Bundesrechnungshof

Bericht nach § 88 Absatz 2 BHO

an den Haushaltsausschuss des Deutschen Bundestages und
an den Ausschuss für Inneres und Heimat des Deutschen Bundestages

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)

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

Gz.: VII 4 - 0002698 17. September 2024

Die Prüfungsergebnisse auf einen Blick

Umsetzung der NIS-2-Richtlinie: Chance für mehr Informations- und Cybersicherheit nicht verpassen

Die Bundesregierung läuft Gefahr, ihr Ziel zu verfehlen, die Informations- und Cybersicherheit zu verbessern. Sie will die NIS-2-Richtlinie der Europäischen Union 1:1 umsetzen, ihr bereits bekannte Defizite dabei jedoch nicht aufgreifen. Wenige Änderungen am Gesetzentwurf könnten das Sicherheitsniveau in der Bundesverwaltung deutlich erhöhen.

Worum geht es?

Deutschland muss neue Vorgaben der EU zur besseren Informations- und Cybersicherheit der Wirtschaftsunternehmen und der öffentlichen Verwaltung in nationales Recht umsetzen. Hierzu hat das Bundesministerium des Innern und für Heimat (BMI) einen entsprechenden Gesetzentwurf erarbeitet. Nach mehrfachen Ressortabstimmungen bleibt dieser in zentralen Punkten hinter den selbst gesteckten Zielen zurück. Wichtige Regelungen sollen nicht für die gesamte Bundesverwaltung in einheitlicher Weise verbindlich sein. Die Folge wäre ein „Flickenteppich“, der die Informations- und Cybersicherheit aller Beteiligten gefährden kann.

Was ist zu tun?

Im parlamentarischen Verfahren sollte der Gesetzentwurf nachgebessert werden. Insbesondere sollten die zentralen Vorgaben zur Informations- und Cybersicherheit für alle Bundesbehörden einheitlich gelten. Ausnahmen hiervon sind zu begrenzen. Der IT-Grundschutz als zentrales Instrument für die Informationssicherheit muss für alle Bundesbehörden und -einrichtungen gleichermaßen verbindlich sein. Die Funktion einer Koordinatorin oder eines Koordinators für Informationssicherheit ist mit angemessenen Aufgaben und Befugnissen auszustatten. Die Bedarfe der Bundesbehörden an zusätzlichen Haushaltsmitteln sind kritisch zu hinterfragen.

Was ist das Ziel?

Die Bundesverwaltung stärkt ihre Informations- und Cybersicherheit auf der Grundlage einheitlich geltender gesetzlicher Vorgaben. Bundesbehörden weisen bereits nach drei Jahren nach, dass sich ihre Informations- und Cybersicherheit deutlich verbessert hat. Die Koordinatorin oder der Koordinator steuert Informationssicherheit ressortübergreifend. Nach fünf Jahren zeigt die Evaluierung des Gesetzes anhand von messbaren Indikatoren auf, an welchen Stellen der Gesetzgeber die Regelungen bei Bedarf anpassen sollte.

Inhaltsverzeichnis

0 Abkürzungsverzeichnis

A

AA *Auswärtiges Amt*

B

BBK *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe*
BKAmt *Bundeskanzleramt*
BKG *Bundesamt für Kartographie und Geodäsie*
BMBF *Bundesministerium für Bildung und Forschung*
BMI *Bundesministerium des Innern und für Heimat*
BMVg *Bundesministerium der Verteidigung*
BSI *Bundesamt für Sicherheit in der Informationstechnik*
BSIG *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)*
BSIG-E *Entwurf eines Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen*
BWV *Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung*

C

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

E

EU *Europäische Union*

G

GAD *Gesetz über den Auswärtigen Dienst*
GGO *Gemeinsame Geschäftsordnung der Bundesministerien*

H

Haushaltsausschuss *Haushaltsausschuss des Deutschen Bundestages*

I

ISB *Informationssicherheitsbeauftragte/r*
IT-SiG 2.0 *IT-Sicherheitsgesetz 2.0*

K

KRITIS-Betreiber *Betreiber Kritischer Infrastrukturen*
KRITIS-DachG *Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen*

N

NdB *Netze des Bundes*
NIS-2-Richtlinie *Zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit*
NIS2UmsuCG *Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)*
NKR *Nationaler Normenkontrollrat*
NKRG *Gesetz zur Einsetzung eines Nationalen Normenkontrollrates*

U

UP Bund *Umsetzungsplan Bund*

V

VSA *Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung)*

1 Zusammenfassung

0.1 Die Bundesregierung ist verpflichtet, die sogenannte NIS-2-Richtlinie der EU[1] in nationales Recht umzusetzen. Hierzu hat das BMI langwierig den Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, NIS2UmsuCG)[2] erarbeitet und innerhalb der Bundesregierung abgestimmt. Am 24. Juli 2024 hat das Bundeskabinett den Regierungsentwurf beschlossen. Dieser liegt nunmehr dem Deutschen Bundestag zur Beratung vor. Mit ihm will die Bundesregierung den Ordnungsrahmen, den sie vor drei Jahren mit dem IT-Sicherheitsgesetz 2.0[3] (IT-SiG 2.0) geschaffen hat, auf rund 29 500 Unternehmen erweitern. Zusätzlich will sie wesentliche nationale Anforderungen an das Informationssicherheitsmanagement des Bundes gesetzlich verankern. Anlass hierfür geben aus Sicht der Bundesregierung die verschärfte Bedrohungslage, u. a. infolge der aktuellen geopolitischen Situation („Zeitenwende“) und die Erkenntnis, dass die Bundesverwaltung ihr Informationssicherheitsniveau flächendeckend steigern muss. (Tzn. 1.1 bis 1.4)

0.2 Der Präsident des Bundesrechnungshofes hat in seiner Funktion als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung (BWV) zu mehreren Referentenentwürfen umfangreich Stellung genommen. Das BMI hat zahlreiche Hinweise des BWV nicht aufgegriffen. Da einige davon für die Informations- und Cybersicherheit von besonderer Bedeutung sind, hält der Bundesrechnungshof es für geboten, den Haushaltsausschuss des Deutschen Bundestages (Haushaltsausschuss) und den Ausschuss für Inneres und Heimat des Deutschen Bundestages über diese in Kenntnis zu setzen. Mit dem vorliegenden Bericht unterbreitet er zum Regierungsentwurf konkrete Änderungsvorschläge.

Der Bundesrechnungshof hat dem BMI seine Änderungs- und Ergänzungsvorschläge zum Regierungsentwurf des NIS2UmsuCG zur Stellungnahme vorgelegt. Die Stellungnahme des BMI ist in dem vorliegenden Bericht berücksichtigt. (Tz. 1.5)

0.3 Der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist das grundlegende Regelwerk für die Informationssicherheit. Er ist für die Bundesverwaltung aufgrund eines Kabinettbeschlusses aus dem Jahr 2017 verbindlich.

---

1 Zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit.

2 Im NIS2UmsuCG verwendet die Bundesregierung – bereits im Namen des Gesetzes beginnend – die beiden Begriffe „Cybersicherheit“ und „Informationssicherheit“ ohne nähere Erläuterung weitgehend synonym. In dem Wissen, dass die beiden Begriffe eine durchaus leicht differenzierte Bedeutung haben (Cybersicherheit ist die IT-Sicherheit der im Cyberraum auf Datenebene vernetzten beziehungsweise vernetzbaren informationstechnischen Systeme, während Informationssicherheit den Schutz von Informationen zum Ziel hat, wobei diese sowohl u. a. auf Papier oder in Rechnern gespeichert sein können), verwendet auch der Bundesrechnungshof diese in dem vorliegenden Bericht in einem weitgehend synonymen Verständnis.

3 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (BGBl. 2021 I S. 1 122).

Damit sollen die Bundesbehörden für sich selbst und für den über die Netze des Bundes (NdB) zusammengeschlossenen Informationsverbund ein hinreichendes Informationssicherheitsniveau erreichen und aufrechterhalten. Die bisher nur untergesetzliche Festlegung dieses Instruments hat sich nach Ansicht der Bundesregierung bislang als nicht ausreichend effektiv erwiesen. Die Bundesverwaltung hat ihr Informationssicherheitsniveau bisher nicht flächendeckend wirksam gesteigert. Anstatt den IT-Grundschutz konsequenterweise für alle Bundesbehörden gesetzlich zu verankern, beschränkt der Gesetzentwurf dies nur auf die Bundesministerien und das Bundeskanzleramt (BKAmt). In einer vernetzten Bundesverwaltung ist dies weder sachgerecht noch im Vergleich zu den strikten gesetzlichen Verpflichtungen der Wirtschaftsunternehmen angemessen.
Der Bundesrechnungshof hat empfohlen, dass der IT-Grundschutz für die gesamte Bundesverwaltung einheitlich gesetzlich vorgegeben wird.

Das BMI hat hierzu keine Stellungnahme abgegeben. (Tz. 2.1)

0.4 Verschiedene Regelungen in dem Gesetzentwurf ermöglichen es, ganze Einrichtungen der Bundesverwaltung[4] oder Teile von diesen aus dem Anwendungsbereich des NIS2UmsuCG auszunehmen. Für den Geschäftsbereich des Auswärtigen Amts (AA) soll sich dies unmittelbar aus dem Gesetz ergeben. Konkrete Gründe hierfür sind allenfalls für den eng umrissenen Teil der sogenannten Auslands-IT nachvollziehbar. In anderen Fällen sollen die Informationssicherheitsbeauftragten (ISB) der Ressorts die alleinige Befugnis erhalten, Einrichtungen innerhalb ihres Ressorts von gesetzlichen Verpflichtungen unter bestimmten Bedingungen teilweise oder insgesamt zu befreien.
Der Bundesrechnungshof hat empfohlen, diese Ausnahmeregelungen zu begrenzen oder alternativ zumindest gleichwertige Ausgleichsmaßnahmen verbindlich vorzusehen.

Das BMI hat darauf hingewiesen, dass es rechtlich nicht zu beanstanden sei, das AA aus dem Anwendungsbereich der NIS2UmsuCG auszunehmen. Eine Aufspaltung in „Auslands-“ und „Inlands-IT“ würde zu verschiedenen Regelungsrahmen in derselben Behörde, Rechtsunsicherheit und erheblichen Einschränkungen der operativen Funktionsweise des AA führen. Zu den Ausnahmeregelungen für die übrige Bundesverwaltung hat sich das BMI nicht geäußert.

Der Bundesrechnungshof hält die Argumentation des BMI für nicht schlüssig. Es ist nicht ersichtlich, dass die Kontrolle der in Deutschland betriebenen IT des Auswärtigen Dienstes durch das BSI zu einer Rechtsunsicherheit und erheblichen Einschränkungen der operativen Funktionsweise des AA oder des Auswärtigen Dienstes führen könnten. Vielmehr dürften diese Kontrollen zu einem hohen Sicherheitsniveau

[4] Zu den Einrichtungen der Bundesverwaltung zählen neben den Bundesbehörden auch Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts als Teil der mittelbaren Bundesverwaltung (vgl. § 29 Absatz 1 BSIG-E).

beitragen. Der Bundesrechnungshof regt deswegen dringend an, mit dem NIS2UmsuCG keine über das IT-SiG 2.0 hinausgehenden Ausnahmen für das AA zu schaffen. Vielmehr sollte das NIS2UmsuCG das BSI auch gegenüber dem Auswärtigen Dienst stärken und helfen, dort die Informations- und Cybersicherheit zu verbessern.
Der Bundesrechnungshof hält es weiterhin für erforderlich, die Ausnahmeregelungen auch für die übrige Bundesverwaltung zu begrenzen, um ein bundesweit einheitlich hohes Sicherheitsniveau zu erreichen. (Tzn. 2.2 und 2.3)

0.5 Betreiber kritischer Infrastrukturen sind seit Jahren verpflichtet, dem BSI nachzuweisen, dass sie die Vorgaben zur Informations- und Cybersicherheit einhalten. Der Gesetzentwurf sieht vor, dass sie diese Nachweise alle drei Jahre vorlegen müssen. Für Bundesbehörden gelten bisher keine entsprechenden Verpflichtungen. Das BSI hat zwar seit drei Jahren die Befugnis zu Kontrollen in der Bundesverwaltung, kann diese aber derzeit aufgrund fehlender Personalressourcen nicht flächendeckend sicherstellen.
Der Bundesrechnungshof unterstützt daher die Absicht der Bundesregierung, dass auch die Bundesbehörden einen Nachweis über den Stand ihrer Cybersicherheit vorlegen müssen. Die vorgesehene Frist von fünf Jahren hält er allerdings für unangemessen lang. Er hat empfohlen, diese analog zur Wirtschaft auf drei Jahre festzulegen.

Das BMI hat sich hierzu nicht geäußert. (Tz. 2.4)

0.6 Mit der Koordinatorin oder dem Koordinator für Informationssicherheit will die Bundesregierung eine neue Funktion schaffen. In zahlreichen Staaten und in Wirtschaftsunternehmen gibt es diese unter der Bezeichnung CISO[5] bereits seit längerem. Ein CISO steuert – gegebenenfalls zusammen mit einem Gremium – das Informationssicherheitsmanagement auf der obersten Ebene.
Der Gesetzentwurf sieht lediglich vor, dass die Bundesregierung diese Funktion einrichtet und mit einer Person besetzt. Deren Aufgaben und Befugnisse regelt er nicht. Wie die Koordinatorin oder der Koordinator angesichts des weitgehenden Ressort- und Einstimmigkeitsprinzips[6] in der IT des Bundes ohne eigene Aufgaben und Befugnisse ressortübergreifend die gebotene Wirkung erzielen soll, bleibt unklar. Der Bundesrechnungshof hat empfohlen, die wesentlichen Aufgaben und Befugnisse der Koordinatorin oder des Koordinators für Informationssicherheit gesetzlich zu verankern.

