Deutscher Bundestag **Drucksache 21/2782**

21. Wahlperiode 12.11.2025

Beschlussempfehlung und Bericht

des Innenausschusses (4. Ausschuss)

zu dem Gesetzentwurf der Bundesregierung
– Drucksachen 21/1501, 21/2072, 21/2146 Nr. 1.11 –

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

A. Problem

Die aufgrund neuer geopolitischer Rahmenbedingungen gestiegenen Cybersicherheitsanforderungen werden mit der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27.12.2022, S. 80, im Folgenden NIS-2-Richtlinie) in der gesamten Europäischen Union weiter angeglichen.

Entsprechend der unionsrechtlichen Vorgaben soll der mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 und dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021 geschaffene Ordnungsrahmen durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz auf den Bereich bestimmter Unternehmen erweitert und zusätzlich entsprechende Vorgaben für die Bundesverwaltung eingeführt werden.

B. Lösung

Der Innenausschuss empfiehlt mit dieser Beschlussempfehlung, den Gesetzentwurf im Wesentlichen um folgende Maßnahmen abzuändern und zu ergänzen:

– Ausweitung des Anwendungsbereiches hinsichtlich der Verwaltung auf die Geschäftsbereichsbehörden;

– Ausgestaltung der Rolle des Chief Information Security Officer (CISO Bund) als zentrale Stelle für Informationen zur Cybersicherheit aus der Bundesverwaltung sowie zur Koordinierung von Maßnahmen;

– Anpassungen in den §§ 1,15 des Gesetzes über das Bundesamt für die Sicherheit in der Informationstechnik (BSIG) zur Klarstellung der Aufgabengrundlage des BSI und Anpassungen beim Schwachstellenscan;

– in § 16 BSIG Streichung der 100 000-Kunden-Grenze für Anordnungen gegenüber Telekommunikationsdiensten sowie Aufnahme der Möglichkeit Bereinigungsbefehle auszusenden;

– Umsetzung zweier Anträge des Bundesrates zur Aufnahme der Länder in § 3 Abs. 1 Nr. 18 und 20 BSIG (Unterstützung der Polizeien/Strafverfolgungsbehörden und Beratungs-, Informations- und Warnungsbefugnis des BSI gegenüber den Ländern);

– Aufnahme des § 41 BSIG zur Untersagung des Einsatzes von kritischen Komponenten;

– Klarstellende Ergänzung zum CVD-Prozess in § 5 BSIG.

Annahme des Gesetzentwurfs in geänderter Fassung mit den Stimmen der Fraktionen der CDU/CSU, AfD und SPD gegen die Stimmen der Fraktion BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion Die Linke.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Für den Bundeshaushalt entstehen durch das Gesetz bei der Bundesverwaltung einmalige Ausgaben in Höhe von rund 59 Millionen Euro sowie bis zum Jahr 2029 insgesamt laufende jährliche Ausgaben in Höhe von durchschnittlich rund 212 Millionen Euro (beides in Summe 906 Mio. Euro bis 2029). Die einmaligen Ausgaben umfassen dabei die Sachkosten in den Jahren 2026 bis 2029. Die einmaligen und laufenden jährlichen Ausgaben verteilen sich dabei wie folgt auf den Zeitraum 2026 bis 2029:

	2026	**2027**	**2028**	**2029**
einmalige Ausgaben (in Mio. Euro)	56,11	1,17	0,87	0,77
laufende Ausgaben (in Mio. Euro)	143,92	224,16	239,88	240,19
Ausgaben (gesamt, in Mio. Euro)	**200,04**	**225,33**	**239,97**	**240,27**

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen ist Gegenstand künftiger Haushaltsaufstellungsverfahren.

Mehrausgaben für Länder und Kommunen entstehen nicht

Den Sozialversicherungsträgern entstehen durch das Gesetz insgesamt laufende jährliche Ausgaben in Höhe von rund 16,6 Millionen Euro.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Es entsteht kein Erfüllungsaufwand für die Bürgerinnen und Bürger.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft erhöht sich der jährliche Erfüllungsaufwand um rund 2,3 Milliarden Euro. Insgesamt entsteht einmaliger Aufwand von rund 2,2 Milliarden Euro. Dieser ist fast ausschließlich der Kategorie Einführung oder Anpassung digitaler Prozessabläufe zuzuordnen.

Davon Bürokratiekosten aus Informationspflichten

Es entfallen rund 2,4 Millionen Euro auf Bürokratiekosten aus Informationspflichten.

E.3 Erfüllungsaufwand der Verwaltung

Für die Bundesverwaltung erhöht sich der jährliche Erfüllungsaufwand um 119 Millionen Euro. Der einmalige Erfüllungsaufwand beträgt 63 Millionen Euro. Der jährliche Erfüllungsaufwand der Länder erhöht sich um 166 000 Euro.

F. Weitere Kosten

Keine.

Beschlussempfehlung

Der Bundestag wolle beschließen,

den Gesetzentwurf auf Drucksachen 21/1501, 21/2072 mit folgenden Maßgaben, im Übrigen unverändert anzunehmen:

1. Artikel 1 wird wie folgt geändert:

   a) § 1 Satz 3 wird durch den folgenden Satz ersetzt:

   „Seine Aufgaben führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch.“

   b) § 2 wird wie folgt geändert:

   aa) Nummer 23 wird durch die folgende Nummer 23 ersetzt:

   „23. „kritische Komponenten“ IKT-Produkte, die in einer Rechtsverordnung aufgrund von § 56 Absatz 7 und 8 als kritische Komponenten bestimmt werden;“.

   bb) Nummer 27 wird durch die folgende Nummer 27 ersetzt:

   „27. „NIS-2-Richtlinie“ die Richtlinie (EU) 2022/2555 in der jeweils geltenden Fassung;“.

   c) § 3 Absatz 1 Satz 2 wird wie folgt geändert:

   aa) Nummer 18 wird wie folgt geändert:

   aaa) In Buchstabe a wird nach der Angabe „Bundes“ die Angabe „und der Länder“ eingefügt.

   bbb) Buchstabe b wird durch den folgenden Buchstaben b ersetzt:

   „b) der Verfassungsschutzbehörden des Bundes und der Länder und des Militärischen Abschirmdienstes bei der Auswertung und Bewertung von Informationen, die bei der Beobachtung von Bestrebungen anfallen, die gegen die freiheitliche demokratische Grundordnung, den Bestand des Staates oder die Sicherheit des Bundes oder eines Landes gerichtet sind, oder die bei der Beobachtung sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten im Rahmen der gesetzlichen Befugnisse nach den Verfassungsschutzgesetzen des Bundes und der Länder beziehungsweise dem MAD-Gesetz anfallen,“.

   bb) In Nummer 20 wird nach der Angabe „Bundesverwaltung“ die Angabe „, die Länder“ eingefügt.

   d) § 5 wird wie folgt geändert:

   aa) Absatz 3 wird durch den folgenden Absatz 3 ersetzt:

   „(3) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 1 gibt das Bundesamt die Informationen zu den nach Absatz 2 gemeldeten Schwachstellen unverzüglich an den verantwortlichen Hersteller oder Produktverantwortlichen zum Zwecke der Schließung der Schwachstelle weiter, sofern diese nicht bereits öffent-

lich bekannt ist. Das Bundesamt soll die gemäß Absatz 2 gemeldeten Informationen nutzen, um

1. Dritte über bekannt gewordene Schwachstellen, Schadprogramme oder erfolgte oder versuchte Angriffe auf die Sicherheit in der Informationstechnik zu informieren, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,
2. die Öffentlichkeit oder betroffene Kreise gemäß § 13 zu warnen und zu informieren,
3. Einrichtungen der Bundesverwaltung gemäß § 4 Absatz 2 Nummer 2 über die sie betreffenden Informationen zu unterrichten,
4. besonders wichtige Einrichtungen und wichtige Einrichtungen gemäß § 40 Absatz 3 Nummer 4 Buchstabe a über die sie betreffenden Informationen zu unterrichten,
5. seine Aufgaben als zuständige Behörde, CSIRT und zentrale Anlaufstelle im Sinne der NIS-2-Richtlinie wahrzunehmen.“

bb) Nach Absatz 5 wird der folgende Absatz 6 eingefügt:

„(6) Das Bundesamt veröffentlicht am … [einsetzen: Datum des Tages und Monats des Inkrafttretens nach Artikel 30 dieses Gesetzes sowie die Jahreszahl des auf das Inkrafttreten folgenden Jahres] eine Verfahrensbeschreibung zur Durchführung der Absätze 1 bis 3.“

e) § 15 wird wie folgt geändert:

aa) Absatz 1 wird durch den folgenden Absatz 1 ersetzt:

„(1) Das Bundesamt kann im Rahmen seiner Aufgabe nach § 3 Absatz 1 Satz 2 Nummer 1 zur Detektion von bekannten Schwachstellen und anderen Sicherheitsrisiken Abfragen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen durchführen,

1. um festzustellen, ob diese Schnittstellen unzureichend geschützt und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können, oder
2. wenn die Einrichtungen der Bundesverwaltung, der besonders wichtigen oder der wichtigen Einrichtungen darum ersuchen.

Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, darf es diese nur zum Zwecke der Übermittlung nach § 8 Absatz 6 und 7 verarbeiten. Sofern die Voraussetzungen des § 8 Absatz 6 und 7 nicht vorliegen, sind Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, unverzüglich zu löschen.“

bb) Absatz 2 wird durch den folgenden Absatz 2 ersetzt:

„(2) Wird durch Abfragen gemäß Absatz 1 Satz 1 eine Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, informiert das Bundesamt als allgemeine Meldestelle für die Sicherheit in der Informationstechnik nach § 5 darüber unverzüglich die für das informationstechni-

sche System Verantwortlichen. Gehört das informationstechnische System zu einer Einrichtung der Bundesverwaltung, sind zugleich die Informationssicherheitsbeauftragten der betroffenen Einrichtung der Bundesverwaltung nach § 45 und des übergeordneten Ressorts nach § 46 zu informieren. Das Bundesamt soll dabei auf bestehende Möglichkeiten zur Abhilfe des Sicherheitsrisikos hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigem Aufwand oder über eine Bestandsdatenabfrage nach § 12 möglich, so ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen, wenn überwiegende Sicherheitsinteressen nicht entgegenstehen.“

f) § 16 wird durch den folgenden § 16 ersetzt:

„§ 16

Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von Telekommunikationsdiensten

(1) Zur Abwehr erheblicher Gefahren für die in Absatz 3 genannten Schutzgüter kann das Bundesamt anordnen, dass ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes

1. die in § 169 Absatz 6 und 7 des Telekommunikationsgesetzes bezeichneten Maßnahmen trifft oder
2. technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme verteilt,

sofern und soweit der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten dazu technisch in der Lage und es ihm wirtschaftlich zumutbar ist. Vor der Anordnung der Maßnahmen nach Satz 1 Nummer 1 oder 2 durch das Bundesamt ist die Bundesnetzagentur ins Benehmen zu setzen. Vor der Anordnung der Maßnahme nach Satz 1 Nummer 2 durch das Bundesamt ist zusätzlich Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit herzustellen. Die Daten, auf die mit der Maßnahme nach Satz 1 Nummer 2 zugegriffen werden soll, sind in der Anordnung zu benennen. § 8 Absatz 8 Satz 2 bis 8 gilt entsprechend. Widerspruch und Anfechtungsklage gegen die Anordnungen nach Satz 1 haben keine aufschiebende Wirkung.

