtlinie der Europäischen Union 16

1.4 Stellungnahmen des BWV zu den Referentenentwürfen 16

2 NIS-2-Umsetzung nachbessern, um Cybersicherheit im Bund zu stärken 18

2.1 IT-Grundschutz und Risikomanagement für die gesamte Bundesverwaltung gesetzlich verankern (Artikel 1, § 29 Absatz 2, § 44 Absatz 2 BSIG-E) 18

2.2 Ausnahmeregelungen für das Auswärtige Amt begrenzen und Parallelstrukturen verhindern (Artikel 1, §§ 7 Absatz 6, 29 Absatz 3 und 44 Absatz 1 BSIG-E) 22

2.3 Bundesverwaltung auf das Regelungsregime verpflichten und Ausnahmeregelungen der Ressorts beschränken (Artikel 1, § 46 Absatz 5 BSIG-E) 25

2.4 Einrichtungen der Bundesverwaltung bei Nachweisen nicht bevorteilen (Artikel 1, § 43 Absatz 1 BSIG-E) 26

2.5 Informationssicherheit als Verantwortung der Leitungsebene festlegen (Artikel 1, § 43 Absatz 1 Satz 1 BSIG-E) 28

2.6 Rolle und Befugnisse der Koordinatorin oder des Koordinators für Informationssicherheit gesetzlich festlegen (Artikel 1, § 48 BSIG-E) 29

2.7 Mit weiteren Änderungen Befugnisse des BSI stärken 32

3 Haushaltsausgaben und Erfüllungsaufwand der Bundesverwaltung kritisch hinterfragen 34

4 Bisherige Regelungen überprüfen, Evaluation des neuen Gesetzes vorsehen 36

5 Fazit des Bundesrechnungshofes 42

Abkürzungsverzeichnis

A

AA *Auswärtiges Amt*

B

BKAmt *Bundeskanzleramt*
BKG *Bundesamt für Kartographie und Geodäsie*
BMDS *Bundesministerium für Digitales und Staatsmodernisierung*
BMI *Bundesministerium des Innern*
BNetzA *Bundesnetzagentur*
BSI *Bundesamt für Sicherheit in der Informationstechnik*
BSIG *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)*
BWV *Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung*

C

CISO *Chief Information Security Officer*
CRA *Cyber Resilience Act*
CSA *Cyber Security Act*

D

Digitalausschuss *Ausschuss für Digitales und Staatsmodernisierung des Deutschen Bundestages*

E

EnWG *Energiewirtschaftsgesetz*
EU *Europäische Union*

H

Haushaltsausschuss *Haushaltsausschuss des Deutschen Bundestages*

I

Innenausschuss *Innenausschuss des Deutschen Bundestages*
ISB *Informationssicherheitsbeauftragte/r*
IS-Controlling *Informationssicherheitscontrolling*
ISM *Informationssicherheitsmanagement*
IS-Revisionen *Informationssicherheitsrevisionen*
IT-SiG 2.0 *IT-Sicherheitsgesetz 2.0*
ITZBund *Informationstechnikzentrum Bund*

K

KRITIS *Kritische Infrastruktur*

KRITIS-Betreiber *Betreiber Kritischer Infrastrukturen*

L

LÜKEX 23 *Länder- und Ressortübergreifende Krisenmanagementübung (Exercise)*

N

NIS-2-Richtlinie *Zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit*

NIS2UmsuCG *NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz*

NKR *Nationaler Normenkontrollrat*

S

StBA *Statistisches Bundesamt*

U

UP Bund 2017 *Umsetzungsplan Bund 2017*

V

VSA *Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz; Verschlusssachenanweisung*

0 Zusammenfassung

0.1

Die Europäische Union verabschiedete am 14. Dezember 2022 die NIS-2-Richtlinie, um mit dieser die Cybersicherheit in allen Mitgliedstaaten zu stärken. Deutschland war verpflichtet, diese Richtlinie bis zum 17. Oktober 2024 in nationales Recht umzusetzen. Dies ist in der letzten Legislaturperiode nicht gelungen. In der Folge hat die Europäische Union ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet.[1] Das Bundeskabinett hat am 30. Juli 2025 einen neuen Gesetzentwurf beschlossen und zur Beratung an den Deutschen Bundestag übersandt. Die Bundesregierung beabsichtigt mit dem Gesetz, den Ordnungsrahmen des IT-Sicherheitsgesetzes 2.0 (IT-SiG 2.0[2]) auf ca. 29 500 Unternehmen zu erweitern. Darüber hinaus will sie Anforderungen an das Informationssicherheitsmanagement (ISM) für die Bundesverwaltung gesetzlich festlegen. Begründend führt die Bundesregierung zum einen die verschärfte Sicherheitslage bedingt durch die geopolitische Situation an. Zum anderen hätten die bisherigen untergesetzlichen Regelungen nicht ausgereicht, die Informationssicherheit der Bundesverwaltung hinreichend zu verbessern. (Tzn. 1.1 bis 1.3)

0.2

In seiner Funktion als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung (BWV) hat der Präsident des Bundesrechnungshofes mehrfach ausführlich zu den Referentenentwürfen – zuletzt am 30. Juni 2025 – Stellung genommen. Dessen Hinweise und Anregungen hat das Bundesministerium des Innern (BMI) nicht oder nur unzureichend berücksichtigt. Der Bundesrechnungshof sieht es daher als geboten an, einzelne wichtige Hinweise dem Haushaltsausschuss des Deutschen Bundestages (Haushaltsausschuss), dem Innenausschuss des Deutschen Bundestages (Innenausschuss) sowie dem Ausschuss für Digitales und Staatsmodernisierung des Deutschen Bundestages (Digitalausschuss) zur Kenntnis zu geben. Der vorliegende Bericht enthält konkrete Änderungsvorschläge zum Regierungsentwurf.

Der Bundesrechnungshof hat dem BMI seine Änderungs- und Ergänzungsvorschläge zum Regierungsentwurf vorgelegt. Die Stellungnahme des BMI hat er im vorliegenden Bericht berücksichtigt. (Tz. 1.4)

[1] Veröffentlichung der Europäischen Kommission vom 7. Mai 2025, zuletzt abgerufen am 8. August 2025.
[2] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (BGBl. 2021 I S. 1 122).

0.3

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit dem IT-Grundschutz sowie seinen Mindeststandards grundlegende Regelwerke für die Informationssicherheit definiert. Im Jahr 2017 beschloss das Bundeskabinett den sogenannten Umsetzungsplan Bund 2017 (UP Bund 2017). Darin legte es diese Regelwerke für die Bundesverwaltung verbindlich fest. Die eng miteinander vernetzte Bundesverwaltung sollte hierdurch ein hinreichendes Sicherheitsniveau erreichen und aufrechterhalten. Die Bundesregierung hat zwischenzeitlich festgestellt, dass diese untergesetzliche Regelung nicht ausreicht. Die Bundesverwaltung hat das geforderte Sicherheitsniveau nicht flächendeckend erreicht oder nicht wirksam gesteigert. Statt alle Behörden als Konsequenz gesetzlich zur Umsetzung der Vorgaben zu verpflichten, beschränkt der Gesetzentwurf dies allein auf die Bundesministerien und das Bundeskanzleramt (BKAmt). Für eine vernetzte Bundesverwaltung, in der Gefahren für eine Einrichtung sich auf andere auswirken können, ist eine solche Beschränkung mit Risiken behaftet. Sie konterkariert das Ziel eines kohärenten Sicherheitsniveaus in der gesamten Bundesverwaltung und schwächt die Cyberresilienz in einem Kernbereich staatlichen Handelns.

Der Bundesrechnungshof hält es für dringend geboten, den IT-Grundschutz sowie die Maßnahmen des Risikomanagements für die gesamte Bundesverwaltung gesetzlich verbindlich festzulegen.

Das BMI hat hierzu nicht Stellung genommen. (Tz. 2.1)

0.4

Der Gesetzentwurf sieht vor, den Geschäftsbereich des Auswärtigen Amtes (AA) von zentralen Regelungen des Gesetzes auszunehmen. Das AA soll in eigener Zuständigkeit durch ergebnisäquivalente Maßnahmen die Informationssicherheit gewährleisten. Unter die Kontrolle des BSI soll es nicht fallen. Ein solches Vorgehen wäre allein für die Teile der Auslands-IT nachvollziehbar, die ausschließlich im Ausland operieren. Das AA betreibt nach eigenen Angaben einen Großteil der Auslands-IT jedoch aus inländischen Rechenzentren. Daher ist eine solche Ausnahme weder sachgerecht noch wirtschaftlich vertretbar. Die Auslands-IT des AA ist einer der zentralen IT-Dienstleister des Bundes. Sie muss auch deshalb denselben Vorgaben und Kontrollen unterliegen, wie die übrigen Teile der aus Bundeskanzleramt und Bundesministerien definierten Zentralregierung.[3]

Der Bundesrechnungshof empfiehlt, keine Ausnahme für das AA zu definieren oder diese auf den im Ausland befindlichen Teil seiner IT zu beschränken. Insbesondere sollte das Gesetz keine Doppelstrukturen für Kompetenzen und Fähigkeiten des AA neben dem BSI schaffen.

[3] Die Definition der Zentralregierung basiert auf Artikel 2 Absatz 2 Buchstabe f Ziffer i der NIS-2-Richtlinie der Europäischen Union.

Das BMI hat hierzu nicht Stellung genommen. (Tz. 2.2)

0.5

Die Informationssicherheitsbeauftragten (ISB) der Ressorts sollen die Befugnis erhalten, Einrichtungen ihres Ressorts ganz oder teilweise per Ausnahmebescheid von den Verpflichtungen des Gesetzes zu befreien. Die Ressort-ISB müssen sich hierzu mit dem BSI nur ins Benehmen setzen. Das BSI kann seiner Kernaufgabe, Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren, nicht gerecht werden, wenn es aus seiner Sicht nicht begründete Befreiungen von den hierfür maßgeblichen Vorgaben nicht verhindern kann.

Der Bundesrechnungshof hält es für erforderlich, diese Ausnahmen zu begrenzen und die Zustimmung des BSI vorzusehen, um ein einheitliches Sicherheitsniveau in der Bundesverwaltung zu erreichen und aufrecht zu erhalten.

Das BMI hat hierzu keine Stellungnahme abgegeben. (Tz. 2.3)

0.6

Der Gesetzentwurf verpflichtet tausende Unternehmen in Deutschland, dem BSI alle drei Jahre durch externe Prüfungen nachzuweisen, dass sie die Anforderungen der Informationssicherheit erfüllen. Demgegenüber sollen Einrichtungen der Bundesverwaltung den Status ihrer Informationssicherheit erstmals nach fünf Jahren in Form einer standardisierten Erklärung nachweisen. Im Anschluss ist kein festgelegter Turnus für weitere Erklärungen vorgesehen. Weder die längere Frist für den erstmaligen Nachweis, die unspezifizierte Frist für Folgenachweise noch der Verzicht auf Nachweise externer Prüfer tragen den bestehenden Risiken in der Informationssicherheit des Bundes hinreichend Rechnung.

Der Bundesrechnungshof empfiehlt, der Bundesverwaltung die gleichen Nachweispflichten wie den Unternehmen aufzuerlegen. Diese sollten ihren ersten qualifizierten Nachweis ebenfalls bereits nach drei Jahren und anschließend alle drei Jahre Folgenachweise erbringen.

Das BMI hat hierzu keine Stellungnahme abgegeben. (Tz. 2.4)

0.7

Informationssicherheit zu gewährleisten liegt in der Verantwortung der Leitungsebene. Diese hat die Umsetzung der dazu notwendigen Maßnahmen in ihrer Einrichtung zu veranlassen, zu überwachen und für die notwendigen Ressourcen zu sorgen. Sie trägt final alle Risiken, die sich aus der Informationssicherheit ergeben können. Der Gesetzentwurf bleibt hier für Einrichtungen der Bundesverwaltung hinter bestehenden untergesetzlichen Vorgaben

zurück. Danach soll die Leitung nur dafür verantwortlich sein, die Voraussetzungen zu schaffen, um die Informationssicherheit zu gewährleisten.

Der Bundesrechnungshof erwartet, dass die Leitungsebene nicht nur die Voraussetzungen schafft, sondern die Informationssicherheit auch verantwortet. Dies sollte das Gesetz deutlich zum Ausdruck bringen.

Das BMI hat hierzu keine Stellungnahme abgegeben. (Tz. 2.5)

0.8

Die Bundesregierung beabsichtigt, mit der oder dem CISO Bund eine neue Funktion in der Bundesverwaltung zu schaffen. Eine solche Funktion findet sich häufig in Wirtschaftsunternehmen oder auch anderen Staaten. Sie übernimmt Steuerungsaufgaben auf der obersten Leitungsebene. Die oder der CISO Bund soll dabei Anforderungen der Geschäftsprozesse, IT- und Informationssicherheit koordinieren. Sie oder er verantwortet die IT-Sicherheitsstrategie, sorgt für die notwendige Absicherung der IT-gestützten Geschäftsprozesse und das dafür erforderliche Schutzniveau. Der vorliegende Gesetzentwurf benennt jedoch für die oder den CISO Bund keinerlei Aufgaben, Pflichten oder Befugnisse. Im Ergebnis blieben so wesentliche Inhalte dieser Funktion, beispielsweise eine Berichtspflicht an das Parlament oder eine übergreifende Steuerung der Informationssicherheit in der Bundesverwaltung, der Gestaltung durch den Gesetzgeber entzogen.