Das BMI hat in seiner Stellungnahme darauf hingewiesen, dass der Haushaltsausschuss die Bundesregierung dazu aufgefordert hat, ein Konzept zu erarbeiten, das

---

5 Chief Information Security Officer.

6 Das **Ressortprinzip** ist ein deutscher Regierungsgrundsatz, der besagt, dass der Bundesminister seinen Geschäftsbereich selbstständig und unter eigener Verantwortung leitet. Dabei muss er sich an die Richtlinien der Politik halten, die durch den Bundeskanzler vorgegebenen werden. Artikel 65 Satz 2 Grundgesetz.
Das **Einstimmigkeitsprinzip** sieht vor, dass die Ressorts in den Entscheidungsgremien, sofern sie keine anderen Regelungen getroffen haben, sich bei allen Ressorts betreffenden Entscheidungen auf einen gemeinsamen Beschluss einigen müssen.

u. a. Vorschläge zur Einrichtung eines CISO Bund enthalten soll. Eine Ausgestaltung dieser Rolle im Gesetzentwurf würde dieses Konzept vorwegnehmen. Daher sei die Rolle CISO Bund im Gesetzentwurf nur allgemein eingeführt.

Der Bundesrechnungshof weist darauf hin, dass es der Bundesregierung nicht gelungen ist, sich innerhalb von fünf Monaten auf ein gemeinsames Konzept für einen CISO Bund zu einigen. Dies wird der Bedrohungslage in der Bundesverwaltung nicht gerecht. Da der CISO Bund eine wichtige Funktion bei der übergreifenden Steuerung der Informations- und Cybersicherheit in der Bundesverwaltung hat, sollte der Gesetzgeber verpflichtende Leitplanken für dessen Tätigkeit gesetzlich verankern. Der Bundesrechnungshof bleibt daher bei seinen Empfehlungen. (Tz. 2.6)

0.7 Zeitgleich zu der NIS-2-Richtlinie hat die EU auch eine Richtlinie zum physischen Schutz Kritischer Infrastrukturen beschlossen. Das BMI erarbeitet derzeit einen Entwurf des sogenannten KRITIS-Dachgesetzes, mit dem diese Richtlinie in nationales Recht umgesetzt werden soll. Für wesentliche Vollzugs- und Aufsichtsaufgaben soll das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zuständig sein. Informations- und Cybersicherheit sowie physische Sicherheit haben einen engen Bezug. Daher müssen die beiden Gesetze aufeinander abgestimmt sein. Deshalb hat der Bundesrechnungshof bereits im Vorfeld des Regierungsentwurfs des KRITIS-Dachgesetzes darauf hingewiesen, dass beide Gesetze Begriffe sowie Befugnisse einheitlich definieren sollten. Zudem sollten die Gesetze die Voraussetzungen für eine gemeinsame Datenbasis von BSI und BBK schaffen. Die Regelungen sollten vermeiden, dass Daten mehrfach erhoben oder gespeichert werden und Informationen verloren gehen oder sich ihre Weitergabe verzögert. Dies könnte auch Grundlage für ein gemeinsames Lagebild für den KRITIS-Bereich sein.

Das BMI hat in seiner Stellungnahme mitgeteilt, dass es anstrebe, die Regelungen des Gesetzesentwurfs und des zukünftigen KRITIS-DachG größtmöglich aufeinander abzustimmen. So habe es das gemeinsame Melde- und Registrierungsportal[7] als zentralen Grundstein für die künftige Zusammenarbeit von BSI und BBK vorgesehen.

Der Bundesrechnungshof begrüßt, dass das BMI die beiden gesetzlichen Vorhaben aufeinander abstimmen möchte. Er hält an seiner Auffassung fest, dass das NIS2UmsuCG außerdem Regelungen für eine gemeinsame Datenbasis sowie ein gemeinsames Lagebild von BSI und BBK treffen sollte. (Tz. 2.7)

0.8 Die Bundesregierung beziffert die in den Jahren 2026 bis 2029 zusätzlich zu erwartenden Haushaltsausgaben auf insgesamt 810 Mio. Euro. Ursächlich hierfür sind im Wesentlichen der Bedarf an 1 034 zusätzlichen Planstellen und Stellen (im Folgenden: Stellen) sowie die dadurch bedingten Personalausgaben. Die Angaben in der Gesetzesbegründung bilden den Mehrbedarf aus dem NIS2UmsuCG für die Bundesverwaltung nicht belastbar ab. Bedarfe vergleichbarer Ressorts weichen ohne erkennbaren

[7] § 32 Absatz 1 sowie § 33 Absatz 1 BSIG-E.

Grund deutlich voneinander ab. Dies lässt die Annahme zu, dass sie Personal- und Sachmittelbedarfe auch für Aufgaben ausgewiesen haben, die ihnen bereits ohne das NIS2UmsuCG verpflichtend obliegen.
Der Bundesrechnungshof hat darauf hingewiesen, dass mögliche Anforderungen zusätzlicher Haushaltsmittel nach dem Inkrafttreten des NIS2UmsuCG kritisch überprüft werden sollten.

Das BMI hat zugesagt, nach Inkrafttreten des Gesetzes die in diesem dargestellten Mehrbedarfe zu evaluieren. Die vom Bundesrechnungshof angemerkten Zweifel hinsichtlich der für die einzelnen Ressorts angegebenen Zahlen beruhten auf prozentualen Vergleichen. Dabei sei zu berücksichtigen, dass zur Umsetzung der Vorgaben der NIS2-Richtlinie in jedem Ressort zusätzliche Rollen und Funktionen einzurichten und zu besetzen seien. Diese wirkten sich bei kleineren Ressorts naturgemäß stärker aus. Zudem sei zu berücksichtigen, dass je nach Größe der Ressorts der aktuelle Umsetzungsstand bei der Informationssicherheit stark variieren könne.

Der Bundesrechnungshof weist daraufhin, dass alle Ressorts bereits seit Jahren Vorgaben zur Informationssicherheit erfüllen müssen. Aus welchen Gründen einzelne Ressorts diese nicht vollumfänglich einhalten, ist für die Schätzung des zusätzlichen Stellen- und Sachmittelbedarfs für das NIS2UmsuCG unerheblich. Unzureichende Stellen- und Sachmittelanmeldungen der Vergangenheit dürfen nicht dem NIS2UmsuCG zugerechnet werden. Der Bundesrechnungshof hält deswegen an seiner Empfehlung fest. (Tz. 3)

0.9 Zu folgenden Punkten äußerte sich das BMI nicht:

- IT-Grundschutz und Maßnahmen für die gesamte Bundesverwaltung gesetzlich verankern,
- weitreichende Ausnahmeregelungen für Einrichtungen der Bundesverwaltung beschränken,
- Nachweis der Informationssicherheit durch Einrichtungen der Bundesverwaltung in kürzeren Fristen vorsehen sowie
- Verantwortung der Einrichtungsleitung für Informationssicherheit konkretisieren.

Der Bundesrechnungshof geht davon aus, dass das BMI seine Empfehlungen zu diesen Textziffern grundsätzlich mitträgt.

Die zu den übrigen Textziffern vorgetragenen Argumente haben den Bundesrechnungshof in weiten Teilen nicht überzeugt. Er bleibt daher bei seinen Änderungs- und Ergänzungsvorschlägen. (Tz. 4)

2 Einleitung

Der Präsident des Bundesrechnungshofes hat in seiner Funktion als BWV zu mehreren Referentenentwürfen des NIS2UmsuCG umfangreich Stellung genommen. Die Bundesregierung hat einige besonders bedeutsame Anregungen des BWV nicht aufgegriffen. Daher hält der Bundesrechnungshof es für geboten, den Haushaltsausschuss und den Ausschuss für Inneres und Heimat des Deutschen Bundestages unmittelbar zu informieren und Änderungen anzuregen. Die Änderungen haben wir in diesem Bericht nach § 88 Absatz 2 BHO zusammengefasst. Sofern das BMI zu den einzelnen Punkten dieses Berichtes Stellung genommen hat, hat der Bundesrechnungshof diese berücksichtigt und abschließend bewertet.

2.1 Aktuelle Lage zur Cybersicherheit in Staat und Wirtschaft

Die Bedrohung von Staat, Wirtschaft und Gesellschaft im Cyberraum ist so hoch wie nie. Dies hat das BSI erneut in seinem aktuellen Lagebericht festgestellt.[8] Die fortschreitende Digitalisierung, die zunehmende Vernetzung und der verstärkte Einsatz von KI vergrößern die Angriffsflächen erheblich. Cyberkriminelle aus dem In- und Ausland nutzen diese in großem Umfang.[9] Das BMI verweist hierzu auf den kürzlich vom Branchenverband Bitkom e. V vorgestellten Wirtschaftsschutzbericht 2024.[10] Dieser schätzt die unmittelbar durch Cyberangriffe verursachten und bezifferbaren Schäden für die deutsche Wirtschaft. Er zeigt dabei einen starken Zuwachs bei der Schadenshöhe. Im Jahr 2022 lag der Gesamtschaden bei knapp 203 Mrd. Euro. Davon entfielen etwa 128 Mrd. Euro auf Schäden durch Cyberangriffe. Im Jahr 2023 lag der Gesamtschaden bei knapp 206 Mrd. Euro mit einem Anteil von 148 Mrd. Euro für Schäden durch Cyberangriffe. Basierend auf einer neuen Erhebung geht der Bericht für das Jahr 2024 von Gesamtschäden in Höhe von etwa 267 Mrd. aus, wovon etwa 179 Mrd. Euro auf Cyberangriffe entfallen.

Neben dem monetären Schaden geht es für die öffentliche Verwaltung um die Sicherheit und das Vertrauen der Bürgerinnen und Bürger. Denn die Aufrechterhaltung staatlicher Funktionen – insbesondere in Krisensituation – ist gefährdet. Das verdeutlichen in jüngster

---

8 Die Lage der IT-Sicherheit in Deutschland 2023, Hrsg.: BSI, Oktober 2023; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html, abgerufen am 12. August 2024.

9 Bundeslagebild Cybercrime 2023, Hrsg. Bundeskriminalamt, Mai 2024; https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2023/CC_2023.html, abgerufen am 12. August 2024.

10 https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024

Zeit umfangreiche und langandauernde Ausfälle zentraler IT-Dienste auf kommunaler Ebene.[11, 12]

Prüfungserkenntnisse des Bundesrechnungshofes zeigen seit Jahren erhebliche konzeptionelle und technische Defizite in der Absicherung der IT-Infrastrukturen der Bundesbehörden auf. Die Bundesregierung räumt in ihrem vorliegenden Gesetzentwurf selbst ein, dass in vielen Einrichtungen der Bundesverwaltung die Maßnahmen zum Eigenschutz im Bereich der Informationssicherheit defizitär seien. Vor dem Hintergrund der durch aktuelle geopolitische Entwicklungen („Zeitenwende“) abermals verschärften Bedrohungslage habe sich das Risiko für staatliche Einrichtungen zudem weiter erhöht. Gefährdungen aus dem Cyberraum können die Handlungsfähigkeit staatlicher Einrichtungen einschränken.[13] Wenn die Bundesverwaltung bestehende Mängel nicht zügig beseitigt, ist es nach Ansicht des BSI keine Frage, ob es zu einem großflächigen Ausfall kommt, sondern lediglich wann dies geschieht.

Der Bundesrechnungshof erachtet es daher als notwendig, dass das NIS2UmsuCG der Bundesregierung, der Bundesverwaltung und der Wirtschaft vergleichbare Anforderungen und Pflichten vorgibt, um diese Herausforderungen zu adressieren.

2.2 BSI-Gesetz

Gesetzliche Vorgaben für die Informationssicherheit sind in zahlreichen Gesetzen zu finden.[14] Von zentraler Bedeutung ist das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG). Dieses hat der Gesetzgeber zuletzt im Jahr 2021 mit dem IT-SiG 2.0 umfassend geändert. Der Schutz der IT der Bundesverwaltung sollte damit u. a. durch weitere Prüf- und Kontrollbefugnisse des BSI und die Vorgabe von Mindeststandards erhöht werden. Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber) und weitere Unternehmen im besonderen öffentlichen Interesse haben seitdem zusätzliche Pflichten[15] zu erfüllen. Die Begründung zu dem IT-SiG 2.0 wies für das BSI einen Bedarf von 799 zusätzlichen Stellen aus.

Das BSI nimmt diese zusätzlichen Kontroll-, Aufsichts- und Unterstützungsaufgaben bislang nach eigenen Angaben rudimentär, überwiegend mit geringer Intensität und zu Lasten der Bestandsaufgaben wahr. Ursächlich hierfür sei das immer noch große Delta zwischen dem

---

11 Der Cyberangriff auf den Dienstleister Südwestfalen-IT im Oktober 2023 war eine der bisher folgenreichsten Attacken auf den öffentlichen Sektor und lähmte über 70 Kommunen im Einzugsbereich des Dienstleisters; https://www.heise.de/news/Nach-verheerendem-Angriff-auf-Suedwestfalen-IT-205-Kommunen-lassen-IT-pruefen-9651073.html, abgerufen am 13. August 2024.

12 Ein massiver Hackerangriff auf die Verwaltung des Rhein-Pfalz-Kreises führte im Oktober 2022 zu längeren Ausfällen bei Dienstleistungen für die Bürgerinnen und Bürger, https://www.csoonline.com/de/a/massiver-hackerangriff-auf-kreisverwaltung-des-rhein-pfalz-kreises,3674241, abgerufen am 13. August 2024.

13 Gesetzesbegründung zu Artikel 1 des NIS2UmsuCG, § 29.

14 So enthalten beispielsweise das Energiewirtschafts- und das Telekommunikationsgesetz umfangreiche Vorgaben für die Betreiber kritischer Anlagen in diesen Sektoren.

15 Hierzu gehören u. a. Meldepflichten von Störungen, die Registrierung als KRITIS-Betreiber oder der Einsatz von Systemen zur Angriffserkennung.

„anerkannten Erfüllungsaufwand“ für das IT-SiG 2.0 und den seitdem zugewiesenen Stellen. Dies wirkt sich auf das bereits gemäß IT-SiG 2.0 zu erreichende und das künftig weiter zu steigernde Informations- und Cybersicherheitsniveau Deutschlands aus.

