Deutscher Bundestag **Drucksache 20/13184**

20. Wahlperiode 02.10.2024

Gesetzentwurf

der Bundesregierung

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

(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

A. Problem und Ziel

Die moderne Wirtschaft Deutschlands ist für ihr Funktionieren, die Generierung von Wohlstand und Wachstum und auch für ihre Adaptionsfähigkeit auf geänderte wirtschaftspolitische und geopolitische Rahmenbedingungen angewiesen auf funktionierende und resiliente Infrastruktur, sowohl im physischen als auch im digitalen Bereich. Diese Faktoren haben in den vergangenen Jahren erheblich an Bedeutung gewonnen. Unternehmen sehen sich nicht nur in ihrem wirtschaftlichen Tun, sondern auch in dessen praktischer Absicherung vor eine Vielzahl von Herausforderungen gestellt. Europaweit und global vernetzte Prozesse führen ebenso wie die zunehmende Digitalisierung aller Lebens- und somit auch Wirtschaftsbereiche zu einer höheren Anfälligkeit gegenüber externen, vielfach nicht steuerbaren Faktoren. Informationstechnik in kritischen Anlagen sowie in bestimmten Unternehmen spielt dabei eine zentrale Rolle. Ihre Sicherheit und Resilienz bilden auch die Grundlage für die Versorgungssicherheit, von der Versorgung mit Strom und Wasser bis hin zur Entsorgung von Siedlungsabfällen. Gleiches gilt für das Funktionieren der Marktwirtschaft in Deutschland und dem Binnenmarkt der Europäischen Union. Die Vernetzung und enge Verzahnung gerade der Wirtschaft innerhalb Deutschlands und der Europäischen Union resultieren in Interdependenzen bei der Cybersicherheit. Die vor diesem Hintergrund gestiegenen Cybersicherheitsanforderungen an juristische und natürliche Personen, die wesentliche Dienste erbringen oder Tätigkeiten ausüben, 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.

Infolge des völkerrechtswidrigen russischen Angriffskriegs auf die Ukraine hat sich nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im Bericht zur Lage der IT-Sicherheit in Deutschland 2023 die IT-Sicherheitslage insgesamt zugespitzt. Im Bereich der Wirtschaft zählen hierbei Ransomware-Angriffe, Ausnutzung von Schwachstellen, offene oder falsch kon-

figurierte Online-Server sowie Abhängigkeiten von der IT-Lieferkette und in diesem Zusammenhang auch insbesondere Cyberangriffe über die Lieferkette (sogenannte Supply-Chain-Angriffe) zu den größten Bedrohungen. Zusätzlich zu den bereits bekannten Bedrohungen entstanden infolge des russischen Angriffskriegs auf die Ukraine und der damit einhergehenden „Zeitenwende“ auch neue Bedrohungen oder die Einschätzungen zu bereits bekannten Bedrohungen mussten aufgrund veränderter Rahmenbedingungen geändert werden. Beispiele hierfür bestehen im Bereich Hacktivismus, insbesondere mittels Distributed-Denial-of-Service (DdoS)-Angriffen oder auch durch in Deutschland erfolgte Kollateralschäden infolge von Cyber-Sabotage-Angriffen im Rahmen des Krieges. Zudem haben auch Störungen und Angriffe im Bereich der Lieferketten sowohl aus den Bereichen Cybercrime als auch im Rahmen des Krieges zuletzt zugenommen. Diese Phänomene treten nicht mehr nur vereinzelt auf, sondern sind insgesamt Teil des unternehmerischen Alltags geworden. Eine Erhöhung der Resilienz der Wirtschaft gegenüber den Gefahren der digitalen Welt ist daher eine zentrale Aufgabe für die beteiligten Akteure in Staat, Wirtschaft und Gesellschaft, um den Wirtschaftsstandort Deutschland und den Binnenmarkt der Europäischen Union insgesamt robust und leistungs- und funktionsfähig zu halten.

Für das Informationssicherheitsmanagement in der Bundesverwaltung haben sich die bisherigen Steuerungsinstrumente auf überwiegend untergesetzlicher Basis als nicht ausreichend effektiv erwiesen, um eine flächendeckend wirksame Steigerung des Sicherheitsniveaus zu erreichen. Dies haben insbesondere Sachstandserhebungen zum Umsetzungsplan Bund sowie Prüfungen des Bundesrechnungshofs (BRH) bestätigt. Vor dem Hintergrund der durch aktuelle geopolitische Entwicklungen („Zeitenwende“) abermals verschärften Bedrohungslage hat sich das Risiko für staatliche Einrichtungen zudem weiter erhöht, durch Gefährdungen aus dem Cyberraum in ihrer Handlungsfähigkeit eingeschränkt zu werden.

Dieser Entwurf steht im Kontext der Bestrebungen der Europäischen Union und ihrer Mitgliedstaaten zur Erhöhung der Wirtschaftssicherheit und Verbesserung der Resilienz als Antwort auf neue geopolitische Rahmenbedingungen. Mit der am 20. Juni 2023 veröffentlichten Europäischen Strategie für wirtschaftliche Sicherheit identifiziert die Europäische Kommission das Risiko für die Sicherheit kritischer Infrastruktur vor physischen und Cyberangriffen als eines von vier Hauptrisiken für die europäische Volkswirtschaft.

Dieser Entwurf steht außerdem im Kontext der gefährdeten rechtzeitigen Erreichung der Ziele der Resolution der Generalversammlung der Vereinten Nationen vom 25. September 2015 „Transformation unserer Welt: die UN-Agenda 2030 für nachhaltige Entwicklung“. Der Entwurf soll insbesondere zur Erreichung des Nachhaltigkeitsziels 9 der UN-Agenda 2030 beitragen, eine hochwertige, verlässliche und widerstandsfähige Infrastruktur aufzubauen.

B. Lösung, Nutzen

Entsprechend der unionsrechtlichen Vorgaben wird der mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I 2015 S. 1324) und dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021 (BGBl. I 2021, S. 1122) geschaffene Ordnungsrahmen durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz auf den Bereich bestimmter Unternehmen erweitert, zusätzlich werden entsprechende Vorgaben für die Bundesverwaltung eingeführt. Schwerpunktmäßig werden folgende Änderungen vorgenommen:

- Einführung der durch die NIS-2-Richtlinie vorgegebenen Einrichtungskategorien, die mit einer signifikanten Ausweitung des bisher auf Betreiber Kritischer Infrastrukturen, Anbieter digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse beschränkten Anwendungsbereichs einhergeht.
- Der Katalog der Mindestsicherheitsanforderungen des Artikels 21 Absatz 2 NIS-2-Richtlinie wird in das BSI-Gesetz übernommen, wobei in der Intensität der jeweiligen Maßnahme aus Gründen der Verhältnismäßigkeit zwischen den Kategorien ausdifferenziert wird.
- Die bislang einstufige Meldepflicht bei Vorfällen wird durch das dreistufige Melderegime der NIS-2-Richtlinie ersetzt. Dabei soll der bürokratische Aufwand für die Einrichtungen im Rahmen des bestehenden mitgliedstaatlichen Umsetzungsspielraums minimiert werden.
- Ausweitung des Instrumentariums des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im Hinblick auf von der NIS-2-Richtlinie vorgegebene Aufsichtsmaßnahmen.
- Gesetzliche Verankerung wesentlicher nationaler Anforderungen an das Informationssicherheitsmanagement des Bundes und Abbildung der zugehörigen Rollen und Verantwortlichkeiten.
- Harmonisierung der Anforderungen an Einrichtungen der Bundesverwaltung aus nationalen und unionsrechtlichen Vorgaben, um ein insgesamt kohärentes und handhabbares Regelungsregime zu gewährleisten.
- Etablierung eines CISO-Bunds als zentralem Koordinator für Maßnahmen zur Informationssicherheit in Einrichtungen der Bundesverwaltung und zur Unterstützung der Ressorts bei der Umsetzung der Vorgaben für das Informationssicherheitsmanagement.

Ziel der NIS-2-Richtlinie ist die Einführung verbindlicher Maßnahmen für Verwaltung und Wirtschaft, mit denen in der gesamten Europäischen Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll. Wichtige und besonders wichtige Einrichtungen sollen vor Schäden durch Cyberangriffe geschützt und das Funktionieren des europäischen Binnenmarktes verbessert werden. Die Konsequenzen eines Cyberangriffes sind sehr vielfältig und können nicht vollständig quantifiziert werden. So können durch Ransomware-Angriffe Server medizinischer Einrichtungen verschlüsselt werden, was die Aufnahme neuer Notfälle und die ambulante Patientenversorgung tagelang verhindert. Dies etwa sind Risiken und Gefahren für Leib und Leben der Bevölkerung, die nicht in monetären Größen ausgedrückt werden können. Bezogen auf die unmittelbar durch Cyberangriffe verursachten und bezifferbaren Schäden für Unternehmen in Deutschland schätzt der Branchenverband der deutschen Informations- und Telekommunikationsunternehmen (Bitkom e. V.) ein jährliches Gesamtschadensvolumen von rund 223,5 Milliarden Euro für das Jahr 2021. Im Jahr 2022 lag das Gesamtschadensvolumen bei 202,7 Milliarden Euro und im Jahr 2023 voraussichtlich bei 205,9 Milliarden Euro. Im Schnitt verursachen Cyberangriffe für Unternehmen in Deutschland einen jährlichen Gesamtschaden von rund 210,7 Milliarden Euro in den letzten drei Jahren. Dabei hat Bitkom deutsche Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von mindestens 1 Million Euro befragt. Im Unternehmensregister des Statistischen Bundesamts waren im Berichtsjahr 2021 insgesamt rund 3,4 Millionen rechtliche Einheiten registriert, davon beschäftigten 444 055 rechtliche Einheiten mindestens zehn Beschäftigte. Unter der Annahme einer Gleichverteilung des Gesamtschadensvolumens auf die Unternehmen mit mindestens zehn Beschäftigten ergibt sich ein Schadensvolumen pro Un-

ternehmen von rund 500 000 Euro (= 210,7 Milliarden Euro/444 055 Unternehmen). Es ist anzunehmen, dass selbst bei einer vollständigen Umsetzung der von der NIS-2-Richtlinie vorgegebenen Sicherheitsstandards nicht alle Schäden durch Cyberangriffe abgewehrt werden können. Nimmt man jedoch an, dass durch die Umsetzung der vorliegenden Vorgaben die Hälfte des jährlich verursachten Schadens in den zur Umsetzung der NIS-2-Richtlinie verpflichteten Unternehmen abgewehrt werden kann, so ergibt sich pro Unternehmen ein abgewehrter Schaden von rund 250 000 Euro. Hochgerechnet auf die voraussichtlich geschätzte Anzahl betroffener Unternehmen bedeutet dies einen abgewehrten Gesamtschaden in Höhe von ca. 3,6 Milliarden Euro (= 250 000 Euro * 14 500 Unternehmen) für die deutsche Wirtschaft. Zusätzlich zu dem hier geschätzten abgewehrten Schaden in Höhe von ca. 3,6 Milliarden Euro bei den Unternehmen muss ebenfalls ein mangels verfügbarer Daten nicht bezifferbarer abgewehrter Schaden in der öffentlichen Verwaltung sowie weitere Schäden mitberücksichtigt werden.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Für den Bundeshaushalt entstehen durch das Gesetz bei der Bundesverwaltung einmalige Ausgaben in Höhe von rund 38,2 Millionen Euro sowie bis zum Jahr 2029 insgesamt laufende jährliche Ausgaben in Höhe von rund 772,32 Millionen Euro. 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)	36,87	1,17	0,086	0,077
laufende Ausgaben (in Mio. Euro)	155,49	190,98	209,64	216,21
Ausgaben (gesamt, in Mio. Euro)	**192,36**	**192,16**	**209,73**	**216,28**

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden. Dies gilt ebenso für den in Abschnitt E.3 dargestellten Erfüllungsaufwand, sofern dieser haushaltswirksam wird.

Mehrausgaben für Länder und Kommunen entstehen nicht.

Den Sozialversicherungsträgern entstehen durch das Gesetz insgesamt laufende jährliche Ausgaben in Höhe von rund 16,9 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 2,2 Milliarden Euro. Insgesamt entsteht einmaliger Aufwand von rund 2,1 Milliarden Euro. Dieser ist fast ausschließlich der Kategorie Einführung oder Anpassung digitaler Prozessabläufe zuzuordnen.

Davon Bürokratiekosten aus Informationspflichten

Es entfallen rund 1,9 Millionen Euro auf Bürokratiekosten aus Informationspflichten.

E.3 Erfüllungsaufwand der Verwaltung

Für die Bundesverwaltung erhöht sich der jährliche Erfüllungsaufwand um 122,28 Millionen Euro. Der einmalige Erfüllungsaufwand beträgt 38,21 Millionen Euro. Der jährliche Erfüllungsaufwand der Länder erhöht sich um 85 000 Euro.

F. Weitere Kosten

Keine.

BUNDESREPUBLIK DEUTSCHLAND
DER BUNDESKANZLER

WIR FEIERN 75 JAHRE GRUNDGESETZ

Berlin, 2. Oktober 2024

An die
Präsidentin des
Deutschen Bundestages
Frau Bärbel Bas
Platz der Republik 1
11011 Berlin

Sehr geehrte Frau Präsidentin,

hiermit übersende ich den von der Bundesregierung beschlossenen

> Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung
> (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium des Innern und für Heimat.

Die Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Absatz 1 NKRG ist als Anlage 2 beigefügt.

Die Stellungnahme der Bundesregierung zur Stellungnahme des Nationalen Normenkontrollrates ist als Anlage 3 beigefügt.

Der Bundesrat hat in seiner 1047. Sitzung am 27. September 2024 gemäß Artikel 76 Absatz 2 des Grundgesetzes beschlossen, zu dem Gesetzentwurf wie aus Anlage 4 ersichtlich Stellung zu nehmen.

Die Auffassung der Bundesregierung zu der Stellungnahme des Bundesrates ist in der als Anlage 5 beigefügten Gegenäußerung dargelegt.

Mit freundlichen Grüßen

Olaf Scholz

Anlage 1

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

(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) [1, 2]

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

I n h a l t s ü b e r s i c h t

Artikel 1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG)

Artikel 2 Änderung des BND-Gesetzes

Artikel 3 Änderung der Sicherheitsüberprüfungsfeststellungsverordnung

Artikel 4 Änderung der Besonderen Gebührenverordnung des Bundesministeriums des Innern, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich

Artikel 5 Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes

Artikel 6 Änderung der Gleichstellungsbeauftragtenwahlverordnung

Artikel 7 Änderung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Artikel 8 Änderung der BSI-Zertifizierungs- und Anerkennungsverordnung

Artikel 9 Änderung der BSI-IT-Sicherheitskennzeichenverordnung

Artikel 10 Änderung des De-Mail-Gesetzes

Artikel 11 Änderung des E-Government-Gesetz

Artikel 12 Änderung der Passdatenerfassungs- und Übermittlungsverordnung

Artikel 13 Änderung der Personalausweisverordnung

Artikel 14 Änderung des Hinweisgeberschutzgesetzes

Artikel 15 Änderung der Kassensicherungsverordnung

Artikel 16 Änderung des Atomgesetzes

Artikel 17 Änderung des Energiewirtschaftsgesetzes

Artikel 18 Änderung des Messstellenbetriebsgesetzes

Artikel 19 Änderung des Energiesicherungsgesetzes

---

[1] Notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

[2] Dieses Gesetz dient der Umsetzung 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).

Artikel 20 Änderung des Wärmeplanungsgesetzes
Artikel 21 Änderung des Fünften Buches Sozialgesetzbuch
Artikel 22 Änderung der Digitale Gesundheitsanwendungen-Verordnung
Artikel 23 Änderung des Sechsten Buches Sozialgesetzbuch
Artikel 24 Änderung der Verordnung zum Barrierefreiheitsstärkungsgesetz
Artikel 25 Änderung des Elften Buches Sozialgesetzbuch
Artikel 26 Änderung des Telekommunikationsgesetzes
Artikel 27 Änderung der Krankenhausstrukturfonds-Verordnung
Artikel 28 Änderung der Außenwirtschaftsverordnung
Artikel 29 Änderung des Vertrauensdienstegesetzes
Artikel 30 Weitere Änderung des BSI-Gesetzes
Artikel 31 Weitere Änderung des Telekommunikationsgesetzes
Artikel 32 Weitere Änderung der Außenwirtschaftsverordnung
Artikel 33 Inkrafttreten, Außerkrafttreten

Artikel 1

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen

(BSI-Gesetz – BSIG)

Inhaltsübersicht

Teil 1
Allgemeine Vorschriften

§ 1 Bundesamt für Sicherheit in der Informationstechnik
§ 2 Begriffsbestimmungen

Teil 2
Das Bundesamt

Kapitel 1
Aufgaben und Befugnisse

§ 3 Aufgaben des Bundesamtes
§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes
§ 5 Allgemeine Meldestelle für die Sicherheit in der Informationstechnik
§ 6 Informationsaustausch
§ 7 Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte

§ 8 Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes

§ 9 Verarbeitung von Protokollierungsdaten der Kommunikationstechnik des Bundes

§ 10 Anordnungen von Maßnahmen zur Abwendung oder Behebung von Sicherheitsvorfällen

§ 11 Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

§ 12 Bestandsdatenauskunft

§ 13 Warnungen

§ 14 Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen

§ 15 Detektion von Angriffsmethoden und von Sicherheitsrisiken für die Netz- und IT-Sicherheit

§ 16 Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von Telekommunikationsdiensten

§ 17 Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von digitalen Diensten

§ 18 Anordnungen von Maßnahmen des Bundesamtes gegenüber Herstellern von IKT-Produkten

§ 19 Bereitstellung von IT-Sicherheitsprodukten

Kapitel 2

Datenverarbeitung

§ 20 Verarbeitung personenbezogener Daten

§ 21 Beschränkungen der Rechte der betroffenen Person

§ 22 Informationspflicht bei Erhebung von personenbezogenen Daten

§ 23 Auskunftsrecht der betroffenen Person

§ 24 Recht auf Berichtigung

§ 25 Recht auf Löschung

§ 26 Recht auf Einschränkung der Verarbeitung

§ 27 Widerspruchsrecht

Teil 3

Sicherheit in der Informationstechnik von Einrichtungen

Kapitel 1

Anwendungsbereich

§ 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen

§ 29 Einrichtungen der Bundesverwaltung

Kapitel 2

Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten

§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

§ 31 Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

§ 32 Meldepflichten

§ 33 Registrierungspflicht

§ 34 Besondere Registrierungspflicht für bestimmte Einrichtungsarten

§ 35 Unterrichtungspflichten

§ 36 Rückmeldungen des Bundesamtes gegenüber meldenden Einrichtungen

§ 37 Ausnahmebescheid

§ 38 Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

§ 39 Nachweispflichten für Betreiber kritischer Anlagen

§ 40 Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen

§ 41 Untersagung des Einsatzes kritischer Komponenten

§ 42 Auskunftsverlangen

Kapitel 3

Informationssicherheit der Einrichtungen der Bundesverwaltung

§ 43 Informationssicherheitsmanagement

§ 44 Vorgaben des Bundesamtes

§ 45 Informationssicherheitsbeauftragte der Einrichtungen der Bundesverwaltung

§ 46 Informationssicherheitsbeauftragte der Ressorts

§ 47 Wesentliche Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes

§ 48 Amt des Koordinators für Informationssicherheit

Teil 4

Datenbanken der Domain-Name-Registrierungsdaten

§ 49 Pflicht zum Führen einer Datenbank

§ 50 Verpflichtung zur Zugangsgewährung

§ 51 Kooperationspflicht

Teil 5

Zertifizierung, Konformitätserklärung und Kennzeichen

§ 52 Zertifizierung

§ 53 Konformitätsbewertung und Konformitätserklärung

§ 54 Nationale Behörde für die Cybersicherheitszertifizierung

§ 55 Freiwilliges IT-Sicherheitskennzeichen

Teil 6

Verordnungsermächtigungen, Grundrechtseinschränkungen und Berichtspflichten

§ 56 Ermächtigung zum Erlass von Rechtsverordnungen

§ 57 Einschränkung von Grundrechten

§ 58 Berichtspflichten des Bundesamtes

Teil 7

Aufsicht

§ 59 Zuständigkeit des Bundesamtes

§ 60 Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten

§ 61 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

§ 62 Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen

§ 63 Verwaltungszwang

§ 64 Zuwiderhandlungen durch Institutionen der sozialen Sicherung

Teil 8

Bußgeldvorschriften

§ 65 Bußgeldvorschriften

Anlage 1 Sektoren besonders wichtiger und wichtiger Einrichtungen

Anlage 2 Sektoren wichtiger Einrichtungen

Teil 1
Allgemeine Vorschriften

§ 1
Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern und für Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene. Aufgaben gegenüber den Bundesministerien führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch.