(2) Zur Abwehr erheblicher Gefahren für die in Absatz 3 genannten Schutzgüter kann das Bundesamt technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme verteilen. Absatz 1 Satz 2 und 3 gilt entsprechend. Der betroffene Diensteanbieter ist verpflichtet, das Bundesamt bei der Umsetzung nach Satz 1 zu unterstützen und insbesondere alle notwendigen Auskünfte zu erteilen, die zur Erstellung und Verteilung des Befehls notwendig sind.

(3) Schutzgüter gemäß Absatz 1 Satz 1 sind die Verfügbarkeit, Integrität oder Vertraulichkeit

1. der Kommunikationstechnik des Bundes, einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung,
2. von Informations- oder Kommunikationsdiensten oder
3. von Informationen, sofern deren Verfügbarkeit, Unversehrtheit oder Vertraulichkeit durch unerlaubte Zugriffe auf eine erhebliche Anzahl von telekommunikations- oder informationstechnischen Systemen von Nutzern eingeschränkt wird.

(4) Ordnet das Bundesamt eine Maßnahme nach Absatz 1 Satz 1 Nummer 1 an, so kann es gegenüber dem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten auch anordnen, den Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umzuleiten.

(5) Das Bundesamt darf Daten, die von einem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten nach Absatz 1 Satz 1 Nummer 1 und Absatz 4 umgeleitet wurden, verarbeiten, um Informationen über Schadprogramme oder andere Sicherheitsrisiken in informationstechnischen Systemen zu erlangen. Die übermittelten Daten dürfen durch das Bundesamt so lange gespeichert werden, wie dies für die Erfüllung des in Satz 1 genannten Zwecks erforderlich ist, längstens jedoch für drei Monate. § 8 Absatz 8 Satz 2 bis 8 gilt entsprechend. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Gesamtzahl der angeordneten Datenumleitungen.“

g) In § 28 Absatz 5 Satz 4 wird die Angabe „vernachlässigbar ist“ durch die Angabe „eine Nebentätigkeit darstellt“ ersetzt.

h) § 29 Absatz 2 Satz 2 wird gestrichen.

i) § 33 wird wie folgt geändert:

aa) Absatz 2 wird durch den folgenden Absatz 2 ersetzt:

„(2) Betreiber kritischer Anlagen übermitteln mit den Angaben nach Absatz 1 die kritische Dienstleistung, die bei ihnen zum Einsatz kommenden Typen von kritischen Komponenten, die öffentlichen IP-Adressbereiche der von ihnen betriebenen Anlagen sowie die für die von ihnen betriebenen kritischen Anlagen ermittelte Anlagenkategorie und die ermittelten Versorgungskennzahlen gemäß der Rechtsverordnung nach § 56 Absatz 4 sowie den Standort der Anlagen und eine Kontaktstelle. Die Betreiber stellen sicher, dass sie über ihre in Satz 1 genannte Kontaktstelle jederzeit erreichbar sind.“

bb) Absatz 5 wird durch den folgenden Absatz 5 ersetzt:

„(5) Bei Änderungen der nach Absatz 1 oder 2 zu übermittelnden Angaben sind dem Bundesamt geänderte Versorgungskennzahlen sowie Änderungen der bei Betreibern kritischer Anlagen zum Einsatz kommenden Typen von kritischen Komponenten einmal jährlich zu übermitteln und alle anderen Angaben unverzüglich, spätestens jedoch zwei Wochen ab dem Zeitpunkt, zu dem die Einrichtung Kenntnis von der Änderung erhalten hat, zu übermitteln.“

j) § 41 wird durch den folgenden § 41 ersetzt:

„§ 41

Untersagung des Einsatzes von kritischen Komponenten

(1) Das Bundesministerium des Innern kann gegenüber dem Betreiber kritischer Anlagen den Einsatz von kritischen Komponenten eines Herstellers im Benehmen mit dem Bundesministerium für Wirtschaft und Energie im Sektor Energie, dem Bundesministerium für Wirtschaft und Energie sowie dem Bundesministerium für Forschung, Technologie und Raumfahrt im Sektor Weltraum, dem Bundesministerium für Digitales und Staatsmodernisierung in den Sektoren Informationstechnik und Telekommunikation, dem Bundesministerium für Verkehr in den Sektoren Transport und Verkehr, dem Bundesministerium für Gesundheit im Sektor Gesundheit, dem Bundesministerium für Ernährung und Landwirtschaft im Sektor Ernährung, dem Bundesministerium der Finanzen im Sektor Finanzwesen, dem Bundesministerium für Arbeit und Soziales in den Sektoren Sozialversicherungsträger sowie Grundsicherung für Arbeitsuchende und dem Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit in den Sektoren Wasser sowie Siedlungsabfallentsorgung sowie dem Auswärtigen Amt untersagen oder Anordnungen dazu erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt.

(2) Hat das Bundesministerium des Innern einem Betreiber kritischer Anlagen den Einsatz einer kritischen Komponente untersagt oder eine Anordnung dazu erlassen, kann es im Benehmen mit dem in Absatz 1 genannten Bundesministerium

1. dem Betreiber kritischer Anlagen auch den zukünftigen Einsatz weiterer kritischer Komponenten desselben Herstellers und desselben Komponententyps untersagen oder Anordnungen dazu erlassen,
2. allen Betreibern kritischer Anlagen den Einsatz derselben kritischen Komponente desselben Herstellers sowie von weiteren kritischen Komponenten desselben Komponententyps desselben Herstellers untersagen oder Anordnungen erlassen.

Die Entscheidung nach Satz 1 Nummer 2 ergeht als Allgemeinverfügung.

(3) Widerspruch und Klage gegen eine Untersagung oder Anordnung nach den Absätzen 1 und 2 Satz 1 haben keine aufschiebende Wirkung.

(4) Bei der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit nach Absatz 1 kann insbesondere berücksichtigt werden, ob

1. der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird oder zur Zusammenarbeit mit staatlichen Stellen oder Streitkräften eines Drittstaates verpflichtet ist oder von dem Drittstaat hierzu verpflichtet werden kann,

2. der Hersteller an Aktivitäten beteiligt war oder ist, die geeignet waren oder sind, nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland oder eines anderen Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages oder auf deren Einrichtungen zu haben,

3. hinreichende Anhaltspunkte dafür bestehen, dass der Hersteller aus sonstigen Gründen nicht vertrauenswürdig ist,

4. der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Interessen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht.

(5) Der Betreiber kritischer Anlagen ist zur Mitwirkung bei der Ermittlung des Sachverhalts verpflichtet. Dafür hat er auf Verlangen alle für das Verfahren erheblichen Tatsachen vollständig und wahrheitsgemäß mitzuteilen und die ihm bekannten Beweismittel anzugeben.“

k) In § 43 Absatz 1 Satz 2 wird die Angabe „Absatz 1“ durch die Angabe „Satz 1“ ersetzt.

l) § 44 wird durch den folgenden § 44 ersetzt:

„§ 44

Vorgaben des Bundesamtes

(1) Die Einrichtungen der Bundesverwaltung müssen Mindestanforderungen zum Schutz der in der Bundesverwaltung verarbeiteten Informationen erfüllen. Die Mindestanforderungen ergeben sich aus den BSI-Standards und dem Grundschutzkompendium (IT-Grundschutz) sowie aus den Mindeststandards für die Sicherheit in der Informationstechnik des Bundes (Mindeststandards) in den jeweils geltenden Fassungen. Die jeweils geltenden Fassungen werden auf der Internetseite des Bundesamtes veröffentlicht. Die Mindeststandards legt das Bundesamt im Benehmen mit den Ressorts und weiteren obersten Bundesbehörden fest. Der IT-Grundschutz und die Mindeststandards werden durch das Bundesamt regelmäßig evaluiert und entsprechend dem Stand der Technik sowie unter Berücksichtigung der Erfahrungen aus der Praxis und aus der Beratung und Unterstützung nach Absatz 3 fortentwickelt; dabei wird der Umsetzungsaufwand soweit möglich minimiert. Das Bundesamt wird den IT-Grundschutz bis zum 1. Januar 2026 modernisieren und fortentwickeln. Für die Verpflichtung nach Satz 1 gelten die Ausnahmen nach § 7 Absatz 6 und 7 entsprechend.

(2) Durch die Umsetzung der Mindestanforderungen nach Absatz 1 Satz 1 ist die Erfüllung der Vorgaben nach § 30 gewährleistet, soweit nicht die Europäische Kommission einen Durchführungsrechtsakt gemäß Artikel 21 Absatz 5 Unterabsatz 2 der NIS-2-Richtlinie erlässt, in dem die technischen und methodischen Anforderungen über die Mindestanforderungen aus Absatz 1 Satz 1 hinausgehen. Falls eine Einrichtung des Bundes gleichzeitig ein Betreiber kritischer Anlagen ist und die Anforderungen des IT-Grundschutzes und der Mindeststandards den Anforderungen nach § 30 Absatz 9 und § 31 widersprechen, genießen Letztere Vorrang.

(3) Das Bundesamt berät die Einrichtungen der Bundesverwaltung auf Ersuchen bei der Umsetzung und Einhaltung der Mindestanforderungen nach Absatz 1 Satz 1, stellt Hilfsmittel zur Verfügung und unterstützt die Bereitstellung entsprechender Lösungen durch die IT-Dienstleister des Bundes über den gesamten Lebenszyklus.

(4) Das Bundesamt stellt im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 10 technische Richtlinien und Referenzarchitekturen bereit, die von den Einrichtungen der Bundesverwaltung als Rahmen für die Entwicklung sachgerechter Anforderungen an Auftragnehmer – im Sinne einer Eignung – und IT-Produkte – im Sinne einer Spezifikation – für die Durchführung von Vergabeverfahren berücksichtigt werden. Die Vorschriften des Vergaberechts und des Geheimschutzes bleiben unberührt.