Der Deutsche Bundestag hat das BMI verpflichtet, die Wirksamkeit der im IT-SiG 2.0 enthaltenen Maßnahmen bis zum 1. Mai 2025 zu evaluieren und ihm über die Ergebnisse zu berichten. Trotz der anstehenden Novellierung des BSIG hat das BMI diese Evaluierung nicht vorgezogen.[16] Entsprechend fehlten ihm valide und strukturierte Erkenntnisse, die es im vorliegenden Gesetzentwurf hätte berücksichtigen können.

2.2.1 Stellungnahme des BMI

Das BMI teilt mit, es habe die Ergebnisse der bis zum 1. Mai 2023 durchzuführenden Evaluierung der in Artikel 6 Absatz 1 Nummer 1 des IT-SiG 2.0 genannten Vorschriften bei der Novellierung des BSI-Gesetzes berücksichtigt. Die gemäß Artikel 6 Absatz 1 Nummer 2 des IT-SiG 2.0 bis zum 1. Mai 2025 durchzuführende Evaluierung der übrigen Vorschriften des IT-SiG 2.0 erübrige sich. Denn diese würden in weiten Teilen im Zuge der Richtlinienumsetzung im Gesetzentwurf geändert. Die unveränderten Vorschriften würden durch das NIS2UmsuCG bestätigt. Folglich sehe der Entwurf des NIS2UmsuCG in Artikel 7 vor, die letztgenannte gesetzliche Evaluierungspflicht entfallen zu lassen.

2.2.2 Abschließende Bewertung des Bundesrechnungshofes

Das BMI geht nicht darauf ein, dass das BSI viele seiner Aufgaben und Befugnisse aus dem IT-SiG 2.0 derzeit nur rudimentär wahrnimmt. Ohne Evaluation bleibt offen, ob das NIS2UmsuCG die Regelungen so anpasst, dass

- das BSI nun effektiv und effizient seine fortzuführenden, angepassten oder neuen Aufgaben und Befugnisse wahrnehmen kann und
- etwaige Schwächen der bisherigen Regelungen des IT-SiG 2.0 beseitigt werden.

Der Bundesrechnungshof ist weiterhin der Auffassung, dass es sachgerecht gewesen wäre, die Evaluation vorzuziehen. Denn Erkenntnisse zum Vollzug des IT-SiG 2.0 hätten es ermöglicht, Regelungen zur Umsetzung der NIS-2-Richtlinie passgenau auszurichten. Diese Chance hat die Bundesregierung nicht genutzt.

Die Bundesregierung plant nun ausweislich der Gesetzesbegründung, das NIS2UmsuCG spätestens nach fünf Jahren zu evaluieren. Diese Absicht bewertet der Bundesrechnungshof grundsätzlich positiv, nachdem die vollständige Evaluation des IT-SiG 2.0 unterblieben ist. Hierfür ist es wichtig, geeignete messbare Indikatoren zu definieren, anhand derer die

[16] Das BMI ist lediglich der in Artikel 6 Absatz 1 Nummer 1 IT-SiG 2.0 auf einen früheren Zeitpunkt festgelegten Verpflichtung nachgekommen, die Regelungen zu den KRITIS-Betreibern zu evaluieren.

Bundesregierung belastbar die Wirkung der Richtlinienumsetzung belegen und Wechselwirkungen mit anderen Gesetzen bewerten kann. Deutschland unterscheidet sich z. B. im Aufbau seiner Verwaltung, Wirtschaft und Risikoexposition von anderen Staaten. Daher sollte die Bundesregierung darauf achten, Wirkungsindikatoren zu entwickeln, die auch diese nationalen Besonderheiten erfassen. So kann Deutschland die übergreifende Evaluation der Europäischen Kommission zur NIS-2-Richtlinie durch seine spezifische nationale Evaluation ergänzen. Der Bundesrechnungshof erwartet, dass die Bundesregierung hierfür ein Konzept vorlegt.

2.3 NIS-2-Richtlinie der EU

Das Europäische Parlament und der Rat der EU haben die NIS-2-Richtlinie[17] am 14. Dezember 2022 beschlossen. Die EU-Mitgliedstaaten müssen die Richtlinie bis zum 17. Oktober 2024 in nationales Recht umsetzen. Die aktuelle NIS-2-Richtlinie entwickelt die (erste) NIS-Richtlinie aus dem Jahr 2016 weiter. Die NIS-2-Richtlinie soll in der gesamten EU 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 NIS-2-Richtlinie reiht sich ein in eine Reihe von weiteren gesetzlichen Vorgaben, die die EU in Form von Verordnungen beschlossen hat oder in Kürze beschließen will, beispielsweise

- 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]).

---

[17] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nummer 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148, veröffentlicht am 27. Dezember im Amtsblatt L333 der EU.

[18] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der EU 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) Nummer 600/2014, (EU) Nummer 909/2014 und (EU) 2016/1011.

[20] Das Europäische Parlament hat den CRA im März 2024 verabschiedet. Die Zustimmung des Rates wird im Herbst 2024 erwartet.

2.4 NIS2UmsuCG

Um die NIS-2-Richtlinie in nationales Recht umzusetzen, stimmte das BMI im Frühjahr 2023 zunächst innerhalb der Bundesregierung ein Eckpunktepapier ab. Es legte darin fest, dass

- ein Gesetz, das NIS2UmsuCG, die NIS-2-Richtlinie umsetzen soll,
- dessen Artikel 1 im Wesentlichen das BSIG neu fassen soll und
- das Gesetz weitere wesentliche bisher untergesetzliche Regelungen zur Informationssicherheit für den Bereich der Bundesverwaltung erstmals gesetzlich verankern soll; es soll damit über eine reine 1:1-Umsetzung der NIS-2-Richtlinie hinausgehen.

Am 18. Juli 2023 leitete das BMI mit dem ersten Referentenentwurf des NIS2UmsuCG die Ressortabstimmung ein. Nach einjährigen intensiven Verhandlungen innerhalb der Bundesregierung und vier weiteren Referentenentwürfen beschloss das Bundeskabinett den Regierungsentwurf des NIS2UmsuCG am 24. Juli 2024.

2.5 Äußerungen des BWV zu den Gesetzentwürfen

Das BMI hat den Präsidenten des Bundesrechnungshofes in seiner Funktion als BWV bei dem Gesetzesvorhaben beteiligt (§ 45 Absatz 3 Satz 2 GGO[21]). Der BWV hat zu den ersten drei Referentenentwürfen am 16. August 2023, am 18. Januar 2024 und am 24. Mai 2024 umfangreich Stellung genommen. Das BMI hat einzelne der insgesamt annähernd 40 Hinweise des BWV aufgegriffen. In zwei Gesprächen haben der BWV und das BMI die übrigen Hinweise vertieft erörtert. Die Argumente des BMI haben den BWV dabei überwiegend nicht überzeugt. Er hält daher an seinen Änderungsvorschlägen im Wesentlichen fest.

Gemäß § 51 Nummer 4 GGO hat das federführende Bundesministerium im Anschreiben zur Kabinettvorlage anzugeben, welche abweichenden Meinungen aufgrund der Beteiligungen nach § 45 GGO bestehen. Die Kabinettvorlage des BMI enthält keinen Hinweis auf die wesentlichen verbliebenen Kritikpunkte des BWV. Der Bundesrechnungshof und der BWV missbilligen diesen Verstoß gegen die GGO.

2.5.1 Stellungnahme des BMI

Nach Auffassung des BMI erfülle das Anschreiben zur Kabinettvorlage sämtliche Anforderungen der GGO. Über die allgemein gültige Formulierung hinaus, dass es Stellungnahmen und Anregungen im Rahmen der Möglichkeiten berücksichtigt habe, soweit sie sachdienlich waren, hätte es nichts ausführen müssen.

[21] Gemeinsame Geschäftsordnung der Bundesministerien vom 1. September 2000, zuletzt geändert durch Beschluss der Bundesregierung am 1. Juni 2024.

2.5.2 Abschließende Bewertung des Bundesrechnungshofes

§ 51 Satz 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 diese Meinungen als sachdienlich einschätzt. Es ist Aufgabe des BWV, auf ein wirtschaftliches Handeln der Bundesverwaltung und deren dementsprechende Organisation hinzuwirken. Naturgemäß unterscheiden sich häufig die Maßstäbe, anhand derer Ressorts und BWV beurteilen, ob gesetzliche Regelungen sachdienlich und wirtschaftlich sind. Das BMI hätte somit die Bundesregierung über die unterschiedliche Auffassung des BWV informieren müssen.

2.6 CER-Richtlinie der EU, Entwurf des KRITIS-DachG

Zeitgleich zu der NIS-2-Richtlinie ist die EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie[22]) am 16. Januar 2023 in Kraft getreten. Sie verpflichtet die EU-Mitgliedstaaten, kritische Einrichtungen zu identifizieren und deren physische Widerstandsfähigkeit gegenüber Bedrohungen wie Naturgefahren, Terroranschläge oder Sabotageakte zu stärken. Das BMI beabsichtigt, die CER-Richtlinie mit dem Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-DachG) in nationales Recht umzusetzen. Anders als beim NIS2UmsuCG liegt hierzu ein vom Bundeskabinett beschlossener Regierungsentwurf noch nicht vor.

In seinem Eckpunktepapier zum NIS2UmsuCG hat das BMI bekundet, es strebe ein kohärentes Ineinandergreifen der Regelungsregime für den physischen und den digitalen Schutz Kritischer Infrastrukturen an. Denn alle unter der CER-Richtlinie identifizierten Einrichtungen fielen automatisch auch unter das NIS2UmsuCG.

Mit dem KRITIS-DachG sollen dem BBK zentrale Aufgaben, wie beispielsweise die Registrierung oder die Bearbeitung von Sicherheitsvorfällen von Betreibern kritischer Anlagen, übertragen werden. Vergleichbare Aufgaben sieht das NIS2UmsuCG für das BSI vor. Um den Aufwand für die Bundesverwaltung wie auch für die Wirtschaft möglichst gering zu halten, kommt es daher entscheidend darauf an, dass diese beiden Behörden eng zusammenarbeiten und entsprechende Prozesse geeignet gestalten.

[22] Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates.

3 NIS2UmsuCG nachbessern

3.1 IT-Grundschutz und Maßnahmen zum Risikomanagement für die gesamte Bundesverwaltung gesetzlich verankern (Artikel 1[23], § 29 Absatz 2, § 44 Absatz 2 NIS2UmsuCG)

IT-Grundschutz und Mindeststandards des BSI sind wesentliche Instrumente für die Informationssicherheit

Die Bundesregierung stellt in der Begründung des Gesetzentwurfs fest, dass sich die bisherigen Steuerungsinstrumente für das Informationssicherheitsmanagement in der Bundesverwaltung als nicht effektiv genug erwiesen hätten. Die überwiegend untergesetzlichen Regelungen hätten nicht ausgereicht, um flächendeckend das Sicherheitsniveau zu steigern.[24] Mit dem NIS2UmsuCG möchte die Bundesregierung dieses Problem lösen, indem sie wesentliche nationale Anforderungen an das Informationssicherheitsmanagement des Bundes gesetzlich verankert.[25]

Mit dem IT-Grundschutz stellt das BSI das grundlegende Regelwerk bereit, um das Informationssicherheitsniveau in Einrichtungen des Bundes oder Wirtschaftsunternehmen anzuheben und aufrechtzuerhalten. Er ist der bewährte Standard zum Aufbau eines Informationssicherheitsmanagements.[26] Neben technischen Aspekten betrachtet diese ganzheitliche Methodik auch infrastrukturelle, organisatorische und personelle Themen. Der IT-Grundschutz umfasst neben den BSI-Standards

- 200-1 Managementsysteme für Informationssicherheit,
- 200-2 IT-Grundschutz-Methodik,
- 200-3 Risikoanalyse auf Basis des IT-Grundschutzes und
- 200-4 Business Continuity Management

auch das IT-Grundschutz-Kompendium. Dieses enthält konkrete Anforderungen zu Themen der Informationssicherheit (IT-Grundschutzbausteine) sowie Hinweise zu deren Umsetzung.

---

[23] Artikel 1 des Entwurfs des NIS2UmsuCG enthält die Novelle des BSIG. In diesem Bericht bezeichnet der Bundesrechnungshof diese auch als Entwurf des BSIG (BSIG-E).

[24] Gesetzentwurf, Buchstabe A. Problem und Ziel.

[25] Gesetzentwurf, Buchstabe B. Lösung, Nutzen.

[26] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html, abgerufen am 15. August 2024.

Der Umsetzungsplan Bund (UP Bund) ist die vom Bundeskabinett im Jahr 2017 beschlossene Informationssicherheitsleitlinie der Bundesverwaltung. Die Leitlinie gilt für alle Ressorts und Bundesbehörden.[27] Für diese legt sie die im aktuellen IT-Grundschutz des BSI beschriebene Standard-Absicherung[28] als Mindestanforderung für die Informationssicherheit fest.

Die Sicherheitsanforderungen an die IT sind in der Bundesverwaltung unterschiedlich. Beispielsweise haben Sicherheitsbehörden im Regelfall andere (höhere) Anforderungen als Behörden im Forschungsbereich. Um ein gemeinsames Mindestniveau an Informationssicherheit zu erreichen, hat das BSI insgesamt acht sogenannte Mindeststandards für die Bundesverwaltung veröffentlicht.[29]

IT-Grundschutz soll nur für Teile der Bundesverwaltung gesetzlich verankert werden

§ 44 BSIG-E definiert die Vorgaben des BSI zur Informationssicherheit von Einrichtungen der Bundesverwaltung. Gemäß Absatz 1 müssen diese „[…] *die jeweils geltenden Fassungen der Mindeststandards für die Sicherheit in der Informationstechnik des Bundes (Mindeststandards) als Mindestanforderungen zum Schutz der in der Bundesverwaltung verarbeiteten Informationen erfüllen*“. Diese Vorgabe entspricht dem bislang gültigen § 8 Absatz 1 BSIG.