§ 2
Begriffsbestimmungen

Im Sinne dieses Gesetzes ist oder sind

1. „Beinahevorfall“ ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert worden ist oder aus anderen Gründen nicht erfolgt ist;
2. „berechtigte Zugangsnachfrager“
   a) das Bundesamt,
   b) die Landesbehörden, die die Länder als zuständige Behörden für die Aufsicht von Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene nach Artikel 2 Absatz 2 Buchstabe f Nummer ii der NIS-2-Richtlinie bestimmt haben,
   c) Strafverfolgungsbehörden,
   d) die Polizeien des Bundes und der Länder und
   e) die Verfassungsschutzbehörden des Bundes und der Länder;
3. „Bodeninfrastruktur“ den Sektor Weltraum betreffende Einrichtungen, die der Kontrolle des Startes, Fluges oder der eventuellen Landung von Weltraumgegenständen dienen;
4. „Cloud-Computing-Dienst“ ein digitaler Dienst, der auf Abruf die Verwaltung eines skalierbaren und elastischen Pools gemeinsam nutzbarer Rechenressourcen sowie den umfassenden Fernzugang zu diesem Pool ermöglicht, auch wenn die Rechenressourcen auf mehrere Standorte verteilt sind;
5. „Content Delivery Network“ oder „CDN“ eine Gruppe geographisch verteilter, zusammengeschalteter Server, mitsamt der hierfür erforderlichen Infrastruktur, die mit dem Internet verbunden sind, und der Bereitstellung digitaler Inhalte und Dienste für Internetnutzer im Auftrag von Inhalte- und Diensteanbietern dienen, mit dem Ziel der Gewährleistung einer hohen Verfügbarkeit, Zugänglichkeit oder Zustellung mit möglichst niedriger Latenz;
6. „Cyberbedrohung“ eine Cyberbedrohung nach Artikel 2 Nummer 8 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit, ABl. L 151 vom 7.6.2019, S. 15);
7. „Datenverkehr“ die mittels technischer Protokolle übertragenen Daten; es können Telekommunikationsinhalte nach § 3 Absatz 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes enthalten sein;
8. „DNS-Diensteanbieter“ eine natürliche oder juristische Person, die
   a) für Internet-Endnutzer öffentlich verfügbare rekursive Dienste zur Auflösung von Domain-Namen anbietet oder
   b) autoritative Dienste zur Auflösung von Domain-Namen zur Nutzung durch Dritte, mit Ausnahme von Root-Namenservern, anbietet;
9. „Domain-Name-Registry-Dienstleister“ ein Registrar oder eine Stelle, die im Namen von Registraren tätig ist, insbesondere Anbieter oder Wiederverkäufer von Datenschutz- oder Proxy-Registrierungsdiensten;
10. „erhebliche Cyberbedrohung“ eine Cyberbedrohung, die das Potenzial besitzt, die informationstechnischen Systeme, Komponenten und Prozesse auf Grund der besonderen technischen Merkmale der Cyberbedrohung erheblich zu beeinträchtigen; eine Beeinträchtigung ist erheblich, wenn sie erheblichen materiellen oder immateriellen Schaden verursachen kann;
11. „erheblicher Sicherheitsvorfall“ ein Sicherheitsvorfall, der
    a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder

b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann,

sofern durch die Rechtsverordnung nach § 56 Absatz 5 keine konkretisierende Begriffsbestimmung erfolgt;

12. „Forschungseinrichtung“ eine Einrichtung, deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen; Bildungseinrichtungen gelten nicht als Forschungseinrichtungen;

13. „Geschäftsleitung“ eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist; Leiterinnen und Leiter von Einrichtungen der Bundesverwaltung nach § 29 gelten nicht als Geschäftsleitung;

14. „IKT-Dienst“ ein IKT-Dienst nach Artikel 2 Nummer 13 der Verordnung (EU) 2019/881;

15. „IKT-Produkt“ ein IKT-Produkt nach Artikel 2 Nummer 12 der Verordnung (EU) 2019/881;

16. „IKT-Prozess“ ein IKT-Prozess nach Artikel 2 Nummer 14 der Verordnung (EU) 2019/881;

17. „Informationssicherheit“ der angemessene Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen;

18. „Informationstechnik“ ein technisches Mittel zur Verarbeitung von Informationen;

19. „Institutionen der Sozialen Sicherung“ Körperschaften gemäß § 29 des Vierten Buches Sozialgesetzbuch, Arbeitsgemeinschaften gemäß § 94 des Zehnten Buches Sozialgesetzbuch, die Deutsche Gesetzliche Unfallversicherung e. V. sowie die Deutsche Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist;

20. „Internet Exchange Point“ oder „IXP“ eine Infrastruktur, die

    a) die Zusammenschaltung von mehr als zwei unabhängigen autonomen Systemen ermöglicht, die in erster Linie zum Austausch von Internet-Datenverkehr genutzt wird,

    b) nur der Zusammenschaltung autonomer Systeme dient und

    c) nicht voraussetzt, dass

        aa) der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft oder

        bb) den betreffenden Datenverkehr verändert oder diesen anderweitig beeinträchtigt;

21. „Kommunikationstechnik des Bundes“ Informationstechnik, die von einer oder mehreren Einrichtungen der Bundesverwaltung oder im Auftrag einer oder mehrerer Einrichtungen der Bundesverwaltung betrieben wird und der Kommunikation oder dem Datenaustausch innerhalb einer Einrichtung der Bundesverwaltung, der Einrichtungen der Bundesverwaltung untereinander oder der Einrichtungen der Bundesverwaltung mit Dritten dient; nicht als „Kommunikationstechnik des Bundes“ gelten die Kommunikationstechnik des Bundesverfassungsgerichts, der Bundesgerichte, soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes, soweit sie ausschließlich in deren eigener Zuständigkeit betrieben wird;

22. „kritische Anlage“ eine Anlage, die für die Erbringung einer kritischen Dienstleistung erheblich ist; die kritischen Anlagen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 56 Absatz 4 näher bestimmt;

23. „kritische Komponenten“ IKT-Produkte,

    a) die in kritischen Anlagen eingesetzt werden,

    b) bei denen Störungen der Verfügbarkeit, Integrität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit kritischer Anlagen oder zu Gefährdungen für die öffentliche Sicherheit führen können und

c) die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift

aa) als kritische Komponenten bestimmt werden oder

bb) eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren;

werden für einen der in Nummer 24 genannten Sektoren keine kritischen Komponenten und keine kritischen Funktionen, aus denen kritische Komponenten abgeleitet werden können, auf Grund eines Gesetzes unter Verweis auf diese Vorschrift bestimmt, so gibt es in diesem Sektor keine kritischen Komponenten im Sinne dieser Nummer;

24. „kritische Dienstleistung“ eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde;

25. „Managed Security Service Provider“ oder „MSSP“ ein MSP, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt;

26. „Managed Service Provider“ oder „MSP“ ein Anbieter von Diensten im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, -Netzen, -Infrastruktur, -Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung in den Räumlichkeiten der Kunden oder aus der Ferne;

27. „NIS-2-Richtlinie“ die Richtlinie 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) in der jeweils geltenden Fassung;

28. „Online-Marktplatz“ ein Dienst nach § 312l Absatz 3 des Bürgerlichen Gesetzbuchs;

29. „Online-Suchmaschine“ ein digitaler Dienst nach Artikel 2 Nummer 5 der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (ABl. L 186 vom 11.7.2019, S. 57);

30. „Plattform für Dienste sozialer Netzwerke“ eine Plattform, auf der Endnutzer mit unterschiedlichen Geräten insbesondere durch Chats, Posts, Videos und Empfehlungen miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und entdecken können;

31. „Protokolldaten“ Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die

a) zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind und

b) unabhängig vom Inhalt des Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden;

Protokolldaten können Verkehrsdaten nach § 3 Nummer 70 des Telekommunikationsgesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes enthalten;

32. „Protokollierungsdaten“ Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme;

33. „qualifizierter Vertrauensdienst“ ein qualifizierter Vertrauensdienst nach Artikel 3 Nummer 17 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73);

34. „qualifizierter Vertrauensdiensteanbieter“ ein qualifizierter Vertrauensdiensteanbieter nach Artikel 3 Nummer 20 der Verordnung (EU) Nr. 910/2014;

35. „Rechenzentrumsdienst“ ein Dienst, der Strukturen umfasst, die dem vorrangigen Zweck der zentralen Unterbringung, der Zusammenschaltung und dem Betrieb von IT- oder Netzwerkausrüstungen dienen, und die Datenverarbeitungsdienste erbringen, mitsamt allen benötigten Anlagen und Infrastrukturen, insbesondere für die Stromverteilung und die Umgebungskontrolle;

36. „Schadprogramme“ Programme und sonstige informationstechnische Routinen und Verfahren, die dazu dienen, unbefugt Daten zu nutzen oder zu löschen oder unbefugt auf sonstige informationstechnische Abläufe einzuwirken;

37. „Schnittstellen der Kommunikationstechnik des Bundes“ sicherheitsrelevante Netzwerkübergänge innerhalb der Kommunikationstechnik des Bundes sowie zwischen dieser und der Informationstechnik der einzelnen Einrichtungen der Bundesverwaltung, der Informationstechnik von Gruppen von Einrichtungen der Bundesverwaltung oder der Informationstechnik Dritter; nicht als Schnittstellen der Kommunikationstechnik des Bundes gelten die Komponenten an den Netzwerkübergängen, die in eigener Zuständigkeit der in Nummer 21 genannten Gerichte und Verfassungsorgane betrieben werden;

38. „Schwachstelle“ eine Eigenschaft von IKT-Produkten oder IKT-Diensten, die von Dritten ausgenutzt werden kann, um sich gegen den Willen des Berechtigten Zugang zu den IKT-Produkten oder IKT-Diensten zu verschaffen oder die Funktion der IKT-Produkte oder IKT-Dienste zu beeinflussen;

39. „Sicherheit in der Informationstechnik“ die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

    a) in informationstechnischen Systemen, Komponenten oder Prozessen oder

    b) bei der Anwendung informationstechnischer Systeme, Komponenten oder Prozesse;

40. „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt;

41. „Systeme zur Angriffserkennung“ durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme; wobei die Angriffserkennung durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten, erfolgt;

42. „Top Level Domain Name Registry“ eine natürliche oder juristische Person, die die Registrierung von Internet-Domain-Namen innerhalb einer spezifischen Top Level Domain (TLD) verwaltet und betreibt, einschließlich des Betriebs ihrer Namenserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-Zonendateien über die Namenserver, unabhängig davon, ob der Betrieb durch die natürliche oder juristische Person selbst erfolgt oder ausgelagert wird; keine Top Level Domain Name Registry sind Register, die TLD-Namen nur für eigene Zwecke verwenden;

43. „Vertrauensdienst“ ein Vertrauensdienst nach Artikel 3 Nummer 16 der Verordnung (EU) Nr. 910/2014;

44. „Vertrauensdiensteanbieter“ ein Vertrauensdiensteanbieter nach Artikel 3 Nummer 19 der Verordnung (EU) Nr. 910/2014;

45. „weltraumgestützte Dienste“ Dienste, die den Sektor Weltraum betreffen, die auf Daten und Informationen beruhen, die entweder von Weltraumgegenständen erzeugt oder über diese weitergegeben werden und deren Störung zu breiteren Kaskadeneffekten, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Diensten im gesamten Binnenmarkt haben können, führen kann;

46. „Zertifizierung“ die Feststellung einer Zertifizierungsstelle, dass ein Produkt, ein Prozess, ein System, ein Schutzprofil (Sicherheitszertifizierung), eine Person (Personenzertifizierung) oder ein IT-Sicherheitsdienstleister bestimmte Anforderungen erfüllt.

Teil 2
Das Bundesamt

Kapitel 1
Aufgaben und Befugnisse

§ 3
Aufgaben des Bundesamtes

(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende wichtige im öffentlichen Interesse liegende Aufgaben wahr:

1. Gefahren für die Sicherheit in der Informationstechnik des Bundes abwehren;
2. Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen sammeln und auswerten und die gewonnenen Erkenntnisse anderen Stellen zur Verfügung stellen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, und Dritten zur Verfügung stellen, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist;
3. Aufgaben in der Kooperationsgruppe und im CSIRTs-Netzwerk nach Artikel 14 und 15 der NIS-2-Richtlinie wahrnehmen;
4. Sicherheitsrisiken bei der Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen untersuchen, insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik (IT-Sicherheitsprodukte), soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist, einschließlich der Forschung im Rahmen seiner gesetzlichen Aufgaben;
5. Kriterien, Verfahren und Werkzeuge für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und für die Prüfung und Bewertung der Konformität im Bereich der IT-Sicherheit entwickeln;
6. Peer Reviews nach Artikel 19 der NIS-2-Richtlinie durchführen;
7. Sicherheitsanforderungen für die Kommunikationsinfrastruktur der ressortübergreifenden Kommunikationsnetze sowie weiterer staatlicher Kommunikationsinfrastrukturen des Bundes im Benehmen mit den jeweiligen Betreibern festlegen sowie Einhaltung dieser Sicherheitsanforderungen überprüfen;
8. Sicherheit von informationstechnischen Systemen oder Komponenten prüfen und bewerten sowie Sicherheitszertifikate erteilen;
9. Aufgaben und Befugnisse nach Artikel 58 Absatz 7 und 8 der Verordnung (EU) 2019/881 als nationale Behörde für die Cybersicherheitszertifizierung wahrnehmen;
10. Konformität im Bereich der IT-Sicherheit von informationstechnischen Systemen und Komponenten mit technischen Richtlinien des Bundesamtes prüfen und bestätigen;
11. informationstechnische Systeme oder Komponenten, die für die Verarbeitung amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes im Bereich des Bundes oder bei Unternehmen im Rahmen von Aufträgen des Bundes eingesetzt werden sollen, prüfen, bewerten und zulassen;
12. Schlüsseldaten und Betrieb von Krypto- und Sicherheitsmanagementsystemen für informationssichernde Systeme des Bundes herstellen, die im Bereich des staatlichen Geheimschutzes oder auf Anforderung der betroffenen Behörde auch in anderen Bereichen eingesetzt werden;

13. bei organisatorischen und technischen Sicherheitsmaßnahmen unterstützen und beraten sowie technische Prüfungen zum Schutz amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes gegen die Kenntnisnahme durch Unbefugte durchführen;

14. sicherheitstechnische Anforderungen an die einzusetzende Informationstechnik des Bundes und an die Eignung von Auftragnehmern im Bereich von Informationstechnik des Bundes mit besonderem Schutzbedarf entwickeln;

15. IT-Sicherheitsprodukte und IT-Sicherheitsdienstleistungen für Einrichtungen der Bundesverwaltung bereitstellen;

16. die für die Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, insbesondere soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen, unterstützen; dies gilt vorrangig für die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, deren oder dessen Unterstützung im Rahmen der Unabhängigkeit erfolgt, die ihr oder ihm bei der Erfüllung ihrer oder seiner Aufgaben nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) und dem Bundesdatenschutzgesetz zusteht;

17. Einrichtungen der Bundesverwaltung in Fragen der Informationssicherheit, einschließlich der Behandlung von Sicherheitsvorfällen, beraten und unterstützen sowie konkrete, praxisnahe Hilfsmittel zur Umsetzung von Informationssicherheitsvorgaben, insbesondere zur Umsetzung der Vorgaben nach § 30 und § 44, bereitstellen;

18. Unterstützung

    a) der Polizeien und Strafverfolgungsbehörden des Bundes bei der Wahrnehmung ihrer gesetzlichen Aufgaben,

    b) des Bundesamtes für Verfassungsschutz 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 dem Bundesverfassungsschutzgesetz beziehungsweise dem MAD-Gesetz anfallen,

    c) des Bundesnachrichtendienstes bei der Wahrnehmung seiner gesetzlichen Aufgaben;

    die Unterstützung darf nur gewährt werden, soweit sie erforderlich ist, um Tätigkeiten zu verhindern oder zu erforschen, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen; die Unterstützungsersuchen sind durch das Bundesamt aktenkundig zu machen;

19. die zuständigen Stellen der Länder in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik auf deren Ersuchen unterstützen;

20. Einrichtungen der Bundesverwaltung sowie Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen, beraten, informieren und warnen;

21. Verbraucherschutz und Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, insbesondere Beratung und Warnung von Verbrauchern in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;

22. geeignete Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung aufbauen sowie Zusammenarbeit zum Schutz der Sicherheit in der Informationstechnik kritischer Anlagen im Verbund mit der Privatwirtschaft koordinieren;

23. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland, unbeschadet besonderer Zuständigkeiten anderer Stellen;

24. Aufgaben nach § 40 als zentrale Stelle für die Sicherheit in der Informationstechnik besonders wichtiger Einrichtungen und wichtiger Einrichtungen einschließlich des Ersuchens und Erbringens von Amtshilfe nach Artikel 37 der NIS-2-Richtinie;
25. bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 11 unterstützen;
26. Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren im Hinblick auf die Informationssicherheit erarbeiten;
27. einen Stand der Technik von sicherheitstechnischen Anforderungen an IT-Produkte, unter Berücksichtigung bestehender Normen und Standards sowie unter Einbeziehung der betroffenen Wirtschaftsverbände, beschreiben und veröffentlichen;
28. mit nationalen Computer-Notfallteams von Drittländern oder gleichwertigen Stellen von Drittländern kooperieren sowie diese Teams oder Stellen unterstützen; Einsätze des Bundesamtes in Drittländern dürfen nicht gegen den Willen des Staates erfolgen, auf dessen Hoheitsgebiet die Maßnahme stattfinden soll; die Entscheidung über einen Einsatz des Bundesamtes in Drittländern trifft das Bundesministerium des Innern und für Heimat im Einvernehmen mit dem Auswärtigen Amt;
29. mit der Bundesanstalt für Finanzdienstleistungsaufsicht kooperieren und Informationen austauschen, soweit dies für ihre Aufgabenerfüllung erforderlich ist, insbesondere in Bezug auf die ergriffenen Maßnahmen gemäß der Verordnung (EU) 2022/2554; die Bundesanstalt für Finanzdienstleistungsaufsicht übermittelt an das Bundesamt die für dessen Aufgabenerfüllung erforderlichen Informationen.