Aus Sicht des Bundesrechnungshofes sollte der Gesetzgeber die wesentlichen Aufgaben, Pflichten und Befugnisse der oder des CISO Bund im Gesetz vorgeben. Diese sollten insbesondere darauf ausgerichtet sein, alle die Bundesverwaltung insgesamt betreffenden Fragestellungen und Maßnahmen der Informationssicherheit zu verantworten und zu steuern.

Das BMI hat sich in seiner Stellungnahme auf den Haushaltsausschuss gestützt, wonach dieser von der Bundesregierung ein Konzept, u. a. mit Vorschlägen zur Einrichtung einer oder eines CISO Bund, gefordert habe. Sofern das Gesetz diese Rolle nun ausgestalte, nähme es ein ressortgeeintes Konzept vorweg. Daher sei die Funktion der oder des CISO Bund im Gesetzentwurf nur allgemein eingeführt.

Der Bundesrechnungshof weist darauf hin, dass die Bundesregierung das vom Haushaltsausschuss im Februar 2024 geforderte Konzept bereits hätte erstellen können. Dass dies nicht geschah, wird der Bedrohungslage für die Bundesverwaltung nicht gerecht. Die oder der CISO Bund hat eine wichtige Funktion bei der übergreifenden Steuerung der Informations- und Cybersicherheit. Der Gesetzgeber sollte die Befugnisse der Funktion daher gesetzlich festlegen. Der Bundesrechnungshof hält an seinen Empfehlungen fest. (Tz. 2.6)

0.9

Die Bundesregierung beziffert die zusätzlichen Haushaltsausgaben im Gesetz für die Jahre 2026 bis 2029 auf über 900 Mio. Euro. Ursächlich sind im Wesentlichen der Bedarf von 1 276 zusätzlichen Planstellen und Stellen (im Folgenden Stellen) sowie die dadurch bedingten Personalausgaben. Die teilweise sehr unterschiedlichen Angaben der Ressorts lassen Zweifel aufkommen, inwieweit diese ihrem Mehrbedarf nur die neuen Aufgaben aus dem vorliegenden Gesetzentwurf zugrunde gelegt haben. Ein überhöht ausgewiesener Erfüllungsaufwand birgt das Risiko, Forderungen auszulösen, um strenge Vorgaben des Regelungsregimes durch das Gesetz für die Bundesverwaltung (weiter) aufzuweichen (vgl. Tzn. 2.1 und 2.4) und so vermeintlich Ausgaben senken zu können. Der BWV hatte das BMI daher frühzeitig auf das Erfordernis belastbarer Angaben hingewiesen. Ebenso hatte der Nationale Normenkontrollrat (NKR) dies bereits zum Gegenstand seiner letztjährigen Stellungnahme gemacht. Dennoch hat es das BMI versäumt, die Angaben der Ressorts auf der Grundlage eines einheitlichen Verständnisses für die wenigen neu hinzukommenden Aufgaben abzugleichen.

Der Bundesrechnungshof hält es für unbedingt erforderlich, strenge Vorgaben des Regelungsregimes zur Informationssicherheit für die Bundesverwaltung beizubehalten. Zudem sind nach Inkrafttreten des Gesetzes zu erwartende Stellen- und Ausgabenforderungen der Ressorts eingehend zu prüfen. Er weist ausdrücklich darauf hin, dass die von ihm vorgeschlagenen Änderungen am Gesetzestext nicht zu zusätzlichen Haushaltsausgaben führen.

Das BMI hat mitgeteilt, es habe mehrfach bei den Ressorts die zu erwartenden Aufwände abgefragt. Hierzu habe es zahlreiche Handreichungen und Anregungen bereitgestellt, um auf eine einheitliche Darstellung hinzuwirken. Aufgrund des Ressortprinzips habe das BMI jedoch keine Hoheit über die Meldungen der Ressorts. Es teile jedoch die Zweifel des Bundesrechnungshofes und erachte eine kritische Überprüfung der gemeldeten Mehraufwände ebenfalls für ratsam.

Der Bundesrechnungshof sieht sich in seiner Kritik bestätigt und empfiehlt daher nachdrücklich, die gemeldeten Aufwände zu prüfen und ressortübergreifend abzugleichen. (Tz. 3)

0.10

Der vorliegende Gesetzentwurf führt etwa 40 Regelungen des derzeitigen Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG) unverändert fort. Aufgrund der gesetzlichen Vorgabe[4] legte das BMI zum 1. Mai 2023 eine Evaluation der Normen des IT-SiG 2.0 für Kritische Infrastrukturen (KRITIS) und deren Auswirkungen auf Unternehmen vor. Die zum 1. Mai 2025 fällige Evaluation der übrigen Normen des BMI folgte verspätet zum 26. August 2025. Deren Aussagen sind jedoch aufgrund der gewählten Datenbasis und der zugrundeliegenden Bemessungsgrundlagen nur begrenzt tragfähig. So

[4] Vgl. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, Artikel 6 Absatz 1.

benennt das BMI zwar Mängel im bestehenden BSIG, hat diese im Gesetzentwurf jedoch nur an einer Stelle aufgegriffen. Der Bundesrechnungshof sieht besonders kritisch, dass der Evaluation Erkenntnisse fehlen, wie sich Regelungen des BSIG in der Zusammenarbeit mit Dritten auf die Arbeit des BSI und die Cybersicherheitsarchitektur insgesamt ausgewirkt haben.

Der Bundesrechnungshof empfiehlt daher, die Bundesregierung zu verpflichten, das neue Gesetz nach drei Jahren umfassend zu evaluieren und dem Deutschen Bundestag über die Erkenntnisse zu berichten.

Das BMI hat angegeben, der Gesetzentwurf erfülle bereits die Vorgaben des Evaluierungskonzeptes[5]. Es sei insbesondere klar vorgegeben, wer Ergebnisse einer Evaluation erhalten werde. Zudem sei entbehrlich, Kennzahlen für eine Evaluation im Gesetz festzulegen. Denn sonst würde der ergänzende Charakter der nationalen Evaluierung zu der auf europäischer Ebene erschwert. Auch sei eine umfassende Datengrundlage u. a. wegen der vorgesehenen Meldepflichten gegeben. Eine gesetzliche Evaluierungspflicht erachtet das BMI insofern als nicht sachgerecht. Auch das Evaluierungskonzept der Bundesregierung erfordere dies nicht. Das BMI verweist darüber hinaus auf die besondere Dynamik des Rechtsgebietes, bei dem gewisse Unsicherheiten inbegriffen seien.

Die Stellungnahme des BMI überzeugt den Bundesrechnungshof nicht. Dessen Prüfungserkenntnisse zeigen, dass der Bundesregierung die erforderlichen Daten zur Effektivität und Effizienz des Verwaltungshandelns bei der Umsetzung des IT-SiG 2.0 fehlen. So musste das BMI in seinem eigenen Evaluationsbericht zum IT-SiG 2.0 eine schwierige Datenlage einräumen, bei der es nur rückblickend mit verfügbaren Daten und einem daran angelehnten Kennzahlsystem arbeiten konnte. Auch die nun vom Gesetzentwurf vorgesehenen Meldepflichten liefern nicht ausreichend Daten, um diese Lücke zu schließen. Warum des Weiteren die Dynamik des IT-Sicherheitsrechts einer Evaluation entgegensteht, erschließt sich dem Bundesrechnungshof nicht. Er bleibt daher bei seiner Empfehlung. (Tz. 4)

0.11

Das BMI äußerte sich in seiner Stellungnahme zu folgenden Textziffern nicht:

- *IT-Grundschutz und Maßnahmen für die gesamte Bundesverwaltung gesetzlich verankern,*
- *Weitreichende Ausnahmeregelungen für Einrichtungen der Bundesverwaltung beschränken,*
- *Nachweise der Informationssicherheit in kürzeren Fristen für die Einrichtungen der Bundesverwaltung vorsehen und*
- *Verantwortung der Einrichtungsleitung für die Informationssicherheit festhalten.*

Der Bundesrechnungshof geht insofern davon aus, dass das BMI seinen Empfehlungen zu diesen Textziffern nicht widerspricht.

[5] Auf Grundlage des vom Staatssekretärsausschuss für Bessere Rechtsetzung und Bürokratieabbau beschlossenen Evaluierungskonzeptes vom 23. Januar 2013 und 26. November 2022.

Die zu den übrigen Textziffern vorgetragenen Argumente des BMI haben den Bundesrechnungshof nicht überzeugt. Er bleibt daher bei seinen Änderungs- und Ergänzungsvorschlägen für den Gesetzentwurf.

1 Einleitung

Die NIS-2-Richtlinie ist am 14. Dezember 2022 in Kraft getreten und war bis zum 17. Oktober 2024 von den EU-Mitgliedstaaten in nationales Recht umzusetzen. Dies ist der Bundesrepublik Deutschland in der letzten Legislaturperiode nicht gelungen. Zu dem Gesetzentwurf der früheren Bundesregierung[6] hatte der Bundesrechnungshof den Haushaltsausschuss und den Innenausschuss im September 2024 informiert und Änderungen angeregt.[7]

Am 30. Juli 2025 hat die aktuelle Bundesregierung einen neuen Gesetzentwurf beschlossen und im August 2025 dem Deutschen Bundestag zugeleitet.[8] Zuvor hatte der Präsident des Bundesrechnungshofes in seiner Rolle als BWV hierzu Stellung genommen. Wesentliche Empfehlungen des BWV hat das BMI im Kabinettentwurf nicht aufgegriffen. Der Gesetzentwurf bleibt aus Sicht des BWV und des Bundesrechnungshofes weiterhin hinter den gesteckten Zielen, ein einheitliches Cybersicherheitsniveau zu schaffen, zurück. Der Bundesrechnungshof informiert daher erneut mit diesem Bericht nach § 88 Absatz 2 BHO den Haushaltsausschuss, den Innenausschuss und den Digitalausschuss über die aus seiner Sicht gebotenen Änderungen.

1.1 Lage der Informations- und Cybersicherheit in Verwaltung und Wirtschaft

Die Lage der IT-Sicherheit in Deutschland ist nach Einschätzung des BSI besorgniserregend.[9] Die enorm wachsende Zahl an Cyberangriffen und die zunehmende Professionalisierung von Cyberkriminellen stellen Unternehmen und Verwaltung vor große Herausforderungen. Hinzu kommen die zunehmenden geopolitischen Spannungen. Deutschland ist verstärkt Ziel hybrider Angriffe.[10] Allein der deutschen Wirtschaft entstehen nach Darstellung des Branchenverbandes BITKOM[11] durch Cyberattacken jährlich Schäden von 179 Milliarden Euro. Zwei Drittel der Unternehmen sehen ihre Existenz durch einen erfolgreichen Cyberangriff bedroht.[12] Auch die Bundesverwaltung muss bestehende Mängel bei der Absicherung ihrer IT-Systeme und Netze zügig

[6] Bundestagsdrucksache 20/13184 vom 2. Oktober 2024, zuletzt abgerufen am 4. August 2025.
[7] Bericht nach § 88 Absatz 2 BHO an den Haushaltsausschuss und an den Innenausschuss - 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) vom 17. September 2024, Gz.: VII4-0002698.
[8] Bundestagsdrucksache 21/1501 vom 8. September 2025, zuletzt abgerufen am 9. September 2025
[9] Die Lage der IT-Sicherheit in Deutschland 2024, Hrsg.: BSI, Seite 7.
[10] Beispielsweise Drohnen über Militärstützpunkten und kritischer Infrastruktur, sabotierte Unterseekabel in der Ostsee.
[11] Bitkom e. V. (Bitkom; vormals *Bundesverband Informationswirtschaft, Telekommunikation und neue Medien*) ist der Branchenverband der deutschen Informations- und Telekommunikationsbranche.
[12] Pressemitteilung der BITKOM vom 12. November 2024, zuletzt abgerufen am 4. August 2025.

beseitigen. Folge der fortschreitenden Digitalisierung ist, dass sich staatliche Kernfunktionen ohne resiliente Rechenzentren und sichere Netzinfrastrukturen – erst recht in Krisensituationen – nicht aufrechterhalten lassen. Handlungsbedarf hat hier zuletzt die Länder- und Ressortübergreifende Krisenmanagementübung zum Thema „Cyberangriff auf das Regierungshandeln“ (LÜKEX 23) deutlich aufgezeigt.[13]

Um mit der Cybersicherheit weitere Elemente der Verteidigungsfähigkeit Deutschlands zu stärken und hierfür erforderliche Mittel leichter bereitstellen zu können, hat der Deutsche Bundestag im März 2025 u. a. für den „Schutz der informationstechnischen Systeme“ eine sogenannte Bereichsausnahme definiert. Entsprechende Ausgaben sind von der Kreditobergrenze der Schuldenbremse ausgenommen, wenn sie zusammen mit den Ausgaben in weiteren Bereichsausnahmen 1 % des nominalen Bruttoinlandsproduktes übersteigen.[14]

1.2 BSI-Gesetz

Vorgaben für die Informationssicherheit sind in zahlreichen Gesetzen zu finden.[15] Von zentraler Bedeutung ist das BSIG. Dieses hat der Gesetzgeber zuletzt im Jahr 2021 mit dem IT-SiG 2.0 umfassend novelliert. Darin festgelegte weitere Prüf- und Kontrollbefugnisse des BSI und dessen Vorgabe von Mindeststandards sollen den Schutz der IT der Bundesverwaltung erhöhen. Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber) und weitere Unternehmen im besonderen öffentlichen Interesse haben seitdem zusätzliche Pflichten[16] zu erfüllen. Für diese zusätzlichen Aufgaben und Befugnisse wies das IT-SiG 2.0 einen Mehrbedarf des BSI von 799 Stellen aus.