Gemäß Absatz 2 müssen (nur) das BKAmt und die Bundesministerien „[…] *als zusätzliche Mindestanforderungen die BSI-Standards und das IT-Grundschutz-Kompendium des BSI (IT-Grundschutz) in den jeweils geltenden Fassungen einhalten*“. Damit will die Bundesregierung für diese Behörden neben den Mindeststandards auch den IT-Grundschutz gesetzlich verankern. Für die übrigen Einrichtungen der Bundesverwaltung ergebe sich die Verpflichtung, den IT-Grundschutz einzuhalten, unverändert aus dem bestehenden Kabinettbeschluss zum UP Bund.

Zentrale Norm für die Informationssicherheit soll ebenfalls nur für Teile der Bundesverwaltung gelten

Sämtliche Einrichtungen der Bundesverwaltung zählen nach Maßgabe des Gesetzentwurfs zu den „besonders wichtigen Einrichtungen“.[30] Die NIS-2-Richtlinie fordert dies grundsätzlich

---

[27] Im militärischen Bereich des Bundesministeriums für Verteidigung einschließlich des Militärischen Abschirmdienstes sowie der Nachrichtendienste kann im jeweils erforderlichen Maß von den Vorgaben des UP Bund abgewichen werden.

[28] Der BSI-Standard 200-2 unterscheidet zwischen Basis, Standard- und Kern-Absicherung für IT-Systeme. Diese Abstufung ermöglicht es, die Sicherheitsmaßnahmen an den jeweiligen Schutzbedarf anzupassen.

[29] Mindeststandards gibt es derzeit beispielsweise zu den Themen Webbrowser, Nutzung externer Cloud-Dienste, Management mobiler Endgeräte, Videokonferenzsysteme und Nutzerpflichten NdB; vgl. https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mindeststandards_node.html, abgerufen am 29. Juli 2024.

[30] § 29 Absatz 2 Satz 1 BSIG-E.

nur für die von einem EU-Mitgliedstaat gemäß nationalem Recht definierten Einrichtungen der öffentlichen Verwaltung der Zentralregierung.[31, 32] Die Bundesregierung beabsichtigt mit dem NIS2UmsuCG bewusst, darüber hinauszugehen. Sie will insgesamt ein gemeinsames, kohärentes und handhabbares Regelungsregime für die Informationssicherheit erreichen.[33]

§ 30 BSIG-E legt wesentliche Anforderungen fest, um die Informationssicherheit sicherzustellen, und ist damit eine zentrale Norm des neu gefassten BSIG. Die dort aufgelisteten Risikomanagementmaßnahmen sollen für alle 29 500 Unternehmen gelten, die das NIS2UmsuCG nach Schätzungen des BMI betrifft. Allerdings sieht § 29 Absatz 2 Satz 2 BSIG-E vor, dass ausschließlich die Bundesministerien und das BKAmt die in § 30 BSIG-E festgelegten Maßnahmen zum Risikomanagement besonders wichtiger Einrichtungen anzuwenden haben. Warum die übrigen Einrichtungen der Bundesverwaltung hiervon ausgenommen sein sollen, ist der Gesetzesbegründung zu § 29 BSIG-E nicht zu entnehmen.

Weitreichende Ausnahmen vom IT-Grundschutz gefährden das Ziel, das Sicherheitsniveau zu steigern

Im Vergleich zur bisherigen Gesetzeslage würde sich mit dem NIS2UmsuCG im Ergebnis nur eines ändern: Die Bundesministerien und das BKAmt müssten auch den IT-Grundschutz kraft Gesetzes umsetzen. Für die weit überwiegende Anzahl der Einrichtungen der Bundesverwaltung würde es beim Status quo bleiben, der bis dato in § 8 Absatz 1 BSIG und im UP Bund festgelegt ist. Für sie wären unverändert nur die Mindeststandards gesetzlich verankert. Dies hat aber nach Ansicht der Bundesregierung gerade nicht ausgereicht, um den Defiziten bei der Umsetzung von Maßnahmen zum Eigenschutz im Bereich der Informationssicherheit entgegenzuwirken. Aktuelle Prüfungserkenntnisse des Bundesrechnungshofes sowie die Prüfungen des BSI zur IT-Sicherheit der Rechenzentren der Bundesverwaltung bestätigen dies nachdrücklich. Wie die Bundesregierung so das Sicherheitsniveau in der Bundesverwaltung flächendeckend steigern möchte, bleibt unklar.

Die Absicht der Bundesregierung, den IT-Grundschutz und die Maßnahmen zum Risikomanagement nicht einheitlich, sondern in abgestufter Verbindlichkeit festzulegen, steht im deutlichen Widerspruch zu dem Ziel des Gesetzes, ein gemeinsames, kohärentes und handhabbares Regelungsregime für die Informationssicherheit auf Bundesebene zu erreichen. Sie ist auch aus anderen Gründen nicht nachvollziehbar:

- Demnach hätten die Anforderungen an die Informationssicherheit und das Risikomanagement für Sicherheitsbehörden, wie dem Bundeskriminalamt oder der Bundespolizei, eine geringere Verbindlichkeit als die eines Bundesministeriums. Dabei sind es

[31] Artikel 2 Absatz 2 Buchstabe f Ziffer i der NIS-2-Richtlinie.

[32] Unter den Begriff „Zentralregierung“ werden in Deutschland für die Zwecke der Umsetzung der NIS-2-Richtlinie – in Anlehnung an die deutsche Definition von „zentrale Regierungsbehörden“ in der Richtlinie 2014/24/EU – grundsätzlich die Bundesministerien und das BKAmt, jeweils ohne nachgeordneten Bereich, gefasst (vgl. Gesetzesbegründung Teil A. Ziffer V).

[33] Gesetzesbegründung zu § 29 BSIG-E.

vielfach gerade die Fachbehörden in den Geschäftsbereichen, deren unbedingte Handlungsfähigkeit durch den Ausfall von IT-Diensten im Krisen- und Katastrophenfall gefährdet wäre. Der schwere Cyberangriff auf das Bundesamt für Kartographie und Geodäsie (BKG) Ende 2021 verdeutlicht, dass sich längst auch der nachgeordnete Geschäftsbereich im Visier von mutmaßlich staatlichen Angreifern befindet.[34] Die Dienstleistungen des BKG sind u. a. relevant für die Bereiche Verkehr, Katastrophenvorsorge, Innere Sicherheit und Energieversorgung; dies sind ausnahmslos KRITIS-Sektoren, die mit dem NIS2UmsuCG besser abgesichert werden sollen.

- Anderen von diesem Gesetz Betroffenen, z. B. wichtige oder besondere wichtige Einrichtungen, wird es ohne nähere Erläuterung unverständlich sein, warum die zentralen Anforderungen des § 30 BSIG-E für kleine und mittlere Unternehmen bereits ab 50 Mitarbeitern[35] gelten sollen, für nachgeordnete Bundesbehörden mit teilweise mehreren tausend Beschäftigten, z. B. der Zollverwaltung, jedoch nicht.

- Die Vorgabe, dass Behörden der Bundesverwaltung den IT-Grundschutz anzuwenden haben,[36] ergibt sich derzeit aus einem Beschluss des Bundeskabinetts. Anders als eine gesetzlich verankerte Verpflichtung lässt sich dieser von der Exekutive jederzeit abändern oder aufheben.

- Die Bundesregierung verweist in ihrer Gesetzesbegründung ausdrücklich auf sogenannte „Verbundrisiken". Danach sei die „*Kompromittierung der Systeme einer Einrichtung der Bundesverwaltung geeignet, ein Risiko für alle damit vernetzten Einrichtungen darzustellen*".[37] Der Grundsatz „Das schwächste Glied in einer Kette bestimmt die Sicherheit aller" erhält angesichts zunehmender Verflechtung und Konsolidierung der IT eine immer stärkere Relevanz. Die Absicht der Bundesregierung, den IT-Grundschutz und die BSI-Standards nur für wenige Bundesbehörden auf Gesetzesebene zu heben, führt zu einer uneinheitlichen und damit unzureichenden Verbindlichkeit. Gerade der Schutz der in einem gemeinsamen Informationsverbund vernetzten Bundesverwaltung muss für alle Beteiligten unbedingt einheitlich verbindlich sein.

Mit Blick auf etwaige zusätzliche Ausgaben- oder Stellenbedarfe weist der Bundesrechnungshof darauf hin, dass die Standard-Anforderungen des IT-Grundschutzes einschließlich der BSI-Standards bereits seit dem Jahr 2017 für die Einrichtungen der Bundesverwaltung auf untergesetzlicher Ebene umzusetzen sind. Ein Mehrbedarf an Haushaltsmitteln ließe sich aus einer gesetzlichen Verankerung dieser bereits geltenden Regeln daher nicht ableiten.

---

[34] https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/07/cyberangriff-bkg.html, abgerufen am 15. August 2024.

[35] Unternehmen bestimmter Einrichtungsarten, die mindestens 50 Mitarbeiter beschäftigen, gelten als wichtige Einrichtungen; vgl. § 28 Absatz 2 Nummer 3 BSIG-E.

[36] Ausnahmen gelten gemäß UP Bund für das Bundesministerium der Verteidigung (BMVg) einschließlich BAMAD, Bundesnachrichtendienst und Bundesamt für Verfassungsschutz sowie für Einrichtungen des Bundes, die in das Europäische System der Zentralbanken (ESZB) eingebunden sind.

[37] Gesetzesbegründung zu § 2 Nummer 21 BSIG-E.

Um das Ziel des Gesetzes, wesentliche nationale Anforderungen an das Informationssicherheitsmanagement des Bundes gesetzlich zu verankern, umzusetzen, empfiehlt der Bundesrechnungshof, dem IT-Grundschutz für alle Einrichtungen der Bundesverwaltung unmittelbaren Gesetzesrang einzuräumen. Ferner sollten alle Einrichtungen der Bundesverwaltung gesetzlich verpflichtet sein, die Anforderungen an das Risikomanagement nach § 30 BSIG-E zu erfüllen.

Empfehlung für geänderte Fassung des Artikel 1, § 29 Absatz 2:[38]

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.***~~

Empfehlung für geänderte Fassung des Artikel 1, § 44 Absatz 1 Satz 1:

Die Einrichtungen der Bundesverwaltung müssen die ~~***jeweils geltenden Fassungen der***~~ Mindeststandards für die Sicherheit in der Informationstechnik des Bundes (Mindeststandards)***, die BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) in den jeweils geltenden Fassungen*** als Mindestanforderungen zum Schutz der in der Bundesverwaltung verarbeiteten Informationen erfüllen.

Empfehlung für geänderte Fassung des Artikel 1, § 44 Absatz 2 Satz 1 und 2:

~~***Das Bundeskanzleramt und die Bundesministerien müssen als zusätzliche Mindestanforderungen dD***~~ie BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) ***werden*** in den jeweils geltenden Fassungen ~~***einhalten. Die jeweils geltenden Fassungen werden***~~ auf der Internetseite des Bundesamtes veröffentlicht.

3.1.1 Stellungnahme des BMI

Zu diesem Punkt hat das BMI nicht Stellung genommen.

[38] Die textlichen Änderungsvorschläge des Bundesrechnungshofes sind durch fette und kursive Formatierung kenntlich gemacht.

3.1.2 Abschließende Bewertung des Bundesrechnungshofes

Da sich das BMI zu den Vorschlägen nicht geäußert hat, geht der Bundesrechnungshof davon aus, dass es der Argumentation nicht widerspricht und dieser folgt, den IT-Grundschutz und Maßnahmen zum Risikomanagement für die gesamte Bundesverwaltung gesetzlich zu verankern.

Der Bundesrechnungshof bleibt bei seinen Änderungsvorschlägen.

3.2 Ausnahmeregelungen für das Auswärtige Amt begrenzen (Artikel 1, §§ 7 Absatz 6, 29 Absatz 3, 44 Absatz 1 NIS2UmsuCG)

§ 7 Absatz 6 BSIG-E sieht vor, dass das BSI den im Ausland belegenen oder für das Ausland oder für Anwender im Ausland betriebenen Teil der Auslandsinformations- und -kommunikationstechnik (sog. Auslands-IT) nicht kontrollieren darf. Näheres soll eine Verwaltungsvereinbarung zwischen AA und BMI regeln. Gegenüber der bisherigen Regelung in § 4a Absatz 5 BSIG schränkt die Streichung des Wortes „ausschließlich“ in § 7 Absatz 6 BSIG-E die Kontrollmöglichkeiten des BSI im AA weiter ein.

Gemäß § 29 Absatz 3 BSIG-E soll zusätzlich der gesamte Geschäftsbereich des AA von weiteren Regelungen des BSIG ausgenommen werden. Das AA soll im Einvernehmen mit dem BMI eine allgemeine Verwaltungsvorschrift erlassen, um die Ziele der NIS-2-Richtlinie ergebnisäquivalent umzusetzen. § 44 Absatz 1 Satz 5 BSIG-E nimmt die Auslands-IT zudem aus der gesetzlichen Verpflichtung aus, die Mindeststandards des BSI einhalten zu müssen.

Der Bundesrechnungshof erachtet diese Ausnahmen, die deutlich über den aktuellen § 4a Absatz 5 BSIG hinausgehen, für sehr bedenklich. Dies gilt insbesondere im Hinblick darauf, dass das AA als einer der IT-Dienstleister des Bundes zentrale und kritische IT-Dienstleistungen für die Bundesverwaltung auch im Inland bereitstellt:

- Die Bundesregierung bezieht sich in ihrer Begründung für die Ausnahmeregelung auf den Erwägungsgrund 8 der NIS-2-Richtlinie. Danach gilt 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*“. Hieraus ist nach Ansicht des Bundesrechnungshofes weder eine Grundlage für den Entfall des Wortes „ausschließlich“ in § 7 Absatz 6 BSIG-E noch für eine pauschale unbegrenzte Ausnahme für den gesamten Geschäftsbereich des AA (inkl. dem Bundesamt für Auswärtige Angelegenheiten) ersichtlich. Zwar hat das AA eine große Zahl von Vertretungen im Ausland und ist dort mit vielen unterschiedlichen örtlichen, rechtlichen und personellen Gegebenheiten konfrontiert. Die Gefährdungen für die Informationssicherheit dürften jedoch mindestens genauso hoch sein wie im Inland. Das Risiko von Angriffen auf zentrale IT-Infrastrukturen der

Bundesverwaltung dürfte an den exponierten Zugangspunkten im Ausland sogar höher sein als im Inland. Als unabhängiger fachkundiger Dritter könnte das BSI die besonderen Rahmenbedingungen der Auslands-IT bei seinen Kontrollen genauso wie das AA berücksichtigen. Der Aufbau von Doppelstrukturen würde vermieden.