(2) Das Bundesamt kann die Länder auf Ersuchen bei der Sicherung ihrer Informationstechnik unterstützen.

(3) Das Bundesamt kann besonders wichtige Einrichtungen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen.

§ 4

Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes

(1) Das Bundesamt ist die zentrale Meldestelle für die Zusammenarbeit der Einrichtungen der Bundesverwaltung in Angelegenheiten der Sicherheit in der Informationstechnik.

(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe

1. alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderlichen Informationen, insbesondere zu Schwachstellen, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise, zu sammeln und auszuwerten,
2. die Einrichtungen der Bundesverwaltung unverzüglich über die sie betreffenden Informationen nach Nummer 1 und die in Erfahrung gebrachten Zusammenhänge zu unterrichten,
3. den Einrichtungen der Bundesverwaltung Empfehlungen zum Umgang mit den Gefahren bereitzustellen.

(3) Ausgenommen von den Unterrichtungspflichten nach Absatz 2 Nummer 2 sind Informationen, die aufgrund von Regelungen zum Geheimschutz oder Vereinbarungen mit Dritten nicht weitergegeben werden dürfen oder deren Weitergabe im Widerspruch zu der verfassungsrechtlichen Stellung eines Abgeordneten des Bundestages oder eines Verfassungsorgans oder der gesetzlich geregelten Unabhängigkeit einzelner Stellen stünde.

§ 5

Allgemeine Meldestelle für die Sicherheit in der Informationstechnik

(1) Zur Wahrnehmung der Aufgaben nach § 3 nimmt das Bundesamt als zentrale Stelle für Meldungen von Dritten Informationen über Sicherheitsrisiken in der Informationstechnik entgegen und wertet diese Informatio-

nen aus. Das Bundesamt ist dabei der nationale Koordinator für die Zwecke einer koordinierten Offenlegung von Schwachstellen nach Artikel 12 Absatz 1 der NIS-2-Richtlinie.

(2) Das Bundesamt nimmt zur Wahrnehmung der Aufgaben nach Absatz 1 Informationen zu Schwachstellen, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen sowie zu Sicherheitsvorfällen, Cyberbedrohungen und Beinahevorfällen entgegen. Das Bundesamt richtet hierzu geeignete Meldemöglichkeiten ein. Die Meldungen können anonym erfolgen. Erfolgt die Meldung nicht anonym, kann der Meldende zum Zeitpunkt der Meldung oder später verlangen, dass seine personenbezogenen Daten nur anonymisiert weitergegeben werden dürfen. Dies gilt nicht in den Fällen des § 8 Absatz 6 und 7 Satz 1. Eine Übermittlung der personenbezogenen Daten in den Fällen von § 8 Absatz 6 und 7 Satz 1 hat zu unterbleiben, wenn für das Bundesamt erkennbar ist, dass die schutzwürdigen Interessen des Meldenden das Allgemeininteresse an der Übermittlung überwiegen. Zu berücksichtigen ist dabei auch die Art und Weise, in der der Meldende die Erkenntnisse gewonnen hat. Die Entscheidung nach Satz 6 muss dem oder der behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem oder einer weiteren Bediensteten des Bundesamtes, der oder die die Befähigung zum Richteramt hat, zur vorherigen Prüfung vorgelegt werden.

(3) 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.

(4) Eine Weitergabe nach Absatz 3 Nummer 1, 2 oder 4 erfolgt nicht, soweit die gemäß Absatz 2 gemeldeten Informationen

1. Betriebs- und Geschäftsgeheimnisse von Dritten beinhalten und die Maßnahmen nach Absatz 3 nicht ohne Bekanntgabe dieser Betriebs- und Geschäftsgeheimnisse durchgeführt werden können oder
2. auf Grund von Vereinbarungen des Bundesamtes mit Dritten nicht übermittelt werden dürfen.

(5) Sonstige gesetzliche Meldepflichten, Regelungen zum Geheimschutz, gesetzliche Übermittlungshindernisse und Übermittlungsregelungen bleiben unberührt.

§ 6

Informationsaustausch

(1) Das Bundesamt betreibt eine Online-Plattform zum Informationsaustausch mit wichtigen Einrichtungen, besonders wichtigen Einrichtungen und Einrichtungen der Bundesverwaltung. Es kann die beteiligten Hersteller, Lieferanten oder Dienstleister zum Austausch über Cyberbedrohungen, Schwachstellen, Beinahevorfälle und IT-Sicherheitsmaßnahmen sowie zur Aufdeckung und Abwehr von Cyberangriffen hinzuziehen. Das Bundesamt kann weiteren Stellen die Teilnahme ermöglichen.

(2) Das Bundesamt gibt Teilnahmebedingungen für den Informationsaustausch und die Plattformnutzung zwischen den Teilnehmenden vor.

§ 7

Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte

(1) Das Bundesamt ist befugt, die Sicherheit der Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zum Betrieb der Kommunikationstechnik des Bundes erforderlich sind, zu kontrollieren. Es kann hierzu

1. die Bereitstellung der zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1 und 20 erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen mit Bezug zur Kommunikationstechnik des Bundes einschließlich Aufbau- und Ablauforganisation verlangen sowie
2. Unterlagen und Datenträger des Betreibers der jeweiligen Kommunikationstechnik des Bundes oder eines mit Betriebsleistungen beauftragten Dritten einsehen und die unentgeltliche Herausgabe von Kopien dieser Unterlagen und Dokumente, auch in elektronischer Form, verlangen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen des Betreibers entgegenstehen.

(2) Dem Bundesamt ist in den Zeiten, zu denen die Räume normalerweise für die jeweilige geschäftliche oder betriebliche Nutzung zur Verfügung stehen, Zugang zu den Grundstücken und Betriebsräumen, einschließlich Datenverarbeitungsanlagen und -geräten, die für die Kommunikationstechnik des Bundes verwendet werden, zu gewähren, soweit dies zur Erfüllung der Zwecke nach Absatz 1 erforderlich ist.

(3) Bei Anlagen eines Dritten, bei dem eine Schnittstelle zur Kommunikationstechnik des Bundes besteht, kann das Bundesamt auf der Schnittstellenseite der Einrichtung nur mit Zustimmung des Dritten die Sicherheit der Schnittstelle kontrollieren. Es kann hierzu mit Zustimmung des Dritten die zur Aufgabenerfüllung erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen einsehen sowie Unterlagen und Datenträger des Betreibers einsehen und unentgeltlich Kopien, auch in elektronischer Form, anfertigen.

(4) Das Bundesamt informiert über das Ergebnis seiner Kontrolle nach den Absätzen 1 bis 3

1. den jeweiligen überprüften Betreiber,
2. die oder den Informationssicherheitsbeauftragten des Ressorts und
3. die zuständige Rechts- und Fachaufsicht.

(5) Das Bundesamt führt vor der Finalisierung des Prüfberichts eine Sachverhaltsklärung mit der geprüften Einrichtung durch. Mit der Mitteilung soll das Bundesamt Vorschläge zur Verbesserung der Informationssicherheit, insbesondere zur Beseitigung der festgestellten Mängel, verbinden. Für die Mitteilung an Stellen außerhalb des Betreibers gilt § 4 Absatz 3 entsprechend. Das Bundesamt kann im Benehmen mit dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts Einrichtungen der Bundesverwaltung anweisen, die Vorschläge zur Verbesserung innerhalb einer angemessenen Frist umzusetzen.

(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 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 eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern und für Heimat und dem Auswärtigen Amt.

(7) Die Befugnisse nach den Absätzen 1 bis 3 gelten im Geschäftsbereich des Bundesministeriums der Verteidigung nicht für die Kontrolle der Informations- und Kommunikationstechnik, die von den Streitkräften für ihre Zwecke oder dem Militärischen Abschirmdienst genutzt wird. Nicht ausgenommen ist die Informations- und Kommunikationstechnik von Dritten, insbesondere von IT-Dienstleistern, soweit sie nicht ausschließlich für die Zwecke der Streitkräfte betrieben wird. Die Bestimmungen für die Schnittstellen der Kommunikationstechnik des Bundes bleiben von den Sätzen 1 und 2 unberührt. Näheres regelt eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern und für Heimat und dem Bundesministerium der Verteidigung.

(8) Stellt das Bundesamt im Rahmen seiner Kontrollen fest, dass ein Verstoß gegen die Verpflichtungen dieses Gesetzes eine offensichtliche Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 dieser Verordnung zu melden ist, so unterrichtet es unverzüglich die zuständigen Aufsichtsbehörden.

(9) Das Bundesamt unterrichtet den Haushaltsausschuss des Deutschen Bundestages kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über die Anwendung dieser Vorschrift.

§ 8

Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes

(1) Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes

1. Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist,
2. die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen und sonstigen erheblichen Gefahren für die Kommunikationstechnik des Bundes erforderlich ist.

Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, müssen die automatisierte Auswertung dieser Daten und deren anschließende vollständige und nicht wiederherstellbare Löschung unverzüglich erfolgen. Die Verwendungsbeschränkungen gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten. Die Einrichtungen der Bundesverwaltung sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu einrichtungsinternen Protokolldaten nach Satz 1 Nummer 1 sowie zu Schnittstellendaten nach Satz 1 Nummer 2 sicherzustellen. Protokolldaten der Bundesgerichte dürfen nur in deren Einvernehmen erhoben werden.

(2) Protokolldaten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für 18 Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte dafür bestehen, dass diese im Falle der Bestätigung eines Verdachts nach Absatz 4 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen, oder zur Erkennung und Abwehr anderer Schadprogramme oder sonstiger erheblicher Gefahren für die Kommunikationstechnik des Bundes erforderlich sein können. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt und dass ein Zugriff auf Daten, die länger als drei Monate gespeichert sind, nur bei Vorliegen tatsächlicher Erkenntnisse über die Betroffenheit des Bundes mit einem Schadprogramm oder einer sonstigen erheblichen Gefahr für die Kommunikationstechnik des Bundes erfolgt. Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht automatisierte Verarbeitung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. Soweit hierzu die Wiederherstellung pseudonymisierter Protokolldaten erforderlich ist, muss diese durch die Präsidentin oder den Präsidenten des Bundesamtes oder die Vertretung im Amt angeordnet werden. Die Entscheidung ist zu dokumentieren.

(3) Protokolldaten dürfen vor ihrer Pseudonymisierung und Speicherung nach Absatz 2 zur Sicherstellung einer fehlerfreien automatisierten Auswertung manuell verarbeitet werden. Liegen Hinweise vor, dass die fehlerfreie automatisierte Auswertung wegen eines erheblichen Fehlers erschwert wird, darf der Personenbezug von Protokolldaten zur Sicherstellung der fehlerfreien automatisierten Auswertung wiederhergestellt werden, sofern dies im Einzelfall erforderlich ist. Absatz 2 Satz 3 bis 6 gilt entsprechend.

(4) Eine über die Absätze 1 und 2 hinausgehende Verwendung personenbezogener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass

1. diese Daten ein Schadprogramm enthalten,
2. diese Daten durch ein Schadprogramm übermittelt wurden,

3. diese Daten im Zusammenhang mit einer sonstigen erheblichen Gefahr für die Kommunikationstechnik des Bundes stehen oder
4. sich aus diesen Daten Hinweise auf ein Schadprogramm oder eine sonstige erhebliche Gefahr für die Kommunikationstechnik des Bundes ergeben können,

und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen. Im Falle der Bestätigung des Verdachts ist die weitere Verarbeitung personenbezogener Daten zulässig, soweit dies erforderlich ist

1. zur Abwehr des Schadprogramms der sonstigen erheblichen Gefahren für die Kommunikationstechnik des Bundes,
2. zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen, oder
3. zur Erkennung und Abwehr anderer Schadprogramme oder Gefahren für die Kommunikationstechnik des Bundes.

Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. Es dürfen die erforderlichen technischen Maßnahmen getroffen werden, um eine sonstige erhebliche Gefahr für die Kommunikationstechnik des Bundes zu beseitigen. Das Bundesamt kann die Daten an die betroffene Einrichtung der Bundesverwaltung übermitteln, soweit dies für eine Verwendung nach den Sätzen 1 bis 4 erforderlich ist. Die nicht automatisierte Verwendung der Daten nach den Sätzen 1 und 2 darf nur durch einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet werden. Die Anordnung nach Satz 4 muss die daraus erwachsenden Übermittlungsbefugnisse nach Absatz 6 berücksichtigen.

(5) Die Beteiligten des Kommunikationsvorgangs sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder seiner Wirkungen oder von sonstigen erheblichen Gefahren für die Kommunikationstechnik des Bundes, die von einem Schadprogramm ausgehen, zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen. Die Unterrichtung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde und wenn anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. Das Bundesamt legt Fälle, in denen es von einer Benachrichtigung absieht, dem behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem weiteren Bediensteten des Bundesamtes, der die Befähigung zum Richteramt hat, zur Kontrolle vor. Wenn der behördliche Datenschutzbeauftragte der Entscheidung des Bundesamtes widerspricht, ist die Benachrichtigung nachzuholen. Die Entscheidung über die Nichtbenachrichtigung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach zwölf Monaten zu löschen. In den Fällen der Absätze 6 und 7 erfolgt die Benachrichtigung durch die dort genannten Behörden in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. Enthalten diese Vorschriften keine Bestimmungen zu Benachrichtigungspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.

(6) Das Bundesamt kann die nach Absatz 4 verwendeten personenbezogenen Daten an die Strafverfolgungsbehörden zur Verfolgung einer mittels eines Schadprogramms oder im Rahmen einer sonstigen erheblichen Gefahr für die Kommunikationstechnik des Bundes begangenen Straftat nach den §§ 202a, 202b, 303a oder 303b des Strafgesetzbuches übermitteln. Es kann diese Daten ferner übermitteln

1. an die Polizeien des Bundes und der Länder zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht,
2. an das Bundesamt für Verfassungsschutz zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht erkennen lassen, sowie an den Militärischen Abschirmdienst, wenn sich diese Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministeriums der Verteidigung richten,
3. an den Bundesnachrichtendienst zur Unterrichtung über Tatsachen, die einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbarer schädlich wirkender informationstechnischer Mittel auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland erkennen lassen.

(7) Für sonstige Zwecke kann das Bundesamt die Daten nach Absatz 4 Satz 1 übermitteln

1. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Absatz 2 der Strafprozessordnung bezeichneten Straftat,
2. an die Polizeien des Bundes und der Länder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist,
3. an die Verfassungsschutzbehörden des Bundes und der Länder sowie an den Militärischen Abschirmdienst, wenn tatsächliche Anhaltspunkte für Bestrebungen in der Bundesrepublik Deutschland vorliegen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Absatz 1 des Bundesverfassungsschutzgesetzes oder § 1 Absatz 1 des MAD-Gesetzes genannten Schutzgüter gerichtet sind,
4. an den Bundesnachrichtendienst, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Straftaten nach § 3 Absatz 1 Nummer 8 des Artikel 10-Gesetzes plant, begeht oder begangen hat und dies von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland ist,

Die Übermittlung nach Satz 1 Nummer 1 und 2 bedarf der vorherigen gerichtlichen Zustimmung. Für das Verfahren nach Satz 1 Nummer 1 und 2 gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Zuständig ist das Amtsgericht, in dessen Bezirk das Bundesamt seinen Sitz hat. Die Übermittlung nach Satz 1 Nummer 3 und 4 erfolgt nach Anordnung des Bundesministeriums des Innern und für Heimat; die §§ 9 bis 16 des Artikel 10-Gesetzes gelten entsprechend.

(8) Eine über die vorstehenden Absätze hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an Dritte sind unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden aufgrund der Maßnahmen der Absätze 1 bis 4 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 erlangt, dürfen diese Erkenntnisse und Daten nicht verwendet werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. Dies gilt auch in Zweifelsfällen. Die Tatsache der Erlangung und Löschung dieser Erkenntnisse ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr folgt, in dem die der Dokumentation erstellt worden ist. Werden im Rahmen der Absätze 5 oder 6 Inhalte oder Umstände der Kommunikation von in § 53 Absatz 1 Satz 1 der Strafprozessordnung genannten Personen übermittelt, auf die sich das Zeugnisverweigerungsrecht dieser Personen erstreckt, ist die Verwertung dieser Daten zu Beweiszwecken in einem Strafverfahren nur insoweit zulässig, als Gegenstand dieses Strafverfahrens eine Straftat ist, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht ist.

(9) Vor Aufnahme der Datenerhebung und -verwendung hat das Bundesamt ein Datenerhebungs- und -verwendungskonzept zu erstellen und für Kontrollen durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bereitzuhalten. Das Konzept hat dem besonderen Schutzbedürfnis der Regierungskommunikation Rechnung zu tragen. Die für die automatisierte Auswertung verwendeten Kriterien sind zu dokumentieren. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt das Ergebnis seiner Kontrollen nach § 16 des Bundesdatenschutzgesetzes auch den Ressorts mit.