Tatsächlich erhielt das BSI nur 232 Stellen. Nach eigenen Angaben kann es seine neuen Aufgaben nach dem IT-SiG 2.0 nur rudimentär wahrnehmen.

Der Deutsche Bundestag verpflichtete das BMI, die Wirksamkeit der im IT-SiG 2.0 enthaltenen Maßnahmen bis zum 1. Mai 2025 zu evaluieren und ihm über die Ergebnisse zu berichten.[17] Das BMI hat diese Evaluierung beim Statistischen Bundesamt (StBA) und beim BSI im Februar 2025 beauftragt. Der vorliegende Gesetzentwurf lässt nicht erkennen, ob und in welcher Form die Bundesregierung etwaige Ergebnisse dieser Evaluierung darin berücksichtigt hat.

[13] Auswertungsbericht LÜKEX 23 vom 6. Juni 2024, Hrsg.: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; zuletzt abgerufen am 7. August 2025.
[14] Artikel 115 Absatz 2 Satz 4 Grundgesetz.
[15] So enthalten beispielsweise das Energiewirtschafts- und das Telekommunikationsgesetz umfangreiche Vorgaben für die Betreiber kritischer Anlagen in diesen Sektoren.
[16] Hierzu gehören u. a. Meldepflichten von Störungen, die Registrierung als KRITIS-Betreiber oder der Einsatz von Systemen zur Angriffserkennung.
[17] Artikel 6 Absatz 1 Nummer 2 IT-SiG 2.0.

1.3 NIS-2-Richtlinie der Europäischen Union

Die NIS-2-Richtlinie entwickelt die (erste) NIS-Richtlinie aus dem Jahr 2016 weiter und soll in der gesamten Europäischen Union ein hohes gemeinsames Cybersicherheitsniveau sicherstellen, um

- → die Anfälligkeit der EU-Mitgliedstaaten gegenüber Cyberbedrohungen zu senken und
- → einer Fragmentierung des Binnenmarktes als Folge national bislang uneinheitlich umgesetzter Cybersicherheitsvorgaben entgegenzuwirken.

Dazu sollen strengere Cybersicherheitsmaßnahmen, Meldepflichten für Sicherheitsvorfälle und eine verbesserte Zusammenarbeit zwischen den EU-Mitgliedstaaten beitragen.

Die EU-Kommission wird gemäß Artikel 40 der NIS-2-Richtlinie deren Umsetzung zum 17. Oktober 2027 und danach regelmäßig alle 36 Monate evaluieren und dem Europäischen Parlament sowie dem EU-Rat berichten.

Die NIS-2-Richtlinie steht im Zusammenhang mit weiteren gesetzlichen Vorgaben, die die Europäische Union in Form von Verordnungen beschlossen hat oder in Kürze beschließen will. Dazu zählen beispielsweise Regelungen für einen EU-weiten Rahmen

- → für die Zertifizierung von Sicherheitsmaßnahmen (Cyber Security Act, CSA[18]),
- → zur Regulierung des Finanzsektors hinsichtlich der Cybersicherheit (DORA-Verordnung[19]) sowie
- → zur Sicherheit von Produkten mit digitalen Elementen (Cyber Resilience Act, CRA[20]).

1.4 Stellungnahmen des BWV zu den Referentenentwürfen

Gemäß § 45 Absatz 3 Satz 2 Gemeinsame Geschäftsordnung der Bundesministerien (GGO)[21] beteiligte das BMI den Präsidenten des Bundesrechnungshofes in dessen Funktion als BWV bei dem vorliegenden Gesetzesvorhaben. Dessen Aufgabe ist es, auf ein wirtschaftliches Handeln und eine effiziente Organisation der Bundesverwaltung hinzuwirken. Dieser nahm sowohl in der abgelaufenen als auch in der laufenden

[18] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik.

[19] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nummer 1060/2009, (EU) Nummer 648/2012, (EU) 600/2014, (EU) 909/2014 und (EU) 2016/1011.

[20] Das Europäische Parlament hat den CRA im März 2024 verabschiedet. Das Europäische Parlament und der Europäische Rat haben am 23. Oktober 2024 zugestimmt. Die Veröffentlichung erfolgte am 22. November 2024 im Amtsblatt der Europäischen Union.

[21] GGO vom 1. September 2000, zuletzt geändert durch Beschluss der Bundesregierung vom 1. Juni 2024.

Legislaturperiode umfangreich zu den verschiedenen Referentenentwürfen Stellung – zuletzt am 30. Juni 2025. Das BMI griff nur einzelne Hinweise[22] des BWV auf.

§ 51 Nummer 4 GGO gibt vor, im Anschreiben zur Kabinettvorlage unbeschadet des § 22 GGO anzugeben, welche abweichenden Meinungen aufgrund der Beteiligungen nach den §§ 45 und 47 GGO bestehen. Dabei ist unerheblich, ob das BMI als federführendes Bundesministerium diese Meinungen als sachdienlich einschätzt oder nicht. Sowohl in der Übersendung der Kabinettvorlage[23] am 23. Juli 2024 an das Bundeskanzleramt als auch in der Vorlage[24] am 28. Juli 2025 hat es das BMI unterlassen, auf die vom BWV eingebrachten Kritikpunkte hinzuweisen. Der Bundesrechnungshof und der BWV missbilligen diesen erneuten Verstoß gegen die GGO ausdrücklich.

1.4.1 Stellungnahme des BMI

Das BMI hat mitgeteilt, dass die Kabinettvorlage sämtliche Anforderungen der GGO erfüllt habe. Es habe darin allgemeingültig formuliert, dass es Stellungnahmen und Anregungen nach Möglichkeit berücksichtigt habe, sofern diese sachdienlich waren.

1.4.2 Abschließende Bewertung des Bundesrechnungshofes

§ 51 Satz 4 GGO gibt vor, dass in Anschreiben von Kabinettvorlagen – unbeschadet des § 22 GGO – anzugeben ist, welche abweichenden Meinungen aufgrund der Beteiligungen nach den §§ 45 und 47 GGO bestehen. Ob das BMI diese als sachdienlich einschätzt, ist unerheblich. Der BWV hat auf ein wirtschaftliches Handeln der Bundesverwaltung hinzuwirken. Die Maßstäbe, anhand derer Ressorts und der BWV beurteilen, ob gesetzliche Regelungen sachdienlich und wirtschaftlich sind, unterscheiden sich naturgemäß. Insofern hätte das BMI die Bundesregierung über die abweichende Auffassung des BWV informieren müssen.

[22] Der BWV hat 38 Hinweise an das BMI formuliert.
[23] Kabinettsache des BMI CI1.17002/41#24 vom 23. Juli 2024.
[24] Kabinettsache des BMI CI1.17002/41#28 vom 28. Juli 2025.

2 NIS-2-Umsetzung nachbessern, um Cybersicherheit im Bund zu stärken

2.1 IT-Grundschutz und Risikomanagement für die gesamte Bundesverwaltung gesetzlich verankern (Artikel 1 § 29 Absatz 2 § 44 Absatz 2 BSIG-E)

Einrichtungen der Bundesverwaltung setzen Vorgaben der Informationssicherheit nicht ausreichend um

Das BSI ist Herausgeber des Regelwerkes „IT-Grundschutz“ und schreibt dieses fort. Der IT-Grundschutz umfasst technische, infrastrukturelle, organisatorische und personelle Aspekte der Informationssicherheit.

Das Bundeskabinett verabschiedete im Jahr 2017 den UP Bund 2017 und erklärte diesen für die Einrichtungen der Bundesverwaltung als verbindlich.[25] Nach den Vorgaben des UP Bund 2017 ist der IT-Grundschutz[26] als Mindestanforderung für alle Bundesbehörden verpflichtend umzusetzen.

Die Bundesregierung stellt in der Begründung des Gesetzentwurfs jedoch fest, dass sich „die bisherigen Steuerungsinstrumente auf überwiegend untergesetzlicher Basis (etwa Umsetzungsplan Bund) […] nicht als ausreichend effektiv erwiesen [haben], um eine flächendeckende wirksame Steigerung des Sicherheitsniveaus zu erreichen“.[27] Aktuelle Prüfungserkenntnisse des Bundesrechnungshofes stützen diese Aussage.[28] Einrichtungen der Bundesverwaltung kommen ihrer untergesetzlichen Verpflichtung auch acht Jahre nach dem Kabinettbeschluss nicht ausreichend nach. Als eine Gesetzesfolge erwartet die Bundesregierung, dass „[…] durch die gesetzliche Verankerung bisheriger untergesetzlicher Regelungen des Informationssicherheitsmanagements die IT-Sicherheit der öffentlichen Bundesverwaltung weiter gestärkt werden [wird]“.[29]

[25] Ausnahmen hiervon sind im Geschäftsbereich des Bundesministeriums der Verteidigung sowie bei den Nachrichtendiensten des Bundes möglich.

[26] Der IT-Grundschutz definiert im Standard BSI-200-2 die Abstufungen Basis-, Standard- und Kern-Absicherung, um je nach Schutzbedarf der jeweiligen IT-Systeme notwendige Maßnahmen zu ergreifen. Einrichtungen der Bundesverwaltung müssen die Standard-Absicherung umsetzen.

[27] Gesetzentwurf, Problem und Ziel, S. 2; Begründung des Gesetzentwurfes, Allgemeiner Teil, Abschnitt I „Zielsetzung und Notwendigkeit der Regelungen“, S. 107; Zu § 29 (Einrichtungen der Bundesverwaltung), S. 164.

[28] Bericht des Bundesrechnungshofes nach § 88 Absatz 2 BHO an den Haushaltsausschuss „Vorhaben der Cybersicherheit“, Gz.: VII 4 - 0000583/III, vom 16. Oktober 2024.

[29] Gesetzentwurf, Kapitel VI. Gesetzesfolgen, 1. Rechts- und Verwaltungsvereinfachung, S. 110.

Gesetzentwurf führt zu Zwei-Klassen-Informationssicherheit

Der Gesetzentwurf sieht in § 44 Absatz 2 BSIG-E vor, nur das BKAmt und die Bundesministerien zu verpflichten, den IT-Grundschutz einzuhalten. Für die übrigen Einrichtungen der Bundesverwaltung bestünde diese Verpflichtung weiterhin nur auf Grundlage des Kabinettbeschlusses zum UP Bund 2017.

Zwar fordert die NIS-2-Richtlinie, nur die im nationalen Recht definierten Einrichtungen der Zentralregierung als „besonders wichtige Einrichtungen" zu definieren.[30,31] „Um auf Bundesebene auch vor dem Hintergrund von Verflechtung und Konsolidierung der IT insgesamt ein gemeinsames, kohärentes und handhabbares Regime zu erreichen", beabsichtigt die Bundesregierung, über diese Vorgabe hinauszugehen.[32] So finden die Regelungen für besonders wichtige Einrichtungen grundsätzlich für alle Einrichtungen der Bundesverwaltung Anwendung (Generalklausel in § 29 Absatz 2 BSIG-E).

Die zentrale Norm des BSIG-E zur Informationssicherheit findet sich in § 30. Diese listet Risikomanagementmaßnahmen auf und legt grundlegende Anforderungen fest. § 30 BSIG-E soll in Deutschland für ca. 29 500 Unternehmen – und zwar unabhängig davon, ob diese „besonders wichtig" oder (nur) „wichtig" sind – gelten, nicht jedoch für die weit überwiegende Mehrzahl der Einrichtungen der Bundesverwaltung. Mit Ausnahme der Bundesministerien und des BKAmtes nimmt § 29 Absatz 2 Satz 2 BSIG-E diese von der Verpflichtung des § 30 BSIG-E aus. Den von ihr damit verfolgten Zweck und die beabsichtigte Wirkung erläutert die Bundesregierung in der Gesetzesbegründung nicht.

Gesetz schafft weitreichende Ausnahmen statt einheitliches Sicherheitsniveau

Die weitgehenden Ausnahmen von den gesetzlichen Verpflichtungen laufen dem ausdrücklichen Ziel der Bundesregierung, das Sicherheitsniveau in der Bundesverwaltung flächendeckend wirksam zu steigern, zuwider. Ein uneinheitliches Regelungsregime für die Bundesverwaltung ist aus mehreren Gründen nicht nachvollziehbar und nicht sachgerecht.

In der Gesetzesbegründung weist die Bundesregierung selbst auf sogenannte „Verbundrisiken" hin. Sobald ein Cyberangriff Systeme einer Bundeseinrichtung kompromittiert, wäre dies wegen der Vernetzung auch ein Risiko für alle übrigen Einrichtungen des Bundes. Die IT-Konsolidierung des Bundes und die zunehmend stärkere Verflechtung aller Bundeseinrichtungen erfordert es, den gemeinsamen Informationsverbund einheitlich zu schützen. Dem entgegen steht der im Gesetzentwurf gewählte

[30] Gemäß Artikel 2 Absatz 2 Buchstabe f Ziffer i der NIS-2-Richtlinie.
[31] Laut der Gesetzesbegründung in Teil A, Ziffer V liegt für den Begriff „Zentralregierung" die deutsche Definition der „zentralen Regierungsbehörden" zugrunde. Hierzu zählen das BKAmt und die Bundesministerien ohne ihre jeweiligen nachgeordneten Bereiche.
[32] Vgl. Gesetzesbegründung Teil B „Besonderer Teil" zu § 29 (Einrichtungen der Bundesverwaltung), S. 165.