- Da dem AA die Kontrolle wesentlicher Teile seiner eigenen Informations- und Kommunikation obliegen soll und es die Ziele der NIS-2-Richtlinie im gesamten Geschäftsbereich umzusetzen hat, muss es hierfür „ergebnisäquivalente" Maßnahmen ergreifen. Es muss daher Dienste und qualifiziertes Personal bereitstellen und somit ähnliche Anstrengungen unternehmen wie das BSI für die übrige Bundesverwaltung. Synergien werden unzureichend genutzt und es steigt der Personalaufwand sowie die Gefahr von Mehrfachentwicklungen und -arbeit. Zudem müssen das BSI und das AA über die Ergebnisäquivalenz der Maßnahmen befinden. Dies kann kein einmaliger Prozess für die Verwaltungsvorschrift sein, sondern er ist von BMI und AA aufgrund sich verändernder Rahmenbedingungen und Bedrohungslagen regelmäßig zu wiederholen. Angesichts der Haushaltslage ist ein solch aufwands- und voraussichtlich auch ausgabenintensives Vorgehen kaum zu rechtfertigen.

- Der Geschäftsbereich des AA ist bereits seit dem Jahr 2015 gesetzlich verpflichtet, die Mindeststandards des BSI einzuhalten.[39] Ihn aus dieser Verpflichtung herauszunehmen, kann nicht mit der Bereichsausnahme der NIS-2-Richtlinie begründet werden. Hinzu kommt, dass § 44 Absatz 1 Satz 3 BSIG-E die Möglichkeit eröffnet, in sachlich gerechtfertigten Fällen, beispielsweise an einzelnen Auslandsvertretungen, von den Mindeststandards abweichen zu dürfen.

- § 4a BSIG ist seit Dezember 2021 in Kraft. Dennoch haben es BMI und AA bisher nicht vermocht, die dort vorgesehene Verwaltungsvereinbarung zu schließen und so die Kontrollrechte des BSI und die Zusammenarbeit zwischen BSI und AA angemessen zu regeln. Um einen regelungsfreien Raum und damit einen Verstoß gegen die NIS-2-Richtlinie im Kernbereich der Zentralregierung zu vermeiden, muss die allgemeine Verwaltungsvorschrift nach § 29 Absatz 3 Satz 2 BSIG-E sehr zeitnah vereinbart und vom AA erlassen werden. Ein verbindlicher Zeitpunkt sollte hierfür im Gesetz vorgegeben werden.

Der Bundesrechnungshof hält es für erforderlich, dass die Bundesregierung mit dem NIS2UmsuCG die seit dem IT-SiG 2.0 bestehende Kontrolllücke beim AA zeitnah schließt und keine weiteren Ausnahmen vorsieht, die nicht von der eingeschränkten Bereichsausnahme der NIS-2-Richtlinie für die Auslands-IT des AA abgedeckt sind.

[39] § 8 Absatz 1 Satz 1 BSIG.

Empfehlung für geänderte Fassung des Artikels 1, § 7 Absatz 6:

Ausgenommen von den Befugnissen nach den Absätzen 1 bis 3 sind Kontrollen der Auslandsinformations- und -kommunikationstechnik nach § 9 Absatz 2 des Gesetzes über den Auswärtigen Dienst, soweit sie im Ausland belegen ist oder ***ausschließlich*** für das Ausland oder für Anwender im Ausland betrieben wird. Die Bestimmungen für die Schnittstellen der Kommunikationstechnik des Bundes im Inland bleiben davon unberührt. Näheres zu Satz 1 regelt ***bis zum 31. Dezember 2025*** eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern und für Heimat und dem Auswärtigen Amt.

Empfehlung für geänderte Fassung des Artikel 1, § 29 Absatz 3:

~~Die~~ Der Geschäftsbereich***~~e des Auswärtigen Amts und~~*** des Bundesministerium***s*** der Verteidigung sowie der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz ***sowie die Auslandsinformations- und -kommunikationstechnik nach § 9 Absatz 2 des Gesetzes über den Auswärtigen Dienst, soweit sie im Ausland belegen ist oder ausschließlich für das Ausland oder für Anwender im Ausland betrieben wird,*** sind zusätzlich zu den Regelungen gemäß Absatz 2 Satz 2 von den Regelungen der § 7 Absatz 5 Satz 4, § 10, 13 Absatz 1 Nummer 1 Buchstabe e sowie der §§ 30, 33 und 35 ausgenommen. Das Auswärtige Amt erlässt im Einvernehmen mit dem Bundesministerium des Innern und für Heimat ***bis zum 31. Dezember 2025*** eine allgemeine Verwaltungsvorschrift, um die Ziele der NIS-2-Richtlinie im Geschäftsbereich des Auswärtigen Amtes durch ergebnisäquivalente Maßnahmen umzusetzen.

Empfehlung für geänderte Fassung des Artikel 1, § 44 Absatz 1 Satz 5:

Für die Verpflichtung nach Satz 1 gelten die Ausnahmen nach § 7 Absatz ***~~6 und~~*** 7 entsprechend.

3.2.1 Stellungnahme des BMI

Das BMI gibt an, das AA berücksichtige Erwägungsgrund 8 der NIS-2-Richtlinie. Es wolle unterschiedliche Rechtsregime für die Auslandsvertretungen und die Zentrale des AA vermeiden.
Die Regelung auf im Ausland belegene oder ausschließlich für das Ausland oder für Anwender im Ausland betriebene Systeme des AA zu beschränken, ginge über die Anforderungen der Richtlinie hinaus (1:1-Umsetzung). Dies wäre rechtlich nicht ohne grundlegende Änderungen des Gesetzes über den Auswärtigen Dienst (GAD) möglich. Zudem zöge dies technisch und personell unverhältnismäßigen Aufwand nach sich.

- Rechtlich: Zentrale und Auslandsvertretungen des AA bildeten eine einheitliche Bundesbehörde, deren „Auslands-IT“ den gesamten Geschäftsbereich umfasst (§ 2 i. V. m. § 9

Absatz 2 GAD). Eine Aufspaltung in „Auslands-“ und „Inlands-IT“ würde zu verschiedenen Regelungsrahmen in derselben Behörde, Rechtsunsicherheit und erheblichen Einschränkungen der operativen Funktionsweise des AA führen.
- Technisch: Die Auslands-IT steuere aus zum Großteil im Inland belegenen Rechenzentren Dienstleistungen für alle Auslandsvertretungen und den gesamten Geschäftsbereich. Eine Trennung würde einen kompletten Neuaufbau der derzeitigen IT-Umgebung des AA erfordern. Dies wäre weder mit vertretbarem finanziellem, personellem und technischem Aufwand machbar, noch ohne Sicherheitseinbußen zu erreichen. Synergien würden dagegen nicht erreicht. Vielmehr würde im AA der Aufbau von Doppelsystemen und -strukturen mit dauerhaft hohem Kostenaufwand erforderlich.

Demgegenüber werde ein hohes Sicherheitsniveau sichergestellt, wenn das AA die inländischen Sicherheitsanforderungen, wie vorgesehen, umsetze. Dies werde in einem kontinuierlichen Verbesserungsprozess und in enger Zusammenarbeit mit dem BSI geschehen. Hierzu würden die im Gesetzentwurf vorgesehenen Verwaltungsvereinbarungen die Basis liefern, die bereits in Vorbereitung seien.

3.2.2 Abschließende Bewertung des Bundesrechnungshofes

Die Argumentation des BMI ist nicht schlüssig. Nach seinen Angaben betreibt das AA die zentralen Dienste der Auslands-IT schon jetzt trotz unterschiedlicher Rechtslagen und Situationen vor Ort zum Großteil in Deutschland. Zudem stellt es als Dienstleister des Bundes wichtige IT-Dienste für die übrige Bundesverwaltung bereit. Hierzu zählt z. B. die Verschlusssachenkommunikation. Für diese ist verbindlich vorgeschrieben, die Verschlusssachenanweisung zu beachten. Ihren Regelungen unterliegt auch das AA. Auch ist das AA als Teil des Auswärtigen Dienstes an die Regierungsnetze des Bundes angeschlossen. Es muss die entsprechenden Nutzerpflichten erfüllen. Daher kann es nicht sachgerecht sein, dem BSI für die in Deutschland zentral betriebenen IT-Systeme keine Kontrollrechte zu übertragen. Nur dann kann das BSI die Verbundrisiken im Inland angemessen bewerten und vermittels seiner Expertise reduzieren helfen. Das AA müsste somit auch für die in Deutschland betriebene IT kein eigenes Kontrollwesen aufbauen und unterhalten. Es könnte sich der bewährten Dienste des BSI bedienen und Doppelstrukturen in der Bundesverwaltung vermeiden.
Die Argumentation, es seien

- unterschiedliche Regelungsregime für die im Inland und die im Ausland betriebene IT des Auswärtigen Dienstes einzurichten oder
- gar eine technische Trennung herbeizuführen und damit einen kompletten kostenintensiven Neuaufbau der derzeitigen IT-Umgebung zu veranlassen,

wenn das AA nicht in der vorgesehenen Weise von den Verpflichtungen des NIS2UmsuCG ausgenommen würde, kann der Bundesrechnungshof nicht folgen.

Es ist nicht ersichtlich, dass z. B. die Kontrolle der in Deutschland betriebenen IT des Auswärtigen Dienstes durch das BSI zu einer Rechtsunsicherheit und erheblichen Einschränkungen

der operativen Funktionsweise des AA oder des Auswärtigen Dienstes als Ganzes führen könnten. Vielmehr dürften diese zu einem durchgängig hohen Sicherheitsniveau beitragen.

Grundsätzlich kann es sein, dass unterschiedliche Anforderungen der Nutzer im Ausland auch bei zentralen in Deutschland betriebenen IT-Diensten zu Besonderheiten und Abweichungen führen. Keinesfalls darf dies aber bedeuten, dass Sicherheitsmaßnahmen für in Deutschland betriebene zentrale Dienste des Auswärtigen Dienstes vermindert werden. Ganz im Gegenteil ist zu fordern, dass zusätzliche Maßnahmen durch das AA ergriffen werden, um die zentral betriebenen Teile der IT aufgrund der erhöhten Risiken für die Informationssicherheit besonders zu schützen.
Auch angesichts der Tatsache, dass BMI und AA es nicht vermochten, in rund drei Jahren die vom IT-SiG 2.0 geforderte Verwaltungsvereinbarung zu schließen, hält der Bundesrechnungshof an seiner Empfehlung fest. Er regt aus Gründen der Wirtschaftlichkeit und Informationssicherheit dringend an, mit dem NIS2UmsuCG keine über den Stand des IT-SiG 2.0 hinausgehenden Ausnahmen für das AA zu schaffen. Vielmehr sollte das NIS2UmsuCG das BSI auch gegenüber dem Auswärtigen Dienst stärken und helfen, dort die Informations- und Cybersicherheit zu verbessern.

3.3 Weitreichende Ausnahmeregelung für Einrichtungen der Bundesverwaltung beschränken (Artikel 1, § 46 Absatz 5 NIS2UmsuCG)

Die ISB der Ressorts sollen gemäß § 46 Absatz 5 BSIG-E die alleinige Befugnis erhalten, Einrichtungen innerhalb ihres Ressorts von Verpflichtungen nach den §§ 28 bis 48 BSIG-E teilweise oder insgesamt zu befreien („Opt-Out“). Voraussetzung ist, dass dadurch „*keine nachteiligen Auswirkungen für die Informationssicherheit des Bundes zu befürchten sind*“. Mit dem BSI soll hierzu nur das Benehmen herzustellen sein; das heißt, dessen Einvernehmen wäre nicht erforderlich.

Im umgekehrten Fall, in dem für bestimmte Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts die Einbeziehung in den Geltungsbereich des Gesetzes angeordnet werden kann („Opt-In“), soll das Einvernehmen zwischen zuständigem Ressort und BSI hingegen ausdrücklich erforderlich sein.[40] Dies sei nach der Gesetzesbegründung notwendig, um die im Falle einer Nicht-Anordnung „*potentiellen nachteiligen Auswirkungen für die Informationssicherheit des Bundes angemessen einschätzen zu können*“.

Der Bundesrechnungshof erachtet es für die Informationssicherheit der Bundesverwaltung als kritisch, den Ressort-ISB mit dem § 46 Absatz 5 BSIG-E ein so weitreichendes Recht für Ausnahmebescheide (bis hin zu ganzen Bundesbehörden) einzuräumen. Denn hierfür soll schon die Einschätzung des Ressort-ISB ausreichen, dass keine nachteiligen Auswirkungen zu befürchten sind. Sofern solche Einrichtungen an die NdB angeschlossen sind, könnten

[40] § 29 Absatz 1 Nummer 3 BSIG-E.

Fehleinschätzungen die Sicherheit des gesamten Informationsverbundes empfindlich schwächen. Ein Grund, warum für einen Ausnahmebescheid nicht ebenfalls ein Einvernehmen mit dem BSI erzielt werden muss, ist nicht ersichtlich.

Empfehlung für geänderte Fassung des Artikel 1, § 46 Absatz 5 Satz 1:

Der oder die Informationssicherheitsbeauftragte des Resorts kann im ***Einvernehmen*** ~~***Benehmen***~~ mit dem Bundesamt Einrichtungen der Bundesverwaltung innerhalb des Ressorts von Verpflichtungen nach diesem Teil teilweise oder insgesamt durch Erteilung eines Ausnahmebescheids befreien.