(10) Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über

1. die Anzahl der Vorgänge, in denen Daten nach Absatz 6 Satz 1, Absatz 6 Satz 2 Nummer 1 oder Absatz 7 Nummer 1 übermittelt wurden, aufgegliedert nach den einzelnen Übermittlungsbefugnissen,
2. die Anzahl der personenbezogenen Auswertungen nach Absatz 4 Satz 1, in denen der Verdacht widerlegt wurde,
3. die Anzahl der Fälle, in denen das Bundesamt nach Absatz 5 Satz 2 oder 3 von einer Benachrichtigung der Betroffenen abgesehen hat.

(11) Das Bundesamt unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Ausschuss für Inneres und Heimat des Deutschen Bundestages über die Anwendung dieser Vorschrift.

§ 9

Verarbeitung von Protokollierungsdaten der Kommunikationstechnik des Bundes

(1) Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zum Betrieb der Kommunikationstechnik des Bundes erforderlich sind, Protokollierungsdaten, die durch den Betrieb von Kommunikationstechnik des Bundes anfallen, verarbeiten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen, Fehlern oder Sicherheitsvorfällen in der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist und Geheimschutzinteressen oder überwiegende Sicherheitsinteressen der betroffenen Stellen nicht entgegenstehen.

(2) Die Einrichtungen der Bundesverwaltung sind verpflichtet, das Bundesamt bei Maßnahmen nach Absatz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu einrichtungsinternen Protokollierungsdaten nach Absatz 1 sicherzustellen. Hierzu dürfen sie dem Bundesamt die entsprechenden Protokollierungsdaten übermitteln. § 8 Absatz 1 Satz 5, Absatz 2 bis 5, 9 und 10 gilt entsprechend. § 7 Absatz 7 gilt für die Verpflichtung nach Satz 1 entsprechend.

§ 10

Anordnungen von Maßnahmen zur Abwendung oder Behebung von Sicherheitsvorfällen

Das Bundesamt kann im Einzelfall gegenüber Einrichtungen der Bundesverwaltung Maßnahmen anordnen, die zur Abwendung oder Behebung eines gegenwärtigen Sicherheitsvorfalls erforderlich sind. Ferner kann das Bundesamt die Einrichtungen der Bundesverwaltung zur Berichterstattung innerhalb einer angemessenen Frist zu den nach Satz 1 angeordneten Maßnahmen auffordern. Der oder die jeweils zuständige Informationssicherheitsbeauftragte des Ressorts wird über Anweisungen und Aufforderungen nach den Sätzen 1 und 2 durch das Bundesamt informiert. Der Bericht ist dem Bundesamt und zugleich dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts zu übermitteln. Für die Berichterstattung gilt § 4 Absatz 3 entsprechend.

§ 11

Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Einrichtung der Bundesverwaltung oder einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Einrichtung oder des betroffenen Betreibers oder einer anderen für die Einrichtung oder den Betreiber zuständigen Behörde die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. Soweit das Bundesamt erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort ergreift, werden hierfür keine Gebühren oder Auslagen für die Tätigkeit des Bundesamtes erhoben. Hiervon unberührt bleiben etwaige Kosten für die Hinzuziehung qualifizierter Dritter.

(2) Ein herausgehobener Fall nach Absatz 1 liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder wenn die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichem Interesse ist.

(3) Das Bundesamt darf bei Maßnahmen nach Absatz 1 personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten verarbeiten, soweit dies zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich und angemessen ist. Die Daten sind unverzüglich zu

löschen, sobald sie für die Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems nicht mehr benötigt werden. Wenn die Daten in Fällen des Absatzes 4 an eine andere Behörde zur Erfüllung von deren gesetzlichen Aufgaben weitergegeben worden sind, darf das Bundesamt die Daten abweichend von Satz 2 bis zur Beendigung der Unterstützung dieser Behörden weiterverarbeiten. Eine Nutzung zu anderen Zwecken ist unzulässig. § 8 Absatz 8 ist entsprechend anzuwenden.

(4) Das Bundesamt darf Informationen, von denen es im Rahmen dieser Vorschrift Kenntnis erlangt, nur mit Einwilligung des Ersuchenden weitergeben, es sei denn, die Informationen lassen keine Rückschlüsse auf die Identität des Ersuchenden zu oder die Informationen können entsprechend § 8 Absatz 6 und 7 übermittelt werden. Hiervon sind erforderliche Informationsaustausche zwischen dem Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe nach § 3 Absatz 7 des Dachgesetzes zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz) ausgenommen. Zugang zu den in Verfahren nach Absatz 1 geführten Akten wird Dritten nicht gewährt.

(5) Das Bundesamt kann sich bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden der Hilfe qualifizierter Dritter bedienen, wenn dies zur rechtzeitigen oder vollständigen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich ist. Die hierdurch entstehenden Kosten hat der Ersuchende zu tragen. Das Bundesamt kann den Ersuchenden auch auf qualifizierte Dritte verweisen. Das Bundesamt und vom Ersuchenden oder vom Bundesamt nach Satz 1 beauftragte Dritte können einander bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden Daten übermitteln. Hierfür gilt Absatz 3 entsprechend.

(6) Soweit es zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems erforderlich ist, kann das Bundesamt vom Hersteller des informationstechnischen Systems verlangen, an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken.

(7) In begründeten Einzelfällen kann das Bundesamt auch bei anderen als den in Absatz 1 genannten Einrichtungen tätig werden, wenn das Bundesamt darum ersucht wurde und wenn es sich um einen herausgehobenen Fall nach Absatz 2 handelt. Ein begründeter Einzelfall liegt in der Regel vor, wenn eine Stelle eines Landes betroffen ist.

(8) Im Falle von Anlagen oder Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, ist in Fällen der Absätze 1, 4, 5 und 7 vor Tätigwerden des Bundesamtes das Benehmen mit den zuständigen atomrechtlichen Aufsichtsbehörden des Bundes und der Länder herzustellen. Im Falle von Anlagen oder Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, haben bei Maßnahmen des Bundesamtes nach diesem § 11 die Vorgaben aufgrund des Atomgesetzes Vorrang.

§ 12

Bestandsdatenauskunft

(1) Das Bundesamt darf zur Erfüllung seiner gesetzlichen Aufgabe nach § 3 Absatz 1 Satz 1 Nummer 1, 2, 20, 24 oder 25 von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, über Bestandsdaten gemäß § 3 Nummer 6 des Telekommunikationsgesetzes und über die nach § 172 des Telekommunikationsgesetzes erhobenen Daten (§ 174 Absatz 1 Satz 1 des Telekommunikationsgesetzes) Auskunft verlangen. Die Auskunft nach Satz 1 darf nur verlangt werden zum Schutz der Versorgung der Bevölkerung in den Sektoren des § 2 Nummer 24 oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme einer besonders wichtigen Einrichtung oder wichtigen Einrichtung abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und wenn die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um die Betroffenen nach Absatz 4 vor dieser Beeinträchtigung zu warnen, über diese Beeinträchtigung zu informieren oder bei der Beseitigung zu beraten oder zu unterstützen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 174 Absatz 1 Satz 3, § 177 Absatz 1 Nummer 3 des Telekommunika-

tionsgesetzes). Die rechtlichen und tatsächlichen Grundlagen des Auskunftsverlangens sind aktenkundig zu machen.

(3) Der auf Grund eines Auskunftsverlangens Verpflichtete hat die zur Auskunftserteilung erforderlichen Daten unverzüglich und vollständig zu übermitteln.

(4) Nach erfolgter Auskunft weist das Bundesamt die besonders wichtige Einrichtung oder die wichtige Einrichtung auf die bei ihr drohenden Beeinträchtigungen hin. Nach Möglichkeit weist das Bundesamt die besonders wichtige Einrichtung oder die wichtige Einrichtung auf technische Mittel hin, mittels derer die festgestellten Beeinträchtigungen durch die besonders wichtige Einrichtung oder die wichtige Einrichtung selbst beseitigt werden können.

(5) Das Bundesamt kann personenbezogene Daten, die es im Rahmen dieser Vorschrift verarbeitet, entsprechend § 8 Absatz 6 und 7 übermitteln.

(6) In den Fällen des Absatzes 2 ist die betroffene Person über die Auskunft zu benachrichtigen. Im Falle der Weitergabe der Information nach § 8 Absatz 6 oder wenn Tatsachen die Annahme rechtfertigen, dass die Voraussetzungen einer Weitergabe nach § 8 Absatz 6 vorliegen, ergeht darüber keine Benachrichtigung an die betroffene Person, sofern und solange überwiegende schutzwürdige Belange Dritter entgegenstehen. Wird nach Satz 2 die Benachrichtigung zurückgestellt oder wird von ihr abgesehen, sind die Gründe aktenkundig zu machen.

(7) Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über

1. die Gesamtzahl der Vorgänge, in denen Daten nach Absatz 1 oder Absatz 2 an das Bundesamt übermittelt wurden, und
2. die Übermittlungen nach Absatz 5.

(8) Das Bundesamt hat den Verpflichteten für ihm erteilte Auskünfte eine Entschädigung zu gewähren. Der Umfang der Entschädigung bemisst sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes; die Vorschriften über die Verjährung in § 2 Absatz 1 und 4 des Justizvergütungs- und -entschädigungsgesetzes finden entsprechende Anwendung.

§ 13

Warnungen

(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 20 und 21 kann das Bundesamt

1. die folgenden Warnungen und Informationen an die Öffentlichkeit oder an die betroffenen Kreise richten:
   a) Warnungen vor Schwachstellen und anderen Sicherheitsrisiken in informationstechnischen Produkten und Diensten,
   b) Warnungen vor Schadprogrammen,
   c) Warnungen bei einem Verlust oder einem unerlaubten Zugriff auf Daten,
   d) Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten und
   e) Informationen über Verstöße besonders wichtiger Einrichtungen oder wichtiger Einrichtungen gegen die Pflichten aus diesem Gesetz sowie
2. Sicherheitsmaßnahmen und Einsatz bestimmter Sicherheitsprodukte empfehlen.

Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist.

(2) Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung der Warnungen zu informieren. Diese Informationspflicht besteht nicht,

1. wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet würde oder

2. wenn berechtigterweise davon ausgegangen werden kann, dass der Hersteller an einer vorherigen Benachrichtigung kein Interesse hat.

Soweit entdeckte Schwachstellen oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen einschränken. Kriterien für die Auswahl des zu warnenden Personenkreises nach Satz 3 sind insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers.

(3) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 20 und 21 kann das Bundesamt die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts und Dienstes

1. vor Schwachstellen in informationstechnischen Produkten und Diensten und vor Schadprogrammen warnen, wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik hiervon ausgehen, oder
2. Sicherheitsmaßnahmen sowie den Einsatz bestimmter informationstechnischer Produkte und Dienste empfehlen.

Stellen sich die an die Öffentlichkeit gegebenen Informationen im Nachhinein als falsch heraus oder stellen sich die zugrunde liegenden Umstände als unzutreffend wiedergegeben heraus, ist dies unverzüglich öffentlich bekannt zu machen. Warnungen nach Satz 1 sind sechs Monate nach der Veröffentlichung zu entfernen, wenn nicht weiterhin hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik bestehen. Wird eine Warnung nach Satz 3 nicht entfernt, so ist diese Entscheidung regelmäßig zu überprüfen.

§ 14

Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen

(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 20, 21, 24 oder 25 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es kann sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen.

(2) Soweit erforderlich, kann das Bundesamt für Untersuchungen nach Absatz 1 Satz 1 von Herstellern informationstechnischer Produkte und Systeme alle notwendigen Auskünfte, insbesondere auch zu technischen Details, verlangen. In dem Auskunftsverlangen gibt das Bundesamt die Rechtsgrundlage, den Zweck des Auskunftsverlangens und die benötigten Auskünfte an und legt eine angemessene Frist für die Übermittlung der Auskünfte fest. Das Auskunftsverlangen enthält ferner einen Hinweis auf die in § 65 vorgesehenen Sanktionen.

(3) Das Bundesamt gibt Auskünfte sowie die aus den Untersuchungen gewonnen Erkenntnisse unverzüglich an die zuständigen Aufsichtsbehörden des Bundes oder, sofern keine Aufsichtsbehörde vorhanden ist, an das jeweilige Ressort weiter, wenn Anhaltspunkte bestehen, dass diese sie zur Erfüllung ihrer Aufgaben benötigen.

(4) Die Auskünfte und die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 20, 21, 24 und 25 genutzt werden. Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 20, 21, 24 und 25 erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben. Von einer Gelegenheit zur Stellungnahme kann abgesehen werden, wenn die Erkenntnisse ohne erkennbaren Bezug zum Hersteller oder zu den untersuchten informationstechnischen Produkten und Systemen weitergegeben oder veröffentlicht werden.

(5) Kommt ein Hersteller der Aufforderung des Bundesamtes nach Absatz 2 Satz 1 nicht oder nur unzureichend nach, kann das Bundesamt hierüber die Öffentlichkeit informieren. Es kann hierbei den Namen des Herstellers sowie die Bezeichnung des betroffenen Produkts oder Systems angeben und darlegen, inwieweit der Hersteller seiner Auskunftspflicht nicht nachgekommen ist. Zuvor ist dem Hersteller mit angemessener Frist Gelegenheit zur Stellungnahme zu gewähren. § 13 Absatz 2 Satz 2 gilt entsprechend.

§ 15

Detektion von Angriffsmethoden und von Sicherheitsrisiken für die Netz- und IT-Sicherheit

(1) Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 20 oder 24 zur Detektion von bekannten Schwachstellen und anderen Sicherheitsrisiken bei Einrichtungen der Bundesverwaltung, bei besonders wichtigen Einrichtungen oder bei wichtigen Einrichtungen 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 entsprechenden Einrichtungen darum ersuchen.

Die dadurch gewonnenen Erkenntnisse dürfen nur zum Zweck der Information nach Absatz 2 verwendet werden. Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, sind diese unverzüglich zu löschen.

(2) Wird durch Abfragen gemäß Absatz 1 eine bekannte Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, informiert das Bundesamt darüber unverzüglich die für das informationstechnische 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.

(3) Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Anzahl der gemäß Absatz 1 durchgeführten Abfragen.

(4) Das Bundesamt legt der Bundesbeauftragten oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu den Abfragen nach Absatz 1 auf Anforderung eine Liste der geprüften Systeme der Einrichtungen der Bundesverwaltung, der besonders wichtigen Einrichtungen und der wichtigen Einrichtungen zur Kontrolle vor.

(5) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, die einem Angreifer einen erfolgreichen Angriff vortäuschen, um den Einsatz von Schadprogrammen oder andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf dabei die zur Auswertung der Funktionsweise der Schadprogramme und Angriffsmethoden erforderlichen Daten verarbeiten.

§ 16

Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von Telekommunikationsdiensten

(1) Zur Abwehr erheblicher Gefahren für die in Absatz 2 genannten Schutzgüter kann das Bundesamt anordnen, dass ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes (Anbieter von öffentlich zugänglichen Telekommunikationsdiensten) mit mehr als 100 000 Kunden

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 Einvernehmen mit der Bundesnetzagentur herzustellen. 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) 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.

(3) 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.

(4) Das Bundesamt darf Daten, die von einem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten nach Absatz 1 Satz 1 Nummer 1 und Absatz 3 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.

§ 17

Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von digitalen Diensten

Das Bundesamt kann in Einzelfällen zur Abwehr erheblicher Gefahren für informationstechnische Systeme einer Vielzahl von Nutzern, die von digitalen Diensten von Anbietern von digitalen Diensten nach § 2 Absatz 2 Nummer 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes ausgehen, die durch ungenügende technische und organisatorische Vorkehrungen nach § 19 Absatz 4 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes unzureichend gesichert sind und dadurch keinen hinreichenden Schutz bieten vor

1. unerlaubten Zugriffen auf die für diese digitalen Dienste genutzten technischen Einrichtungen oder
2. Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

gegenüber dem jeweiligen Anbieter von digitalen Diensten nach § 2 Absatz 2 Nummer 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes anordnen, dass dieser die jeweils zur Herstellung des ordnungsgemäßen Zustands seiner digitalen Dienste erforderlichen technischen und organisatorischen Maßnahmen ergreift, um den ordnungsgemäßen Zustand seiner digitalen Dienste herzustellen. Die Zuständigkeit der Aufsichtsbehörden der Länder bleibt im Übrigen unberührt.

§ 18

Anordnungen von Maßnahmen des Bundesamtes gegenüber Herstellern von IKT-Produkten

Soweit erforderlich, kann das Bundesamt von einem Hersteller, deren IKT-Produkte von erheblichen Sicherheitsvorfällen betroffen sind, die Mitwirkung an der Beseitigung oder Vermeidung erheblicher Sicherheitsvorfälle bei besonders wichtigen Einrichtungen und wichtigen Einrichtungen verlangen.

§ 19

Bereitstellung von IT-Sicherheitsprodukten

Die Bereitstellung von IT-Sicherheitsprodukten durch das Bundesamt nach § 3 Absatz 1 Satz 2 Nummer 15 erfolgt durch Eigenentwicklung oder nach Durchführung von Vergabeverfahren aufgrund einer entsprechenden Bedarfsfeststellung. IT-Sicherheitsprodukte können nur in begründeten Ausnahmefällen durch eine Eigenentwicklung des Bundesamtes zur Verfügung gestellt werden. Die Vorschriften des Vergaberechts und der Bundeshaushaltsordnung bleiben unberührt. Wenn das Bundesamt IT-Sicherheitsprodukte bereitstellt, können die Einrichtungen der Bundesverwaltung oder von ihnen beauftragte Dritte diese Produkte beim Bundesamt abrufen.

Kapitel 2

Datenverarbeitung

§ 20

Verarbeitung personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten durch das Bundesamt ist zulässig, wenn die Verarbeitung zur Erfüllung seiner im öffentlichen Interesse liegenden Aufgaben erforderlich ist.

(2) Die Verarbeitung personenbezogener Daten durch das Bundesamt zu anderen Zwecken als demjenigen, zu dem die Daten ursprünglich erhoben wurden, ist unbeschadet von Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 in der jeweils geltenden Fassung und von § 23 des Bundesdatenschutzgesetzes zulässig, wenn

1. die Verarbeitung erforderlich ist
   a) zur Sammlung, Auswertung oder Untersuchung von Informationen über Sicherheitsrisiken oder Sicherheitsvorkehrungen für die Informationstechnik oder
   b) zur Unterstützung, Beratung oder Warnung in Fragen der Sicherheit in der Informationstechnik und
2. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

(3) Eine Verarbeitung von besonderen Kategorien personenbezogener Daten durch das Bundesamt ist abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 und unbeschadet des § 22 Absatz 1 des Bundesdatenschutzgesetzes zulässig, wenn

1. die Verarbeitung erforderlich ist zur Abwehr einer erheblichen Gefahr für die Netz-, Daten- oder Informationssicherheit,
2. ein Ausschluss dieser Daten von der Verarbeitung die Erfüllung der Aufgaben des Bundesamtes unmöglich machen oder diese erheblich gefährden würde und
3. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss dieser Daten von der Verarbeitung überwiegt.