(5) Für die Einrichtungen der Bundesverwaltung kann das Bundesministerium des Innern im Einvernehmen mit den anderen Ressorts festlegen, dass sie verpflichtet sind, nach § 19 bereitgestellte IT-Sicherheitsprodukte beim Bundesamt abzurufen. Eigenbeschaffungen der Einrichtungen der Bundesverwaltung sind in diesem Fall nur zulässig, wenn das spezifische Anforderungsprofil den Einsatz abweichender Produkte erfordert. Dies gilt nicht für die in § 2 Nummer 21 genannten Gerichte und Verfassungsorgane sowie die Auslandsinformations- und -kommunikationstechnik gemäß § 7 Absatz 6.“

m) § 48 wird durch den folgenden § 48 ersetzt:

„§ 48

Amt des Koordinators für Informationssicherheit

(1) Die Leitung des Bundesamtes für Sicherheit in der Informationstechnik nimmt die Aufgaben der Koordinatorin oder des Koordinators der Bundesregierung für Informationssicherheit wahr. Die Fachaufsicht über das Bundesamt in Bezug auf seine Rolle als Koordinatorin oder Koordinator für Informationssicherheit liegt beim Bundesministerium für Digitales und Staatsmodernisierung.

(2) Die Koordinatorin oder der Koordinator koordiniert das operative Informationssicherheitsmanagement des Bundes. Im Benehmen mit den obersten Bundesbehörden entwickelt sie oder er Programme zur Gewährleistung der Informationssicherheit des Bundes und schreibt diese fort.

(3) Auf Basis der durch das Bundesamt erhaltenen Informationen wahrt die Koordinatorin oder der Koordinator den Überblick über den Stand der Informationssicherheit in der Bundesverwaltung. Auf dieser Grundlage beaufsichtigt sie oder er die Umsetzung der Programme zur Gewährleistung der Informationssicherheit des Bundes.

(4) Die Koordinatorin oder der Koordinator unterstützt die Ressorts bei der Umsetzung der Vorgaben nach diesem Gesetz und wirkt gemeinsam mit dem Bundesministerium für Digitales und Staatsmodernisierung im Benehmen mit dem Bundesministerium des Innern auf ein angemessenes Verhältnis zwischen dem Einsatz von Informationstechnik und Informationssicherheit hin.

(5) Zur Wahrnehmung ihrer oder seiner Aufgaben hat die Koordinatorin oder der Koordinator ein direktes halbjährliches Vortragsrecht vor den zuständigen Ausschüssen des Deutschen Bundestages zu den in den Absätzen 1 bis 3 benannten Themen.

(6) Die Koordinatorin oder der Koordinator wird bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben beteiligt, soweit sie Fragen der Informationssicherheit berühren.“

n) § 56 wird wie folgt geändert:

aa) Nach Absatz 6 werden die folgenden Absätze 7 und 8 eingefügt:

„(7) Das Bundesministerium des Innern kann durch Rechtsverordnungen, die nicht der Zustimmung des Bundesrates bedürfen, für jeweils einen der in § 2 Nummer 24 aufgeführten Sektoren im Einvernehmen mit dem in § 41 Absatz 1 für den jeweiligen Sektor genannten Bundesministerium kritische Komponenten im Sinne des § 2 Nummer 23 bestimmen. In der Rechtsverordnung kann eine Komponente als kritische Komponente bestimmt werden, wenn

1. es sich bei der Komponente um ein IKT-Produkt handelt,
2. die Komponente in kritischen Anlagen eingesetzt wird,
3. die Komponente eine kritische Funktion realisiert und
4. eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der Komponente zu einer Beeinträchtigung der Funktionsfähigkeit kritischer Anlagen oder zu anderen Beeinträchtigungen der öffentlichen Ordnung oder Sicherheit führen könnte.

(8) Die in § 41 Absatz 1 genannten Bundesministerien können dem Bundesministerium des Innern einen Vorschlag für den Erlass einer Rechtsverordnung im Sinne des Absatzes 7 vorlegen. Das Vorschlagsrecht betrifft nur den Sektor im Sinne des § 2 Nummer 24, für den das jeweilige Bundesministerium in § 41 Absatz 1 genannt wird.“

o) § 58 wird wie folgt geändert:

aa) In Absatz 4 wird die Angabe „erstmals zum 18. Januar 2025 und in der Folge alle drei Monate“ durch die Angabe „jeweils zum 18. Januar, 18. April, 18. Juli und zum 18. Oktober eines jeden Jahres“ ersetzt.

bb) In Absatz 5 wird die Angabe „erstmals“ gestrichen und wird die Angabe „2025“ durch die Angabe „2027“ ersetzt.

p) § 65 wird durch den folgenden § 65 ersetzt:

„§ 65

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer entgegen § 39 Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 56 Absatz 4 Satz 1 einen Nachweis nicht richtig oder nicht vollständig erbringt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. einer vollziehbaren Anordnung nach

   a) § 11 Absatz 6, § 16 Absatz 1 Satz 1 Nummer 1, auch in Verbindung mit Absatz 3, Nummer 2, § 17 Satz 1 oder § 39 Absatz 1 Satz 5,

   b) § 14 Absatz 2 Satz 1,

   c) den §§ 18, 40 Absatz 5 Satz 1 oder nach § 61 Absatz 3 Satz 1 oder Absatz 6 Satz 1 oder 3 oder Absatz 7 Satz 1 oder 3 oder Absatz 8, jeweils auch in Verbindung mit § 62, oder

   d) § 35 Absatz 1 Satz 1 oder § 36 Absatz 2 Satz 1

   zuwiderhandelt,

2. entgegen § 30 Absatz 1 Satz 1 eine dort genannte Maßnahme nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig ergreift,

3. entgegen § 30 Absatz 1 Satz 3 die Einhaltung der Verpflichtung nicht, nicht richtig oder nicht vollständig dokumentiert,

4. entgegen § 32 Absatz 1 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

5. entgegen § 32 Absatz 2 Satz 2 eine Abschlussmeldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt,

6. entgegen § 33 Absatz 1 oder 2 Satz 1, jeweils auch in Verbindung mit einer Rechtsverordnung nach § 56 Absatz 4 Satz 1, oder entgegen § 34 Absatz 1 eine Angabe nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

7. entgegen § 33 Absatz 2 Satz 2 nicht sicherstellt, dass er erreichbar ist,

8. entgegen § 34 Absatz 2 das Bundesamt nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,

9. entgegen § 35 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

10. entgegen § 39 Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 56 Absatz 4 Satz 1 einen Nachweis nicht oder nicht rechtzeitig erbringt,

11. entgegen § 41 Absatz 5 Satz 2 eine Mitteilung oder Angabe nicht, nicht richtig, nicht vollständig, oder nicht rechtzeitig macht,

12. entgegen § 49 Absatz 3 Satz 1 eine dort genannte Vorgabe oder ein dort genanntes Verfahren nicht vorhält,

13. entgegen § 49 Absatz 3 Satz 2 oder Absatz 4 eine dort genannte Vorgabe, ein dort genanntes Verfahren oder Daten nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig zugänglich macht,

14. entgegen § 50 Absatz 1 Satz 1 einen Zugang nicht oder nicht rechtzeitig gewährt,

15. entgegen § 52 Absatz 2 Satz 4, § 53 Absatz 1 Satz 4, § 54 Absatz 6 Satz 2 oder § 55 Absatz 4 Satz 1 ein dort genanntes Zertifikat, eine dort genannte Erklärung oder ein dort genanntes Kennzeichen verwendet,

16. entgegen § 53 Absatz 3 Satz 2 oder § 54 Absatz 2 Satz 2 tätig wird oder

17. entgegen § 61 Absatz 5 Satz 3 das Betreten eines dort genannten Raums nicht gestattet, eine dort genannte Aufzeichnung, ein dort genanntes Schriftstück oder eine dort genannte Unterlage nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt oder eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt.

(3) Ordnungswidrig handelt, wer eine in Absatz 1 bezeichnete Handlung fahrlässig begeht.

(4) Ordnungswidrig handelt, wer gegen die Verordnung (EU) 2019/881 in der Fassung vom 19. Dezember 2024 verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 55 Absatz 1 eine dort genannte Angabe nicht, nicht richtig, nicht vollständig oder nicht binnen eines Monats nach Ausstellung zugänglich macht oder

2. entgegen Artikel 56 Absatz 8 Satz 1 eine Information nicht, nicht richtig, nicht vollständig oder nicht unverzüglich nach Feststellung einer Sicherheitslücke oder Unregelmäßigkeit gibt.

(5) Die Ordnungswidrigkeit kann geahndet werden:

1. in den Fällen des Absatzes 2 Nummer 1 Buchstabe d, Nummer 2 bis 5 und 9,

   a) bei besonders wichtigen Einrichtungen nach § 28 Absatz 1 Satz 1 mit einer Geldbuße bis zu zehn Millionen Euro,

   b) bei wichtigen Einrichtungen im Sinne des § 28 Absatz 2 Satz 1 mit einer Geldbuße bis zu sieben Millionen Euro,

2. in den Fällen des Absatzes 2 Nummer 11 mit einer Geldbuße bis zu fünf Millionen Euro,

3. in den Fällen des Absatzes 2 Nummer 1 Buchstabe a mit einer Geldbuße bis zu zwei Millionen Euro,

4. in den Fällen des Absatzes 1 und des Absatzes 2 Nummer 10 mit einer Geldbuße bis zu einer Million Euro,

5. in den Fällen des Absatzes 2 Nummer 1 Buchstabe c, Nummer 6, 8, 12 bis 16 und des Absatzes 4 mit einer Geldbuße bis zu fünfhunderttausend Euro und

6. in den Fällen des Absatzes 2 Nummer 1 Buchstabe b, Nummer 7 und 17 und des Absatzes 3 mit einer Geldbuße bis zu hunderttausend Euro.

In den Fällen des Satzes 1 Nummer 3 und 4 ist § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten anzuwenden.

(6) Gegenüber einer besonders wichtigen Einrichtung im Sinne des § 28 Absatz 1 Satz 1 mit einem Gesamtumsatz von mehr als 500

Millionen Euro kann abweichend von Absatz 5 Satz 1 Nummer 1 Buchstabe a, auch in Verbindung mit § 30 Absatz 2 Satz 2 des Gesetzes über Ordnungswidrigkeiten, eine Ordnungswidrigkeit in den Fällen des Absatzes 2 Nummer 1 Buchstabe d, Nummer 2 bis 5 und 9 mit einer Geldbuße bis zu 2 Prozent des Gesamtumsatzes geahndet werden.

(7) Gegenüber einer wichtigen Einrichtung im Sinne des § 28 Absatz 2 Satz 1 mit einem Gesamtumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 5 Satz 1 Nummer 1 Buchstabe b, auch in Verbindung mit § 30 Absatz 2 Satz 2 des Gesetzes über Ordnungswidrigkeiten, eine Ordnungswidrigkeit in den Fällen des Absatzes 2 Nummer 1 Buchstabe d, Nummer 2 bis 5 und 9 mit einer Geldbuße bis zu 1,4 Prozent des Gesamtumsatzes geahndet werden.