3.3.1 Stellungnahme des BMI

Zu diesem Punkt hat das BMI nicht Stellung genommen.

3.3.2 Abschließende Bewertung des Bundesrechnungshofes

Das BMI hat sich zu diesem Vorschlag nicht geäußert. Der Bundesrechnungshof geht daher davon aus, dass es der Argumentation nicht widerspricht und dieser folgt, Ausnahmeregelungen für Einrichtungen der Bundesverwaltung zu beschränken.

Der Bundesrechnungshof bleibt bei seinem Änderungsvorschlag.

3.4 Nachweis der Informationssicherheit durch Einrichtungen der Bundesverwaltung in kürzeren Fristen vorsehen (Artikel 1, § 43 Absatz 4 NIS2UmsuCG)

Einrichtungen der Bundesverwaltung sollen dem BSI erstmals fünf Jahre nach Inkrafttreten des NIS2UmsuCG einen Nachweis darüber vorlegen, inwieweit sie die Anforderungen an die Informationssicherheit umgesetzt haben. Diese Frist hält der Bundesrechnungshof für zu lang. Sie sollte auf drei Jahre reduziert werden. Dies ist die Frist, die das NIS2UmsuCG auch für die Nachweise der Betreiber kritischer Anlagen[41] und anderer besonders wichtiger Einrichtungen[42] vorsieht. Auch hält der Bundesrechnungshof es für unzureichend, dass die Einrichtungen der Bundesverwaltung den Nachweis anschließend nur „regelmäßig“ wiederholen müssen. Hier sollte – wie bei den Betreibern kritischer Anlagen – eine konkrete Zeitspanne von drei Jahren gesetzlich festgelegt werden.

[41] § 39 Absatz 1 Satz 1 BSIG-E.
[42] § 61 Absatz 3 Satz 1 BSIG-E.

Ein Grund, warum für die Einrichtungen der Bundesverwaltung eine deutlich längere Frist gelten soll als für Wirtschaftsunternehmen, ist nicht ersichtlich. Die Bedrohungen aus dem Cyberraum sind vergleichbar, ebenso die Anforderungen aus dem NIS2UmsuCG. Hinzu kommt die Vorbildfunktion, die die Bundesverwaltung einnehmen sollte. Dass die Einrichtungen der Bundesverwaltung bei der Nachweispflicht hinter Wirtschaftsunternehmen zurückbleiben sollen, hält der Bundesrechnungshof für ein falsches Signal.

Den IT-Steuerungsgremien des Bundes fehlt derzeit ein Überblick über den Umsetzungsstand zur Informationssicherheit in der Bundesverwaltung.[43] Zweck der neuen Regelung ist daher richtigerweise, Transparenz über die Informationssicherheitslage in der Bundesverwaltung zu schaffen.[44] Diese kann aber weder zeitnah noch fortlaufend erreicht werden, wenn Einrichtungen der Bundesverwaltung erst im Jahr 2030 erste Nachweise vorlegen müssen und dann die erneute Vorlage nicht klar terminiert ist. Auch die Kontrollen des BSI schaffen hier vorerst keine Abhilfe. Denn nur wenige Prüfungen des BSI nach § 4a BSIG (künftig § 7 BSIG-E) sind derzeit angelaufen. Flächendeckende Befunde zur Informationssicherheit der Bundesverwaltung werden voraussichtlich noch für längere Zeit auf sich warten lassen. Ein gesetzlich festgelegter, für alle Einrichtungen der Bundesverwaltung identischer Turnus würde zumindest in diesem zeitlichen Abstand standardisierte und vergleichbare Aussagen zur Informationssicherheitslage auf der Grundlage einheitlicher Nachweise ermöglichen.

Empfehlung für geänderte Fassung des Artikel 1, § 43 Absatz 4 Satz 2:

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

3.4.1 Stellungnahme des BMI

Zu diesem Punkt hat das BMI nicht Stellung genommen.

3.4.2 Abschließende Bewertung des Bundesrechnungshofes

Da sich das BMI zu dem Vorschlag nicht geäußert hat, geht der Bundesrechnungshof davon aus, dass es der Argumentation nicht widerspricht und dieser folgt, den Nachweis der Informationssicherheit durch Einrichtungen der Bundesverwaltung in kürzeren Fristen vorzusehen.

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

[44] Gesetzesbegründung zu § 43 Absatz 4 BSIG-E.

Der Bundesrechnungshof bleibt bei seinem Änderungsvorschlag.

3.5 Verantwortung der Einrichtungsleitung für Informationssicherheit konkretisieren (Artikel 1, § 43 Absatz 1 NIS2UmsuCG)

Gemäß § 43 Absatz 1 BSIG-E soll die Einrichtungsleitung (nur) für die „Voraussetzungen für die Gewährleistung der Informationssicherheit“ verantwortlich sein. Ohne erkennbaren Grund bleibt diese Formulierung hinter den Anforderungen des UP Bund zurück. Dieser fordert: „*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 […].*“[45] Auch der IT-Grundschutz legt fest, dass „*die oberste Managementebene jeder Behörde […] für die Gewährleistung der Informationssicherheit nach innen und außen*“ verantwortlich ist.[46]

Die Pflicht, die Informationssicherheit zu gewährleisten, umfasst zwar auch, die Voraussetzungen dafür zu schaffen, geht jedoch deutlich darüber hinaus. Sie greift nämlich auch dann, wenn es der Behördenleitung im Einzelfall nicht möglich sein sollte, die für die Informationssicherheit benötigten Ressourcen bereitzustellen oder Prozesse zu etablieren. Die Behördenleitung bleibt auch in diesem Fall verantwortlich und muss daraus erwachsende Risiken bewerten, behandeln und gegebenenfalls übernehmen. Das NIS2UmsuCG sollte in dieser für das Informationssicherheitsmanagement in der Bundesverwaltung zentralen Frage der Verantwortungszuweisung nicht hinter die Bestimmungen des UP Bund und des IT-Grundschutzes zurückfallen.

Empfehlung für geänderte Fassung des Artikel 1, § 43 Absatz 1:

Die Leitung der Einrichtung ist dafür verantwortlich, unter Berücksichtigung der Belange des IT-Betriebs die ***~~Voraussetzungen zur Gewährleistung der~~*** Informationssicherheit zu ***gewährleisten ~~schaffen~~***.

3.5.1 Stellungnahme des BMI

Zu diesem Punkt hat das BMI nicht Stellung genommen.

[45] UP Bund 2017, Kapitel 3.2 „ISMS – Organisation und Aufgaben innerhalb des Ressorts/der Einrichtung“.
[46] BSI-Standard 200-1, Kapitel 4.1 (Aufgaben und Pflichten des Managements).

3.5.2 Abschließende Bewertung des Bundesrechnungshofes

Das BMI hat sich zu dem Vorschlag nicht geäußert. Der Bundesrechnungshof geht daher davon aus, dass es der Argumentation nicht widerspricht und dieser folgt, die Verantwortung der Einrichtungsleitung für Informationssicherheit zu konkretisieren.

Der Bundesrechnungshof bleibt bei seinem Änderungsvorschlag.

3.6 Aufgaben und Befugnisse der Koordinatorin oder des Koordinators für Informationssicherheit im Gesetz festlegen (Artikel 1, § 48 NIS2UmsuCG)

Mit dem Koordinator oder der Koordinatorin für Informationssicherheit will die Bundesregierung eine Funktion schaffen, die es in Wirtschaftsunternehmen, aber auch in zahlreichen Staaten bereits seit längerem unter dem Begriff CISO gibt. Der zunehmenden Bedeutung der Cybersicherheit entsprechend steuert dieser – gegebenenfalls zusammen mit einem Gremium – das Informationssicherheitsmanagement auf der obersten Ebene.

Gemäß § 48 BSIG-E ist (lediglich) vorgesehen, dass die Bundesregierung eine Koordinatorin oder einen Koordinator für Informationssicherheit bestellt. Auch die Gesetzesbegründung zu dieser Regelung klärt weder die organisatorische Stellung noch die Aufgaben und die Befugnisse der neuen Funktion.

Derzeit stehen nach Ansicht des Bundesrechnungshofes u. a. das Ressort- und Einstimmigkeitsprinzip einer wirksamen Steuerung der zentralen IT des Bundes entgegen. Daraus sollte die Bundesregierung für die ressortübergreifende Steuerung der Informationssicherheit lernen. Es genügt eben nicht, einen Koordinator oder eine Koordinatorin zu benennen, um die gebotene Wirkung zu erzielen. Damit wird die Bundesregierung den Herausforderungen, die sich aus potenziell widerstreitenden Interessen des IT-Betriebs und der Informationssicherheit bei gleichzeitigen Ressourcenengpässen und mangelndem Überblick ergeben, kaum gerecht werden können.

Die letzten Jahre haben gezeigt, dass insbesondere der IT-Rat als höchstes IT-Steuerungsgremium des Bundes der Informationssicherheit keine hinreichende Bedeutung beigemessen hat.[47] Hier fehlt es an einer Funktion, der zentrale Informations-, Unterstützungs- und Koordinierungsaufgaben zukommen. Grundlage hierfür muss u. a. ein ressortübergreifendes

[47] Vgl. Bemerkungen 2022 des Bundesrechnungshofes zur Haushalts- und Wirtschaftsführung des Bundes – Ergänzungsband –, Bundestagsdrucksache 20/6530 Nummer 24: „Informationssicherheit: IT-Rat bleibt trotz erheblicher Defizite untätig“; https://www.bundesrechnungshof.de/SharedDocs/Downloads/DE/Berichte/2023/ergaenzungsband-2022/bemerkung-24.pdf?__blob=publicationFile&v=2, abgerufen am 21. August 2024.

Informationssicherheitscontrolling sein, das von der Koordinatorin oder dem Koordinator zu verantworten wäre.

Der Haushaltsausschuss des Deutschen Bundestages (Haushaltsausschuss) hat sich in den letzten Jahren verstärkt mit Themen der Informationssicherheit befasst. Beispielhaft genannt seien seine Maßgabebeschlüsse zur Einführung eines übergreifenden Informationssicherheitscontrollings, zur auskömmlichen Finanzierung von Maßnahmen der Cybersicherheit oder zur Einrichtung eines CISO Bund. Bislang sieht der Gesetzentwurf einen jährlichen Bericht des BMI an den Ausschuss für Inneres und Heimat des Deutschen Bundestages über die „Anwendung des Gesetzes“ (§ 58 Absatz 3 BSIG-E) sowie einen jährlichen Bericht des BSI an den Haushaltsausschuss zu den Kontrollen nach § 7 BSIG-E (§ 7 Absatz 9 BSIG-E) vor. Darüber, wie wirksam die Bundesverwaltung bewilligte Haushaltsmittel für die Informationssicherheit eingesetzt und welches übergreifende Informationssicherheitsniveau sie damit erreicht hat, informieren diese Berichte nicht. Gleichwohl stellen diese Informationen eine wichtige Grundlage für die Bewilligung von Haushaltsmitteln und die Kontrolle des Haushaltsmitteleinsatzes durch den Gesetzgeber dar. Ein jährlicher ressortübergreifender Bericht der Koordinatorin oder des Koordinators an den Haushaltsausschuss könnte diesen Informationsbedarf decken. Darüber hinaus regt der Bundesrechnungshof an, der Koordinatorin oder dem Koordinator anlassbezogen das Recht einzuräumen, zu Gesetzesvorhaben und Vorgängen, die die Informations- und Cybersicherheit der Einrichtungen der Bundesverwaltung betreffen, gegenüber dem Deutschen Bundestag oder seinen Ausschüssen Stellung zu nehmen.

Auch wenn das NIS2UmsuCG nicht festlegt, welche Kriterien eine Koordinatorin oder ein Koordinator für Informationssicherheit erfüllen muss und welche Bundesbehörde diese Funktion stellt, so sollten Aufgaben und Befugnisse dieser Funktion umfassend im Gesetz verankert sein.

Empfehlung für ergänzte Fassung des § 48 BSIG-E:

Amt des Koordinators für Informationssicherheit***; Aufgaben, Befugnisse***

(1) Die Bundesregierung bestellt eine Koordinatorin oder einen Koordinator für Informationssicherheit.

(2) Dem Koordinator oder der Koordinatorin für Informationssicherheit obliegt die zentrale Koordinierung des Informationssicherheitsmanagements des Bundes. Er oder sie koordiniert die Informationssicherheitsleitlinien des Bundes und unterstützt die Ressorts bei der Umsetzung der Vorgaben zur Informationssicherheit. Dabei wirkt er oder sie auf ein angemessenes Verhältnis zwischen dem Einsatz von Informationstechnik und Informationssicherheit hin.

(3) Die Ressorts beteiligen den Koordinator oder die Koordinatorin für Informationssicherheit bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben, soweit sie Fragen der Informationssicherheit berühren. Er oder sie kann der Bundesregierung Vorschläge machen und Stellungnahmen zuleiten. Die Ressorts unterstützen den Koordinator oder die Koordinatorin bei der Erfüllung seiner oder ihrer Aufgaben.

Zusätzliche Anregung für ergänzte Fassung des § 48 BSIG-E:

(4) Der Koordinator oder die Koordinatorin kann zu Gesetzesvorhaben und Vorgängen, die die Informations- und Cybersicherheit der Einrichtungen der Bundesverwaltung betreffen, gegenüber dem Deutschen Bundestag oder seinen Ausschüssen Stellung nehmen. Er oder sie unterrichtet den Haushaltsausschuss des Deutschen Bundestages kalenderjährlich jeweils bis zum 31. März des dem Berichtsjahr folgenden Jahres zum übergreifenden Stand der Informationssicherheit in der Bundesverwaltung, zu den ***dafür eingesetzten Ressourcen und zu deren Wirkung.***

3.6.1 Stellungnahme des BMI

Das BMI verweist darauf, dass der Haushaltsausschuss die Bundesregierung mit Maßgabebeschluss 20(8)5989 vom 21. Februar dazu aufgefordert hatte, ein Konzept zu erarbeiten, das u. a. Vorschläge zur Einrichtung eines CISO Bund enthalten soll. Nach dem Verständnis der Bundesregierung müsste eine gesetzliche Verankerung der Aufgaben und Befugnisse des CISO Bund auf Grundlage eines entsprechend ausgearbeiteten ressortgeeinten Konzepts der Bundesregierung erfolgen. Eine Ausgestaltung der Rolle CISO Bund im Gesetzentwurf würde das o. g. Konzept vorwegnehmen. Daher wurde im Gesetzentwurf die Rolle CISO Bund zunächst nur allgemein eingeführt.