(4) Das Bundesamt sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes vor.

§ 21

Beschränkungen der Rechte der betroffenen Person

Für die Rechte der betroffenen Person gegenüber dem Bundesamt gelten ergänzend zu den in der Verordnung (EU) 2016/679 enthaltenen Ausnahmen die nachfolgenden Beschränkungen. Soweit dieses Gesetz keine oder geringere Beschränkungen der Rechte der betroffenen Person enthält, gelten für die Beschränkungen im Übrigen die Regelungen des Bundesdatenschutzgesetzes ergänzend.

§ 22

Informationspflicht bei Erhebung von personenbezogenen Daten

(1) Die Pflicht zur Information gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 13 Absatz 4 und Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, wenn

1. die Informationserteilung die ordnungsgemäße Erfüllung der in der Zuständigkeit des Bundesamtes liegenden Aufgaben gefährden würde oder
2. die Informationserteilung die öffentliche Sicherheit oder Ordnung oder die Gewährleistung der Netz- und Informationssicherheit auf sonstige Weise gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde

und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift das Bundesamt geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 13 Absatz 1 und 2 und Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Das Bundesamt hält schriftlich fest, aus welchen Gründen es von einer Information der betroffenen Person abgesehen hat.

§ 23

Auskunftsrecht der betroffenen Person

(1) Das Recht auf Auskunft gemäß Artikel 15 Absatz 1 und 2 der Verordnung (EU) 2016/679 besteht nicht, wenn und soweit

1. die Auskunftserteilung die ordnungsgemäße Erfüllung der Aufgaben gefährden würde, die in der Zuständigkeit des Bundesamtes liegen,
2. die Auskunftserteilung
   a) die öffentliche Sicherheit oder die Gewährleistung der Netz- und Informationssicherheit gefährden würde oder
   b) sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Auskunftserteilung strafrechtliche Ermittlungen oder die Verfolgung von Straftaten gefährden würde

und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.

(2) § 34 Absatz 2 bis 4 des Bundesdatenschutzgesetzes gilt entsprechend.

§ 24

Recht auf Berichtigung

(1) Das Recht der betroffenen Person auf Berichtigung und Vervollständigung gemäß Artikel 16 der Verordnung (EU) 2016/679 besteht nicht, wenn und soweit die Erfüllung der Rechte der betroffenen Person die ordnungsgemäße Erfüllung der in der Zuständigkeit des Bundesamtes liegenden Aufgaben gefährden würde und deswegen das Interesse der betroffenen Person an der Ausübung dieser Rechte zurücktreten muss.

(2) In den Fällen des Absatzes 1 hat die betroffene Person einen Anspruch darauf, den Daten für die Dauer der Verarbeitung eine Gegendarstellung beizufügen, sofern dies für eine faire und transparente Verarbeitung erforderlich ist.

§ 25

Recht auf Löschung

(1) Im Fall der nicht automatisierten Verarbeitung besteht die Pflicht des Bundesamtes zur Löschung personenbezogener Daten gemäß Artikel 17 Absatz 1 und 2 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 genannten Ausnahmen nicht, wenn

1. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und
2. das Interesse der betroffenen Person an der Löschung als gering anzusehen ist.

In diesem Fall tritt an die Stelle der Löschung eine Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679. Die Sätze 1 und 2 sind nicht anzuwenden, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

(2) Ist die Löschung lediglich für eine etwaige gerichtliche Überprüfung von Maßnahmen nach § 8 Absatz 4 zurückgestellt, dürfen die Daten ohne Einwilligung der betroffenen Person nur zu diesem Zweck verwendet werden. Sie sind für andere Zwecke in der Verarbeitung einzuschränken. § 8 Absatz 8 bleibt unberührt.

§ 26

Recht auf Einschränkung der Verarbeitung

Die Pflicht des Bundesamtes zur Einschränkung der Verarbeitung gemäß Artikel 18 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 besteht für die Dauer der Überprüfung der Richtigkeit der personenbezogenen Daten nicht, wenn

1. die Verarbeitung oder Weiterverarbeitung durch dieses Gesetz ausdrücklich geregelt ist oder
2. die Einschränkung der Verarbeitung die Abwehr von Gefahren für die Sicherheit in der Informationstechnik gefährden würde.

§ 27

Widerspruchsrecht

Das Recht der betroffenen Person auf Widerspruch gemäß Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 besteht nicht, wenn

1. an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder

2. eine Rechtsvorschrift das Bundesamt zur Verarbeitung verpflichtet.

Darüber hinaus darf das Bundesamt die personenbezogenen Daten ergänzend zu Artikel 21 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 so lange verarbeiten, bis das Bundesamt geprüft hat, ob zwingende schutzwürdige Gründe für die Verarbeitung bestehen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.

Teil 3

Sicherheit in der Informationstechnik von Einrichtungen

Kapitel 1

Anwendungsbereich

§ 28

Besonders wichtige Einrichtungen und wichtige Einrichtungen

(1) Als besonders wichtige Einrichtung gelten

1. Betreiber kritischer Anlagen,
2. qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter,
3. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die
   a) mindestens 50 Mitarbeiter beschäftigen oder
   b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen,
4. sonstige natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten, die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen sind und die
   a) mindestens 250 Mitarbeiter beschäftigen oder
   b) einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen.

Davon ausgenommen sind Einrichtungen der Bundesverwaltung, sofern sie nicht gleichzeitig Betreiber kritischer Anlagen sind.

(2) Als wichtige Einrichtungen gelten

1. Vertrauensdiensteanbieter,
2. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die
   a) weniger als 50 Mitarbeiter beschäftigen und
   b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen,

3. natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet, die einer der in den Anlagen 1 und 2 bestimmten Einrichtungsarten zuzuordnen sind und die

   a) mindestens 50 Mitarbeiter beschäftigen oder

   b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen.

Davon ausgenommen sind besonders wichtige Einrichtungen und Einrichtungen der Bundesverwaltung.

(3) Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nach den Absätzen 1 und 2 ist auf

1. die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen und
2. außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft die Empfehlung der Kommission 2003/361/EG vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20. Mai 2003, S. 36) mit Ausnahme von Artikel 3 Absatz 4 des Anhangs anzuwenden.

Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung der Kommission 2003/361/EG sind nicht hinzuzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse unabhängig von seinen Partner- oder verbundenen Unternehmen ist.

(4) Die §§ 30, 31, 32, 35, 36, 38, 39, 61 und 62 sind nicht anzuwenden auf besonders wichtige Einrichtungen und wichtige Einrichtungen, die

1. ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,
2. Energieversorgungsnetze oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 1 des Gesetzes vom 14. Mai 2024 (BGBl. 2024 I Nr. 161) geändert worden ist, betreiben und den Regelungen des § 5c des Energiewirtschaftsgesetzes unterliegen.

Satz 1 gilt nicht für die dort aufgeführten besonders wichtigen und wichtigen Einrichtungen, soweit sie über die in Satz 1 Nummer 1 und 2 genannten Anlagen hinaus weitere kritische Anlagen nach § 2 Nummer 22 betreiben oder aufgrund weiterer Tätigkeiten einer der in Anlage 1 oder 2 bestimmten Einrichtungsarten zuzuordnen sind. Satz 2 gilt für alle informationstechnischen Systeme, die für den Betrieb der weiteren kritischen Anlagen erforderlich sind.

(5) Die §§ 30, 31, 32, 35, 36, 38 und 39 gelten nicht für

1. Finanzunternehmen nach Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 und Unternehmen, für die die Anforderungen der Verordnung (EU) 2022/2554 auf Grund von § 1a Absatz 2 des Kreditwesengesetzes oder § 293 Absatz 5 des Versicherungsaufsichtsgesetzes gelten,
2. die Gesellschaft für Telematik nach § 306 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch, Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 311 Absatz 6 und § 325 des Fünften Buches Sozialgesetzbuch zugelassenen Dienste und Betreiber von Diensten, soweit sie die Telematikinfrastruktur für nach § 327 Absatz 2 bis 5 des Fünften Buches Sozialgesetzbuch bestätigte Anwendungen nutzen.

(6) § 32 gilt nicht für Betreiber kritischer Anlagen, soweit sie eine Anlage für Unternehmen nach Absatz 5 Nummer 1 betreiben.

(7) Ein Betreiber kritischer Anlagen ist eine natürliche oder juristische Person oder eine rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine oder mehrere kritische Anlagen ausübt. Abweichend von Satz 1 hat im Sektor Finanzwesen bestimmenden Einfluss auf eine Anlage, wer die tatsächliche Sachherrschaft ausübt. Die rechtlichen und wirtschaftlichen Umstände bleiben insoweit unberücksichtigt.

(8) Dieses Gesetz findet keine Anwendung auf rechtlich unselbstständige Organisationseinheiten von Gebietskörperschaften und auf juristische Personen, an denen ausschließlich Gebietskörperschaften, ausgenommen der Bund, beteiligt sind, wenn sie

1. zu dem Zweck errichtet wurden, im öffentlichen Auftrag Leistungen für Verwaltungen zu erbringen, und
2. durch vergleichbare landesrechtliche Vorschriften unter Bezugnahme auf diesen Absatz reguliert werden.

§ 29

Einrichtungen der Bundesverwaltung

(1) Einrichtungen der Bundesverwaltung im Sinne dieses Gesetzes sind, mit Ausnahme der Institutionen der Sozialen Sicherung und der Bundesbank,

1. Bundesbehörden,
2. öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung sowie
3. weitere Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen, ungeachtet ihrer Rechtsform, auf Bundesebene, soweit durch das Bundesamt im Einvernehmen mit dem jeweils zuständigen Ressort angeordnet.

(2) 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.

(3) Die Geschäftsbereiche des Auswärtigen Amts und des Bundesministeriums der Verteidigung sowie des Bundesnachrichtendienstes und des Bundesamtes für Verfassungsschutz sind zusätzlich zu den Regelungen gemäß Absatz 2 Satz 2 von den Regelungen des § 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 eine allgemeine Verwaltungsvorschrift, um die Ziele der NIS-2-Richtlinie im Geschäftsbereich des Auswärtigen Amts durch ergebnisäquivalente Maßnahmen umzusetzen.

Kapitel 2

Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten

§ 30

Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die nach Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen nach Satz 1 sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

(3) Der von der Europäischen Kommission gemäß Artikel 21 Absatz 5 Unterabsatz 1 der NIS-2-Richtlinie erlassene Durchführungsrechtsakt zur Festlegung der technischen und methodischen Anforderungen an die in Absatz 1 genannten Maßnahmen in Bezug auf DNS-Diensteanbieter, Top Level Domain Name Registries, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter hat für die vorgenannten Einrichtungsarten Vorrang.

(4) Sofern die Europäische Kommission einen Durchführungsrechtsakt gemäß Artikel 21 Absatz 5 Unterabsatz 2 der NIS-2-Richtlinie erlässt, in dem die technischen und methodischen Anforderungen sowie erforderlichenfalls die sektoralen Anforderungen der in Absatz 2 genannten Maßnahmen festgelegt werden, so gehen diese Anforderungen den in Absatz 2 genannten Maßnahmen vor, soweit sie diesen entgegenstehen.

(5) Sofern die Durchführungsrechtsakte der Europäischen Kommission nach Artikel 21 Absatz 5 der NIS-2-Richtlinie keine abschließenden Bestimmungen über die technischen und methodischen Anforderungen sowie erforderlichenfalls über die sektoralen Anforderungen an die in Absatz 2 genannten Maßnahmen in Bezug auf besonders wichtige Einrichtungen und wichtige Einrichtungen enthalten, können diese Bestimmungen vom Bundesministerium des Innern und für Heimat im Benehmen mit den jeweils betroffenen Ressorts durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, unter Berücksichtigung der möglichen Folgen unzureichender Maßnahmen sowie der Bedeutung bestimmter Einrichtungen präzisiert und erweitert werden.

(6) Besonders wichtige Einrichtungen und wichtige Einrichtung dürfen durch Rechtsverordnung nach § 56 Absatz 3 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden, wenn diese über eine Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen.

(7) Unbeschadet der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten dürfen der Austausch von Informationen nach § 6 oder die freiwillige Meldung nach § 5 nicht dazu führen, dass der meldenden Einrichtung zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte.

(8) Besonders wichtige Einrichtungen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Diese vorgeschlagenen Sicherheitsstandards müssen Durchführungsrechtsakte der Europäischen Kommission so berücksichtigen, dass sie nicht im Widerspruch zu den dort genannten Anforderungen stehen sowie darin enthaltende Vorgaben nicht unterschritten werden. Das Bundesamt stellt auf Antrag fest, ob die vorgeschlagenen Sicherheitsstandards branchenspezifisch und geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt

1. im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe;
2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes.

Im Sektor Gesundheitswesen ist, soweit keine zuständige Aufsichtsbehörde des Bundes besteht, abweichend von Satz 4 Nummer 2 das Benehmen mit dem Bundesministerium für Gesundheit herzustellen.

(9) Betreiber kritischer Anlagen können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach § 39 Absatz 1 vorschlagen. Absatz 8 Satz 2 bis 5 gelten entsprechend.

§ 31

Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

(1) Für Betreiber kritischer Anlagen gelten für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, im Vergleich zu anderen informationstechnischen Systemen, Komponenten und Prozessen besonders wichtiger Einrichtungen auch über das Schutzniveau dieser Einrichtungen hinausgehende Maßnahmen nach § 30 Absatz 1 Satz 1 als verhältnismäßig, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht.

(2) Betreiber kritischer Anlagen sind verpflichtet, Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Dabei soll der Stand der Technik eingehalten werden. Der hierfür erforderliche Aufwand soll nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen.

§ 32

Meldepflichten

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, folgende Informationen an eine vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete gemeinsame Meldestelle zu melden:

1. unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;
2. unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Meldung über diesen Sicherheitsvorfall, in der die in Nummer 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;
3. auf Ersuchen des Bundesamtes eine Zwischenmeldung über relevante Statusaktualisierungen;
4. spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Nummer 2, vorbehaltlich Absatz 2, eine Abschlussmeldung, die Folgendes enthält:

a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;

b) Angaben zur Art der Bedrohung beziehungsweise ihrer zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;

c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;

d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

Die Verpflichtung nach Satz 1 gilt frühestens ab Einrichtung des Meldewegs.

(2) Dauert der Sicherheitsvorfall zum im Absatz 1 Nummer 4 genannten Zeitpunkt noch an, legt die betreffende Einrichtung statt einer Abschlussmeldung zu diesem Zeitpunkt eine Fortschrittsmeldung vor. Die Abschlussmeldung ist dem Bundesamt nach abschließender Bearbeitung des Sicherheitsvorfalls durch die betreffende Einrichtung vorzulegen.

(3) Betreiber kritischer Anlagen sind zusätzlich verpflichtet, Angaben zur Art der betroffenen Anlage und der kritischen Dienstleistung sowie zu den Auswirkungen des Sicherheitsvorfalls auf diese Dienstleistung zu übermitteln, wenn ein erheblicher Sicherheitsvorfall Auswirkungen auf die von ihnen betriebene kritische Anlage hat oder haben könnte.

(4) Das Bundesamt legt die Einzelheiten zur Ausgestaltung des Meldeverfahrens und zur Konkretisierung der Meldungsinhalte nach Anhörung der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe fest, soweit sie möglichen Durchführungsrechtsakten der Europäischen Kommission nicht widersprechen. Die Informationen nach Satz 1 werden durch das Bundesamt auf dessen Internetseite veröffentlicht.

(5) Das Bundesamt stellt den zuständigen Aufsichtsbehörden des Bundes unverzüglich die bei ihm eingegangenen Meldungen zur Verfügung.

(6) Das Bundesamt kann meldenden Einrichtungen nach Maßgabe des § 36 Absatz 1 Angebote zu deren Unterstützung bei der Behebung des Sicherheitsvorfalls machen.

§ 33

Registrierungspflicht

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sowie Domain-Name-Registry-Dienstanbieter sind verpflichtet, spätestens drei Monate, nachdem sie erstmals oder erneut als eine der vorgenannten Einrichtungen gelten oder Domain-Name-Registry-Dienste anbieten, dem Bundesamt über eine gemeinsam vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit folgenden Angaben zu übermitteln:

1. Name der Einrichtung, einschließlich der Rechtsform und falls einschlägig der Handelsregisternummer,
2. Anschrift und aktuelle Kontaktdaten, einschließlich E-Mail-Adresse, öffentliche IP-Adressbereiche und Telefonnummern,
3. relevanter in Anlage 1 oder 2 genannter Sektor oder, falls einschlägig, Branche,
4. Auflistung derjenigen Mitgliedstaaten der Europäischen Union, in denen die Einrichtung Dienste der in Anlage 1 oder 2 genannten Einrichtungsarten erbringt, und
5. die für die Tätigkeiten, aufgrund derer die Registrierung erfolgt, zuständigen Aufsichtsbehörden des Bundes und der Länder.

(2) Betreiber kritischer Anlagen übermitteln mit den Angaben nach Absatz 1 die kritische Dienstleistung, die öffentlichen IP-Adressbereiche der von ihnen betriebenen Anlagen sowie die für die von ihnen betriebenen kritischen Anlagen ermittelte Anlagenkategorie und ermittelte 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.

(3) Die Registrierung von besonders wichtigen Einrichtungen und wichtigen Einrichtungen und Domain-Name-Registry-Diensteanbietern kann das Bundesamt im Einvernehmen mit den jeweils zuständigen Aufsichtsbehörden auch selbst vornehmen, wenn ihre Pflicht zur Registrierung nicht erfüllt wird.

(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.

(5) Bei Änderungen der nach Absatz 1 oder 2 zu übermittelnden Angaben sind dem Bundesamt geänderte Versorgungskennzahlen 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.

(6) Das Bundesamt legt die Einzelheiten zur Ausgestaltung des Registrierungsverfahrens im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe fest. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamtes.

§ 34

Besondere Registrierungspflicht für bestimmte Einrichtungsarten

(1) Eine Einrichtung der in § 60 Absatz 1 Satz 1 genannten Einrichtungsart ist verpflichtet, spätestens drei Monate, nachdem sie als eine der vorgenannten Einrichtungen gelten, dem Bundesamt die folgenden Angaben zu übermitteln:

1. Name der Einrichtung;
2. einschlägiger Sektor, Branche und Einrichtungsart wie in Anlage 1 bestimmt;
3. Anschrift der Hauptniederlassung in der Europäischen Union nach § 60 Absatz 2 und ihrer sonstigen Niederlassungen in der Europäischen Union oder, falls er nicht in der Europäischen Union niedergelassen ist, Anschrift seines nach § 60 Absatz 3 benannten Vertreters;
4. aktuelle Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern der Einrichtung und soweit erforderlich, ihres nach § 60 Absatz 3 benannten Vertreters;
5. die Mitgliedstaaten der Europäischen Union, in denen die Einrichtung Dienste erbringt, und
6. die öffentlichen IP-Adressbereiche der Einrichtung.