(8) Gesamtumsatz im Sinne der Absätze 6 und 7 ist die Summe aller Umsatzerlöse, die das Unternehmen, dem die besonders wichtige Einrichtung oder die wichtige Einrichtung angehört, in dem der Behördenentscheidung vorausgegangenen Geschäftsjahr weltweit erzielt hat. Der Gesamtumsatz kann geschätzt werden.

(9) § 17 Absatz 2 des Gesetzes über Ordnungswidrigkeiten ist in den Fällen des Absatzes 5 Satz 1 Nummer 1 sowie der Absätze 6 und 7 nicht anzuwenden.

(10) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist

1. in den Fällen des Absatzes 2 Nummer 11 das Bundesministerium des Innern und
2. in den Fällen der Absätze 1, 3 und 4 sowie in den Fällen des Absatzes 2, die nicht in Nummer 1 genannt sind, das Bundesamt.

(11) Verhängen die in Artikel 55 oder 56 der Verordnung (EU) 2016/679 genannten Aufsichtsbehörden gemäß Artikel 58 Absatz 2 Buchstabe i der Verordnung (EU) 2016/679 eine Geldbuße, so darf eine weitere Geldbuße für einen Verstoß nach diesem Gesetz, der sich aus demselben Verhalten ergibt wie jener Verstoß, der Gegenstand der Geldbuße nach Artikel 58 Absatz 2 Buchstabe i der Verordnung (EU) 2016/679 war, nicht verhängt werden.“

2. In Artikel 8 Nummer 8 wird Buchstabe b durch den folgenden Buchstaben b ersetzt:

‚b) Absatz 1 wird wie folgt geändert:

aa) In der Angabe vor Nummer 1 wird die Angabe „Finanz- und Versicherungswesen“ durch die Angabe „Finanzwesen“ und die Angabe „§ 10 Absatz 1 Satz 1 des BSI-Gesetzes“ durch die Angabe „§ 56 Absatz 4 in Verbindung mit § 2 Nummer 24 des BSI-Gesetzes“ ersetzt.

bb) In Nummer 4 wird die Angabe „Derivatgeschäften;“ durch die Angabe „Derivatgeschäften.“ ersetzt.

cc) Nummer 5 wird gestrichen.‘

3. Artikel 17 wird wie folgt geändert:

a) Nummer 2 wird wie folgt geändert:

aa) Nach § 5c Absatz 6 Satz 2 werden die folgenden Sätze eingefügt:

„Die Befugnis der Bundesnetzagentur nach Satz 1 besteht bis zum Erlass einer Rechtsverordnung nach § 56 Absatz 7 des BSI-Gesetzes für den Sektor Energie fort. Eine von der Bundesnetzagentur auf der Grundlage von Satz 1 oder auf der Grundlage von § 11 Absatz 1a Satz 2 des Energiewirtschaftsgesetzes in der am … [einsetzen: Datum des Tages vor dem Inkrafttreten nach Artikel 30 dieses Gesetzes] geltenden Fassung erlassene Allgemeinverfügung ist mit dem Inkrafttreten einer Rechtsverordnung nach § 56 Absatz 7 des BSI-Gesetzes, für Energieversorgungnetze und Energieanlagen aufzuheben.“

b) Nummer 6 Buchstabe b wird durch den folgenden Buchstaben b ersetzt:

‚b) Absatz 2 wird durch die folgenden Absätze 2 bis 8 ersetzt:

„(2) Die Ordnungswidrigkeit kann geahndet werden:

1. in den Fällen des Absatzes 1 Nummer 3b bis 3e

   a) bei besonders wichtigen Einrichtungen nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes mit einer Geldbuße bis zu zehn Millionen Euro und

   b) bei wichtigen Einrichtungen nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes mit einer Geldbuße bis zu sieben Millionen Euro,

2. in den Fällen des Absatzes 1 Nummer 3i bis 3l mit einer Geldbuße bis zu fünf Millionen Euro,

3. in den Fällen des Absatzes 1 Nummer 1a, 1d, 3 Buchstabe b, Nummer 4 und 5 Buchstabe b, der Absätze 1b und 1c Nummer 2 und 6 mit einer Geldbuße bis zu einer Millionen Euro,

4. in den Fällen des Absatzes 1 Nummer 5 Buchstabe f mit einer Geldbuße bis zu dreihunderttausend Euro,

5. in den Fällen des Absatzes 1 Nummer 1, 1b, 1c, 2a, 2b, 3 Buchstabe a, Nummer 3a, 3f bis 3h, 4a bis 4c und 5 Buchstabe c und d, des Absatzes 1a Nummer 1, des Absatzes 1c Nummer 1, 3 bis 5 und 9 und der Absätze 1d und 1e mit einer Geldbuße bis zu hunderttausend Euro,

6. in den Fällen des Absatzes 1 Nummer 2 und 5 Buchstabe e mit einer Geldbuße bis zu fünfzigtausend Euro und

7. in den Fällen des Absatzes 1 Nummer 5 Buchstabe a, des Absatzes 1a Nummer 2 und des Absatzes 1c Nummer 7 und 8 mit einer Geldbuße bis zu zehntausend Euro.

(3) Gegenüber einer besonders wichtigen Einrichtung im Sinne des § 28 Absatz 1 Satz 1 des BSI-Gesetzes mit einem Gesamtumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 2 Nummer 1 Buchstabe a, auch in Verbindung mit § 30 Absatz 2 Satz 2 des Gesetzes über Ordnungswidrigkeiten, eine Ordnungswidrigkeit in den Fällen des Absatzes 1 Nummer 3b bis 3e mit einer Geldbuße bis zu 2 Prozent des Gesamtumsatzes geahndet werden.

(4) Gegenüber einer wichtigen Einrichtung im Sinne des § 28 Absatz 2 Satz 1 des BSI-Gesetzes mit einem Gesamtumsatz

von mehr als 500 Millionen Euro kann abweichend von Absatz 2 Nummer 1 Buchstabe b, auch in Verbindung mit § 30 Absatz 2 Satz 2 des Gesetzes über Ordnungswidrigkeiten, eine Ordnungswidrigkeit in den Fällen des Absatzes 1 Nummer 3b bis 3e mit einer Geldbuße bis zu 1,4 Prozent des Gesamtumsatzes geahndet werden.

(5) Gegenüber einem Transportnetzbetreiber oder einem vertikal integrierten Unternehmen mit einem Gesamtumsatz von mehr als zehn Millionen Euro kann abweichend von Absatz 2 Nummer 3, auch in Verbindung mit § 30 Absatz 2 Satz 2 des Gesetzes über Ordnungswidrigkeiten, eine Ordnungswidrigkeit in den Fällen des Absatzes 1 Nummer 3 Buchstabe b mit einer Geldbuße von bis zu 10 Prozent des Gesamtumsatzes geahndet werden.

(6) Gegenüber einem Transportnetzbetreiber oder einem vertikal integrierten Unternehmen mit einem Gesamtumsatz von mehr als 1 Million Euro kann abweichend von Absatz 2 Nummer 5, auch in Verbindung mit § 30 Absatz 2 Satz 2 des Gesetzes über Ordnungswidrigkeiten, eine Ordnungswidrigkeit in den Fällen des Absatzes 1e mit einer Geldbuße von bis zu 10 Prozent des Gesamtumsatzes abzüglich der Umlagen nach § 12 des Energiefinanzierungsgesetzes geahndet werden.

(7) Gesamtumsatz im Sinne der Absätze 3 bis 6 ist die Summe aller Umsatzerlöse, die das Unternehmen, dem die besonders wichtige Einrichtung oder die wichtige Einrichtung angehört, der Transportnetzbetreiber oder das vertikal integrierte Unternehmen in dem der Behördenentscheidung vorausgegangenen Geschäftsjahr weltweit erzielt hat. Der Gesamtumsatz kann geschätzt werden.

(8) § 17 Absatz 2 des Gesetzes über Ordnungswidrigkeiten ist in den Fällen des Absatzes 2 Nummer 1 sowie der Absätze 3 und 4 nicht anzuwenden.“ ‘

4. Artikel 25 Nummer 12 wird durch die folgende Nummer 12 ersetzt:

‚12. § 167 wird wie folgt geändert:

a) Absatz 1 Satz 1 Nummer 2 wird wie folgt geändert:

aa) Die Angabe „§ 2 Absatz 13 Satz 1 Nummer 3 Buchstabe b des BSI-Gesetzes“ wird durch die Angabe „§ 2 Nummer 23 Buchstabe c Doppelbuchstabe bb des BSI-Gesetzes“ ersetzt.

bb) Die Angabe „§ 2 Absatz 13 des BSI-Gesetzes“ wird durch die Angabe „§ 2 Nummer 23 des BSI-Gesetzes“ ersetzt.

b) Nach Absatz 1 wird der folgende Absatz 2 eingefügt:

„(2) Die Befugnis der Bundesnetzagentur nach Absatz 1 Nummer 2 besteht bis zum Erlass einer Rechtsverordnung nach § 56 Absatz 7 des BSI-Gesetzes für den Sektor Informationstechnik und Telekommunikation im Sinne des § 2 Nummer 24 fort. Eine von der Bundesnetzagentur auf der Grundlage von Absatz 1 Satz 1 Nummer 2 erlassene Allgemeinverfügung ist mit dem Inkrafttreten einer Rechtsverordnung nach § 56 Absatz 7 des BSI-

Gesetzes für den Sektor Informationstechnik und Telekommunikation aufzuheben.“

c) Der bisherige Absatz 2 wird zu Absatz 3.‘

Berlin, den 12. November 2025

Der Innenausschuss

Josef Oster
Amtierender Vorsitzender

Marc Henrichmann
Berichterstatter

Steffen Janich
Berichterstatter

Johannes Schätzl
Berichterstatter

Dr. Konstantin von Notz
Berichterstatter

Jan Köstering
Berichterstatter

Bericht der Abgeordneten Marc Henrichmann, Steffen Janich, Johannes Schätzl, Dr. Konstantin von Notz und Jan Köstering

I. Überweisung

Der Gesetzentwurf auf **Drucksache 21/1501** wurde in der 21. Sitzung des Deutschen Bundestages am 11. September 2025 an den Innenausschuss federführend sowie an den Haushaltsausschuss und den Ausschuss für Digitales und Staatsmodernisierung zur Mitberatung überwiesen. Die Unterrichtung durch die Bundesregierung zur Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung auf **Drucksache 21/2072** wurde am 9. Oktober 2025 gemäß § 80 Absatz 3 der Geschäftsordnung auf Nummer 1.11 der Drucksache 21/2146 an die beteiligten Ausschüsse überwiesen.