3.6.2 Abschließende Bewertung des Bundesrechnungshofes

Die Forderung des Haushaltsausschusses an die Bundesregierung, u. a. ein Konzept für einen CISO Bund einzurichten, datiert vom 21. Februar 2024. Der Kabinettentwurf des NIS2UmsuCG, welcher lediglich die Rolle des CISO (hier: der Koordinatorin oder des Koordinators) nicht aber ihre oder seine Rechten und Pflichten definiert, wurde am 24. Juli 2024 von der Bundesregierung verabschiedet. Der Bundesregierung ist es demnach nicht gelungen, sich innerhalb von fünf Monaten auf ein gemeinsames Konzept für die Koordinatorin oder den Koordinator zu einigen. Dies wird der Bedrohungslage in der Bundesverwaltung nicht gerecht.
Da der Koordinatorin oder dem Koordinator eine wichtige Funktion bei der übergreifenden Steuerung der Informations- und Cybersicherheit in der Bundesverwaltung zukommt, sollte der Gesetzgeber verpflichtende Leitplanken für deren oder dessen Tätigkeit gesetzlich regeln. So kann er verhindern, dass die Bundesregierung die neue Funktion infolge unterschiedlicher Ressortinteressen unzureichend ausgestaltet und Haushaltsmittel für eine „Türschildlösung“ verausgabt.

Der Bundesrechnungshof bleibt daher bei seinen Empfehlungen.

3.7 Kohärenz zwischen NIS2UmsuCG und KRITIS-DachG verbessern

Das KRITIS-DachG soll sektorübergreifende Mindeststandards normieren, um durch physische Sicherungsmaßnahmen die Resilienz Kritischer Infrastrukturen zu stärken. Das NIS2UmsuCG soll dies flankieren, indem es für wichtige und besonders wichtige Einrichtungen (einschließlich der Kritischen Infrastrukturen) notwendige Sicherungsmaßnahmen für die Cyber- und Informationssicherheit regelt. Beide Gesetze stehen daher in enger Abhängigkeit zueinander. Eine Kohärenz dieser Gesetze ist zwingend notwendig, um deren Regelungen und Maßgaben möglichst wirtschaftlich und unbürokratisch umsetzen zu können. Dies gilt einerseits für die Wirtschaftsunternehmen, die die Regelungen einhalten und umsetzen müssen. Andererseits gilt dies auch für die mit der Aufsicht betrauten Behörden, in erster Linie das BSI und das BBK, aber auch Landes- und kommunale Behörden, die mit BSI und BBK die Aufsicht über Betreiber kritischer Anlagen gewährleisten sollen. Die jeweiligen Gesetze sehen für Letztere eine enge Abstimmung und Zusammenarbeit vor. Sie müssen daher hinsichtlich

- ihrer Wirkung abgestimmt und widerspruchsfrei,
- der definierten Befugnisse und Zuständigkeiten redundanzfrei und eindeutig sowie
- des gemeinsamen Wirkens von BBK und BSI zielgerichtet und effektiv sein.

Anders als das NIS2UmsuCG ist das KRITIS-DachG derzeit noch Gegenstand von regierungsinternen Abstimmungen. Der Bundesrechnungshof sieht in den ihm vorliegenden Entwurfsfassungen von NIS2UmsuCG und KRITIS-DachG die notwendige Kohärenz noch nicht hinreichend gegeben. Folgende Beispiele verdeutlichen dies:

Begriffsbestimmungen nicht einheitlich gehalten

Der Entwurf des KRITIS-DachG definiert die Begriffe „Risiko“ und „Risikoanalyse“.[48] Entsprechende Definitionen fehlen dem NIS2UmsuCG, obwohl die Begriffe im Umfeld der Cyber- und Informationssicherheit von zentraler Bedeutung sind (vgl. insbesondere § 30 BSIG-E [Risikomanagementmaßnahmen]).

Der Begriff „Risiko“ sollte daher im NIS2UmsuCG angelehnt an die NIS-2-Richtlinie[49] und in Übereinstimmung mit dem KRITIS-DachG-E festgelegt werden.

Ebenso sollte auch ein einheitliches Verständnis für den Begriff der „Risikoanalyse“ bestehen. Im Geltungsbereich des NIS2UmsuCG ist dieser im einschlägigen BSI-Standard 200-3[50] umfassender definiert als dies im Entwurf des KRITIS-DachG derzeit der Fall ist.

Empfehlung für ergänzte Fassung des Artikels 1, § 2:

Im Sinne dieses Gesetzes ist oder sind

36. „Risiko“ das Potenzial für Ausfälle oder Beeinträchtigungen, die durch einen Vorfall verursacht werden, das als eine Kombination des Ausmaßes eines Ausfalls oder einer Beeinträchtigung und der Wahrscheinlichkeit des Eintretens des Vorfalls zum Ausdruck gebracht wird;

37. „Risikoanalyse“ ein Prozess, in dem Risiken identifiziert, eingeschätzt und bewertet sowie Maßnahmen ermittelt werden, um diese Risiken zu behandeln;

Die Bundesregierung sollte auch ihren Entwurf des KRITIS-DachG dem vorgenannten Vorschlag für das NIS2UmsuCG entsprechend anpassen.

Befugnisse bei Registrierungspflicht nicht einheitlich

Sowohl der Entwurf des KRITIS-DachG als auch des NIS2UmsuCG sehen eine Registrierungspflicht für KRITIS-Betreiber vor. Beide Gesetze berücksichtigen auch den Fall, dass KRITIS-Betreiber ihrer Registrierungspflicht nicht nachkommen. In solchen Fällen sollen BSI und BBK die Befugnis erhalten, von den KRITIS-Betreibern Unterlagen und Auskünfte einzufordern.[51] Das NIS2UmsuCG schränkt die Befugnis des BSI dabei jedoch ein. Bei Geheimschutz- oder überwiegenden Sicherheitsinteressen können KRITIS-Betreiber die Herausgabe von Auskünften und Unterlagen verweigern. Im KRITIS-DachG-E ist diese Einschränkung für das BBK nicht

[48] § 2 Nummer 6 und 7 KRITIS-DachG-E.
[49] Artikel 6 Nummer 9.
[50] BSI Standard 200-3 – Risikoanalyse auf Basis von IT-Grundschutz.
[51] § 33 Absatz 4 BSIG-E, § 8 Absatz 2 Satz 2 KRITIS-DachG-E.

enthalten. Dort ist geregelt, dass KRITIS-Betreiber in solchen Fällen die erforderlichen Informationen auf andere Weise zur Verfügung stellen müssen. Gründe, warum das BSI hier – im Vergleich zum BBK – nur über geringere Befugnisse bei Auskunftsverlangen gegenüber KRITIS-Betreibern erhalten soll, sind nicht ersichtlich.

Empfehlung für geänderte Fassung des Artikel 1, § 33 Absatz 4:

Rechtfertigen Tatsachen die Annahme, dass eine Einrichtung ihre Pflicht zur Registrierung nach Absatz 1 oder 2 nicht erfüllt, so hat diese Einrichtung dem Bundesamt auf Verlangen die aus Sicht des Bundesamtes für die Bewertung erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen und Auskunft zu erteilen~~, *soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen entgegenstehen*~~. ***Können bestimmte Unterlagen oder Auskünfte aus Gründen des Geheimschutzes oder überwiegender Sicherheitsinteressen nicht vorgelegt oder erteilt werden, stellt die Einrichtung die erforderlichen Informationen auf andere Weise zur Verfügung.***

Zweckbindung für gemeinsame Datenbasis regeln

NIS2UmsuCG und KRITIS-DachG sind eng miteinander verzahnt. Daher müssen das BSI und das BBK in den unterschiedlichsten Prozessen einvernehmlich miteinander agieren. In besonderem Maße betrifft dies

- das Registrierungsverfahren,[52]
- das Meldeverfahren und die konkreten Meldungsinhalte[53] und
- das Verfahren, wie Nachweise[54] zu erbringen und zu prüfen sind.

BSI und BBK sollten auf der Grundlage einer gemeinsamen Datenbasis diese Verfahren etablieren und miteinander kooperieren. Denn physische Sicherheitsvorfälle können bei kritischen Dienstleistungen unmittelbar die Informations- und Cybersicherheit beeinflussen[55] oder umgekehrt.[56] Auch sind sie nicht immer trennscharf voneinander abzugrenzen. Wenn BSI und BBK ihre entsprechenden Meldungen in einem gemeinsamen Datenstand ablegen und bearbeiten, steigert dies ihre Reaktionsfähigkeit. Beide Behörden müssen sofort und unmittelbar den gleichen Sachstand kennen, um sich abstimmen und handeln zu können. Dies muss insbesondere auch gelten, weil sich im Laufe eines Sicherheitsvorfalls die

[52] § 33 Absatz 6 BSIG-E, § 8 Absatz 8 KRITIS-DachG-E.
[53] § 32 Absatz 4 BSIG-E, § 18 Absatz 3 KRITIS-DachG-E.
[54] § 39 Absatz 2 Nummer 3 BSIG-E, § 16 Absatz 8 KRITIS-DachG-E.
[55] Ausfälle der Stromversorgung können z. B. die Funktionsfähigkeit von Rechenzentren und darin befindlichen IT-Systemen direkt in Mitleidenschaft ziehen.
[56] Am 19. Juli 2024 verursachte eine Störung der Sicherheitsanwendung „Crowdstrike Falcon Sensor“ des Herstellers Crowdstrike unmittelbar Ausfälle in IT-gestützten Geschäftsprozessen. Im Ergebnis mussten beispielsweise Flughäfen ihren Betrieb einstellen bzw. einschränken; https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2024/2024-257485-10F1.pdf?__blob=publicationFile&v=3, abgerufen am 13. August 2024.

Schwerpunkte zwischen den Zuständigkeitsbereichen verschieben können. Auch mit Blick auf knappe personelle und finanzielle Ressourcen bei BSI und BBK wäre es schwer nachvollziehbar, wenn diese jeweils in eigener Hoheit eine redundante Datenhaltung betreiben. Hinzu käme, dass beide Behörden zusätzlichen Aufwand hätten, um getrennte Datenstände synchron zu halten. Es wäre daher zielführend, in beiden Gesetzen die Zweckbindung so zu gestalten, dass BSI und BBK gleichermaßen auf die Daten zugreifen können. In diese Überlegungen sollten auch die Informationsbedarfe der weiteren Aufsichtsbehörden einbezogen werden. Die Vorgaben des Daten- und gegebenenfalls des Geheimschutzes sind für die gemeinsame Datenbasis zu beachten. Angesichts knapper Haushaltsmittel gilt es auf jeden Fall, keine unnötigen Mehrfachstrukturen aufzubauen, alle Automatisierungsmöglichkeiten auszuschöpfen und Redundanzen zu vermeiden.

Gemeinsames Lagebild erstellen

Des Weiteren sollten BSI und BBK die gemeinsame Datenbasis nutzen, um ein gemeinsames aktuelles Lagebild zu den Bedrohungen für die physische Sicherheit und die Cybersicherheit von KRITIS zu erstellen. Bislang sieht das NIS2UmsuCG (nur) vor, dass das BSI ein Lagebild bezüglich der Sicherheit in der Informationstechnik von kritischen Anlagen kontinuierlich aktualisiert.[57] Der vorliegende Entwurf des KRITIS-DachG begründet keine Verpflichtung für ein derartiges Lagebild zur physischen Sicherheit von kritischen Anlagen.

Ein gemeinsames Lagebild sollte tagesaktuell die Bedrohungslage darstellen und allen Stellen mit einem berechtigten Interesse zur Verfügung stehen. Zwei Lagebilder mit möglicherweise widersprüchlichen Aussagen gilt es zu vermeiden. Es bedarf eines „All-Gefahren-Überblicks“, den BSI und BBK – zumindest bezogen auf die KRITIS-Betreiber – gemeinsam erstellen sollten.

Empfehlung für geänderte Fassung des Artikel 1, § 40 Absatz 3:

Zur Wahrnehmung seiner Aufgabe als zentrale Meldestelle hat das Bundesamt

3. das Lagebild bezüglich der Sicherheit in der Informationstechnik von kritischen Anlagen, besonders wichtigen Einrichtungen und wichtigen Einrichtungen kontinuierlich zu aktualisieren ***und gemeinsam mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe um Informationen zur physischen Sicherheit zu ergänzen*** und

3.7.1 Stellungnahme des BMI

Das BMI strebe weiterhin eine größtmögliche Kohärenz zwischen den Regelungen des Gesetzentwurfs und des zukünftigen KRITIS-DachG an. Zur gemeinsamen Datenbasis und einem gemeinsamen Lagebild von BSI und BBK äußert sich das BMI nicht. Mit den Regelungen des

[57] § 40 Absatz 3 Nummer 3 BSIG-E.

§ 32 Absatz 1 sowie § 33 Absatz 1 BSIG-E für ein gemeinsames Melde- und Registrierungsportal sei bereits ein zentraler Grundstein für die zukünftige Zusammenarbeit von BSI und BBK gelegt.

Aufgrund der unterschiedlichen Stadien der beiden Gesetzgebungsverfahren könne es jedoch noch zeitweise zu ungewollten Abweichungen kommen. Gegebenenfalls seien auch im parlamentarischen Verfahren noch Angleichungen vorzunehmen.