(2) Im Fall einer Änderung der gemäß Absatz 1 übermittelten Angaben unterrichten die Einrichtungen der in § 60 Absatz 1 Satz 1 genannten Einrichtungsart das Bundesamt unverzüglich über diese Änderung, jedoch spätestens innerhalb von drei Monaten ab dem Tag, an dem die Änderung eingetreten ist.

(3) Mit Ausnahme der in Absatz 1 Nummer 6 genannten Angaben leitet das Bundesamt die nach diesem § 34 übermittelten Angaben an die Agentur der Europäischen Union für Cybersicherheit weiter.

(4) Das Bundesamt kann für die Übermittlung der Angaben nach den Absätzen 1 und 2 einen geeigneten Meldeweg vorsehen.

§ 35

Unterrichtungspflichten

(1) Im Fall eines erheblichen Sicherheitsvorfalls kann das Bundesamt besonders wichtigen Einrichtungen und wichtigen Einrichtungen anordnen, die Empfänger ihrer Dienste unverzüglich über diesen erheblichen Sicherheitsvorfall zu unterrichten, der die Erbringung des jeweiligen Dienstes beeinträchtigen könnte. Das Bundesamt setzt die für die Einrichtung zuständige Aufsichtsbehörde des Bundes über Anweisungen nach Satz 1 in

Kenntnis. Die Unterrichtung nach Satz 1 kann auch durch eine Veröffentlichung auf der Internetseite der Einrichtung erfolgen.

(2) Einrichtungen nach Absatz 1 Satz 1 aus den Sektoren Finanzwesen, Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende, digitale Infrastruktur, Verwaltung von IKT-Diensten und Digitale Dienste teilen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste und dem Bundesamt unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mit, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen informieren zugleich diese Empfänger auch über die erhebliche Cyberbedrohung selbst. Die Pflichten nach Satz 1 oder 2 gelten nur dann, wenn in Abwägung der Interessen der Einrichtung und des Empfängers die Interessen des Empfängers überwiegen.

§ 36

Rückmeldungen des Bundesamtes gegenüber meldenden Einrichtungen

(1) Im Fall einer Meldung einer Einrichtung gemäß § 32 übermittelt das Bundesamt dieser unverzüglich und nach Möglichkeit innerhalb von 24 Stunden eine Bestätigung über den Eingang der Meldung und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operative Beratung zu Abhilfemaßnahmen. Das Bundesamt kann auf Ersuchen der betreffenden Einrichtung zusätzliche technische Unterstützung leisten.

(2) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Sicherheitsvorfall zu verhindern oder zu bewältigen, oder liegt die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann das Bundesamt nach Anhörung der betreffenden Einrichtung diese dazu verpflichten, die Öffentlichkeit über den erheblichen Sicherheitsvorfall zu informieren. Das Bundesamt kann entsprechend der Voraussetzungen nach Satz 1 die Öffentlichkeit auch selbst informieren. Handelt es sich bei der betreffenden Einrichtung um eine Einrichtung der Bundesverwaltung, gilt für die Information der Öffentlichkeit § 4 Absatz 3 entsprechend.

§ 37

Ausnahmebescheid

(1) Das Bundesministerium des Innern und für Heimat kann auf Vorschlag des Bundeskanzleramts, des Bundesministeriums der Justiz, des Bundesministeriums der Verteidigung, des Bundesministeriums der Finanzen, der Ministerien für Inneres und Justiz der Länder oder auf eigenes Betreiben eine besonders wichtige Einrichtung oder eine wichtige Einrichtung von Verpflichtungen nach diesem Gesetz nach Maßgabe des Absatzes 2 teilweise befreien (einfacher Ausnahmebescheid) oder nach Maßgabe des Absatzes 3 insgesamt befreien (erweiterter Ausnahmebescheid), sofern die Einrichtung Vorgaben einhält, die den Verpflichtungen nach diesem Gesetz gleichwertig sind. Die Entscheidung nach Satz 1 erfolgt mit dem jeweils zuständigen Ministerium im Einvernehmen, im Fall der Ministerien für Inneres und Justiz der Länder im Benehmen.

(2) Einrichtungen, die

1. in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, (relevante Bereiche) tätig sind oder Dienste erbringen oder
2. ausschließlich für Behörden, die Aufgaben in relevanten Bereichen erfüllen, tätig sind oder Dienste erbringen,

können für diese Tätigkeiten oder Dienste von den Risikomanagementmaßnahmen nach § 30 und den Meldepflichten nach § 32 befreit werden. Die Sicherheit in der Informationstechnik dieser Einrichtungen muss in diesen Fällen anderweitig gewährleistet sein und beaufsichtigt werden.

(3) Einrichtungen, die ausschließlich in relevanten Bereichen tätig sind oder Dienste erbringen, können insgesamt von den in Absatz 2 genannten Pflichten und von den Registrierungspflichten nach § 33 und § 34 befreit werden. Absatz 2 Satz 2 gilt entsprechend.

(4) Die Absätze 1 bis 3 gelten nicht, wenn die betreffende Einrichtung ein Vertrauensdiensteanbieter ist.

(5) Ein Ausnahmebescheid nach diesem Gesetz ist zu widerrufen, wenn nachträglich Tatsachen eintreten, die zur Ablehnung einer Erteilung einer Ausnahme hätten führen müssen. Abweichend von Satz 1 kann im Falle eines vorübergehenden Wegfalls der Voraussetzungen des Absatzes 2 Nummer 1 oder 2 von einem Widerruf abgesehen werden.

§ 38

Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.

(2) Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.

(3) Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

§ 39

Nachweispflichten für Betreiber kritischer Anlagen

(1) Betreiber kritischer Anlagen haben die Umsetzung der Maßnahmen nach § 30 Absatz 1 Satz 1 in Verbindung mit § 31 Absatz 1 und 2 Satz 1 zu einem vom Bundesamt im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe festgelegten Zeitpunkt, frühestens drei Jahre nachdem sie erstmals oder spätestens drei Jahre nachdem sie erneut als ein Betreiber einer kritischen Anlage gelten, und anschließend alle drei Jahre dem Bundesamt durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachzuweisen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich Angaben über die dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln die Vorlage eines geeigneten Mängelbeseitigungsplanes und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen. Das Bundesamt kann die Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen.

(2) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Prüfungen und Erbringung der Nachweise nach Absatz 1 folgende Anforderungen festlegen:

1. Anforderungen an die Art und Weise der Durchführung,
2. Anforderungen an die Geeignetheit der zu erbringenden Nachweise sowie
3. nach Anhörung der betroffenen Betreiber und Einrichtungen und der betroffenen Wirtschaftsverbände fachliche und organisatorische Anforderungen an die prüfenden Stellen im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamtes.

(3) Abweichend von Absatz 1 Satz 1 legt das Bundesamt für Betreiber kritischer Anlagen, die bis zum Inkrafttreten dieses Gesetzes Betreiber Kritischer Infrastrukturen waren nach § 2 Absatz 10 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist, den Zeitpunkt der Nachweiserbringung auf frühestens drei Jahre nach Erbringung des letzten Nachweises nach § 8a Absatz 3 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist, fest.

§ 40

Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen

(1) Das Bundesamt ist die nationale Verbindungsstelle sowie die zentrale Melde- und Anlaufstelle für die Aufsicht für besonders wichtige Einrichtungen und wichtige Einrichtungen in der Sicherheit in der Informationstechnik.

(2) Zur Wahrnehmung seiner Aufgabe als nationale Verbindungsstelle koordiniert das Bundesamt

1. die grenzüberschreitende Zusammenarbeit der Länderbehörden, die die Länder als zuständige Behörden für die Aufsicht von Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene nach Artikel 2 Absatz 2 Buchstabe f Nummer ii der NIS-2-Richtlinie bestimmt haben, sowie der Bundesnetzagentur und der Bundesanstalt für Finanzdienstleistungsaufsicht mit den für die Überwachung der Anwendung der NIS-2-Richtlinie zuständigen Behörden anderer Mitgliedstaaten und gegebenenfalls mit der Europäischen Kommission und der Agentur der Europäischen Union für Cybersicherheit sowie
2. die sektorübergreifende Zusammenarbeit der in Nummer 1 genannten Länderbehörden, des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, der Bundesnetzagentur und der Bundesanstalt für Finanzdienstleistungsaufsicht.

(3) Zur Wahrnehmung seiner Aufgabe als zentrale Meldestelle hat das Bundesamt

1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen zu sammeln und auszuwerten, insbesondere Informationen zu Schwachstellen, zu Schadprogrammen und zu Angriffen,
2. die Relevanz dieser Informationen nach Nummer 1 für die Verfügbarkeit kritischer Dienstleistungen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zu analysieren,
3. das Lagebild bezüglich der Sicherheit in der Informationstechnik von kritischen Anlagen, besonders wichtigen Einrichtungen und wichtigen Einrichtungen kontinuierlich zu aktualisieren und
4. unverzüglich
   a) die Betreiber kritischer Anlagen über sie betreffende Informationen nach den Nummern 1 bis 3 nach § 33 Absatz 1 Nummer 2 zu unterrichten und
   b) die zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union über nach Absatz 5 oder nach vergleichbaren Regelungen gemeldete erhebliche Störungen, die Auswirkungen in diesem Mitgliedstaat haben, unter Berücksichtigung der Interessen nationaler Sicherheit und Verteidigung zu unterrichten und
   c) das Auswärtige Amt über nach § 32 Absatz 1 gemeldete erhebliche Sicherheitsvorfälle mit internationalem Bezug zu unterrichten und
   d) im Rahmen vorab zwischen dem Bundesamt und den Empfängern abgestimmter Prozesse zur Weitergabe und Wahrung der notwendigen Vertraulichkeit die zu diesem Zweck dem Bundesamt von den Ländern als zentrale Kontaktstellen benannten Behörden oder die zuständigen Behörden des Bundes über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen zu unterrichten.

(4) Zur Wahrnehmung seiner Aufgabe als zentrale Anlaufstelle hat das Bundesamt

1. Anfragen der in Absatz 2 genannten Stellen anzunehmen und an die zuständigen in Absatz 2 genannten Stellen weiterzuleiten,
2. Antworten auf die in Absatz 2 Nummer 2 genannten Anfragen zu erstellen und dabei die in Absatz 1 genannten Stellen zu beteiligen oder Antworten der in Absatz 2 genannten Stellen an die in Absatz 2 genannten Stellen weiterzuleiten, nach § 32 eingegangene Meldungen an zentrale Anlaufstellen der anderen betroffenen Mitgliedstaaten der Europäischen Union weiterzuleiten,
3. wenn ein erheblicher Sicherheitsvorfall zwei oder mehr Mitgliedstaaten der Europäischen Union betrifft, die anderen betroffenen Mitgliedstaaten und die Agentur der Europäischen Union für Cybersicherheit über den erheblichen Sicherheitsvorfall zu unterrichten, wobei die Art der gemäß § 32 Absatz 2 erhaltenen Informationen mitzuteilen und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen zu wahren ist.

(5) Während eines erheblichen Sicherheitsvorfalls gemäß § 32 Absatz 1 kann das Bundesamt im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes von den betroffenen Betreibern kritischer Anlagen die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen. Betreiber kritischer Anlagen sind befugt, dem Bundesamt auf Verlangen die zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten zu übermitteln, soweit dies zur Bewältigung eines erheblichen Sicherheitsvorfalls erforderlich ist.

(6) Soweit im Rahmen dieser Vorschrift personenbezogene Daten verarbeitet werden, ist eine über die vorstehenden Absätze hinausgehende Verarbeitung zu anderen Zwecken unzulässig. § 8 Absatz 8 Satz 3 bis 9 ist entsprechend anzuwenden.

§ 41

Untersagung des Einsatzes kritischer Komponenten

(1) Ein Betreiber kritischer Anlagen hat den geplanten erstmaligen Einsatz einer kritischen Komponente gemäß § 2 Nummer 23 dem Bundesministerium des Innern und für Heimat vor ihrem Einsatz anzuzeigen. In der Anzeige sind die kritische Komponente und die geplante Art ihres Einsatzes anzugeben. Satz 1 gilt für einen Betreiber kritischer Anlagen nicht, wenn dieser den Einsatz einer anderen kritischen Komponente desselben Typs für dieselbe Art des Einsatzes bereits nach Satz 1 angezeigt hat und ihm der Einsatz nicht untersagt wurde.

(2) Das Bundesministerium des Innern und für Heimat kann den geplanten erstmaligen Einsatz einer kritischen Komponente gegenüber dem Betreiber kritischer Anlagen im Benehmen mit den in § 56 Absatz 4 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt bis zum Ablauf von zwei Monaten nach Eingang der Anzeige nach Absatz 1 untersagen oder Anordnungen erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Bei der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit kann insbesondere berücksichtigt werden, ob

1. der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird,
2. der Hersteller bereits an Aktivitäten beteiligt war oder ist, die 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 hatten, oder
3. der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht.

Vor Ablauf der Frist von zwei Monaten nach Anzeige nach Absatz 1 ist der Einsatz nicht gestattet. Das Bundesministerium des Innern und für Heimat kann die Frist gegenüber der Einrichtung um weitere zwei Monate verlängern, wenn die Prüfung besondere Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist.

(3) Kritische Komponenten gemäß § 2 Nummer 23 dürfen nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber dem Betreiber der kritischen Anlage abgegeben hat. Die Garantieerklärung ist der Anzeige nach Absatz 1 beizufügen. Aus der Garantieerklärung muss hervorgehen, wie der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zweck von Sabotage, Spionage oder Terrorismus, auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Anlage einwirken zu können. Das Bundesministerium des Innern und für Heimat legt die Einzelheiten der Mindestanforderungen an die Garantieerklärung im Einvernehmen mit den in § 56 Absatz 4 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Die Einzelheiten der Mindestanforderungen an die Garantieerklärung müssen aus den Schutzzielen der Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit und Funktionsfähigkeit der kritischen Anlage folgen und die Vermeidung von Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere im Sinne von Absatz 2 Satz 2, adressieren, die aus der Sphäre des Herstellers der kritischen Komponente, insbesondere aus dessen Organisationsstruktur, stammen. Die Sätze 1 und 2 gelten erst ab der Bekanntmachung der Allgemeinverfügung nach Satz 4 und nicht für bereits vor diesem Zeitpunkt eingesetzte kritische Komponenten. Soweit Änderungen der Allgemeinverfügung erfolgen, sind diese für bereits nach diesem Absatz abgegebene Garantieerklärungen unbeachtlich.

(4) Das Bundesministerium des Innern und für Heimat kann den weiteren Einsatz einer kritischen Komponente gegenüber dem Betreiber kritischer Anlagen im Einvernehmen mit den in § 56 Absatz 4 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen oder Anordnungen erlassen, wenn der weitere Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt, insbesondere, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist. Absatz 2 Satz 2 gilt entsprechend.

(5) Ein Hersteller einer kritischen Komponente kann insbesondere dann nicht vertrauenswürdig sein, wenn hinreichende Anhaltspunkte dafür bestehen, dass

1. er gegen die in der Garantieerklärung eingegangen Verpflichtungen verstoßen hat,
2. in der Garantieerklärung angegebene Tatsachenbehauptungen unwahr sind,
3. er Sicherheitsüberprüfungen und Penetrationsanalysen an seinem Produkt und in der Produktionsumgebung nicht im erforderlichen Umfang in angemessener Weise unterstützt,
4. Schwachstellen oder Manipulationen an seinem Produkt nicht unverzüglich, nachdem er davon Kenntnis erlangt, beseitigt und dem Betreiber kritischer Anlagen meldet,
5. die kritische Komponente auf Grund von Mängeln ein erhöhtes Gefährdungspotenzial aufweist oder aufgewiesen hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Anlage einwirken zu können, oder
6. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die spezifisch geeignet sind oder waren, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Anlage einwirken zu können.

(6) Wurde nach Absatz 4 der weitere Einsatz einer kritischen Komponente untersagt, kann das Bundesministerium des Innern und für Heimat im Einvernehmen mit den in § 56 Absatz 4 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt

1. den geplanten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und
2. den weiteren Einsatz kritischer Komponenten desselben Typs und desselben Herstellers unter Einräumung einer angemessenen Frist untersagen.

(7) Bei schwerwiegenden Fällen nicht vorliegender Vertrauenswürdigkeit nach Absatz 5 kann das Bundesministerium des Innern und für Heimat den Einsatz aller kritischen Komponenten des Herstellers im Einvernehmen mit den in § 56 Absatz 4 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen.

§ 42

Auskunftsverlangen

Zugang zu den Informationen und Akten in Angelegenheiten nach Teil 2 (§§ 4 bis 10) und Teil 3 dieses Gesetzes wird nicht gewährt. Die Akteneinsichtsrechte von Verfahrensbeteiligten bleiben unberührt.

Kapitel 3

Informationssicherheit der Einrichtungen der Bundesverwaltung

§ 43

Informationssicherheitsmanagement

(1) Die Leitung der Einrichtung der Bundesverwaltung ist dafür verantwortlich, unter Berücksichtigung der Belange des IT-Betriebs die Voraussetzungen zur Gewährleistung der Informationssicherheit zu schaffen.

(2) Die Leitung der Einrichtung der Bundesverwaltung muss regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Informationssicherheit zu erlangen sowie die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

(3) Soweit öffentlich-rechtlich oder privatrechtlich organisierte Stellen mit Leistungen für Informationstechnik des Bundes beauftragt werden, ist vertraglich sicherzustellen, dass sie sich zur Einhaltung der Voraussetzungen zur Gewährleistung der Informationssicherheit verpflichten. Dies gilt auch für den Fall, dass Schnittstellen zur Kommunikationstechnik des Bundes eingerichtet werden. Die Pflichten der Leitung der Einrichtung der Bundesverwaltung nach Absatz 1 bleiben hiervon unberührt.

(4) Die Registrierung von Einrichtungen der Bundesverwaltung nach § 33 obliegt der Leitung der Einrichtung der Bundesverwaltung. Die Einrichtungen der Bundesverwaltung weisen dem Bundesamt die Erfüllung der Anforderungen nach Absatz 1 spätestens fünf Jahre nach Inkrafttreten dieses Gesetzes und anschließend regelmäßig nach seinen Vorgaben nach.