II. Stellungnahmen der mitberatenden Ausschüsse

Der **Haushaltsausschuss** hat in seiner 23. Sitzung am 12. November 2025 mit den Stimmen der Fraktionen der CDU/CSU, AfD und SPD gegen die Stimmen der Fraktion BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion Die Linke die Annahme des Gesetzentwurfs auf Drucksachen 21/1501, 21/2072 in geänderter Fassung empfohlen. Seine Stellungnahme gemäß § 96 GO-BT wird er gesondert abgeben.

Der **Ausschuss für Digitales und Staatsmodernisierung** hat in seiner 11. Sitzung am 12. November 2025 mit den Stimmen der Fraktionen der CDU/CSU, AfD und SPD gegen die Stimme der Fraktion BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion Die Linke die Annahme des Gesetzentwurfs auf Drucksachen 21/1501, 21/2072 in geänderter Fassung empfohlen.

III. Beratungsverlauf und Beratungsergebnisse im federführenden Ausschuss

Der Innenausschuss hat in seiner 9. Sitzung am 8. Oktober 2025 einvernehmlich beschlossen, zum Gesetzentwurf auf Drucksachen 21/1501, 21/2072 eine öffentliche Anhörung durchzuführen. Die öffentliche Anhörung, an der sich sieben Sachverständige beteiligt haben, hat der Innenausschuss in seiner 11. Sitzung am 13. Oktober 2025 durchgeführt. Hinsichtlich des Ergebnisses der Anhörung wird auf das Protokoll der 11. Sitzung (Protokoll 21/11) verwiesen.

Der **Innenausschuss** hat den Gesetzentwurf auf Drucksachen 21/1501, 21/2072 in seiner 16. Sitzung am 12. November 2025 abschließend beraten und empfiehlt die Annahme des Gesetzentwurfs in der aus der Beschlussempfehlung ersichtlichen Fassung mit den Stimmen der Fraktionen der CDU/CSU, AfD und SPD gegen die Stimmen der Fraktion BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion Die Linke.

Die Änderungen entsprechen dem Änderungsantrag der Fraktionen der CDU/CSU und SPD auf Ausschussdrucksache 21(4)096, der zuvor mit den Stimmen der Fraktionen der CDU/CSU, AfD und SPD bei Stimmenthaltung der Fraktionen BÜNDNIS 90/DIE GRÜNEN und Die Linke angenommen wurde.

IV. Begründung

1. Begründung zum Änderungsantrag

Zur Begründung allgemein wird auf Drucksache 21/1501 verwiesen. Die vom Innenausschuss auf Grundlage des Änderungsantrags der Fraktionen der CDU/CSU und SPD auf Ausschussdrucksache 21(4)096 vorgenommenen Änderungen begründen sich wie folgt:

Zu Artikel 1

Zu § 1 Satz 3

Redaktionelle Anpassung zur Klarstellung, dass alle Aufgaben des Bundesamtes auf der Grundlage wissenschaftlich-technischer Erkenntnisse durchgeführt werden. Fach- und Rechtsaufsicht des zuständigen Ministeriums werden nicht berührt.

Zu § 2

Zu Nummer 23

Kritische Komponenten sind IKT-Produkte im Sinne von § 2 Nummer 15, die aufgrund von § 56 Absatz 7 und 8 in einer Rechtsverordnung als kritische Komponenten bestimmt werden. Die Neuformulierung vereinheitlicht und vereinfacht das Verfahren zur Bestimmung kritischer Komponenten und erleichtert damit die Anwendung der Regelung in der Praxis.

Zu Nummer 27

Streichung einer überflüssigen Klammer, redaktionelle Anpassung.

Zu § 3

Zu Nummer 18

Die Unterstützungsleistung des Bundesamtes erfolgt innerhalb der Grenzen und entsprechend der Anforderungen der Amtshilfe (kodifizierte Amtshilfe).

Gegenstandslos ist der folgende letzte Satz der Begründung des Regierungsentwurfes auf Bundestagdrucksache 21/1501, S. 135: „Die Möglichkeit der Leistung von Amtshilfe des Bundesamtes gegenüber den Ländern ist von der Änderung des bisherigen § 3 Absatz 1 Satz 2 Nummer 13 unberührt.“

Zu Nummer 20

Die Unterstützungsleistung des Bundesamtes erfolgt innerhalb der Grenzen und entsprechend der Anforderungen der Amtshilfe (kodifizierte Amtshilfe).

Gegenstandslos ist der folgende letzte Satz der Begründung des Regierungsentwurfes auf Bundestagdrucksache 21/1501, S. 136: „Die Möglichkeit der Leistung von Amtshilfe des Bundesamtes gegenüber den Ländern ist von der Änderung des bisherigen § 3 Absatz 1 Satz 2 Nummer 14 unberührt.“

Zu § 5

Zu Absatz 3

§ 5 Absatz 3 Satz 1 normiert die Pflicht des Bundesamtes, ihm bekannt gewordene Schwachstellen unverzüglich an den jeweiligen Verantwortlichen zu melden, sodass dieser auf die Behebung der Schwachstelle hinwirken kann. Über den Verweis auf § 3 Absatz 1 Satz 1 („Das Bundesamt fördert die Sicherheit in der Informationstechnik.“) wird klargestellt, dass die Weitergabe ausschließlich der schnellstmöglichen Schließung der Schwachstelle dienen darf. Sofern im Einzelfall damit zu rechnen ist, dass die Information des Herstellers der Sicherheit in der Informationstechnik nicht dienlich wäre, kann das BSI daher stattdessen von den anderen Instrumenten des § 5 – etwa einer öffentlichen Warnung– Gebrauch machen.

Zu Absatz 6

§ 5 Absatz 6 schreibt die bisherige Verwaltungspraxis des Bundesamts, den Prozess der Schwachstellenmeldung in einer sogenannten „CVD-Policy“ öffentlich zu dokumentieren, gesetzlich fest.

Zu § 15

Zu Absatz 1

Schwachstellen an den Schnittstellen zu öffentlichen Telekommunikationsnetzen können eine Bedrohung für die Informationssicherheit insbesondere von Einrichtungen des Bundes, sowie von besonders wichtigen und wichtigen Einrichtungen darstellen. Zur Erkennung dieser Bedrohungen ist die bisherige Befugnis für Abfragen nicht ausreichend. Die Neuregelung in Absatz 1 ermöglicht es dem Bundesamt, nach diesen Schwachstellen an den

Schnittstellen zu öffentlichen Telekommunikationsnetzen zu suchen. Der § 15 Absatz 1 Satz 2 führt hinsichtlich Löschverpflichtung den bislang geltenden § 7b Absatz 1 Satz 4 fort.

Zu Absatz 2

Es ist bereits logisch vorgegeben, dass das Bundesamt nur bereits bekannte Schwachstellen abfragen kann. In Absatz 2 Satz 1 ist das Wort „bekannte“ irreführend und daher zu streichen. Erkennt das Bundesamt im Rahmen der Abfrage ein Sicherheitsrisiko bei einer Einrichtung des Bundes bzw. einer besonders wichtigen oder wichtigen Einrichtung, hat es die jeweilig für das IT-System Verantwortlichen zu informieren. Erkennt das Bundesamt bei anderen Stellen Sicherheitsrisiken soll das Bundesamt auch diese Stellen im Rahmen der zur Verfügung stehenden Befugnisse als Allgemeine Meldestelle für die Sicherheit in der Informationstechnik nach § 5, insbesondere Absatz 3 und 4, darüber informieren.

Zu § 16

Zu Absatz 1

Mit den Änderungen in Absatz 1 Satz 1 wird dem Bundesamt ermöglicht, gegenüber bisher von der Regelung nicht erfassten Anbietern (Telekommunikationsdienste mit 100 000 oder weniger Kunden) öffentlich zugänglicher Telekommunikationsdienste Anordnungen zur Abwehr erheblicher Gefahren der in Absatz 3 genannten Schutzgüter auszusprechen. Die Erweiterung ist notwendig, da andernfalls eine Vielzahl von Nutzern, denen über kleinere (etwa regionale) Anbieter Telekommunikationsdienstleistungen zur Verfügung gestellt werden, nicht entsprechend geschützt werden können. Zugleich wird wie bisher sichergestellt, dass die jeweiligen Anbieter technisch zu den angeordneten Maßnahmen in der Lage sein und ihnen diese wirtschaftlich zumutbar sein müssen. Dabei ist zu berücksichtigen, dass sich der Stand der Technik seit Einführung der ursprünglichen Regelung (s. BT-Drs. 19/26106) fortentwickelt hat und zumindest auch Anbieter, die verpflichtenden Regelungen für den Betrieb von DNS-Diensten im jeweiligen Sicherheitskatalog nach § 167 TKG unterliegen, diese Voraussetzungen erfüllen.

Mit der Änderung in Absatz 1 Satz 2 wird vorgegeben, dass das Bundesamt sich mit der Bundesnetzagentur vor Anordnung von Maßnahmen ins Benehmen setzt. Das Bundesamt tauscht sich regelmäßig mit der Bundesnetzagentur auf verschiedenen Ebenen zur IT-Sicherheit von Telekommunikationsdiensten aus. Auch hat die bisherige Umsetzung der Regelung in Absatz 1 gezeigt, dass zwischen BNetzA und BSI ein gemeinsames Verständnis über dessen Anwendung und die zu begegnende Gefahr besteht. Auf das bisherige Erfordernis des Einvernehmens in Satz 2 kann daher verzichtet werden.

Zu Absatz 2

Mit dem neuen Absatz 2 wird es dem Bundesamt ermöglicht, selbst Bereinigungsbefehle an von einem konkret benannten Schadprogramm betroffenes informationstechnisches System auszusenden. Damit wird die bestehende Regelung in § 7c Absatz 1 Nummer 2 BSI-Gesetz (alt) die dem Bundesamt bereits eine entsprechende Anordnungsbefugnis gegenüber Anbietern öffentlicher Telekommunikationsdienstleistungen einräumt, durch die Möglichkeit zur Selbstvornahme unter gleichen Voraussetzungen ergänzt. Bereits nach der bestehenden Regelung in § 7c Absatz 1 Nummer 2 BSI-Gesetz (alt) obliegt es regelmäßig dem BSI, die technischen Möglichkeiten zur Bereinigung zu analysieren und technische Befehle dem Diensteanbieter zuzuliefern (vgl. BT-Drs. 19/26106, 74). Mit der Neuregelung wird auch sichergestellt, dass entsprechende Maßnahmen auch dann durchgeführt werden können, wenn diese einem Diensteanbieter technisch nicht möglich ist, weil als vorausgegangene Maßnahmen nach Absatz 1 Nummer 1 eine Umleitung des Datenverkehrs auf informationstechnische Systeme des Bundesamts nach Absatz 4 erfolgt ist und deshalb nur das Bundesamt Bereinigungsbefehle an das jeweils betroffen System aussenden kann.