Ansatz, gesetzlich nur einen kleinen Teil der Bundesverwaltung zur Umsetzung des IT-Grundschutzes zu verpflichten.

Bundesministerien müssten höhere Anforderungen an die Informationssicherheit und das Risikomanagement erfüllen als nachgeordnete Sicherheitsbehörden wie die Bundespolizei, die Zollverwaltung oder das Bundeskriminalamt. Dabei sind gerade die nachgeordneten Fachbehörden mit ihren Aufgaben – insbesondere in Krisen- oder Katastrophenfällen – mögliche Ziele für Angreifer. Der erfolgreiche Cyberangriff auf das Bundesamt für Kartographie und Geodäsie (BKG) zeigt sehr deutlich, dass Angreifer um die Bedeutung der nachgeordneten Behörden wissen.[33] Da nachgeordnete Behörden – wie das BKG – wichtige Dienstleistungen für KRITIS-Sektoren erbringen,[34] müssen auch diese sich entsprechend absichern und Vorkehrungen für ihre Informationssicherheit treffen. Das BSIG-E sollte sie dazu verpflichten.

Unternehmen, die als wichtige oder besonders wichtige Einrichtungen gelten, werden gegenüber der Verwaltung schlechter gestellt. Bereits Unternehmen ab 50 Beschäftigten[35] müssten die Anforderungen des § 30 BSIG-E umsetzen. Für die Zollverwaltung oder andere nachgeordnete Bundesbehörden mit mehreren Tausend Beschäftigten sollen diese hingegen nicht gelten. Dies wird der Bereitschaft von Unternehmen, den gesetzlichen Regelungen nachzukommen, nicht förderlich sein. Zudem werden gerade Einrichtungen der Bundesverwaltung ihrer Vorbildrolle durch eine solche Ausnahme nicht gerecht.

Der Bundesrechnungshof steht mit dieser Kritik nicht allein. Sachverständige wiesen bei der Anhörung zum ersten Regierungsentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes am 4. November 2024 ebenfalls auf die negativen Konsequenzen hin, Vorgaben zur Informationssicherheit nicht einheitlich, verbindlich und zentral festzuschreiben.[36]

Mit Blick auf etwaige zusätzliche Ausgaben oder Stellenbedarfe weist der Bundesrechnungshof darauf hin, dass der IT-Grundschutz bereits seit dem Jahr 2017 von den Einrichtungen der Bundesverwaltung umzusetzen ist. Ein Mehrbedarf an Haushaltsmitteln ließe sich aus einer gesetzlichen Verankerung dieser bereits geltenden Verpflichtung daher nicht ableiten.

Der Bundesrechnungshof empfiehlt, den IT-Grundschutz für alle Einrichtungen der Bundesverwaltung per Gesetz verbindlich zu machen. Zudem sollte die gesamte Bundesverwaltung verpflichtet sein, die Anforderungen an das Risikomanagement gemäß § 30 BSIG-E umzusetzen. Der Bundesrechnungshof regt daher für die §§ 29 und 44 BSIG-E folgende Änderungen an:

[33] Siehe Pressemitteilung des BMI vom 31. Juli 2024, zuletzt abgerufen am 4. August 2025.
[34] Im Falle des BKG betrifft dies die Bereiche Verkehr, Katastrophenvorsorge, Innere Sicherheit und Energieversorgung.
[35] Vgl. § 28 Absatz 2 Nummer 3 BSIG-E. Unternehmen bestimmter Einrichtungsarten können schon ab 50 Beschäftigten als wichtige Einrichtung gelten.
[36] Wortprotokoll der 90. Sitzung des Ausschusses für Inneres und Heimat, zuletzt abgerufen am 4. August 2025.

Artikel 1 § 29 Absatz 2 BSIG-E

Für Einrichtungen der Bundesverwaltung sind die Regelungen für besonders wichtige Einrichtungen anzuwenden, nicht jedoch die Regelungen der §§ 38, 40 Absatz 3 und der §§ 61 und 65. ~~Für Einrichtungen der Bundesverwaltung, ausgenommen das Bundeskanzleramt und die Bundesministerien, sind zusätzlich die Regelungen des § 30 nicht anzuwenden.~~

Artikel 1 § 44 Absatz 2 BSIG-E

~~Das Bundeskanzleramt und die Bundesministerien~~ Die Einrichtungen der Bundesverwaltung müssen als zusätzliche Mindestanforderungen die BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) in den jeweils geltenden Fassungen einhalten.

2.1.1 Stellungnahme des BMI

Zu diesem Punkt hat das BMI nicht Stellung genommen.

2.1.2 Abschließende Bewertung des Bundesrechnungshofes

Der Bundesrechnungshof geht daher davon aus, dass es der Zielsetzung, den IT-Grundschutz und die Maßnahmen zum Risikomanagement für die gesamte Bundesverwaltung gesetzlich zu verankern, nicht widerspricht.

Der Bundesrechnungshof sieht sich insofern in seinen Empfehlungen bestätigt.

2.2 Ausnahmeregelungen für das Auswärtige Amt begrenzen und Parallelstrukturen verhindern (Artikel 1 §§ 7 Absatz 6, 29 Absatz 3 und 44 Absatz 1 BSIG-E)

Die Auslands-IT wird einem einheitlichen Regelungsregime entzogen und eine bedenkliche Ausnahme in der Zentralregierung geschaffen

Gemäß § 7 Absatz 6 BSIG-E ist die Kommunikations- und Informationstechnik der Auslands-IT der Kontrolle des BSI entzogen, wenn diese „im Ausland belegen ist oder für das Ausland oder für Anwender im Ausland betrieben wird“. Das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) soll mit dem Auswärtigen Amt (AA) in einer Verwaltungsvereinbarung die Details hierzu festlegen. Der vorliegende Gesetzentwurf streicht den in § 4a Absatz 5 BSIG bislang geltenden Zusatz „ausschließlich“ und schränkt die Kontrollfunktion des BSI somit weiter ein.

Des Weiteren soll gemäß § 29 Absatz 3 BSIG-E der gesamte Geschäftsbereich des AA von weiteren Regelungen des BSIG ausgenommen werden. Im Einvernehmen sollen das BMDS und das AA hierzu lediglich über eine Verwaltungsvorschrift sicherstellen, dass das AA in seinem Geschäftsbereich „ergebnisäquivalente Maßnahmen“ umsetzt, um die Ziele der NIS-2-Richtlinie zu erreichen. Darüber hinaus soll die Auslands-IT des AA gemäß § 44 Absatz 1 Satz 5 und Absatz 2 Satz 5 BSIG-E von der Pflicht zur Anwendung der Mindeststandards und des IT-Grundschutzes ebenfalls befreit werden.

Der Bundesrechnungshof hält diese sehr weitreichenden Ausnahmen für bedenklich. Sie gehen weit über die aktuell gültigen Vorgaben des § 4a Absatz 5 BSIG hinaus. Dabei ist die Auslands-IT einer der zentralen IT-Dienstleister des Bundes, der auch im Inland kritische Dienstleistungen für Einrichtungen der Bundesverwaltung erbringt. Insofern erschließen sich für den Bundesrechnungshof folgende Punkte nicht:

→ Als Begründung für die Ausnahmeregelungen für das AA führt die Bundesregierung den Erwägungsgrund 8 der NIS-2-Richtlinie an. Demnach gelte diese „nicht für diplomatische und konsularische Vertretungen der Mitgliedstaaten in Drittländern oder für deren Netz- und Informationssysteme, sofern sich diese Systeme in den Räumlichkeiten der Mission befinden oder für Nutzer in einem Drittland betrieben werden“. Diese Begründung reicht jedoch nicht dafür aus, das Wort „ausschließlich“ in § 7 Absatz 6 BSIG-E zu streichen. Denn das AA ist über seine Auslandsvertretungen mit vielen unterschiedlichen örtlichen Gegebenheiten konfrontiert und gerade die exponierten Zugangspunkte im Ausland stellen eine erhebliche Gefahr für die Informationssicherheit dar. Diese können sich auch auf die übrigen Einrichtungen der Bundesverwaltung

auswirken, mit denen das AA vernetzt ist. Unmittelbare Konsequenzen für die gesamte Bundesverwaltung sind also nicht auszuschließen.

- → § 8 Absatz 1 BSIG verpflichtet das AA bereits seit dem Jahr 2015, die Mindeststandards des BSI einzuhalten. Das AA nunmehr aus dieser Verpflichtung herauszunehmen, ist weder sachgerecht noch nachvollziehbar. Das AA hätte gemäß § 44 Absatz 1 Satz 3 BSIG-E sogar die Möglichkeit, für die Auslandsvertretungen durch sachlich gerechtfertigte Gründe von den Mindeststandards abzuweichen.
- → Gemäß § 4a Absatz 5 BSIG waren das BMI und das AA bereits seit Dezember 2021 verpflichtet, eine entsprechende Verwaltungsvereinbarung zu schließen. Dieser Verpflichtung sind beide Ressorts bisher jedoch nicht nachgekommen. Die Kontrollrechte des BSI und die Zusammenarbeit mit diesem haben das BMI und das AA insofern nicht angemessen geregelt. Somit besteht eine Regelungslücke für die Informationssicherheit im Kernbereich der Zentralregierung. Insoweit sind Zweifel begründet, ob überhaupt eine Verwaltungsvereinbarung ein äquivalentes Kontrollregime zu dem des BSI aufsetzen kann.
- → Das BMI gab in Abstimmung mit dem AA an, dass die Auslands-IT des AA zu einem Großteil aus inländischen Rechenzentren IT-Dienstleistungen für alle Auslandsvertretungen erbringe. Um eine Trennung der IT-Dienstleistungen gemäß der Bereichsausnahme in der NIS-2-Richtlinie zu erreichen, müsse es mit hohem finanziellem und personellem Aufwand seine IT-Umgebung trennen und zukünftig mit Doppelstrukturen betreiben.[37]

Diese Begründung erschließt sich dem Bundesrechnungshof nicht. Einerseits sollte es problemlos möglich sein, gerade die IT-Umgebung in den inländischen Rechenzentren vom BSI kontrollieren zu lassen. Eine Aufteilung wäre daher nicht notwendig. Des Weiteren dürften IT-Systeme und darauf befindliche Daten für IT-Dienste im Ausland oder für Ausländer einen ähnlichen Schutzbedarf aufweisen wie der restliche Informationsverbund des AA. Sollte zudem ein solches IT-System erfolgreich angegriffen und kompromittiert werden, würde es gerade aufgrund seiner Lage in einem inländischen Rechenzentrum ein besonderes Risiko für den restlichen Informationsverbund des AA und die gesamte eng vernetzte Bundesverwaltung darstellen. Denn nach eigenen Angaben müsste das AA eine Trennung von inländischen und ausländischen Dienstleistungen noch kostenintensiv herstellen und dafür Doppelstrukturen schaffen.

Einheitliches Reglungsregime durchsetzen, statt Ausnahmen hinnehmen

Die vorgesehene Ausnahmeregelung für das AA gefährdet ein einheitliches angemessen hohes Informationssicherheitsniveau in der Bundesverwaltung. Als zentraler IT-Dienstleister mit kritischen IT-Diensten für die gesamte Bundesverwaltung muss das

[37] Vgl. Bericht des Bundesrechnungshofes nach § 88 Absatz 2 BHO zum ersten Regierungsentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes vom 17. September 2024, Gz.: VII4-0002698.

AA hohe Maßstäbe der Informationssicherheit erfüllen. Diese gelten beispielsweise auch für das Informationstechnikzentrum Bund. Der Bundesrechnungshof verweist auf den durch die Auslands-IT für die Bundesverwaltung betriebenen IT-Dienst der Verschlusssachenkommunikation. Für diesen muss das AA die zentralen Vorgaben der Verschlusssachenanweisung (VSA) und sich daraus ergebende Pflichten einhalten. Warum es nicht möglich und sachgerecht sein soll, dem BSI Kontrollrechte für die aus Deutschland betriebenen IT-Dienste zu übertragen, erschließt sich nicht. Denn um die ergebnisäquivalenten Maßnahmen zu erreichen, müsste das AA ausgabenintensiv ein eigenes Kontrollwesen parallel zu dem des BSI etablieren. Somit schafft gerade das AA dringend zu vermeidende Doppelstrukturen, die den Bundeshaushalt personell und finanziell belasten werden.

Diese Kritik teilten auch die im Innenausschuss am 4. November 2024 angehörten Sachverständigen.

Der Bundesrechnungshof empfiehlt daher, die Ausnahmeregelungen für das AA (§§ 7 Absatz 6, 29 Absatz 3 und 44 Absatz 1 Satz 5 sowie Absatz 2 Satz 5) zu streichen. Ausschließlich sachlich begründete Ausnahmen für im Ausland befindliche IT-Systeme und Kommunikationstechnik sollten gemäß § 44 Absatz 1 Satz 3 BSIG-E zulässig sein. Das BSI hat als nationale Cybersicherheitsbehörde die Aufgabe gemäß § 3 Absatz 1 Satz 2 Nummer 1 BSIG-E, Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. Das AA sollte daher auf dessen Kompetenzen und Fähigkeiten zurückgreifen und Doppelstrukturen vermeiden.

2.2.1 Stellungnahme des BMI

Zu diesem Punkt hat das BMI nicht Stellung genommen.

2.2.2 Abschließende Bewertung des Bundesrechnungshofes

Da das BMI auf eine Gegenäußerung verzichtete, geht der Bundesrechnungshof davon aus, dass es seinen Bedenken nicht widerspricht. Er bleibt bei seinen Änderungsvorschlägen.