(5) Werden, über die sich aus § 32 ergebenden Meldepflichten hinaus, Einrichtungen der Bundesverwaltung Informationen nach § 4 Absatz 2 Nummer 1 bekannt, die für die Erfüllung von Aufgaben oder für die Sicherheit der Kommunikationstechnik des Bundes von Bedeutung sind, unterrichten die Einrichtungen der Bundesverwaltung das Bundesamt hierüber unverzüglich, soweit andere Vorschriften dem nicht entgegenstehen. Ausgenommen von den Meldepflichten für Einrichtungen der Bundesverwaltung nach § 32 sowie nach Satz 1 dieses Absatzes sind Informationen, die aufgrund von Regelungen zum Geheimschutz oder Vereinbarungen mit Dritten nicht weitergegeben werden dürfen oder deren Weitergabe im Widerspruch zu der verfassungsrechtlichen Stellung eines Abgeordneten des Bundestages oder eines Verfassungsorgans oder der gesetzlich geregelten Unabhängigkeit einzelner Stellen stünde. Die Einrichtungen der Bundesverwaltung melden dem Bundesamt kalenderjährlich jeweils bis zum 31. Januar eines Jahres die Gesamtzahl der nach Satz 2 nicht übermittelten Informationen. Ausgenommen von der Pflicht nach Absatz 5 Satz 3 sind der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz.

(6) Das Bundesministerium des Innern und für Heimat erlässt im Einvernehmen mit den Ressorts allgemeine Verwaltungsvorschriften zur Durchführung des Absatzes 5.

§ 44

Vorgaben des Bundesamtes

(1) Die Einrichtungen der Bundesverwaltung müssen 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. Die Mindeststandards werden vom Bundesamt im Benehmen mit den Ressorts und weiteren obersten Bundesbehörden festgelegt und auf der Internetseite des Bundesamtes veröffentlicht. Abweichungen von den Mindeststandards sind nur in sachlich gerechtfertigten Fällen zulässig, sie sind zu dokumentieren und zu begründen. Für die in § 2 Nummer 21 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach Satz 1 empfehlenden Charakter. Für die Verpflichtung nach Satz 1 gelten die Ausnahmen nach § 7 Absatz 6 und 7 entsprechend.

(2) Das Bundeskanzleramt und die Bundesministerien müssen als zusätzliche Mindestanforderungen die BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) in den jeweils geltenden Fassungen einhalten. Die jeweils geltenden Fassungen werden auf der Internetseite des Bundesamtes veröffentlicht. Der IT-Grundschutz wird 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 4 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.

(3) Durch die Umsetzung der Mindestanforderungen nach Absatz 1 Satz 1 und Absatz 2 Satz 1ist 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 und Absatz 2 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.

(4) Das Bundesamt berät die Einrichtungen der Bundesverwaltung auf Ersuchen bei der Umsetzung und Einhaltung der Mindestanforderungen nach Absatz 1 Satz 1 und Absatz 2 Satz 1, stellt Hilfsmittel zur Verfügung und unterstützt die Bereitstellung entsprechender Lösungen durch die IT-Dienstleister des Bundes über den gesamten Lebenszyklus.

(5) 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.

(6) Für die Einrichtungen der Bundesverwaltung kann das Bundesministerium des Innern und für Heimat 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.

§ 45

Informationssicherheitsbeauftragte der Einrichtungen der Bundesverwaltung

(1) Jede Leitung einer Einrichtung der Bundesverwaltung bestellt für ihre Einrichtung eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten und bestimmt mindestens eine zur Vertretung berechtigte Person.

(2) Für die Erfüllung ihrer Aufgaben ist eine zielgerichtete Befähigung der Informationssicherheitsbeauftragten der Einrichtungen der Bundesverwaltung notwendig. Die Informationssicherheitsbeauftragten der Einrichtungen sowie ihre Vertreter müssen die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde erwerben. Sie sowie ihre Vertreter unterstehen der Fachaufsicht des oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts.

(3) Die Informationssicherheitsbeauftragten der Einrichtungen der Bundesverwaltung sind für den Aufbau und die Aufrechterhaltung des Informationssicherheitsprozesses ihrer Einrichtung zuständig. Sie erstellen ein Informationssicherheitskonzept, das mindestens die Vorgaben des Bundesamtes nach § 44 Absatz 1 erfüllt. Sie wirken auf die operative Umsetzung des Informationssicherheitskonzepts hin und kontrollieren die Umsetzung innerhalb der Einrichtung. Die Informationssicherheitsbeauftragten beraten die Leitung der Einrichtung der Bundesverwaltung in allen Fragen der Informationssicherheit und unterrichten die Leitung der Einrichtung der Bundesverwaltung sowie den oder die jeweils zuständige Informationssicherheitsbeauftragte des Ressorts regelmäßig sowie anlassbezogen über ihre Tätigkeit, über den Stand der Informationssicherheit innerhalb der Einrichtung, über die Mittel- und Personalausstattung sowie über Sicherheitsvorfälle. Ihre Berichts- und Beratungsaufgaben erfüllen sie unabhängig und weisungsfrei.

(4) Die Informationssicherheitsbeauftragten der Einrichtungen sind bei allen Maßnahmen zu beteiligen, die die Informationssicherheit der Einrichtung betreffen. Sie haben ein unmittelbares Vortragsrecht bei der jeweiligen Leitung ihrer Einrichtung sowie bei dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts. Sie dürfen von ihrer jeweiligen Einrichtung wegen der Erfüllung ihrer Aufgaben nicht abberufen oder benachteiligt werden.

§ 46

Informationssicherheitsbeauftragte der Ressorts

(1) Die Leitungen der einzelnen Ressorts sowie die Leitungen weiterer oberster Bundesbehörden bestellen jeweils eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten des Ressorts, der oder dem unter Berücksichtigung der Belange des IT-Betriebs die Steuerung und Überwachung des Informationssicherheitsmanagements innerhalb des Ressorts beziehungsweise innerhalb der obersten Bundesbehörde und ihres Geschäftsbereichs obliegt, und bestimmen mindestens eine zur Vertretung berechtigte Person. Der oder die Informationssicherheitsbeauftragte des Ressorts wirkt auf die Umsetzung der Informationssicherheit in ihrem oder seinem Ressort hin.

(2) Für die Erfüllung ihrer Aufgaben ist eine zielgerichtete Befähigung der Informationssicherheitsbeauftragten der Ressorts notwendig. Der oder die Informationssicherheitsbeauftragte des Ressorts muss die zur Erfüllung seiner oder ihrer Aufgaben erforderliche Fachkunde erwerben.

(3) Die Informationssicherheitsbeauftragten der Ressorts koordinieren jeweils die Fortschreibung von Informationssicherheitsleitlinien für ihr Ressort. Sie unterrichten die Ressortleitung über ihre Tätigkeit und über den Stand der Informationssicherheit innerhalb des Ressorts, über die Mittel- und Personalausstattung sowie über Sicherheitsvorfälle. Ihre Berichts- und Beratungsaufgaben erfüllen sie unabhängig und weisungsfrei.

(4) In begründeten Einzelfällen kann der oder die Informationssicherheitsbeauftragte des Ressorts im Benehmen mit dem oder der jeweiligen IT-Beauftragten des Ressorts den Einsatz bestimmter IT-Produkte in Einrichtungen der Bundesverwaltung innerhalb des jeweiligen Ressorts ganz oder teilweise untersagen. Über eine Untersagung ist das Bundesamt zu unterrichten.

(5) Der oder die Informationssicherheitsbeauftragte des Ressorts kann im Benehmen mit dem Bundesamt Einrichtungen der Bundesverwaltung innerhalb des Ressorts von Verpflichtungen nach diesem Teil teilweise oder insgesamt durch Erteilung eines Ausnahmebescheides befreien. Voraussetzung hierfür ist, dass sachliche Gründe für die Erteilung eines Ausnahmebescheids vorliegen und durch die Befreiung keine nachteiligen Auswirkungen für die Informationssicherheit des Bundes zu befürchten sind. Über erteilte Ausnahmebescheide ist das Bundesamt zu unterrichten. Satz 1 gilt nicht, wenn die jeweilige Einrichtung der Bundesverwaltung die Voraussetzungen des § 28 Absatz 1 Satz 1 oder § 28 Absatz 2 Satz 1 erfüllt.

(6) Der oder die Informationssicherheitsbeauftragte des Ressorts ist bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben innerhalb des Ressorts zu beteiligen, soweit die Vorhaben Fragen der Informationssicherheit berühren. Er oder sie hat ein unmittelbares Vortragsrecht bei der jeweiligen Leitung des Ressorts. Sie dürfen von ihrer jeweiligen Einrichtung wegen der Erfüllung ihrer Aufgaben nicht abberufen oder benachteiligt werden.

§ 47

Wesentliche Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes

(1) Für die Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes sind eigene Informationssicherheitsbeauftragte nach § 45 zu bestellen.

(2) Digitalisierungsvorhaben oder Kommunikationsinfrastrukturen des Bundes sind insbesondere dann wesentlich, wenn dabei Kommunikationstechnik des Bundes ressortübergreifend betrieben wird oder der ressortübergreifenden Kommunikation oder dem ressortübergreifenden Datenaustausch dient.

(3) In der Regel bestellt diejenige Einrichtung den Informationssicherheitsbeauftragten nach Satz 1, die für die Steuerung des Digitalisierungsvorhabens oder der Kommunikationsinfrastrukturen des Bundes verantwortlich ist. Wenn bei ressortübergreifenden Digitalisierungsvorhaben oder Kommunikationsinfrastrukturen eine Bestellung durch Einrichtungen in verschiedenen beteiligten Ressorts und weiteren obersten Bundesbehörden in Betracht kommt und nicht innerhalb einer angemessenen Frist Einvernehmen darüber hergestellt werden kann, durch welche Einrichtung die Bestellung erfolgt, so entscheidet das Bundesministerium des Innern und für Heimat.

(4) Die Informationssicherheitsbeauftragten nach Satz 1 unterstehen entweder der Leitung der Einrichtung oder dem oder der jeweils zuständigen Informationssicherheitsbeauftragten des Ressorts.

(5) Zur Gewährleistung der Informationssicherheit bei der Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben soll die jeweils verantwortliche Einrichtung das Bundesamt frühzeitig beteiligen und dem Bundesamt Gelegenheit zur Stellungnahme geben.

§ 48

Amt des Koordinators für Informationssicherheit

Die Bundesregierung bestellt eine Koordinatorin oder einen Koordinator für Informationssicherheit.

Teil 4

Datenbanken der Domain-Name-Registrierungsdaten

§ 49

Pflicht zum Führen einer Datenbank

(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domain Name Systems zu leisten, haben Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister genaue und vollständige Domain-Namen-Registrierungsdaten in einer eigenen Datenbank mit der gebotenen Sorgfalt zu sammeln und zu pflegen.

(2) Die Datenbank hat die erforderlichen Angaben zu enthalten, anhand derer die Inhaber der Domain-Namen und die Kontaktstellen, die die Domain-Namen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können. Diese Angaben müssen Folgendes umfassen:

1. den Domain-Namen;

2. das Datum der Registrierung;
3. den Namen des Domain-Inhabers, seine E-Mail-Adresse und Telefonnummer;
4. die Kontakt-E-Mail-Adresse und die Telefonnummer der Anlaufstelle, die den Domain-Namen verwaltet, falls diese sich von denen des Domain-Inhabers unterscheiden.

(3) Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister haben Vorgaben und Verfahren, einschließlich Überprüfungsverfahren, vorzuhalten, mit denen sichergestellt wird, dass die Datenbank genaue und vollständige Angaben enthält. Sie haben diese Vorgaben und Verfahren bis zum … [*einfügen: Datum, drei Monate nach Inkrafttreten*] öffentlich zugänglich zu machen.

(4) Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister haben unverzüglich nach der Registrierung eines Domain-Namens die nicht personenbezogenen Domain-Namen-Registrierungsdaten öffentlich zugänglich zu machen.

(5) Das Bundesamt kann die Erfüllung der Vorgaben überprüfen.

§ 50

Verpflichtung zur Zugangsgewährung

(1) Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister haben einem berechtigten Zugangsnachfrager auf begründeten Antrag unter Darlegung eines berechtigten Interesses und soweit dies für die Erfüllung von deren Aufgaben erforderlich ist unverzüglich und in jedem Fall innerhalb von 72 Stunden nach Eingang des Antrags Zugang zu den Domain-Namen-Registrierungsdaten zu gewähren. Liegen die angefragten Informationen nicht vor, so ist dies innerhalb von 24 Stunden nach Eingang des Antrags auf Zugang mitzuteilen.

(2) Die Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister haben die Vorgaben und Verfahren im Hinblick auf die Offenlegung der Domain-Namen-Registrierungsdaten bis zum … [*einfügen: Datum, drei Monate nach Inkrafttreten*] öffentlich zugänglich zu machen.

(3) Das Auskunftsverfahren bei Bestandsdaten gemäß § 22 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes bleibt unberührt.

(4) Das Bundesamt kann die Erfüllung der Vorgaben überprüfen.

§ 51

Kooperationspflicht

Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister sind zur Kooperation verpflichtet, um die in den §§ 49 und 50 festgelegten Verpflichtungen zu erfüllen und insbesondere eine doppelte Erhebung von Domain-Namen-Registrierungsdaten vom Domaininhaber auszuschließen.

Teil 5

Zertifizierung, Konformitätserklärung und Kennzeichen

§ 52

Zertifizierung

(1) Das Bundesamt ist nationale Zertifizierungsstelle der Bundesverwaltung für IT-Sicherheit.

(2) Für bestimmte Produkte oder Leistungen kann beim Bundesamt eine Sicherheits- oder Personenzertifizierung oder eine Zertifizierung als IT-Sicherheitsdienstleister beantragt werden. Die Anträge werden in der zeitlichen Reihenfolge ihres Eingangs bearbeitet; hiervon kann abgewichen werden, wenn das Bundesamt wegen der Anzahl und des Umfangs anhängiger Prüfungsverfahren eine Prüfung in angemessener Zeit nicht durchführen kann und an der Erteilung eines Zertifikats ein öffentliches Interesse besteht. Der Antragsteller hat dem Bundesamt diejenigen Unterlagen vorzulegen und die Auskünfte zu erteilen, deren Kenntnis für die Prüfung und Bewertung der Produkte und Leistungen oder der Eignung der Person sowie für die Erteilung des Zertifikats erforderlich ist. Ein Zertifikat nach Satz 1 darf nur dann für ein Produkt, eine Leistung, eine Person oder einen IT-Sicherheitsdienstleister verwendet werden, wenn das Bundesamt ein entsprechendes Zertifikat erteilt hat und dieses nicht aufgehoben wurde oder auf andere Weise ungültig geworden ist.

(3) Die Prüfung und Bewertung können durch vom Bundesamt nach Absatz 7 anerkannte sachverständige Stellen erfolgen.

(4) Das Sicherheitszertifikat wird erteilt, wenn

1. die informationstechnischen Systeme, Komponenten, Produkte oder Schutzprofile den vom Bundesamt festgelegten Kriterien entsprechen und
2. das Bundesministerium des Innern und für Heimat die Erteilung des Zertifikats nicht nach Absatz 5 untersagt hat.

Vor Erteilung des Sicherheitszertifikats legt das Bundesamt den Vorgang dem Bundesministerium des Innern und für Heimat zur Prüfung nach Absatz 5 vor.

(5) Das Bundesministerium des Innern und für Heimat kann die Erteilung eines Zertifikats nach Absatz 4 im Einzelfall untersagen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen.

(6) Für die Zertifizierung von Personen und IT-Sicherheitsdienstleistern gilt Absatz 4 entsprechend.

(7) Eine Stelle wird als sachverständig im Sinne des Absatzes 3 anerkannt, wenn

1. die sachliche und personelle Ausstattung sowie die fachliche Qualifikation und Zuverlässigkeit der Konformitätsbewertungsstelle den vom Bundesamt festgelegten Kriterien entsprechen und
2. das Bundesministerium des Innern und für Heimat festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen.

Das Bundesamt stellt durch die notwendigen Maßnahmen sicher, dass das Fortbestehen der Voraussetzungen nach Satz 1 regelmäßig überprüft wird.

(8) Sicherheitszertifikate anderer anerkannter Zertifizierungsstellen aus dem Bereich der Europäischen Union werden vom Bundesamt anerkannt, sofern sie eine den Sicherheitszertifikaten des Bundesamtes gleichwertige Sicherheit ausweisen und die Gleichwertigkeit vom Bundesamt festgestellt worden ist.

§ 53

Konformitätsbewertung und Konformitätserklärung

(1) Das Bundesamt kann für die vom Bundesamt in einer Technischen Richtlinie festgelegten Anforderungen und Vorgaben zulassen, dass ein Hersteller oder Anbieter von IKT-Produkten, IKT-Diensten und IKT-Prozessen, die keine Verbraucherprodukte nach § 55 sind, sowie eine Person oder ein IT-Sicherheitsdienstleister eine Selbstbewertung seiner oder ihrer Konformität vornehmen. Der Hersteller oder Anbieter von IKT-Produkten, IKT-Diensten und IKT-Prozessen, die Person oder der IT-Sicherheitsdienstleister kann unter den Voraussetzungen von Satz 1 eine Konformitätserklärung ausstellen, die bestätigt, dass er oder sie die in der Technischen Richtlinie festgelegten Anforderungen erfüllt. Durch die Ausstellung der Konformitätserklärung übernimmt der Hersteller oder Anbieter der IKT-Produkte, IKT-Dienste und IKT-Prozesse, die Person oder der IT-Sicherheitsdienstleister (Aussteller) die Verantwortung dafür, dass das IKT-Produkt, der IKT-Dienst, der IKT-Prozess, die Person

oder die IT-Sicherheitsdienstleistung den in der Technischen Richtlinie festgelegten Anforderungen entspricht. Eine Erklärung nach Satz 3 darf nur dann für ein IKT-Produkt, einen IKT-Dienst und IKT-Prozess, eine Person oder einen IT-Sicherheitsdienstleister verwendet werden, wenn der Hersteller, der Anbieter, die Person oder der IT-Sicherheitsdienstleister diese ausgestellt hat und sie weder widerrufen noch nach Absatz 5 Nummer 3 für ungültig erklärt wurde.

(2) Die Technische Richtlinie nach Absatz 1 kann insbesondere Vorgaben enthalten über

1. den Inhalt und das Format der Konformitätserklärung,
2. Nachweise und Verfahren, die die Angaben der Konformitätserklärung belegen,
3. die Bedingungen für die Aufrechterhaltung, Fortführung und Verlängerung der Konformitätserklärung,
4. die Verwendung eines vom Bundesamt bereitgestellten Kennzeichens und Siegels sowie die Bedingungen für deren Verwendung,
5. die Meldung und Behandlung erkannter Schwachstellen des IKT-Produktes, IKT-Dienstes oder IKT-Prozesses oder der IT-Sicherheitsdienstleistung,
6. die Bereitstellung von Informationen auf der Internetseite des Bundesamtes über die Konformitätserklärung, dessen Aussteller und das IKT-Produkt, den IKT-Dienst, den IKT-Prozess, die Person oder die IT-Sicherheitsdienstleistung oder
7. die Befristung der Geltungsdauer der Konformitätserklärung.