Zu § 28 Absatz 5 Satz 4

Durch die Änderung von „vernachlässigbare Tätigkeit“ in „Nebentätigkeit“ werden unnötige Doppelzuständigkeiten von Bundesamt und BNetzA vermieden, wie sie zum Beispiel im Bereich der thermischen Abfallbeseitigung (Nebentätigkeit: Stromerzeugung) entstehen könnten. Der Begriff der Nebentätigkeit ist dabei weiter zu verstehen als der der „vernachlässigbaren Tätigkeit“ des § 28 Absatz 3.

Mit dieser Änderung wird einem Änderungsvorschlag des Bundesrats Rechnung getragen.

Zu § 29 Absatz 2 Satz 2

Der Anwendungsbereich wird auf die gesamte Bundesverwaltung erstreckt. Die Geschäftsbereichsbehörden werden umfasst.

Absatz 2 dient der grundsätzlichen Erweiterung des Anwendungsbereichs dieses Gesetzes auf Einrichtungen der Bundesverwaltung, die selbst weder besonders wichtige Einrichtungen noch wichtige Einrichtungen sind, sowie zur Festlegung von Abweichungen für Einrichtungen der Bundesverwaltung von den Regelungen für (besonders) wichtige Einrichtungen.

Für Einrichtungen der Bundesverwaltung finden die Regelungen für besonders wichtige Einrichtungen Anwendung, soweit keine Abweichungen für Einrichtungen der Bundesverwaltung geregelt sind. D.h. folgende Regelungen für besonders wichtige Einrichtungen finden Anwendung: §§ 6, 12, 13 Absatz 1 Nummer 1 Buchstabe e, §§ 30, 32, 33, 35, 36, 37, 56 und 59, wobei § 30 durch die Einhaltung von § 44 Absatz 1 erfüllt wird. Folgende Regelungen für besonders wichtige oder wichtige Einrichtungen finden keine Anwendung: §§ 38, 40 Absatz 3, § 61 und 65, da stattdessen folgende abweichende Regelungen Anwendung finden: §§ 4, 7, 10, 43 Absatz 1, 2, 4 und 5.

Zu § 33

Zu Absatz 2

Absatz 2 wird um die Verpflichtung der Betreiber kritischer Anlagen ergänzt, im Zuge der Registrierung auch Angaben zu den bei ihnen zum Einsatz kommenden Typen von kritischen Komponenten an das Bundesamt zu übermitteln. Der Begriff „Typen von kritischen Komponenten“ meint ein bestimmtes Produkt unter Angabe der entsprechenden Versionsnummer. Dies dient u.a. als Ausgleich für den Wegfall der bisherigen Anzeigepflicht nach § 9b BSI-Gesetz (alt). Da die entsprechende Übermittlung dieser Informationen im Rahmen der nach § 33 ohnehin bestehenden Registrierungspflicht erfolgt, ist der zusätzliche Aufwand für die Betreiber kritischer Anlagen gering.

Zu Absatz 5

Um die beim Bundesamt vorliegenden Informationen über die bei den Betreibern kritischer Anlagen zum Einsatz kommenden Typen von kritischen Komponenten einerseits aktuell zu halten, andererseits aber auch den hierdurch entstehenden Mehraufwand möglichst gering zu halten, sieht Absatz 5 vor, dass Änderungen in diesem Bereich von den Betreibern einmal jährlich an das Bundesamt zu übermitteln sind.

Zu § 41

Die Neuregelung beruht auf Erkenntnissen, die im Rahmen der Verwaltungspraxis mit Prüfungen nach § 9b BSI-Gesetz (alt) gewonnen wurden und dient nicht der Umsetzung der NIS-2-Richtlinie; § 9b BSI-Gesetz (alt) war bereits Gegenstand des IT-Sicherheitsgesetzes 2.0.

Um die Sicherheit und Souveränität der kritischen digitalen Infrastruktur weiter zu stärken, entwickelt das Bundesministerium für Digitales und Staatsmodernisierung ein Gesamtkonzept mit Maßnahmen zur Verbesserung der Wettbewerbsfähigkeit und Resilienz der gesamten Wertschöpfungskette.

Die bisherige Anzeigepflicht nach § 9b Absatz 2 BSI-Gesetz (alt) entfällt ersatzlos. Damit entfällt auch die Regelung, wonach vor Ablauf einer Frist von zwei Monaten nach einer Anzeige der Einsatz der betreffenden kritischen Komponenten nicht gestattet war. Auch die bislang in § 9b Absatz 3 BSI-Gesetz vorgesehene Garantieerklärung des Herstellers über seine Vertrauenswürdigkeit gegenüber dem Betreiber entfällt ersatzlos. Dies bedeutet einerseits eine erhebliche Reduzierung der Aufwände für die betroffenen Betreiber kritischer Anlagen.

Andererseits kann das Bundesministerium des Innern künftig unabhängig von einer Anzeige durch Betreiber kritischer Anlagen prüfen, ob der Einsatz von kritischen Komponenten, also IKT-Produkten, die die Voraussetzungen von § 2 Nummer 23 in Verbindung mit § 56 Absatz 7 und 8 BSI-Gesetz erfüllen, die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Das Bundesministerium des Innern kann damit flexibel auf ihm vorliegende Erkenntnisse reagieren. Mit Blick auf die Frage, ob das Bundesministerium des Innern ein Prüfverfahren nach § 41 Absatz 1 einleitet, werden Hinweise und Vorschläge der dort aufgeführten Bundesministerien berücksichtigt.

Entscheidungen des Bundesministeriums des Innern nach Absatz 1 und 2 erfolgen im Benehmen mit dem für den jeweiligen Sektor in § 41 Absatz 1 BSIG-Gesetz genannten Bundesministerium. Für Entscheidungen nach Absatz

2 gilt § 41 Absatz 1 BSI-Gesetz insoweit entsprechend. Das Benehmen dient u.a. dazu, die Fachkompetenz und die Perspektive der betreffenden Bundesministerien mit in das Verwaltungsverfahren und den Entscheidungsprozess einzubeziehen. Die Zusammenarbeit der Bundesministerien ist wegen der Tragweite möglicher Untersagungen und Anordnungen des Bundesministeriums des Innern besonders wichtig. Um eine mögliche Entscheidung im Benehmen mit den im Einzelfall betroffenen Ressorts zu unterstützen und vorzubereiten, ist ein fortlaufender und regelmäßiger Austausch geboten. Diese Zusammenarbeit kann insoweit z.B. im Rahmen eines fortlaufenden und regelmäßigen „interministeriellen Jour Fixes“ erfolgen.

Wie in § 9b BSI-Gesetz (alt) ist die Untersagungs- und Anordnungsbefugnis hinsichtlich kritischer Komponenten, nunmehr im Sinne von § 2 Nummer 23 in Verbindung mit § 56 Absatz 7 und Absatz 8, beschränkt.

Zu Absatz 1

Gemäß § 41 Absatz 1 kann das Bundesministerium des Innern gegenüber dem Betreiber kritischer Anlagen den Einsatz von kritischen Komponenten eines Herstellers im Benehmen mit den für den jeweiligen Sektor genannten Bundesministerien sowie dem Auswärtigen Amt untersagen oder Anordnungen erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Untersagung ist das Verbot des weiteren Einsatzes der betreffenden kritischen Komponente. Das Verbot kann auch so gestaltet werden, dass es erst nach Ablauf einer bestimmen Umsetzungsfrist gilt. Unter Anordnungen sind alle weiteren möglichen Maßnahmen zur Gewährleistung der öffentlichen Ordnung oder Sicherheit zu verstehen, z.B. kann eine Diversifizierung verschiedener Hersteller durch Vorgabe prozentualer Anteile vorgegeben werden, der Einsatz nur in bestimmten Bereichen zulässig bleiben oder ähnliches.

Zu Absatz 2

Absatz 2 erweitert die Untersagungs- und Anordnungsbefugnis des Bundesministeriums des Innern. Wurde gemäß Absatz 1 gegenüber dem Betreiber kritischer Anlagen eine Untersagung oder Anordnung ausgesprochen, kann das Bundesministerium des Innern gegenüber diesem Betreiber kritischer Anlagen auch den zukünftigen Einsatz weiterer kritischer Komponenten desselben Herstellers und desselben Komponententyps untersagen (Satz 1 Nummer 1) bzw. gegenüber allen Betreibern kritischer Anlagen den Einsatz der gleichen kritischen Komponente sowie von kritischen Komponenten desselben Komponententyps untersagen oder Anordnungen erlassen (Satz 1 Nummer 2). Auch bei Absatz 2 kann ein Verbot so gestaltet werden, dass es erst nach Ablauf einer bestimmen Umsetzungsfrist gilt.

Da von einer Entscheidung nach Satz 1 Nummer 2 eine Vielzahl von Betreibern kritischer Anlagen betroffen sein kann, ist es praxisgerecht, dass die entsprechende Entscheidung als Allgemeinverfügung ergeht und im Bundesanzeiger bekannt gegeben werden kann.

Zu Absatz 4

Einige Aspekte, die im Rahmen der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit berücksichtigt werden können, werden in Absatz 4 konkretisiert und bieten den betroffenen Betreibern dadurch eine bessere Orientierung. Das ist für die Betreiber zum Beispiel im Rahmen von Vergabeentscheidungen von Bedeutung und erhöht auch allgemein die Rechts- und Planungssicherheit der Betreiber. Für Prüfung des Tatbestandsmerkmals der voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit kann gemäß Nummer 3 auch berücksichtigt werden, ob der Hersteller der kritischen Komponente aus sonstigen Gründen nicht vertrauenswürdig ist. Anhaltspunkte hierfür liefern u.a. die in Nummer 1 und 2 genannten Aspekte.

Neben einer Kontrolle oder Zusammenarbeit im Sinne von Nummer 1 und einer Beteiligung an Aktivitäten nach Nummer 2 kann bei der Prüfung nach Nummer 3 insbesondere berücksichtigt werden, ob hinreichende Anhaltspunkte dafür bestehen, dass der Hersteller unmittelbar oder mittelbar an Aktivitäten beteiligt war oder ist, die geeignet waren oder sind, nachteilige Auswirkungen auf kritische Anlagen oder Betreiber kritischer Anlagen zu haben. Solche Aktivitäten können beispielsweise dann vorliegen, wenn der Hersteller Schwachstellen oder Manipulationen nicht unverzüglich nachdem er davon Kenntnis erlangt hat, beseitigt und dem Betreiber der kritischen Anlage gemeldet hat oder Hersteller versucht hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Anlage einzuwirken.

Der Begriff „insbesondere“ verdeutlicht, dass die in Absatz 4 genannten Aspekte nicht abschließend aufgeführt werden.

Zu Absatz 5

Die Betreiber kritischer Anlagen sind gemäß Absatz 5 zur Mitwirkung bei der Ermittlung des Sachverhalts verpflichtet. Dafür sind dem Bundesministerium des Innern alle für das Verfahren erheblichen Tatsachen vollständig und wahrheitsgemäß offenzulegen und die den Betreibern kritischer Anlagen bekannten Beweismittel anzugeben.