2.3 Bundesverwaltung auf das Regelungsregime verpflichten und Ausnahmeregelungen der Ressorts beschränken (Artikel 1 § 46 Absatz 5 BSIG-E)

Gemäß § 46 Absatz 5 BSIG-E sollen die ISB der Ressorts (Ressort-ISB) die Befugnis erhalten, Einrichtungen ihres Ressorts in Teilen oder vollständig von den Verpflichtungen der §§ 28 bis 48 BSIG-E auszunehmen. Dieser „Opt-Out" setzt voraus, dass durch ihn „keine nachteiligen Auswirkungen auf die Informationssicherheit des Bundes zu befürchten sind". Die Ressort-ISB müssen sich für einen solchen Schritt mit dem BSI jedoch nur ins Benehmen setzen. Dies bedeutet, dass eine Zustimmung des BSI nicht erforderlich ist.

Im umgekehrten Fall des § 29 Absatz 1 BSIG-E muss das BSI Einvernehmen mit den Ressorts herstellen, um Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts in den Geltungsbereich des Gesetzes einzubeziehen. Laut Gesetzesbegründung sei das Einvernehmen zwischen BSI und Ressort hier notwendig, um potenzielle nachteilige Auswirkungen einschätzen zu können.

Für den Bundesrechnungshof erschließt sich dieses Ungleichgewicht nicht. Kernaufgabe des BSI ist, Gefahren für die Sicherheit in der Informationstechnik des Bundes abzuwehren. Trotzdem soll es den Ressort-ISB erlaubt werden, weitreichend in das Regelungsregime des BSIG-E einzugreifen und dafür nicht einmal die Zustimmung des BSI einholen zu müssen. Nimmt ein oder eine Ressort-ISB ganze Einrichtungen des Ressorts vom Regelungsregime aus, könnte dies zur Folge haben, dass diese – ganz oder teilweise – z. B. ausgabenintensiven Verpflichtungen zum Schutz ihrer IT nicht nachkommen. Unterliegt er oder sie hierbei einer Fehleinschätzung, könnte dies – insbesondere aufgrund der engen Vernetzung der Bundesverwaltung – die Sicherheit des gesamten Informationsverbundes unmittelbar schwächen und gefährden.

Um eine hinreichende Einwirkung des BSI auf beabsichtigte Ausnahmen vom Regelungsregime sicherzustellen, empfiehlt der Bundesrechnungshof, das in § 46 Absatz 5 Satz1 BSIG vorgesehene „Benehmen" in ein „Einvernehmen" abzuändern.

2.3.1 Stellungnahme des BMI

Das BMI hat zu diesem Punkt nicht Stellung genommen.

2.3.2 Abschließende Bewertung des Bundesrechnungshofes

Mangels Stellungnahme des BMI geht der Bundesrechnungshof davon aus, dass es seiner Argumentation nicht widerspricht.

Der Bundesrechnungshof bleibt bei seinen Empfehlungen.

2.4 Einrichtungen der Bundesverwaltung bei Nachweisen nicht bevorteilen (Artikel 1 § 43 Absatz 1 BSIG-E)

Gemäß § 43 Absatz 1 BSIG-E haben die Einrichtungen der Bundesverwaltung dem BSI erstmalig nach fünf Jahren nachzuweisen, dass sie die Anforderungen der Informationssicherheit erfüllen. Anschließend haben sie entsprechende Nachweise nur noch regelmäßig nach den Vorgaben des BSI zu erbringen, ohne dass dieser Turnus genauer spezifiziert wird. Für entsprechende Nachweise ist für die Einrichtungen der Bundesverwaltung zunächst die „Form einer standardisierten Selbsterklärung" vorgesehen".[38] Damit sollen diese nachweisen, die Mindeststandards des BSI sowie den IT-Grundschutz einzuhalten. Der Bundesrechnungshof hält diese Regelungen für die Bundesverwaltung aus folgenden Gründen für nicht zeit- und sachgerecht:

- → Unternehmen, die als Betreiber kritischer Anlagen[39] gelten, müssen dem BSI ihre Nachweise schon nach drei Jahren vorlegen und dann jeweils alle drei Jahre die Folgenachweise. Sie haben diese in Form von Sicherheitsaudits, Prüfungen oder Zertifizierungen zu erbringen. Bei besonders wichtigen Einrichtungen kann das BSI anordnen, drei Jahre nach Inkrafttreten des Gesetzes Nachweise auf Grundlage von Audits, Prüfungen oder Zertifizierungen durch unabhängige Stellen vorzulegen.[40]
- → Unternehmen haben ihre Nachweise durch externe Prüfungen zu erbringen. Für Einrichtungen der Bundesverwaltung ist hingegen eine Selbstauskunft ausreichend, die weniger zeit- und ressourcenaufwändig sein sollte als externe Prüfungen. Gründe, die diese unterschiedliche Vorgehensweise bei Unternehmen und der Bundesverwaltung erläutern, sind dem Gesetzentwurf jedoch nicht zu entnehmen.
- → Einrichtungen der Bundesverwaltung müssen bereits seit dem Jahr 2017 die Anforderungen des UP Bund 2017 erfüllen. Entsprechend haben sie sich derzeit bereits regelmäßig alle drei Jahre Revisionen der Informationssicherheit (IS-Revisionen) zu unterziehen.[41] Insofern sollte die Bundesverwaltung über vorhandene Strukturen und eingeübte Prozesse verfügen, um angelehnt an den Zeitraum der IS-Revisionen ihre initialen Nachweise zu erbringen.
- → Dem Bund fehlt für die Steuerung seiner IT bisher auch ein Überblick zur Informationssicherheit seiner Einrichtungen.[42] Die Nachweise sollen Transparenz über die

[38] Vgl. Gesetzesbegründung, Teil B „Besonderer Teil" zu § 43 BSIG-E.
[39] Vgl. § 39 Absatz 1 Satz 1 BSIG-E.
[40] Vgl. § 61 Absatz 3 Satz 1 BSIG-E.
[41] Nach IT-Grundschutz ist hierbei die Richtlinie des BSI „Informationssicherheitsrevision – Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" in der Version 4.0 vom Dezember 2021 (Abschnitt 3 „IS-Revision in der Institution") anzuwenden.
[42] Bemerkungen 2022 des Bundesrechnungshofes zur Haushalts- und Wirtschaftsführung des Bundes – Ergänzungsband, Bundestagsdrucksache 20/6530 Nummer 24 „Informationssicherheit: IT-Rat bleibt trotz erheblicher Defizite untätig".

Informationssicherheitslage in der Bundesverwaltung herstellen.[43] Müssten die Einrichtungen der Bundesverwaltung erstmals in fünf Jahren, d. h. ab dem Jahr 2030 entsprechende Nachweise vorlegen, wird dieses Ziel kurz- bis mittelfristig nicht zu erreichen sein. Denn die Prüfungen des BSI nach § 4a BSIG (zukünftig § 7 BSIG-E) schließen diese Informationslücke derzeit nicht. Das BSI hat erst wenige Prüfungen begonnen oder abgeschlossen. Aussagekräftige flächendeckende Erkenntnisse zum Stand der Informationssicherheit in der Bundesverwaltung wird das BSI auf diese Weise bestenfalls langfristig gewinnen können. Umso wichtiger wäre es, wenn das BSIG-E für alle Einrichtungen der Bundesverwaltung einen festen und identischen Turnus für Nachweise festlegt. Auf Grundlage dieser Nachweise wären dann belastbare Aussagen zur Lage der Informationssicherheit möglich.

→ Die Europäische Union will die NIS-2-Richtlinie alle drei Jahre evaluieren. Die Bundesverwaltung sollte entsprechend dieses Turnus über einen belastbaren Informationsstand zu ihrer Informationssicherheit verfügen, um sachdienliche Rückmeldungen für die EU-Evaluation liefern zu können.

Die Bundesverwaltung besser zu stellen, kann die Akzeptanz der von der Regulierung betroffenen Unternehmen negativ beeinflussen. Die Frist für Einrichtungen der Bundesverwaltung sollte daher ebenfalls drei Jahre betragen; Folgenachweise im Anschluss sollten turnusmäßig alle drei Jahre zu erbringen sein.

Der Bundesrechnungshof empfiehlt, § 43 Absatz 1 Satz 2 BSIG-E wie folgt zu fassen:

Artikel 1 § 43 Absatz 1 Satz 2 BSIG-E

Die Einrichtungen der Bundesverwaltung weisen dem Bundesamt die Erfüllung der Anforderungen nach Absatz 1 spätestens **drei Jahre** nach Inkrafttreten dieses Gesetzes und anschließend **alle drei Jahre** nach seinen Vorgaben nach.

2.4.1 Stellungnahme des BMI

Das BMI hat zu diesem Punkt nicht Stellung genommen.

2.4.2 Abschließende Bewertung des Bundesrechnungshofes

Das BMI hat sich zu dem Vorschlag, Nachweispflichten für die Bundesverwaltung ebenfalls auf drei Jahre festzusetzen, nicht geäußert. Der Bundesrechnungshof bleibt bei seiner Empfehlung.

[43] Vgl. Gesetzesbegründung, Teil B „Besonderer Teil“ zu § 43 Absatz 4 BSIG-E.

2.5 Informationssicherheit als Verantwortung der Leitungsebene festlegen (Artikel 1 § 43 Absatz 1 Satz 1 BSIG-E)

Informationssicherheit ist auch immer eine Führungsverantwortung. Sie kann in einer Einrichtung nur bestehen, wenn deren Leitung die notwendigen Ressourcen (Personal, Budget, Zeit) bereitstellt sowie die Umsetzung notwendiger Maßnahmen unterstützt. Die Einrichtungsleitung sollte dabei in ihrer Vorbildfunktion sicherheitsorientiert handeln.[44,45] In Folge legt der IT-Grundschutz für die oberste Leitungsebene einer Behörde fest, dass diese „für die Gewährleistung der Informationssicherheit nach innen und außen" die Verantwortung trägt.[46] Der UP Bund 2017 übernahm diese Anforderung des IT-Grundschutzes und legt seit dem Jahr 2017 hierzu fest: „Die Verantwortung für die Gewährleistung der Informationssicherheit trägt die Leitung einer Einrichtung als Teil der allgemeinen Leitungsverantwortung. Sie verantwortet die Einhaltung von gesetzlichen und sonstigen Anforderungen […]."[47]

Im vorliegenden Gesetzentwurf sieht § 43 Absatz 1 Satz 1 BSIG-E nunmehr jedoch nur vor, dass die Einrichtungsleitung „unter Berücksichtigung der Belange des IT-Betriebs die Voraussetzungen zur Gewährleistung der Informationssicherheit zu schaffen" hat. Dies greift deutlich zu kurz. Die Verantwortung für die Gewährleistung der Informationssicherheit der Einrichtung umfasst deutlich mehr, als nur die Voraussetzungen hierfür zu schaffen. Können Einrichtungsleitungen nicht die notwendigen Ressourcen bereitstellen oder Prozesse etablieren, so müssen sie die sich daraus ergebenden Risiken identifizieren, diese bewerten und geeignete Maßnahmen ergreifen. Restrisiken müssen sie gegebenenfalls übernehmen und die Folgen ihres Eintretens verantworten. Das BSIG-E darf hier nicht hinter zentrale Vorgaben des UP Bund 2017 und des IT-Grundschutzes zurückfallen. Es sollte deren bereits seit Jahren etablierte und bewährte Festlegung übernehmen. Der Bundesrechnungshof empfiehlt daher, den § 43 Absatz 1 Satz 1 BSIG-E wie folgt zu fassen:

[44] BSI IT-Grundschutz-Kurs, Lektion 2.3 „Verantwortung und Aufgaben der Leitung", zuletzt abgerufen am 8. August 2025.
[45] Vgl. BSI IT-Grundschutzbaustein ISMS 1.1 – Sicherheitsmanagement.
[46] Vgl. BSI Standard 200-1, Kapitel 4.1 „Aufgaben und Pflichten des Managements".
[47] UP Bund 2017, Kapitel 3.2 „ISMS – Organisation und Aufgaben innerhalb des Ressorts/der Einrichtung".

Artikel 1 § 43 Absatz 1 Satz 1 BSIG-E

Die Leitung **der Einrichtung der Bundesverwaltung** ist **für die Gewährleistung der Informationssicherheit** unter Berücksichtigung der Belange des IT-Betriebs verantwortlich.

2.5.1 Stellungnahme des BMI

Zu diesem Punkt hat das BMI nicht Stellung genommen.

2.5.2 Abschließende Bewertung des Bundesrechnungshofes

Da das BMI sich zur Leitungsverantwortung nicht geäußert hat, geht der Bundesrechnungshof insofern davon aus, dass es dieser nicht widerspricht.

Der Bundesrechnungshof hält seine Empfehlung aufrecht.

2.6 Rolle und Befugnisse der Koordinatorin oder des Koordinators für Informationssicherheit gesetzlich festlegen (Artikel 1 § 48 BSIG-E)

Die Bundesregierung beabsichtigt, eine Koordinatorin oder einen Koordinator für Informationssicherheit zu schaffen. Diese Funktion ist bereits in vielen Wirtschaftsunternehmen und auch zahlreichen Staaten als Chief Information Security Officer (CISO) etabliert. Die Funktion trägt der zunehmenden Bedeutung der Informationssicherheit in Einrichtungen Rechnung und stellt entsprechend eine Steuerungsfunktion auf der obersten Leitungsebene dar. Die oder der CISO soll dabei Anforderungen der Geschäftsprozesse mit denen der IT- und Informationssicherheit koordinieren. Sie oder er verantwortet die IT-Sicherheitsstrategie, sorgt für die notwendige Absicherung der IT-gestützten Geschäftsprozesse und das dafür erforderliche Schutzniveau.