3.7.2 Abschließende Bewertung des Bundesrechnungshofes

Die Ausführungen des BMI bestätigen die Hinweise des Bundesrechnungshofes zum Erfordernis der Kohärenz von KRITIS-DachG und NIS2UmsuCG. Er hält an seiner Auffassung fest, dass das NIS2UmsuCG außerdem Regelungen für eine gemeinsame Datenbasis sowie ein gemeinsames Lagebild von BSI und BBK treffen sollte.

Der Bundesrechnungshof bleibt daher bei seinen Empfehlungen.

4 Haushaltsausgaben und Erfüllungsaufwand für die Verwaltung nicht in allen Fällen belastbar

Die Bundesregierung beziffert die in den Jahren 2026 bis 2029 zusätzlich zu erwartenden Haushaltsausgaben auf insgesamt 810 Mio. Euro. Ursächlich hierfür sind im Wesentlichen der Bedarf an 1 034 zusätzlichen Stellen sowie die dadurch bedingten Personalausgaben.[58]

Dem Bundesrechnungshof ist bewusst, dass die Bundesregierung die mit der NIS-2-Richtlinie verbundenen Ziele ohne zusätzliches Personal nicht erreichen kann. Die Angaben in der Gesetzesbegründung sind allerdings nicht geeignet, den Mehrbedarf aus dem NIS2UmsuCG der Höhe nach belastbar abzubilden. Beispielhaft ist Folgendes nicht plausibel:

a) Der für die einzelnen Ressorts ausgewiesene Stellenmehrbedarf[59] weist zum Teil erhebliche, nicht nachvollziehbare Differenzen auf. So geht das Bundesministerium für Bildung und Forschung (BMBF) – insgesamt rund 1 400 Stellen, keine Geschäftsbereichsbehörden – davon aus, dass es 0,5 zusätzliche Stellen und 244 000 Euro benötigt, um die Verpflichtungen aus dem NIS2UmsuCG umzusetzen. Das Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung – ebenfalls ohne Geschäftsbereich, mit gut 1 100 Stellen kleiner als das BMBF – weist den zusätzlichen Bedarf hingegen mit zwölf Stellen und 12,5 Mio. Euro Ausgaben aus. Warum Ministerien mit ähnlich vielen Beschäftigten bei identischen neuen Anforderungen ihren Ressourcenbedarf mit einer Abweichung um das 20- bis 50-fache beziffern, erschließt sich nicht.

[58] Buchstabe D. des Vorblatts sowie Teil A.VI.3 der Gesetzesbegründung.

[59] Gesetzesbegründung, Teil A., Ziffern VI.3.b. und c. (Haushaltsausgaben und Stellen nach Einzelplänen).

b) Die Bundesbehörden (außerhalb der Geschäftsbereiche des BKAmtes, des BMI und des BMVg) verfügen derzeit nach eigenen Angaben über rund 560 Stellen für die Aufgaben der IT-Sicherheit. Um die neuen Verpflichtungen des NIS2UmsuCG umzusetzen, machen sie einen Bedarf von weiteren 337 Stellen geltend.[60] Dies entspricht einem Mehrbedarf von 60 % gegenüber dem Status quo. Bezogen auf einzelne Ressorts ergeben sich dabei auffällige, nicht erklärbare Abweichungen von diesem Durchschnittswert: Für den Geschäftsbereich des Bundesministeriums der Finanzen (Einzelplan 08) sind sieben Stellen ausgewiesen; bei derzeit bereits vorhandenen 233 Stellen entspricht dies 3 %. Beim Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV, Einzelplan 16) beträgt der Mehrbedarf hingegen 350 %.[61]

c) Das NIS2UmsuCG führt auch bei den Aufsichtsbehörden zu zusätzlichem Aufwand, da die Zahl der zu beaufsichtigenden Einrichtungen stark zunehmen wird. Die Bundesregierung beziffert diesen für das BSI auf 476 Stellen[62], davon allein 305 Stellen für Grundsatzaufgaben und Befugnisse[63]. Bezogen auf die derzeit rund 645 hierfür im BSI eingesetzten Stellen bedeutet dies einen Mehrbedarf von annähernd 50 %. Die Bundesregierung begründet diesen u. a. mit dem Hinweis darauf, dass „*künftig alle Einrichtungen der Bundesverwaltung in den Anwendungsbereich des BSIG*“ fallen. Diese Aussage erweckt zu Unrecht den Eindruck, dass dies nach dem IT-SiG 2.0 bislang nicht der Fall ist. Dabei ist der Geltungsbereich im NIS2UmsuCG für die Bundesbehörden weitgehend unverändert.[64]

Eine nähere Analyse dieser und weiterer Angaben zu den Haushaltsausgaben und zum Erfüllungsaufwand lässt die Annahme zu, dass

- den Angaben ein teilweise unterschiedliches Verständnis darüber zugrunde liegt, was an neuen Aufgaben mit dem NIS2UmsuCG auf die Ressorts zukommt, und
- Personal- und Sachmittelbedarfe auch für Aufgaben ausgewiesen werden, die die Ressorts bereits aufgrund der derzeit schon bestehenden Regelungen (u. a. UP Bund, Mindeststandards nach § 8 BSIG, § 50 Absatz 2 VSA[65]) verpflichtend wahrzunehmen haben.

---

[60] Gesamtbedarf von 1 034,2 Stellen abzüglich der für die Einzelpläne 04 (BKAmt), 06 (BMI) und 14 (BMVg) ausgewiesenen Stellenbedarfe (insgesamt 697,7).

[61] Aktuell verfügt das BMUV nach eigenen Angaben über acht Stellen für IT-Sicherheit; für die Umsetzung des NIS2UmsuCG hält es lt. Gesetzesbegründung weitere 28 für erforderlich.

[62] Gesetzesbegründung, Teil A., Ziffer VI.4.c.aa.bbb (Erfüllungsaufwand für die Vollzugsaufgaben der Verwaltung).

[63] Ebd., Vorgabe 4.3.5, §§ 3 bis 27 BSIG-E.

[64] Der Geschäftsbereich des AA soll sogar zukünftig in weiten Teilen nicht mehr der Aufsicht durch das BSI unterliegen (vgl. Tz. 2.2).

[65] 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.

Dies würde gegen die Vorgaben zur Darstellung des Erfüllungsaufwands in Regelungsvorhaben der Bundesregierung[66] verstoßen. Gemäß § 2 Absatz 1 NKRG[67] umfasst dieser den gesamten messbaren Zeitaufwand und die Kosten, die bei Bürgerinnen und Bürgern, der Wirtschaft sowie der öffentlichen Verwaltung entstehen. Dabei ist ausschließlich die zu erwartende Änderung des Erfüllungsaufwands maßgebend. Aufwände, die bereits heute anfallen, sind nicht unmittelbare Folge des NIS2UmsuCG und dürfen folglich nicht zum Erfüllungsaufwand gerechnet werden.

Der Bundesrechnungshof sieht sich in dieser Einschätzung von der Stellungnahme des Nationalen Normenkontrollrates (NKR) bestätigt. Unter Hinweis auf den bereits existierenden UP Bund hat dieser darauf aufmerksam gemacht, dass diesbezügliche Aufwände als „Sowieso-Kosten“ nicht zum Erfüllungsaufwand gezählt werden dürften. In ihrer Stellungnahme hat die Bundesregierung darauf hingewiesen, dass jedes Ressort seinen Mehraufwand aus dem NIS2UmsuCG in eigener Verantwortung ermittelt habe und die Ergebnisse aus Zeitgründen nur teilweise plausibilisiert werden konnten.

Insgesamt begründen die dargestellten Beispiele und die Stellungnahme der Bundesregierung aus Sicht des Bundesrechnungshofes Zweifel daran, inwieweit der aus der Umsetzung des NIS2UmsuCG entstehende Mehrbedarf an Personal- und Sachmitteln durchgängig sachgerecht ermittelt ist. Nach Inkrafttreten des Gesetzes zu erwartende Stellen- und Ausgabenforderungen der Ressorts sollten daher eingehend auf den Prüfstand gestellt werden.

4.1 Stellungnahme des BMI

Das BMI gibt an, die dargestellten Mehrbedarfe für die Umsetzung des Gesetzes basierten auf den Bewertungen der einzelnen Ressorts. Um zu einer einheitlichen Einschätzung zu kommen, habe das BMI zahlreiche Handreichungen bereitgestellt. Ferner habe es bei der Ressortabstimmung um kritische Prüfung der einzelnen Zulieferungen gebeten. Für eine kohärente Ermittlung und Darstellung der Erfüllungsaufwände habe es eine einheitliche Erhebungsmethode genutzt und das Statische Bundesamt frühzeitig hinzugezogen. Aufgrund des verfassungsrechtlich verankerten Ressortprinzips habe sich das BMI auf die Richtigkeit der Zulieferungen der einzelnen Ressorts verlassen müssen und keinerlei Hoheit über das Ergebnis. Es teile das Ansinnen, nach Inkrafttreten des Gesetzes die in diesem dargestellten Mehrbedarfe zu evaluieren. Das Statistische Bundesamt solle den geschätzten und im Gesetzentwurf dargelegten Erfüllungsaufwand validieren. Seine Ergebnisse könnten dann über die bei den einzelnen Behörden tatsächlich entstandenen Kosten Aufschluss geben.

Die vom Bundesrechnungshof angemerkten Zweifel hinsichtlich der zu den einzelnen Ressorts angegebenen Zahlen beruhten im Übrigen auf prozentualen Vergleichen. Dabei sei

[66] Leitfaden zur Ermittlung und Darstellung des Erfüllungsaufwands in Regelungsvorhaben der Bundesregierung, Ziffer 2.3; Hrsg.: Statistisches Bundesamt im Auftrag der Bundesregierung und des Nationalen Normenkontrollrates, Fünfte aktualisierte Fassung, erschienen im September 2022 auf Grundlage des Beschlusses des Staatssekretärsausschusses vom 11. Oktober 2018.

[67] Gesetz zur Einsetzung eines Nationalen Normenkontrollrates.

jedoch zu berücksichtigen, dass zur Umsetzung der Vorgaben der NIS2-Richtlinie in jedem Ressort – grundsätzlich unabhängig von der Ressortgröße – zunächst zusätzliche Rollen und Funktionen einzurichten und zu besetzen seien. Diese wirkten sich bei kleineren Ressorts naturgemäß stärker aus. Insoweit sei eine rein prozentuale Betrachtung unter ausdrücklicher Nennung eines einzelnen Ressorts nicht geeignet, die unterschiedlichen Erfüllungsaufwände der Ressorts kritisch zu bewerten. Zudem sei zu berücksichtigen, dass insbesondere je nach Größe der Ressorts der aktuelle Umsetzungsstand bei der Informationssicherheit stark variieren könne. Grund dafür sei unter anderem, dass sich infolge der Pandemie und der umfassenden Umstrukturierung und Modernisierung der IT-Infrastruktur Prioritäten beim Einsatz vorhandenen Personals für Informationssicherheit unterschiedlich stark ausgewirkt hätten.

4.2 Abschließende Bewertung des Bundesrechnungshofes

BMI und Bundesrechnungshof stimmen darin überein, dass nach Inkrafttreten des Gesetzes die dargestellten Mehrbedarfe zu evaluieren sind.

Alle Ressorts müssen bereits seit dem Jahr 2017 die Vorgaben des UP Bund erfüllen. Aus welchen Gründen (Pandemie, Umstrukturierung der IT, Modernisierung der IT, Prioritäten beim Personaleinsatz) einzelne Ressorts diese Maßgaben nicht vollumfänglich einhalten, ist für die Schätzung des zusätzlichen Stellen- und Sachmittelbedarfs für das NIS2UmsuCG unerheblich. Unzureichende Stellen- und Sachmittelanmeldungen der Vergangenheit dürfen nun nicht dem NIS2UmsuCG zugerechnet werden. Im Laufe des Gesetzgebungsverfahrens korrigierten die Ressorts ihre Personalbedarfsschätzungen bereits drastisch. Die Ressorts müssen ihre schon zuvor bestehenden Bedarfe außerhalb des Gesetzgebungsprozesses geltend machen. Dabei muss die Bundesregierung auf einen einheitlichen Maßstab für die Personal- und Sachmittelbemessung im Bereich der Informations- und Cybersicherheit achten.

5 Fazit des Bundesrechnungshofes

Die Stellungnahme des BMI konnte den Bundesrechnungshof in weiten Teilen nicht überzeugen. Soweit das BMI sich zu Empfehlungen nicht geäußert hat, geht der Bundesrechnungshof davon aus, dass es dessen Argumentation nicht widerspricht. Die vom Bundesrechnungshof vorgeschlagenen Änderungen am Gesetzentwurf entsprechen den Zielen der NIS-2-Richtlinie und fördern einen ordnungsgemäßen und wirtschaftlichen Gesetzesvollzug, indem sie

- den IT-Grundschutz und Maßnahmen zum Risikomanagement für die gesamte Bundesverwaltung gesetzlich verankern,
- Ausnahmeregelungen für das AA begrenzen,
- weitreichende Ausnahmeregelungen für Einrichtungen der Bundesverwaltung beschränken,
- den Nachweis der Informationssicherheit durch Einrichtungen der Bundesverwaltung in kürzeren Fristen vorsehen,

- die Verantwortung der Leitungsebene für die Informationssicherheit konkretisieren,
- Aufgaben und Befugnisse der Koordinatorin oder des Koordinators für Informationssicherheit festlegen und
- die Kohärenz zwischen NIS2UmsuCG und KRITIS-DachG verbessern.

Der Bundesrechnungshof regt daher an, die von ihm vorgeschlagenen Änderungen im Gesetzgebungsprozess zu berücksichtigen. Zudem fordert er, die von den Ressorts geltend gemachten Mehrbedarfe nach Inkrafttreten des Gesetzes zu evaluieren.

Beglaubigt: Rogall, Tarifbeschäftigte

Wegen elektronischer Bearbeitung ohne Unterschrift und Dienstsiegelabdruck.