§ 9b BSI-Gesetz (alt) sah keine Mitwirkungspflichten der Betreiber an den Verfahren vor. Dies hat zu Schwierigkeiten in der Prüfpraxis geführt, da es für die Prüfungen insbesondere auf solche Informationen ankommt, die in der Regel nur oder vor allem bei den Betreibern vorliegen. Absatz 5 sieht daher nunmehr eine umfangreiche Pflicht der Betreiber zur Übermittlung von Auskünften und Dokumenten vor. Die Zuwiderhandlung stellt eine Ordnungswidrigkeit dar, für die § 65 ein Bußgeld vorsieht.

Zu § 43 Absatz 1 Satz 2

Es wurde eine redaktionelle Korrektur vorgenommen.

Zu § 44

Es werden Folgeänderungen aufgrund der Erstreckung des Anwendungsbereiches dieses Gesetzes auf die gesamte Bundesverwaltung vorgenommen. Der bisherige Absatz 2 wird gestrichen und es werden inhaltliche Ergänzungen in den übrigen Absätzen vorgenommen.

Zu Absatz 1

Absatz 1 knüpft an den bisherigen § 8 Absatz 1 BSIG (alt) an und verankert neben den dort bereits geregelten Mindeststandards gleichrangig für die in § 29 etablierte Kategorie der Einrichtungen der Bundesverwaltung auch den IT-Grundschutz, der bereits bisher durch Kabinettsbeschluss zum Umsetzungsplan Bund verpflichtend umzusetzen ist. Der IT-Grundschutz besteht derzeit aus den BSI-Standards 200-1, 200-2, 200-3 und dem IT-Grundschutzkompendium. Die entwicklungsoffene Formulierung im Tatbestand ohne Nummerierung schließt deren Nachfolgestandards sowie eine darüberhinausgehende Fortentwicklung der Bestandteile des IT-Grundschutzes mit ein. Maßgebend für die einzuhaltenden Mindestanforderungen sind die jeweils geltenden Fassungen der Bestandteile des IT-Grundschutzes und der Mindeststandards, die auf der BSI-Internetseite (aktuelle URLs: www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html und www.bsi.bund.de/DE/Themen/Oeffentliche-Verwal-tung/Mindeststandards/Mindeststandards_node.html) veröffentlicht werden und dauerhaft zugänglich sind. Die Begrifflichkeit der „Mindestanforderungen“ wurde entsprechend aus dem Umsetzungsplan Bund übernommen. Über diese Mindestanforderungen hinaus kann jede Einrichtung individuell je nach Risikoeinschätzung weitere Informationssicherheitsmaßnahmen umsetzen. Um die Nachweisfrist von fünf Jahren ab Inkrafttreten (§ 43 Absatz 1 Satz 2) bei weiterhin knappen finanziellen und personellen Ressourcen einhalten zu können, muss sichergestellt werden, dass der IT-Grundschutz so effizient und unbürokratisch wie möglich ausgestaltet ist. Das Bundesamt wird den IT-Grundschutz daher modernisieren, mit der Maßgabe, den Umfang und die bei der Umsetzung entstehenden Dokumentationspflichten auf das notwendige Mindestmaß zu reduzieren, eine Priorisierung der Anforderungen vorzunehmen und die Anwendung von Automatisierungstools weitestgehend zu ermöglichen. Die im bisherigen § 8 Absatz 1 Satz 3 BSIG (alt) vorgesehene Möglichkeit zur Abweichung wird abgelöst durch die Kompetenz der Ressort-Informationssicherheitsbeauftragten, Ausnahmebescheide gemäß § 46 Absatz 5 zu erlassen.

Zu Absatz 2

Unter Berücksichtigung der Erwägungsgründe der NIS-2-Richtlinie zu den Anforderungen an ein Risikomanagement, insbesondere Erwägungsgründe 78 bis 82, sowie der Tatsache, dass eine Institution mit einem ISO 27001-Zertifikat auf der Basis des IT-Grundschutzes belegen kann, dass die umgesetzten Maßnahmen zur Informationssicherheit anerkannten internationalen Standards entsprechen, wird festgestellt, dass der IT-Grundschutz in Kombination mit den vom Bundesamt bereitgestellten Mindeststandards die Anforderungen an das Risikomanagement nach § 30 erfüllt und folglich auch bei Vorliegen voneinander abweichender technischer Termini materiell das dort vorgegebene Schutzniveau erreicht wird. Soweit die Europäische Kommission Durchführungsrechtsakte hierzu erlässt, genießen diese bis zu deren Integration in den IT-Grundschutz oder die Mindeststandards Vorrang.

Die bestehenden Vorgaben des Bundesamtes entfalten dann nur noch konkretisierende Wirkung, soweit die Durchführungsrechtsakte Auslegungsspielräume lassen.

Zu Absatz 3

Die Beratung durch das Bundesamt wird ergänzt um die Erstellung von Hilfsmitteln gemäß § 3 Absatz 1 Nummer 17 und die Unterstützung der Bereitstellung entsprechender Lösungen durch die IT-Dienstleister des Bundes. Bei Ergänzungen der genannten Vorgaben nimmt das Bundesamt im Rahmen des Konsultationsverfahrens eine grobe Aufwandsschätzung vor.

Zu Absatz 4

Die Vorschrift führt den bisherigen § 8 Absatz 2 BSIG (alt) fort, ergänzt um die Bereitstellung von Referenzarchitekturen.

Zu Absatz 5

Die Vorschrift führt Teile des bisherigen § 8 Absatz 3 BSIG (alt) fort. Hier enthalten ist die Befugnis, Nutzungsvorgaben für die Einrichtungen der Bundesverwaltung zu machen. Die allgemeine Befugnis des Bundesamts zur Bereitstellung von IT-Sicherheitsprodukten verbleibt mit § 19 in Teil 2. Die Zuständigkeit für die Nutzungsvorgaben wird aus sachlichen Gründen auf das Bundesministerium des Innern im Einvernehmen mit den anderen Ressorts (z.B. durch Mehrheitsbeschluss in einem geeigneten Gremium) verlagert und die Begrifflichkeiten werden vereinheitlichend erweitert zu „Einrichtungen der Bundesverwaltung“. Die Erweiterung erfolgt vor dem Hintergrund, dass eine Abrufverpflichtung über das Bundesamt nur dann erfolgen kann, wenn sachliche Gründe es erfordern, sodass im Ergebnis das Schutzgut der Sicherheit in der Informationstechnik des Bundes schwerer wiegt als Autonomie der Einrichtungen der Bundesverwaltung. Vergaberechtliche Aspekte bleiben unberührt und sind in die Entscheidungsfindung einzubeziehen. Auf Grundlage des Kabinettbeschlusses zur IT-Konsolidierung können IT-Sicherheitsprodukte auch durch andere Einrichtungen der Bundesverwaltung bereitgestellt werden.

Zu § 48

Die neue Vorschrift regelt die Einrichtung einer Koordinatorin oder eines Koordinators der Bundesregierung für Informationssicherheit (so genannter „Chief Information Security Officer“ der Bundesregierung, kurz „CISO Bund“).

Zu Absatz 1

Absatz 1 regelt die Wahrnehmung der Rolle des CISO Bund durch die Leitung des Bundesamtes sowie die diesbezügliche Fachaufsicht.

Zu den Absätzen 2 und 3

Absätze 2 und 3 dienen der Festlegung der Aufgaben und Befugnisse des CISO Bund. Der CISO greift auf die Durchsetzungsbefugnisse des Bundesamtes zurück, insbesondere das Inkraftsetzen von Vorgaben für die Bundesverwaltung gemäß §§ 30 und 40, die Überwachung von Risiken in der Informationssicherheit des Bundes mittels Kontrollen nach § 7 und zur Abwendung oder Behebung von Sicherheitsvorfällen nach § 10. Deren operativ unabhängige Wahrnehmung wird dadurch gewährleistet, dass dafür kein Einvernehmen mit den beaufsichtigten Einrichtungen der Bundesverwaltung herzustellen ist. Wie in § 1 geregelt, führen das Bundesamt und damit auch dessen Leitung in der Rolle des CISO Bund die Aufgaben auf Grundlage wissenschaftlich-technischer Erkenntnisse durch.

Zu Absatz 4

Absatz 4 legt die Pflicht des CISO Bund zur Unterstützung der Ressorts unter Berücksichtigung eines angemessenen Verhältnisses zwischen dem Einsatz von Informationstechnik und Informationssicherheit fest. Die Unterstützung durch die Ressorts erfolgt in einem angemessenen Umfang, u.a. aus der Bereitstellung von Hilfsmitteln, bewährten Methoden und Vorgehensweisen („Best Practice“) sowie Erfahrungsaustausch und -dokumentation zur Nachnutzung. Zudem ist die Einrichtung eines „Kompetenzzentrums operative Sicherheitsberatung des Bundes“ (KoSi Bund) geplant. Diese Unterstützungspflicht wird gemeinsam mit dem Bundesministerium für Digitales und Staatsmodernisierung und im Benehmen mit dem Bundesministerium des Innern umgesetzt, um einen fachlichen Austausch zu den betroffenen Themen der Informationstechnik und Informationssicherheit sicherzustellen.

Zu Absatz 5

Absatz 5 definiert ein halbjährliches Vortragsrecht vor den zuständigen Ausschüssen des Deutschen Bundestages.

Zu Absatz 6

Absatz 6 sieht Beteiligungsrechte für den CISO Bund zur effektiven Wahrnehmung der Aufgaben vor.

Zu § 56

Zu Absatz 7

Die Rechtsverordnungen zur Bestimmung, welche Komponenten kritische Komponenten im Sinne des § 2 Nummer 23 sind und somit der Prüfung nach § 41 Absatz 1 unterfallen, erlässt das Bundesministerium des Innern gemäß Satz 1 im jeweiligen Einvernehmen mit dem für den Sektor in § 41 Absatz 1 genannten Bundesministerium. Dadurch wird gewährleistet, dass die Expertise des für den jeweiligen Sektor zuständigen Bundesministeriums bei der Bestimmung von kritischen Komponenten angemessen berücksichtigt wird.

Ein IKT-Produkt kann gemäß Satz 2 als kritische Komponente im Sinne von § 2 Nummer 23 bestimmt werden, wenn die Komponente in kritischen Anlagen im Sinne von § 2 Nummer 22 eingesetzt wird, sie eine kritische Funktion realisiert und eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der Komponente zu einer Beeinträchtigung der Funktionsfähigkeit kritischer Anlagen oder zu anderen Beeinträchtigungen der öffentlichen Ordnung oder Sicherheit führen könnte.