Das BSIG-E nennt jedoch keinerlei Aufgaben und Befugnisse der oder des CISO Bund. § 48 BSIG-E sieht nur vor, dass die Bundesregierung eine oder einen CISO Bund bestellt. Auch der Gesetzesbegründung sind keine Details zu Stellung, Aufgaben und Befugnissen der oder des CISO Bund zu entnehmen. Das BMI hatte hierzu mitgeteilt, der Haushaltsausschuss habe die Bundesregierung mit einem Maßgabebeschluss im Februar 2024 aufgefordert, ein Konzept für die Einrichtung einer oder eines CISO Bund zu erstellen. Ein solches Konzept müsse laut BMI die Grundlage für eine gesetzliche Verankerung und daher ressortgeeint sein. Ohne dieses könne das BMI die Funktion der

oder des CISO Bund im Gesetz nur allgemein umreißen. Ein solches Konzept liegt nach über einem Jahr noch nicht vor.

Für den Bundesrechnungshof ist dieses Vorgehen mit Blick auf die großen Herausforderungen der Informationssicherheit in der Bundesverwaltung nicht akzeptabel und nicht zielführend. Bisher haben das Ressort- und das Einstimmigkeitsprinzip eine wirksame Steuerung der zentralen IT des Bundes und deren Konsolidierung erschwert. Es reicht nicht aus, eine Funktion CISO Bund zu schaffen, ohne dieser Steuerungsbefugnisse an die Hand zu geben. Damit diese eine Wirkung in der Bundesverwaltung erzielt, muss das BSIG-E angemessene strategisch steuernde Aufgaben und Befugnisse normieren. Die oder der CISO Bund muss nicht nur die Befähigung, sondern auch die Befugnis besitzen, die unterschiedlichen Interessen von IT-Betrieb, Informationssicherheit und Bedarfsträgern trotz knapper Ressourcen in Einklang zu bringen.

Zudem hatte der IT-Rat als ehemals höchstes IT-Steuerungsgremium des Bundes der Informationssicherheit in den letzten Jahren nicht die notwendige Bedeutung beigemessen.[48] Insbesondere mangelte es ihm an einem ressortübergreifenden Informationssicherheitscontrolling (IS-Controlling). Daher konnte er weder Sachstände zur Informationssicherheit zentral bewerten noch aus den vorliegenden Informationen die notwendigen Maßnahmen ableiten. Der Bundesrechnungshof vertritt die Auffassung, dass die oder der CISO Bund ein IS-Controlling verantworten sollte.

Auch der Haushaltsausschuss hatte in den vergangenen Jahren mehrfach in Maßgabebeschlüssen ein übergreifendes IS-Controlling eingefordert. Damit wollte er eine auskömmliche Finanzierung von Maßnahmen der Informationssicherheit überwachen, um deren Wirksamkeit bewerten zu können. Die gemäß § 58 Absatz 3 BSIG-E vorgesehenen Berichte des BMI an den Innenausschuss zur „Anwendung des Gesetzes“ oder der jährliche Bericht des BSI an den Haushaltsausschuss zu seinen Kontrollen nach § 7 Absatz 9 BSIG-E adressieren dies nicht. Insofern fehlt eine wichtige Grundlage, um den Haushaltsmitteleinsatz für Informationssicherheit in der Bundesverwaltung zu kontrollieren und zu steuern. Gerade vor dem Hintergrund der Bereichsausnahme für den Schutz informationstechnischer Systeme[49] ist eine solche Kontrollmöglichkeit dringend geboten. Denn die Bundesregierung muss den Einsatz von Haushaltsmitteln für Informationssicherheit zielgerichtet steuern und Fehlanreizen oder Mehrfachentwicklungen entgegenwirken.

Der Bundesrechnungshof regt daher an, § 48 BSIG-E um folgende Aufgaben und Befugnisse der oder des CISO Bund zu ergänzen:

[48] Bemerkungen 2022 des Bundesrechnungshofes zur Haushalts- und Wirtschaftsführung des Bundes – Ergänzungsband, Bundestagsdrucksache 20/6530 Nummer 24 „Informationssicherheit: IT-Rat bleibt trotz erheblicher Defizite untätig“.

[49] Vgl. Artikel 115 Absatz 2 Satz 4 Grundgesetz.

→ Erstellung einer IT-Sicherheitsstrategie für die gesamte Bundesverwaltung.
→ Festlegung von Sicherheitsanforderungen und -zielen für die Bundesverwaltung.
→ Festlegung und Fortschreibung des zentralen IS-Controllings der Bundesverwaltung.
→ Verpflichtung aller Ressorts, den CISO Bund bei der Erfüllung seiner Aufgaben zu unterstützen.
→ Zentrale ressortübergreifende Koordinierung des Informationssicherheitsmanagements.
→ Entwicklung, Steuerung und Fortschreibung von Programmen, um die Informationssicherheit der Einrichtungen der Bundesverwaltung zu gewährleisten, im Benehmen mit den Ressorts.
→ Pflicht zur Beteiligung an allen Gesetzes-, Verordnungs- und sonstigen Verfahren, sofern diese Fragen der Informationssicherheit berühren.
→ Recht, der Bundesregierung Vorschläge und Stellungnahmen zuzuleiten, wenn Vorgänge der Bundesverwaltung die Informationssicherheit betreffen.
→ Verpflichtung aller Einrichtungen der Bundesverwaltung, IT-Sicherheitsprodukte nach § 19 BSIG-E zu nutzen.
→ Zustimmungsvorbehalt zu allen ressortübergreifenden Belangen der Informationssicherheit[50].
→ Recht zur Stellungnahme zu allen Gesetzesvorhaben und Vorgängen, die die Informationssicherheit betreffen, gegenüber dem Deutschen Bundestag und dessen Gremien.
→ Pflicht, den Haushaltsausschuss einmal im Kalenderjahr zum Stand der Informationssicherheit in der Bundesverwaltung sowie der dazu eingesetzten Haushaltsmittel und deren Wirkung zu informieren.

Zudem regt der Bundesrechnungshof an, gesetzlich festzulegen, dass die oder der CISO Bund neben Managementfähigkeiten über die notwendigen Qualifikationen, Erfahrungen sowie Sachkunde im Bereich der Informationssicherheit verfügt. Dies stellt sicher, die Funktion CISO Bund entsprechend ihrer Bedeutung auszufüllen.

2.6.1 Stellungnahme des BMI

Das BMI hat auf den Maßgabebeschluss des Haushaltsausschusses vom 21. Februar 2024 verwiesen. Darin hatte dieser die Bundesregierung aufgefordert, ein Konzept u. a. mit Vorschlägen zu erarbeiten, wie eine Rolle CISO Bund einzurichten wäre. Aus Sicht der Bundesregierung könne sie Funktion und Befugnisse der oder des CISO Bund erst auf Grundlage dieses geforderten ressortgeeinten Konzepts definieren. Eine Ausgestaltung der Rolle CISO Bund im jetzigen Gesetzentwurf hätte dem fehlenden Konzept

[50] Ein solcher Zustimmungsvorbehalt sollte analog zu dem des BMDS für alle wesentlichen IT-Ausgaben der Einrichtungen der Bundesverwaltung orientieren. Vgl. Organisationserlass des Bundeskanzlers vom 6. Mai 2025, Abschnitt XIII.

vorgegriffen. Insofern ist die Rolle CISO Bund im Gesetzentwurf zunächst nur allgemein eingeführt.

2.6.2 Abschließende Bewertung des Bundesrechnungshofes

Die Forderung des Haushaltsausschusses, ein Konzept für die oder den CISO Bund zu erstellen, datiert bereits vom 21. Februar 2024. Die Bundesregierung hat sich seitdem jedoch nicht auf ein solches geeinigt. Dies wird der Bedrohungslage für die Bundesverwaltung, auf die das BMI selbst in seiner Stellungnahme hinweist, nicht gerecht. Denn der oder dem CISO Bund kommt eine wichtige Steuerungsfunktion der Informations- und Cybersicherheit in der Bundesverwaltung zu. Der Gesetzgeber sollte daher Befugnisse und Aufgaben der oder des CISO Bund verpflichtend regeln. So kann der Gesetzgeber verhindern, dass die Rolle des CISO Bund infolge unterschiedlicher Ressortinteressen unzureichend ausgestaltet wird und Haushaltsmittel für Informations- und Cybersicherheit unsachgemäß verausgabt werden.

Der Bundesrechnungshof hält daher an seinen Empfehlungen fest.

2.7 Mit weiteren Änderungen Befugnisse des BSI stärken

An folgenden Stellen sollte der Gesetzentwurf konkretisiert beziehungsweise korrigiert werden, um das BSI bei seiner Aufgabenwahrnehmung zu stärken.

→ Gemäß § 3 Absatz 1 BSIG-E ist es Kernaufgabe des BSI, Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. § 7 Absatz 1 BSIG-E gibt dem BSI hierzu die Befugnis, die Kommunikationstechnik des Bundes und ihre Komponenten sowie die technische Infrastruktur zu kontrollieren. Der Innenausschuss schlug im November 2024 hierzu vor, dem BSI in § 7 Absatz 1 BSIG-E auch die Befugnis für Penetrationstests bei Einrichtungen der Bundesverwaltung und den Netzen des Bundes zu übertragen. Dies zielte darauf ab, technische Prüfungen[51] ebenfalls im BSIG-E zu regeln und so die Befugnis des BSI klarzustellen. Der vorliegende Gesetzentwurf greift diesen Vorschlag nicht auf. Dem BSI fehlt somit gerade im vernetzten Bereich der Bundesverwaltung die Möglichkeit, seine Erkenntnisse und Fähigkeiten zu nutzen, um Schwachstellen in den Informationssicherheitsmaßnahmen präventiv zu erkennen und auf deren Behebung unmittelbar hinzuwirken. § 7 Absatz 1 BSIG-E sollte daher wie folgt ergänzt werden:

[51] U. a. Penetrationstests, Webchecks oder Attack Surface Checks.

Artikel 1 § 7 Absatz 1 Satz 2 Nummer 3 (neu) BSIG-E

3. technische Prüfungen (u. a. Penetrationstests, Webchecks oder Attack Surface Checks) durchführen.

→ Gemäß § 3 Absatz 1 Satz 2 Nummer 16 BSIG-E ist es Aufgabe des BSI, „für die Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, insbesondere soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen" zu unterstützen. Insofern ist es angemessen, dass es daran beteiligt werden soll, den sogenannten IT-Sicherheitskatalog im novellierten Energiewirtschaftsgesetz (EnWG) einvernehmlich mit der BNetzA zu erstellen.[52]

§ 5c Absatz 2 Satz 6 EnWG-E sieht jedoch vor, dass die BNetzA den IT-Sicherheitskatalog alle zwei Jahre ohne Beteiligung des BSI aktualisiert. Zudem kann das BSI dessen Aktualisierung nicht selbst anstoßen und somit nicht aufgrund eigener Erkenntnisse aktiv werden. Es erschließt sich hier nicht, warum BNetzA und BSI nicht einvernehmlich die IT-Sicherheitskataloge aktualisieren sollten. Folgende Ergänzung des § 5c Absatz 2 Satz 6 EnWG-E sollte dies klarstellen:

Artikel 17 § 5c Absatz 2 Satz 6 EnWG-E

Das Bundesamt und die Bundesnetzagentur überprüfen den IT-Sicherheitskatalog alle zwei Jahre. Die BNetzA aktualisiert diesen bei Bedarf **im Einvernehmen mit dem Bundesamt.**

2.7.1 Stellungnahme des BMI

Das BMI hat sich in seiner Stellungnahme nicht zu diesem Punkt geäußert.

2.7.2 Abschließende Bewertung des Bundesrechnungshofes

Der Bundesrechnungshof bleibt bei seinen Empfehlungen.

[52] Artikel 17, § 5c Absatz 2 Satz 1 EnWG-E.

3 Haushaltsausgaben und Erfüllungsaufwand der Bundesverwaltung kritisch hinterfragen

Die Bundesregierung beziffert die in den Jahren 2026 bis 2029 zusätzlich zu erwartenden Haushaltsausgaben für den Bund auf insgesamt 906 Mio. Euro. Diese resultieren im Wesentlichen aus dem Bedarf an 1 276 zusätzlichen Stellen sowie den dadurch bedingten Personalausgaben.[53] Zu dem dafür ursächlichen Mehraufwand hatten BMI und StBA die Ressorts befragt. Viele Behörden meldeten dem BMI hierbei, ihre Schätzungen seien mit zum Teil großen Unsicherheiten behaftet.

Eine nähere Analyse der Angaben zu den Haushaltsausgaben in der Gesetzesbegründung zeigt, dass diese nicht geeignet sind, den Mehrbedarf der Höhe nach belastbar abzubilden. Vielmehr ist die Annahme gerechtfertigt, dass

- → den Rückmeldungen an das BMI ein teilweise unterschiedliches Verständnis darüber zugrunde liegt, welche neuen Aufgaben infolge des Gesetzes auf die Ressorts zukommen und
- → Personal- und Sachmittelbedarfe auch für Aufgaben ausgewiesen werden, die die Ressorts bereits aufgrund der derzeit schon bestehenden Regelungen (u. a. UP Bund 2017, Mindeststandards nach § 8 BSIG, § 50 Absatz 2 VSA[54]) verpflichtend wahrzunehmen haben.

Der Bundesrechnungshof sieht sich in dieser Einschätzung durch die erneute Stellungnahme des NKR bestätigt.[55] Der NKR hat, wie auch bereits bei der Vorlage des Gesetzes im Jahr 2024,[56] darauf hingewiesen, dass „es sich bei dem dargestellten erheblichen Mehrbedarf an Planstellen teilweise um Sowieso-Aufwände handeln könnte". Trotz der Stellungnahmen des NKR und des Berichtes des Bundesrechnungshofes aus dem Jahr 2024 hat das BMI es versäumt, offensichtliche Fehleinschätzungen der Ressorts zu ihrem Mehrbedarf zu plausibilisieren und zu korrigieren. Vielmehr hat sich der Erfüllungsaufwand gegenüber dem Gesetzentwurf des Jahres 2024 sogar weiter erhöht. So meldet das Bundesministerium der Finanzen für das Informationstechnikzentrum Bund (ITZBund) nunmehr 248 zusätzliche Stellen an. Die Gesetzesbegründung verweist auf einen "signifikante[n] Mehraufwand“ des zentralen IT-Dienstleisters des Bundes. Dieser müsse z. B. bei kundenbezogenen Prüfungen nach § 7 BSIG-E dem BSI

[53] Buchstabe D. des Vorblatts sowie Teil A.VI.3 der Gesetzesbegründung, S. 111ff.
[54] Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), § 50 Absatz 2: Die Verarbeitung von Verschlusssachen ist nur zulässig, wenn die Einrichtung der Bundesverwaltung die Standards zur Informationssicherheit des BSI einhält.
[55] Stellungnahme des NKR gem. § 6 Absatz 1 NKRG, NKR-Nummer 7657, BMI 28. Juli 2025
[56] Bundestagsdrucksache 20/13184 vom 2. Oktober 2024, Anlage 2, Seite 173; zuletzt abgerufen am 4. August 2025.

zuarbeiten. Da § 7 BSIG-E jedoch § 4a BSIG entspricht, muss das ITZBund diese Aufgabe bereits seit dem IT-Sicherheitsgesetz 2.0 erbringen. Die Begründung für seinen Mehrbedarf ist somit nicht nachvollziehbar.

Insgesamt gibt dies Anlass zu zweifeln, inwieweit der aus der Umsetzung des BSIG-E entstehende Mehrbedarf an Personal- und Sachmitteln durchgängig sachgerecht ermittelt ist. Ein überhöht ausgewiesener Erfüllungsaufwand birgt das Risiko, Forderungen nach einer (weiteren) Aufweichung der Vorgaben für die Bundesverwaltung auszulösen, um so vermeintlich Ausgaben senken zu können. Darauf hatte der BWV das BMI frühzeitig hingewiesen und diesem empfohlen, derartigen möglichen Bestrebungen mit einer realistischen Abschätzung der ausschließlich zusätzlich entstehenden Ausgaben und Stellenbedarfe entgegenzutreten. Der aktuelle Gesetzentwurf und der Abgleich mit vorherigen Referentenentwürfen machen allerdings deutlich, dass dieses Risiko eingetreten ist. Nicht belastbare, überhöhte Angaben einzelner Resorts zum Erfüllungsaufwand hatten zur Folge, dass zunächst vorgesehene Regelungen, mit denen die Cybersicherheit in der Bundesverwaltung gesteigert werden soll, aus dem Gesetzentwurf entfallen sind. Dies betrifft insbesondere die gesetzliche Verankerung des IT-Grundschutzes und der Risikomanagementmaßnahmen (vgl. Tz. 2.1) sowie ursprünglich für die Bundesbehörden vorgesehene Nachweisfristen von drei Jahren (vgl. Tz. 2.4).

Ergänzend zu diesen die Gesetzesbegründung betreffenden Hinweisen hält der Bundesrechnungshof es für unbedingt erforderlich, die nach Inkrafttreten des Gesetzes zu erwartenden Stellen- und Ausgabenforderungen der Ressorts eingehend zu prüfen. Hierbei ist insbesondere ein Beschluss des Rechnungsprüfungsausschusses vom 11. Juli 2025 zu beachten. Hiernach sollen die Ressorts Stellen nur noch anmelden, wenn sie u. a. geprüft haben, ob sie vakante Stellen für die zusätzlichen neuen Aufgaben nutzen und ggf. in die entsprechenden Bereiche verlagern können. Nach Darstellung der Bundesregierung verfügen die Ressorts derzeit über in Summe 4 415 Stellen im Bereich der IT-Sicherheit.[57] Davon sind 3 730 Stellen besetzt und 685 vakant. Die Zahl vakanter Stellen entspricht etwas mehr als der Hälfte des Stellenbedarfs, den die Ressorts für das BSIG-E beziffert haben.

3.1 Stellungnahme des BMI

Das BMI hat darauf verwiesen, dass die im Gesetzentwurf dargestellten Mehraufwände sich aus den Einzelfallbewertungen der Ressorts ergeben. Das BMI habe diese im Verlauf der Ressortabstimmungen wiederholt abgefragt. Hierzu habe es Handreichungen und Anregungen bereitgestellt, um die Bewertungen der Ressorts einheitlich darstellen zu können. Die Rückmeldungen verantworteten aber aufgrund des Ressortprinzips die jeweiligen Ressorts und nicht das BMI.

[57] Bundestagsdrucksache 20/14639 Nummer 25; Antwort des Parlamentarischen Staatssekretärs Johann Saathoff vom 22. Januar 2025.

Es teile aber die vom Bundesrechnungshof angebrachten Zweifel zu den eingebrachten Mehraufwänden und halte eine kritische Überprüfung für ratsam. Hierzu seien - unter Berücksichtigung der Argumente des Bundesrechnungshofes - die Stellen- und Ausgabenforderungen im Zuge der Haushaltsaufstellungsverfahren zu plausibilisieren und zu prüfen.

3.2 Abschließende Bewertung des Bundesrechnungshofes

Der Bundesrechnungshof sieht sich insofern bestätigt, dass Zweifel an den dargestellten Mehraufwänden angebracht und diese kritisch zu hinterfragen sind.

Alle Ressorts müssen bereits seit dem Jahr 2017 Pflichten des UP Bund 2017 erfüllen. Entsprechende Bedarfe dieser bestehenden Verpflichtungen dürfen sich nicht in zusätzlichen Stellen- und Sachmittelaufwänden der NIS-2-Umsetzung niederschlagen. Bereits während des Gesetzgebungsverfahrens korrigierten die Ressorts ihre Bedarfsschätzungen drastisch. Ihre schon zuvor bestehenden Bedarfe müssen die Ressorts insofern außerhalb des Gesetzgebungsprozesses geltend machen. Hierbei muss die Bundesregierung einen einheitlichen Maßstab für Personal- und Sachmittelbemessungen im Bereich der Informations- und Cybersicherheit beachten.

4 Bisherige Regelungen überprüfen, Evaluation des neuen Gesetzes vorsehen

Mit dem ersten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) aus dem Jahr 2015 sowie dem nachfolgenden IT-SiG 2.0 aus dem Jahr 2021 normierte der Gesetzgeber wesentliche Grundlagen, um die Sicherheit in der Informationstechnik in KRITIS und in der Bundesverwaltung zu schaffen und aufrechtzuerhalten. Der vorliegende Entwurf eines neuen BSIG baut in weiten Teilen auf diesen bestehenden Normen auf, dehnt dabei den Anwendungsbereich auf weitere Unternehmen aus und erweitert die Vorgaben für die Bundesverwaltung. Insofern erklärt die Gesetzesbegründung durchweg, dass die jeweiligen Regelungen des neuen BSIG-E nur die des bisherigen BSIG fortführen.

Gemäß § 6 Absatz 1 Nummer 1 und 2 IT-SiG 2.0 sollte das BMI dem Deutschen Bundestag zwei Evaluationsberichte über „die Wirksamkeit der in diesem Gesetz enthaltenen Maßnahmen für die Erreichung der mit diesem Gesetz verfolgten Ziele“ vorlegen. Den ersten Bericht legte das BMI am 2. Mai 2023 vor. Er betraf ausschließlich die Normen

zur KRITIS-Regulierung und damit nur einen kleinen Teil des IT-SiG 2.0.[58] Zudem betrachtete er nur die Auswirkungen auf KRITIS-Betreiber der Wirtschaft. Insbesondere das Verwaltungshandeln im Bereich der KRITIS-Regulierung betrachtete diese Evaluierung nicht. Hierzu fehlen somit Erkenntnisse. Der zweite Bericht sollte hingegen alle übrigen Normen des Gesetzes und dessen Wirksamkeit insgesamt betrachten. Diesen legte das BMI verspätet zum 26. August 2025 vor. Als Datengrundlagen nutzte das BMI hierbei „Daten des BMI und BSI". Zudem griff es für die Nachmessung von Erfüllungsaufwänden auf Daten des StBA zurück. Die Aussagekraft des Evaluationsberichts ist aufgrund der begrenzten Datengrundlage nicht tragfähig. Insbesondere ist kritisch anzumerken, dass das BMI zwar im Bericht selbst Mängel an Regelungen des BSIG erkennt. Im vorliegenden Gesetzentwurf diese aber nur an einer Stelle aufgreift.[59] Darüber hinaus beruhen Erkenntnisse zu Folgen der Regelungen größtenteils nur auf Annahmen des BMI. Belegbare Fakten, die diese stützen, sind dem Bericht nicht zu entnehmen.

Damit fehlen weiterhin belastbare Erkenntnisse für das vorliegende Gesetzgebungsverfahren, für das die Bundesregierung allein den Erfüllungsaufwand bis zum Jahr 2029 mit rund 900 Mio. Euro beziffert. Der erste Evaluationsbericht hat nicht bewertet, wie effizient und effektiv Behörden bei der Aufsicht über die KRITIS-Betreiber zusammenwirken und ob bereits das IT-SiG 2.0 dies maßgeblich unterstützt hat. Es bleibt insofern offen, ob

- → die Fortführung der betreffenden Regelungen und vereinzelte Änderungen im neuen BSIG-E für dessen wirksame und zugleich bürokratiearme Ausgestaltung notwendig sind und
- → ob sie die Aufgaben und Befugnisse des BSI sinnvoll anpassen oder ergänzen.

Darüber hinaus wäre es bedeutsam gewesen, wenn die gesetzlich vorgeschriebene zweite Evaluation **belastbare** Antworten zu Fragen der Zielerreichung, der Wirkung und der Wirtschaftlichkeit gegeben hätte. Insbesondere hat auch die zweite Evaluation keine Erkenntnisse zu den Auswirkungen auf die Zusammenarbeit des BSI mit anderen Aufsichtsbehörden und Dritten geliefert. Auch diese hätten notwendige Änderungsbedarfe am BSIG-E aufzeigen können. Aufgrund der o. g. Aspekte fehlen der Bundesregierung, dem Gesetzgeber und dem Bundesrechnungshof fundierte Einschätzungen u. a. zu folgenden Regelungen:

- → Gemäß § 4 Absatz 5 BSIG sind weite Teile der Auslands-IT des AA von Kontrollen des BSI ausgenommen. Der neue § 7 Absatz 6 BSIG-E übernimmt diese Ausnahme mit nahezu identischem Wortlaut, erweitert sie zudem noch durch Wegfall des Zusatzes „ausschließlich" (vgl. Tz. 2.2). Ohne eine Evaluation der bisherigen Ausnahmeregelung bleibt unklar, welche Auswirkungen diese auf die Sicherheit der Auslands-IT und auf

[58] Gemäß § 6 Absatz 1 Satz 1 waren im ersten Bericht nur § 2 Absatz 10, die §§ 8a, 8b, 8d und 8e sowie § 10 Absatz 1 zu evaluieren.

[59] Vom BMI als notwendig erkannte Änderungen an Regelungen des § 7d BSIG flossen in den § 17 BSIG-E ein.

zusätzlich erforderliche Aufwände im AA hatte. Die Ausnahmeregelung einfach unverändert fortzuschreiben oder sogar zu erweitern, kann so Risiken bergen, die ohne eine Evaluation unerkannt bleiben.

→ Das BSIG-E führt erstmalig die Funktion eines Ressort-ISB ein, die auf Ebene der Ressorts das ISM steuern und überwachen. Die Ressort-ISB sollen gemäß § 46 Absatz 5 BSIG-E auch weitreichende Befugnisse erhalten. Diese sollen ihnen erlauben, einzelne Einrichtungen ihres Ressorts vom Regelungsregime des BSIG-E auszunehmen. Dem Gesetz oder der Begründung ist jedoch nicht zu entnehmen, warum der oder die Ressort-ISB sich hierzu nicht in Einvernehmen mit dem BSI setzen muss (vgl. Tz. 2.3). Gerade für solch weitreichende Einschnitte in den Wirkungsbereich des BSI wären belegbare Fakten wichtig, welche Fälle in der Vergangenheit eine solche Ausnahme erforderlich gemacht hätten und welche negative Wirkung hierbei ein Einvernehmen des BSI entfaltet hätte.

→ Das aktuelle BSIG sieht in § 8b Absatz 3 vor, dass das BSI die KRITIS-Betreiber selbst registrieren kann, wenn diese ihrer Pflicht hierzu nicht nachkommen. Das BSI hat dann die zuständige Aufsichtsbehörde des Bundes zu informieren. Gemäß § 28 Absatz 1 BSIG-E gelten KRITIS-Betreiber als besonders wichtige Einrichtungen. § 33 Absatz 3 BSIG-E sieht vor, dass das BSI nunmehr das Einvernehmen mit der zuständigen Aufsichtsbehörde herstellen muss, um besonders wichtige Einrichtungen selbst zu registrieren. Offen bleibt, auf welcher Grundlage das BSI im Vergleich zum bisher gültigen BSIG eingeschränkt wird. Es verursacht dem BSI und der jeweiligen Aufsichtsbehörde Aufwand, das Einvernehmen herzustellen. Zudem kann ein Zeitverlust eintreten. Es wäre daher relevant zu wissen, welche Vorteile die Umsetzung des § 33 BSIG-E gegenüber der bisherigen Regelung bietet und warum das BSI nicht bereits aufgrund der bestehenden Regelung sachgerecht und effektiv handeln kann.