Zu Absatz 8

Hinsichtlich der Rechtsverordnung, in der kritische Komponenten bestimmt werden, kommt den Einvernehmens-Ministerien im Sinne von § 56 Absatz 7 in Verbindung mit § 41 Absatz 1 ein Vorschlagsrecht zu.

Zu § 58

Zu Absatz 4

Es wird hier der Einreichungsturnus entsprechend der Anforderungen der NIS-2 Richtlinie deutlicher dargestellt.

Gegenstandslos ist zudem der folgende letzte Satz der Begründung des Regierungsentwurfes auf Bundestagdrucksache 21/1501, S. 169: „Die Daten für das Kalenderjahr 2024, die bislang nicht aufgrund des bisherigen § 11 Absatz 6 übermittelt wurden, sollen als Teil der erstmaligen Übermittlung im von der NIS-2-Richtlinie vorgegebenen Dreimonatszeitraum übermittelt werden.“

Zu Absatz 5

Es wird der Einreichungsturnus entsprechend der Anforderungen der NIS-2 Richtlinie deutlicher dargestellt. Eine erste Übermittlung nach Artikel 3 Absatz 5 der NIS-2-Richtlinie ist zum 17. April 2025 erfolgt; der Turnus sieht alle zwei Jahre vor.

Zu § 65

Zu Absatz 2

Mit der Ergänzung von Nummer 11 wird das Unterlassen der in § 41 Absatz 5 vorgesehenen Mitwirkung des Betreibers einer kritischen Infrastruktur bei der Ermittlung des Sachverhaltes bußgeldbewehrt. Damit wird der Bedeutung der Mitwirkung des Betreibers für die Sachverhaltsaufklärung bei der Anwendung von § 41 Rechnung getragen.

Zu Absatz 5

Angesichts der Signifikanz eines Verstoßes ist die Ahndung mit der Maximalhöhe von 10 Millionen Euro angesetzt.

Zu den Absätzen 6, 7, 8 und 9

Es wurden redaktionelle Versehen korrigiert.

Zu Artikel 8 Nummer 8 Buchstabe b

Es wird in Artikel 8 Nummer 8 Buchstabe b die Nummer 5 des § 7 Absatz 1 BSI-KritisVO gestrichen, um eine Trennung des Sektors Finanzwesen vom Sektor Sozialversicherung sowie Grundsicherung für Arbeitssuchende zu erreichen.

Zu Artikel 17

Es wurden redaktionelle Versehen korrigiert.

Zu § 5c Absatz 12 (ENWG n.F. aus aktuellem Entwurf NIS-2-Umsetzungsgesetz-IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz)

Die Änderungen im EnWG sind Folgeänderungen aufgrund der veränderten Regelungssystematik im BSI-Gesetz.

Zu Artikel 25

Zu § 167 (Katalog von Sicherheitsanforderungen)

Die Änderungen im TKG sind Folgeänderungen aufgrund der veränderten Regelungssystematik im BSI-Gesetz.

2. Begründung der Fraktionen im Ausschuss

Die **Fraktion der CDU/CSU** betont, mit der Umsetzung der NIS-2-Richtlinie in nationales Recht nun ein Projekt zum Erfolg zu führen, das wegen der Cybersicherheitslage keinen Aufschub mehr erlaube. Auch weil die Umsetzungsfrist der Richtlinie am 17. Oktober 2024 geendet sei, habe man in Anbetracht einer möglichen Vertragsstrafe unter Hochdruck arbeiten müssen und dennoch ein gutes Ergebnis erzielt. Man sehe die massiven Bedrohungen im Cyberraum durch Akteure wie China und deswegen sei es in letzter Konsequenz richtig, dass die Bundesregierung die Möglichkeit habe, kritische Komponenten zu untersagen, wenn sie die nationale Sicherheit gefährdeten. Für dieses sensible Thema habe man eine abgewogene Lösung gefunden: Die Liste der kritischen Komponenten werde durch das BMI im Einvernehmen mit dem jeweiligen Fachministerium erstellt. Die Untersagung erfolge durch das BMI lediglich im Benehmen mit den zuständigen Fachministerien. Zukünftig werde das BSI alle ihm gemeldeten Schwachstellen den Herstellern und Produktverantwortlichen melden. Dies sei richtig und finde auch die Zustimmung des BSI. Durch den Änderungsantrag würden nun auch die nachgeordneten Behörden in den Anwendungsbereich der NIS-2-Richtline einbezogen – Ausnahmen hätten eine überaus schlechte Signalwirkung gehabt. Dass die Bundesverwaltung das ihr 2017 durch den Umsetzungsplan (UP) Bund auferlegte hohe Schutzniveau bis heute nicht erreicht habe, könne so nicht bleiben und müsse in Zukunft scharf beobachtet werden. Auch die Rolle des CISO Bund, d.h. die Einführung eines IT-Sicherheitsmanagements und entsprechende Berichtspflichten, werde durch den Gesetzentwurf entsprechend der Vorgaben der NIS-2-Richtlinie geregelt. Damit sei der Gesetzentwurf ein großer Schritt nach vorne, wenn auch nicht der letzte, hin zu mehr Cybersicherheit. Man werbe um Zustimmung.

Die **Fraktion der AfD** betont, bereits auf die zahlreichen Vorfälle aufmerksam gemacht zu haben, in denen in jüngerer Zeit Behörden, KRITIS-Betreiber oder auch ganz normale mittelständische Unternehmen Cyberangriffen ausgesetzt gewesen seien – seien es Flughäfen wie in Hamburg oder in Berlin oder DDoS-Angriffe auf die Kommunalverwaltung oder Hackerangriffe auf Industriebetriebe. Vor Cyberangriffen sei niemand gefeit. Auch politische Parteien seien wiederholt angegriffen worden und auch Stadtverwaltungen wie Trier und Ludwigshafen seien lahmgelegt worden. Der Gesetzentwurf finde einen angemessenen Ausgleich zwischen dem Erfordernis von Sicherheitsstandards und dem Schutz kleinerer Unternehmen vor Bürokratisierung. Es sei zu begrüßen, dass sonstige Unternehmen mit weniger als 250 Mitarbeitern und weniger als 50 Millionen Euro Jahresumsatz von der Anwendung ausgenommen seien. Man habe bereits darauf hingewiesen, dass nicht erklärbar sei, warum eine Unterstützungshandlung des BSI gegenüber dem Verfassungsschutz nur in Fällen von Bestrebungen gegen die freiheitlich-demokratische Grundordnung erfolgen solle und nicht bei Fällen von Ausländerextremismus, der sich gegen Menschen im Ausland richte – also etwa von Grauen Wölfen gegenüber den Türken in der Türkei. Die Koalitionsfraktionen erstreckten nun mittels des Änderungsantrags den Begriff der Unterstützung nach § 3 Absatz 1 Nummer 18 b BSIG auf alle gesetzlichen Befugnisse des Verfassungsschutzes. An der Stelle erfreue der erfolgreiche Hinweis, den man in Richtung der Fraktion der CDU/CSU gegeben habe. Auch die Meldung von Schwach-

stellen, die das BSI erkannt habe, die aber noch nicht öffentlich bekannt seien, an Hersteller und Produktionsverantwortliche, sei sinnvoll. Die Fraktion der AfD werde daher in der Sache zustimmen.

Die **Fraktion der SPD** hebt die Herausforderung, einerseits der aktuellen Cybersicherheitslage Rechnung getragen zu müssen und andererseits den Zeitdruck aufgrund des laufenden Vertragsverletzungsverfahrens hervor. Man danke daher besonders der Fraktion der CDU/CSU und dem BMI für die intensive und konstruktive Zusammenarbeit. Im parlamentarischen Verfahren sei nun der Anwendungsbereich des Gesetzes hinsichtlich der Verwaltung auf die Geschäftsbereichsbehörden ausgeweitet worden. Dies sei folgerichtig, da sich die Behörden des Bundes die Netze teilten und untereinander wiederum vernetzt seien. Die Untersagungsmöglichkeiten für die kritischen Komponenten seien durchaus streitbar. Aber durch die Teilung dieses Prozesses in die Erstellung einer Liste möglicher kritischer Komponenten unter Beteiligung der Ressorts und letzter Entscheidung durch das BMI über die Untersagung selbst, sei diese Möglichkeit sachgerecht. In diesem Gesetzgebungsverfahren habe das Parlament bewiesen, wie wichtig es sei, bei der inneren Sicherheit nachzuschärfen.

Die **Fraktion BÜNDNIS 90/DIE GRÜNEN** stellt voran, es sei überfällig, dass dieses Gesetz beschlossen werde. Die Frist zur Umsetzung der NIS-2-Richtlinie sei bereits im Oktober 2024 abgelaufen. Diese Verzögerung sei angesichts der Bedrohungslage im Cyberbereich unverantwortlich. Zu kritisieren sei das nicht vorgesehene Schwachstellenmanagement. Zudem sei nicht davon auszugehen, dass das BMI tatsächlich von konkreten Schwachstellen erfahre, sodass die Problematik bei der Nutzung von Schwachstellen bestehen bleibe. Deutschland sei das weltweit am meisten angegriffene Land im Cyberbereich, was noch weiter zunehmen werde, daher sei die vorgesehene Regelung unzureichend. Auch werde die Bundesregierung der europarechtlichen Vorgabe der Unabhängigkeit des CISO Bund nicht gerecht. Zudem gebe es kein echtes KRITIS-Dachgesetz, das den physischen und digitalen Schutz hinreichend miteinander verknüpfe. Die Fraktion könne diesem Gesetzentwurf daher nicht zustimmen.

Die **Fraktion Die Linke** kritisiert, es sei nicht nachvollziehbar, dass die Bundesregierung angesichts der großen sozialen Auswirkungen bei Systemausfällen nicht die Möglichkeit nutze, die Kommunen in den Wirkungskreis dieses Gesetzes aufzunehmen. Der Wissenschaftliche Dienst des Deutschen Bundestages habe ausgearbeitet, dass diese Einbeziehung im Sinne der NIS-2-Richtlinie wäre und rechtliche Hürden dem nicht entgegenstünden. Dies sei in der Sachverständigenanhörung ebenfalls deutlich geworden. Die Umsetzung der NIS-2-Richtlinie sei dringend nötig und überfällig. Umso fataler sei es, die Kommunen hier nicht einzubinden, da dies im Gesamtgefüge zu weiteren Sicherheitsrisiken führen werde. Es sei nicht nachvollziehbar, weshalb Anknüpfungspunkt für die Einbeziehung in den Anwendungsbereich nicht die Kritikalität der Unternehmen sei, anstatt auf Beschäftigten- und Umsatzzahlen abzustellen.

Berlin, den 12. November 2025

Marc Henrichmann
Berichterstatter

Steffen Janich
Berichterstatter

Johannes Schätzl
Berichterstatter

Dr. Konstantin von Notz
Berichterstatter

Jan Köstering
Berichterstatter