→ Ebenso bleibt offen, ob es sinnvoll ist, dass das BSI gemäß § 29 BSIG-E nur im Einvernehmen mit den Ressorts weitere Körperschaften, Anstalten oder Stiftungen des öffentlichen Rechts als relevante Einrichtungen erklären darf. Gemäß § 8 Absatz 1 Nummer 2 BSIG legt ausschließlich das zuständige Ressort für diese fest, dass die BSI IT-Mindeststandards anzuwenden sind. Insofern stärkt das BSIG-E an dieser Stelle das BSI. Es liegen aber keine Erkenntnisse vor, ob Ressorts hiervon Gebrauch gemacht haben und ob das BSI hier abweichende Meinungen vertrat. Somit bleibt offen, ob es nicht der Kompetenz des BSI als nationaler Cybersicherheitsbehörde zuwiderlief, wenn Ressorts dessen Meinung hierzu unberücksichtigt lassen konnten und ob dies nachweislich negative Auswirkungen verhindert hat.

→ Darüber hinaus fehlen mangels Evaluation Erkenntnisse zur Zusammenarbeit des BSI mit Aufsichtsbehörden, z. B. gemäß § 7a Absatz 3, § 7c Absatz 1 oder § 8a Absatz 2 BSIG. Da sich das BSI aufgrund des BSIG-E mit unterschiedlichen Einrichtungen der Bundesverwaltung in Einvernehmen oder Benehmen setzen muss, wären solche Erkenntnisse notwendig, um die Ausgestaltung des BSIG-E zu begründen.

→ § 39 Absatz 1 BSIG-E führt den bisherigen § 8a Absatz 3 BSIG fort. Hierzu bleibt unklar, ob es sachgerecht und angemessen ist, dass das BSI gemäß § 39 Absatz 1 BSIG-E nur im Einvernehmen mit einer Aufsichtsbehörde des Bundes eine Mängelbehebung

verlangen kann. Offen bleibt auch, warum dies dann nicht für Aufsichtsbehörden gilt, die nicht Teil der Bundesverwaltung sind. Welche Vor- und Nachteile diese Unterschiede in der Zusammenarbeit des BSI mit den verschiedenen Aufsichtsbehörden bedingen, erschließt sich so nicht.

→ Das BSIG-E regelt in § 61 Absatz 6 BSIG-E, dass das BSI gegenüber wichtigen oder besonders wichtigen Einrichtungen im Benehmen mit der Aufsichtsbehörde Maßnahmen zur Verhütung oder Behebung von Sicherheitsvorfällen anordnen kann. Sofern Gefahr im Verzug ist, entfällt das Benehmen mit der Aufsichtsbehörde. Diese Regelung findet sich im aktuellen BSIG nicht. Im Vergleich mit § 39 Absatz 1 BSIG-E entsteht somit ein Gefälle in der Zusammenarbeit von BSI und Aufsichtsbehörden. Unklar bleibt, warum einerseits eine Abstimmung des BSI im Einvernehmen mit der zuständigen Aufsichtsbehörde notwendig ist, es andererseits aber nur ein Benehmen benötigt. Relevant wäre insbesondere, ob dies in beiden Fällen einem effizienten Verwaltungshandeln dient.

→ Weitere wichtige Erkenntnisse einer Evaluation des IT-SiG 2.0 betreffen die Erfüllungsaufwände der Bundesverwaltung und des BSI im Besonderen. In der zweiten Evaluierung des IT-SiG 2.0 kam das BMI mehrfach zu der Erkenntnis, dass die Personalausstattung des BSI unzureichend gewesen sei. Das BSI habe daher neue Aufgaben des IT-SiG 2.0 nur zu Lasten von Bestandsaufgaben wahrnehmen können. Konkretere Aussagen zum genauen Defizit der Personalausstattung des BSI sind dem Bericht jedoch nicht zu entnehmen. Insofern bleibt offen, mit welchem Personaleinsatz das BSI seine Aufgaben wirksam hätte wahrnehmen können. So beruht die Einschätzung zu einer wirksameren Informationssicherheit infolge des IT-SiG 2.0 allein auf Annahmen des BMI.

→ Konkrete Erkenntnisse der Evaluation von Personal- und Sachaufwänden wären aber auch mit Blick auf die restlichen Einrichtungen der Bundesverwaltung relevant. Diese hätten ebenso erheben sollen, welche zusätzlichen Aufwände aufgrund der Aufgaben nach dem IT-SiG 2.0 bestehen. Auf Grundlage dieser Erkenntnisse hätte das BMI ein einheitliches Verständnis für Aufgaben und Maßnahmen in der Bundesverwaltung etablieren können. Dementsprechend wären Rückmeldungen der Bundesbehörden auch nicht mit einer zum Teil großen Unsicherheit belegt. Im Ergebnis müsste es möglich sein, abzugrenzen, welche Aufgaben die Bundesverwaltung bereits aufgrund des IT-SiG 2.0 zu erbringen hat und welche durch das BSIG-E jetzt wirklich neu hinzukommen. (vgl. Tz. 3)

Sofern dem BMI im Einzelfall genaue Erkenntnisse zur Wirksamkeit des aktuellen BSIG vorliegen, sollte es diese in das Gesetzgebungsverfahren einbringen.

Der hier vorliegende Gesetzentwurf enthält in der Begründung[60] die Absicht, eine „umfassende Evaluierung der Maßnahmen dieses Gesetzes spätestens nach fünf Jahren“ durchzuführen. Angesichts der Versäumnisse und fehlenden belastbaren Erkenntnisse bei der Evaluation des IT-SiG 2.0 hält der Bundesrechnungshof dieses Vorgehen nicht

[60] Vgl. Teil A „Allgemeiner Teil“, Abschnitt VIII „Befristung und Evaluierung“.

für ausreichend. Er empfiehlt daher, im BSIG-E bereits eine Evaluierung nach drei Jahren gesetzlich festzulegen.

Dies nur in der Gesetzesbegründung einzubringen, hält der Bundesrechnungshof für nicht ausreichend verbindlich. Er regt daher an, dass das BMI unter Mitwirkung des BMDS aufgrund seiner neuen Zuständigkeit dem Deutschen Bundestag zu den Fortschritten aus dem BSIG-E verpflichtend berichtet. Solche Sachstands- und Fortschrittsberichte bieten auch eine Kontroll- und Steuerungsfunktion für diesen wichtigen Bereich der Informationssicherheit in Bundesverwaltung und Wirtschaft. Die Evaluation des BSIG-E sollte dabei insbesondere auch das Verwaltungshandeln mit betrachten, um daraus Maßnahmen für ein effizienteres und effektiveres Handeln der Verwaltung ableiten zu können. Der Bundesrechnungshof regt daher an, folgende Regelung in das BSIG-E aufzunehmen:

> Das Bundesministerium des Innern berichtet dem Deutschen Bundestag unter Mitwirkung des Bundesministeriums für Digitalisierung und Staatsmodernisierung und unter Einbeziehung von wissenschaftlichem Sachverstand über die Wirksamkeit der in diesem Gesetz enthaltenen Maßnahmen für die Erreichung der mit diesem Gesetz verfolgten Ziele bis zum 1. Juli 2028.

4.1 Stellungnahme des BMI

Das BMI hat dargelegt, dass die gesetzliche Pflicht, eine zweite Stufe der Evaluierung des IT-SiG 2.0 durchzuführen, bei rechtzeitigem Inkrafttreten des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) gestrichen worden wäre. Dieses habe in der letzten Legislaturperiode jedoch nicht mehr verabschiedet werden können. Daher habe das BMI die Evaluation nunmehr in einem engen zeitlichen Rahmen durchführen müssen.

Diese Evaluation zeige u. a., dass die tatsächlichen Erfüllungsaufwände hinter den ursprünglich geschätzten zurückblieben. Begründet sei dies dadurch, dass das BSI Schwierigkeiten hatte, Personal zu gewinnen. Aber auch inhaltliche Schwächen der Normen hätten dazu beigetragen. Es sei daher prioritär, dass das BSI die kalkulierte Personalstärke für eine erfolgreiche Anwendung des Regelungsregimes erreiche. Laut BMI seien diese Erkenntnisse bereits in den Gesetzentwurf eingeflossen.

Darüber hinaus erachtet das BMI eine gesetzlich festgelegte Evaluation für nicht notwendig und nicht zielführend. Der Gesetzentwurf erfülle bereits das vom Staatssekretärsausschuss für „Bessere Rechtsetzung und Bürokratieabbau“ beschlossene Evaluierungskonzept. Unklarheiten über die Adressaten der Evaluationsergebnisse bestehen aus Sicht des BMI nicht. Sofern eine Evaluation gesetzlich weitergehend festgelegt

werde, sieht das BMI einen Konflikt mit der Evaluation der NIS-2-Richtlinie auf EU-Ebene. Zudem sei eine umfassende Datengrundlage gegeben. Denn u. a. aufgrund der Meldepflichten würden alle notwendigen Daten erhoben. Abschließend hat das BMI angegeben, dass eine gesetzliche Festlegung für eine Evaluation nicht sachgerecht sei. Grund hierfür sei die besondere Dynamik des nationalen IT-Sicherheitsrechts. Insofern sei eine gewisse Unsicherheit Teil der Regelungsmaterie und ließe sich daher nur durch Gesetzesänderungen an diese Entwicklungen anpassen. Dies sehe das BMI als nicht sachgerecht an.

4.2 Abschließende Bewertung des Bundesrechnungshofes

Die Ausführungen des BMI überzeugen den Bundesrechnungshof nicht. Das BMI stellte selbst inhaltliche Schwächen bei den Normen des IT-SiG 2.0 fest. Allerdings fanden diese nur an einer Stelle Eingang in den aktuellen Gesetzentwurf.

Zudem berücksichtigte das BMI bei seiner Datengrundlage nur seine eigenen Daten und die des BSI. Gerade bezüglich der Wirksamkeit der Normen, welche die Zusammenarbeit des BSI mit anderen Stellen der Bundesverwaltung – insbesondere anderen Aufsichtsbehörden – regeln, liefert die Evaluation keine Erkenntnisse. Die vom Bundesrechnungshof in diesem Bericht adressierten Fragestellungen bleiben daher offen.

Zudem erschließt sich nicht, warum eine Evaluation der nationalen Regelungen in Konflikt mit der auf EU-Ebene durchzuführenden treten könnte. Vielmehr sollte gerade eine nationale Evaluation Deutschland in die Lage versetzen, wichtige Impulse auf Ebene der europäischen Gesetzgebung zu geben. Zudem verkennt die Aussage des BMI zur Datengrundlage, dass Daten aus der Meldepflicht mitnichten die Zusammenarbeit des BSI mit anderen Einrichtungen der Bundesverwaltung hinreichend erfassen.

Darüber hinaus kann der Bundesrechnungshof nicht nachvollziehen, warum eine Dynamik im Bereich des nationalen IT-Sicherheitsrechts einer Evaluation entgegenstünde. Gerade weil es eine solche Dynamik gibt, sollte die Bundesregierung die Wirksamkeit des Regelungsregimes zeitgerecht evaluieren. Nur so kann sie Missstände oder Fehlentwicklungen erkennen und diesen konkret begegnen.

Der Bundesrechnungshof bleibt daher bei seiner Empfehlung, eine Evaluation gesetzlich zu verankern.

5 Fazit des Bundesrechnungshofes

Die Stellungnahme des BMI hat den Bundesrechnungshof nicht überzeugt. Sofern es sich nicht zu dessen Empfehlungen geäußert hat, geht der Bundesrechnungshof davon aus, dass das BMI seiner Argumentation nicht widerspricht. Die von ihm eingebrachten Empfehlungen dienen den Zielen der NIS-2-Richtlinie. Sie fördern somit einen ordnungsgemäßen und wirtschaftlichen Gesetzesvollzug, da sie

- → den IT-Grundschutz sowie Maßnahmen des Risikomanagements für die gesamte Bundesverwaltung gesetzlich vorschreiben,
- → Ausnahmenregelungen für das AA sinnvoll beschränken,
- → Nachweise der Informationssicherheit durch Einrichtungen der Bundesverwaltung in kürzeren Fristen festlegen,
- → die Verantwortung der Leitungsebene für die Informationssicherheit konkretisieren,
- → Aufgaben und Befugnisse einer oder eines CISO Bund für eine übergreifende Steuerung der Informations- und Cybersicherheit festlegen sowie
- → die Rolle des BSI als nationale Cybersicherheitsbehörde stärken.

Der Bundesrechnungshof empfiehlt daher, die von ihm vorgeschlagenen Änderungen im Gesetzgebungsprozess aufzugreifen und im Gesetz zu berücksichtigen. Zudem fordert er, von den Ressorts eingebrachte Mehrbedarfe bei Personal und Sachmitteln kritisch zu hinterfragen.

Essers Scherwa

Beglaubigt: Schmidt-Koch, Al`n
Wegen elektronischer Bearbeitung ohne Unterschrift und Dienstsiegelabdruck.