(3) Wird in den Vorgaben nach Absatz 2 festgelegt, dass die Angaben der Konformitätserklärung nur durch eine akkreditierte Konformitätsbewertungsstelle nachgewiesen werden können, so kann das Bundesamt auf Antrag Konformitätsbewertungsstellen, die beabsichtigen, im Anwendungsbereich dieses Paragraphen tätig zu werden, eine Befugnis erteilen, wenn die maßgeblichen Voraussetzungen der Technischen Richtlinie erfüllt sind. Ohne eine Befugniserteilung durch das Bundesamt dürfen Konformitätsbewertungsstellen im Anwendungsbereich dieses Paragraphen nicht tätig werden.

(4) Der Aussteller hält die Konformitätserklärung, die technische Dokumentation und alle weiteren einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte, IKT-Dienste und IKT-Prozesse, der Person oder der IT-Sicherheitsdienstleistung mit den festgelegten Kriterien während eines Zeitraums, der vom Bundesamt in der Technischen Richtlinie nach Absatz 1 festgelegt wurde, für das Bundesamt bereit. Eine Kopie der Konformitätserklärung ist dem Bundesamt vorzulegen.

(5) Das Bundesamt kann geeignete Maßnahmen ergreifen, um sicherzustellen, dass die Aussteller von Konformitätserklärungen den Anforderungen des Schemas und den Vorgaben dieses Paragraphen genügen und insbesondere

1. Aussteller von Konformitätserklärungen auffordern, ihm sämtliche Auskünfte zu erteilen, die es für die Erfüllung ihrer Aufgaben benötigt,
2. Untersuchungen in Form von Testkäufen oder Audits bei den Ausstellern von Konformitätserklärungen durchführen, um deren Einhaltung der in der Technischen Richtlinie festgelegten Anforderungen und Vorgaben nach Absatz 1 zu überprüfen und
3. Konformitätserklärungen nach Absatz 1 für ungültig erklären.

(6) Für Maßnahmen nach Absatz 4 kann das Bundesamt Gebühren erheben, sofern es auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen der Technischen Richtlinie oder dieses Paragraphen begründeten.

§ 54

Nationale Behörde für die Cybersicherheitszertifizierung

(1) Das Bundesamt ist die nationale Behörde für die Cybersicherheitszertifizierung nach Artikel 58 Absatz 1 der Verordnung (EU) 2019/881.

(2) Das Bundesamt kann auf Antrag Konformitätsbewertungsstellen, die im Anwendungsbereich der Verordnung (EU) 2019/881 sowie des § 52 dieses Gesetzes tätig werden, eine Befugnis erteilen, als solche tätig zu werden, wenn die Voraussetzungen des maßgeblichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 oder des § 52 dieses Gesetzes erfüllt sind. Ohne eine Befugniserteilung durch das Bundesamt dürfen Konformitätsbewertungsstellen im Anwendungsbereich der Verordnung (EU) 2019/881 nicht tätig werden.

(3) Soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 und nach § 52 dieses Gesetzes erforderlich ist, kann das Bundesamt von Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, von Inhabern europäischer Cybersicherheitszertifikate und von Ausstellern von EU-Konformitätserklärungen im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 die erforderlichen Auskünfte und sonstige Unterstützung, insbesondere die Vorlage von Unterlagen oder Mustern, verlangen. § 3 Absatz 1 Satz 1 und 3 des Akkreditierungsstellengesetzes gilt entsprechend.

(4) Das Bundesamt kann Untersuchungen in Form von Auditierungen nach Artikel 58 Absatz 8 Buchstabe b der Verordnung (EU) 2019/881 bei Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, bei Inhabern europäischer Cybersicherheitszertifikate und bei Ausstellern von EU-Konformitätserklärungen im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 durchführen, um die Einhaltung der Bestimmungen des Titels III der Verordnung (EU) 2019/881 zu überprüfen. § 3 Absatz 1 Satz 1 bis 3 des Akkreditierungsstellengesetzes gilt entsprechend.

(5) Das Bundesamt ist befugt, Betriebsstätten, Geschäfts- und Betriebsräume von Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, und von Inhabern europäischer Cybersicherheitszertifikate im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 in den Zeiten, zu denen die Räume normalerweise für die jeweilige geschäftliche oder betriebliche Nutzung zur Verfügung stehen, zu betreten, zu besichtigen und dort befindliche Unterlagen und Muster zu prüfen, soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 sowie nach § 54 dieses Gesetzes erforderlich ist. § 3 Absatz 1 Satz 1 bis 3 des Akkreditierungsstellengesetzes gilt entsprechend.

(6) Das Bundesamt kann von ihm ausgestellte Cybersicherheitszertifikate oder durch eine Konformitätsbewertungsstelle, der eine Befugnis nach Absatz 2 erteilt wurde, nach Artikel 56 Absatz 6 der Verordnung (EU) 2019/881 ausgestellte Cybersicherheitszertifikate widerrufen oder EU-Konformitätserklärungen im Sinne der Verordnung (EU) 2019/881 für ungültig erklären,

1. sofern diese Zertifikate oder EU-Konformitätserklärungen die Anforderungen nach der Verordnung (EU) 2019/881 oder eines europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 nicht erfüllen oder
2. wenn das Bundesamt die Erfüllung nach Nummer 1 nicht feststellen kann, weil der Inhaber des europäischen Cybersicherheitszertifikats oder der Aussteller der EU-Konformitätserklärung seinen Mitwirkungspflichten nach Absatz 3 nicht nachgekommen ist oder weil er das Bundesamt bei der Wahrnehmung seiner Befugnisse nach Absatz 4 oder im Falle eines Inhabers eines europäischen Cybersicherheitszertifikats auch nach Absatz 5 behindert hat.

Widerrufene Cybersicherheitszertifikate oder für ungültig erklärte EU-Konformitätserklärungen nach Satz 1 dürfen nicht verwendet werden.

(7) Das Bundesamt kann von ihm erteilte Befugnisse nach Absatz 2 widerrufen,

1. sofern die Voraussetzungen des maßgeblichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 oder des § 52 dieses Gesetzes nicht erfüllt sind oder
2. wenn das Bundesamt die Erfüllung dieser Voraussetzungen nicht feststellen kann, weil die Konformitätsbewertungsstelle ihren Mitwirkungspflichten nach Absatz 3 nicht nachgekommen ist oder weil sie das Bundesamt bei der Wahrnehmung seiner Befugnisse nach den Absätzen 4 und 5 behindert hat.

§ 55

Freiwilliges IT-Sicherheitskennzeichen

(1) Das Bundesamt führt zur Information von Verbrauchern über die IT-Sicherheit von Produkten bestimmter vom Bundesamt festgelegter Produktkategorien ein einheitliches IT-Sicherheitskennzeichen ein. Das IT-Sicherheitskennzeichen trifft keine Aussage über die den Datenschutz betreffenden Eigenschaften eines Produktes.

(2) Das IT-Sicherheitskennzeichen besteht aus

1. einer Zusicherung des Herstellers oder Diensteanbieters, dass das Produkt für eine festgelegte Dauer bestimmte IT-Sicherheitsanforderungen erfüllt (Herstellererklärung), und
2. einer Information des Bundesamtes über sicherheitsrelevante IT-Eigenschaften des Produktes (Sicherheitsinformation).

(3) Die IT-Sicherheitsanforderungen, auf die sich die Herstellererklärung bezieht, ergeben sich aus einer Norm oder einem Standard oder aus einer branchenabgestimmten IT-Sicherheitsvorgabe, die die jeweilige Produktkategorie umfasst, sofern das Bundesamt in einem Verfahren, das durch Rechtsverordnung nach § 56 Absatz 2 geregelt wird, festgestellt hat, dass die Norm oder der Standard oder die branchenabgestimmte IT-Sicherheitsvorgabe geeignet ist, ausreichende IT-Sicherheitsanforderungen für die Produktkategorie abzubilden. Ein Anspruch auf diese Feststellung besteht nicht. Liegt keine Feststellung nach Satz 1 vor, ergeben sich die IT-Sicherheitsvorgaben aus einer vom Bundesamt veröffentlichten Technischen Richtlinie, die die jeweilige Produktkategorie umfasst, sofern das Bundesamt eine solche Richtlinie bereits veröffentlicht hat. Wird ein Produkt von mehr als einer oder einem bestehenden, als geeignet festgestellten Norm, Standard, branchenabgestimmten IT-Sicherheitsvorgabe oder Technischen Richtlinie umfasst, richten sich die Anforderungen nach der oder dem jeweils spezielleren bestehenden, als geeignet festgestellten Norm, Standard, branchenabgestimmten IT-Sicherheitsvorgabe oder Technischen Richtlinie.

(4) Das IT-Sicherheitskennzeichen darf nur dann für ein Produkt verwendet werden, wenn das Bundesamt das IT-Sicherheitskennzeichen für dieses Produkt freigegeben hat. Das Bundesamt prüft die Freigabe des IT-Sicherheitskennzeichens für ein Produkt auf Antrag des Herstellers oder Diensteanbieters. Dem Antrag sind die Herstellererklärung zu dem Produkt sowie alle Unterlagen beizufügen, die die Angaben in der Herstellererklärung belegen. Das Bundesamt bestätigt den Eingang des Antrags und prüft die Plausibilität der Herstellererklärung anhand der beigefügten Unterlagen. Die Plausibilitätsprüfung kann auch durch einen vom Bundesamt beauftragten qualifizierten Dritten erfolgen. Für die Antragsbearbeitung kann das Bundesamt eine Verwaltungsgebühr erheben.

(5) Das Bundesamt erteilt die Freigabe des IT-Sicherheitskennzeichens für das jeweilige Produkt, wenn

1. das Produkt zu einer der Produktkategorien gehört, die das Bundesamt durch im Bundesanzeiger veröffentlichte Allgemeinverfügung bekannt gegeben hat,
2. die Herstellererklärung plausibel und durch die beigefügten Unterlagen ausreichend belegt ist und
3. die gegebenenfalls erhobene Verwaltungsgebühr beglichen wurde.

Die Erteilung der Freigabe erfolgt schriftlich und innerhalb einer angemessenen Frist, die in der Rechtsverordnung nach § 56 Absatz 2 bestimmt wird. Den genauen Ablauf des Antragsverfahrens und die beizufügenden Unterlagen regelt die Rechtsverordnung nach § 56 Absatz 2.

(6) Hat das Bundesamt die Freigabe erteilt, ist das Etikett des IT-Sicherheitskennzeichens auf dem jeweiligen Produkt oder auf dessen Umverpackung anzubringen, sofern dies nach der Beschaffenheit des Produktes möglich ist. Das IT-Sicherheitskennzeichen kann auch elektronisch veröffentlicht werden. Wenn nach der Beschaffenheit des Produktes das Anbringen nicht möglich ist, muss die Veröffentlichung des IT-Sicherheitskennzeichens elektronisch erfolgen. Das Etikett des IT-Sicherheitskennzeichens verweist auf eine Internetseite des Bundesamtes, auf der die Herstellererklärung und die Sicherheitsinformationen abrufbar sind. Das genaue Verfahren und die Gestaltung des Verweises sind in der Rechtsverordnung nach § 56 Absatz 2 festzulegen.

(7) Nach Ablauf der festgelegten Dauer, für die der Hersteller oder Diensteanbieter die Erfüllung der IT-Sicherheitsanforderungen zusichert, oder nach Rücknahmeerklärung des Herstellers oder Diensteanbieters gegenüber dem Bundesamt erlischt die Freigabe. Das Bundesamt nimmt einen Hinweis auf das Erlöschen der Freigabe in die Sicherheitsinformation auf.

(8) Das Bundesamt kann prüfen, ob die Anforderungen an die Freigabe des IT-Sicherheitskennzeichens für ein Produkt eingehalten werden. Werden bei der Prüfung Abweichungen von der abgegebenen Herstellererklärung oder Schwachstellen festgestellt, kann das Bundesamt die geeigneten Maßnahmen zum Schutz des Vertrauens der Verbraucher in das IT-Sicherheitskennzeichen treffen, insbesondere

1. Informationen über die Abweichungen oder Schwachstellen in geeigneter Weise in der Sicherheitsinformation veröffentlichen oder
2. die Freigabe des IT-Sicherheitskennzeichens widerrufen.

Absatz 7 Satz 2 gilt entsprechend.

(9) Bevor das Bundesamt eine Maßnahme nach Absatz 8 trifft, räumt es dem Hersteller oder Diensteanbieter die Gelegenheit ein, die festgestellten Abweichungen oder Schwachstellen innerhalb eines angemessenen Zeitraumes zu beseitigen, es sei denn, gewichtige Gründe der Sicherheit der Produkte erfordern eine sofortige Maßnahme. Die Befugnis des Bundesamtes zur Warnung nach § 13 bleibt davon unberührt.

Teil 6

Verordnungsermächtigungen, Grundrechtseinschränkungen und Berichtspflichten

§ 56

Ermächtigung zum Erlass von Rechtsverordnungen

(1) Das Bundesministerium des Innern und für Heimat bestimmt im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 52 und deren Inhalt.

(2) Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz die Einzelheiten der Gestaltung, des Inhalts und der Verwendung des IT-Sicherheitskennzeichens nach § 55, um eine einheitliche Gestaltung des Kennzeichens und eine eindeutige Erkennbarkeit der gekennzeichneten informationstechnischen Produkte zu gewährleisten, sowie die Einzelheiten des Verfahrens zur Feststellung der Eignung branchenabgestimmter IT-Sicherheitsvorgaben und des Antragsverfahrens auf Freigabe einschließlich der diesbezüglichen Fristen und der beizufügenden Unterlagen sowie das Verfahren und die Gestaltung des Verweises auf Sicherheitsinformationen.

(3) Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr, dem Bundesministerium für Bildung und Forschung und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz, welche durch eine besonders wichtige Einrichtung oder eine wichtige Einrichtung eingesetzten Produkte, Dienste oder Prozesse gemäß § 30 Absatz 6 über eine Cybersicherheitszertifizierung verfügen müssen, da sie für die Erbringung der Dienste der Einrichtung maßgeblich sind und Art und Ausmaß

der Risikoexposition der Einrichtung einen verpflichtenden Einsatz von zertifizierten Produkten, Diensten oder Prozessen in diesem Bereich erforderlich machen.

(4) Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz unter Festlegung der in § 2 Nummer 24 genannten Sektoren wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Anlagen als kritische Anlagen im Sinne dieses Gesetzes gelten. Der als bedeutend anzusehende Versorgungsgrad ist anhand branchenspezifischer Schwellenwerte für jede als kritisch anzusehende Dienstleistung zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.

(5) Das Bundesministerium des Innern und für Heimat kann im Einvernehmen mit dem mit dem Bundesministerium für Wirtschaft und Klimaschutz und im Benehmen mit dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, bestimmen, wann ein Sicherheitsvorfall im Hinblick auf seine technischen oder organisatorischen Ursachen oder im Hinblick auf seine Auswirkungen auf die Einrichtung, den Staat, die Wirtschaft oder die Anzahl der von den Auswirkungen Betroffenen als erheblich im Sinne von § 2 Nummer 11 anzusehen ist. Das Bundesministerium kann diese Ermächtigung durch Rechtsverordnung auf das Bundesamt übertragen. Etwaige Durchführungsrechtsakte der Europäischen Kommission gemäß Artikel 23 Absatz 11 Unterabsatz 2 der NIS-2-Richtlinie, die die Voraussetzungen eines erheblichen Sicherheitsvorfalls bestimmen, gehen der Rechtsverordnung nach den Sätzen 1 und 2 insoweit vor.

(6) Das Bundesministerium des Innern und für Heimat kann durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Gesundheit bestimmen, dass das Bundesamt gegenüber zugelassenen Krankenhäusern nach § 108 des Fünften Buches Sozialgesetzbuch zu einem früheren als dem in § 61 Absatz 3 Satz 5 genannten Zeitpunkt die Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in § 61 Absatz 1 genannten Verpflichtungen anordnen kann.

§ 57

Einschränkung von Grundrechten

Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird durch die §§ 7, 8, 9, 11, 12, 15 und 16 eingeschränkt.

§ 58

Berichtspflichten des Bundesamtes

(1) Das Bundesamt unterrichtet das Bundesministerium des Innern und für Heimat über seine Tätigkeit.

(2) Die Unterrichtung nach Absatz 1 dient auch der Aufklärung der Öffentlichkeit durch das Bundesministerium des Innern und für Heimat über Gefahren für die Sicherheit in der Informationstechnik, die mindestens einmal jährlich in einem zusammenfassenden Bericht erfolgt. § 13 Absatz 2 ist entsprechend anzuwenden.

(3) Das Bundesministerium des Innern und für Heimat unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Ausschuss für Inneres und Heimat des Deutschen Bundestages über die Anwendung dieses Gesetzes. Es geht dabei auch auf die Fortentwicklung des maßgeblichen Unionsrechts ein.

(4) Das Bundesamt legt der Agentur der Europäischen Union für Cybersicherheit erstmals zum 18. Januar 2025 und in der Folge alle drei Monate einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu erheblichen Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahevorfällen enthält, die gemäß § 5 Absatz 2 und § 32 gemeldet wurden.

(5) Das Bundesamt übermittelt erstmals zum 17. April 2025 und in der Folge alle zwei Jahre

1. der Europäischen Kommission und der Kooperationsgruppe nach Artikel 14 der NIS-2-Richtlinie für jeden Sektor und Teilsektor gemäß Anhang I oder II der NIS-2-Richtlinie die Anzahl der besonders wichtigen Einrichtungen und wichtigen Einrichtungen, die gemäß § 33 Absatz 1 registriert wurden, und
2. der Europäischen Kommission sachdienliche Informationen über die Anzahl der kritischen Anlagen, über den Sektor und den Teilsektor gemäß Anhang I oder II der NIS-2-Richtlinie, zu dem sie gehören, über die Art der von ihnen erbrachten Dienste und über die Bestimmungen, auf deren Grundlage sie ermittelt wurden.

Teil 7
Aufsicht

§ 59
Zuständigkeit des Bundesamtes

Das Bundesamt ist zuständige Aufsichtsbehörde für die Einhaltung der Vorschriften in Teil 3

1. durch wichtige und besonders wichtige Einrichtungen, die in der Bundesrepublik Deutschland niedergelassen sind,
2. durch Betreiber kritischer Anlagen, deren kritische Anlagen sich auf dem Hoheitsgebiet der Bundesrepublik Deutschland befinden, und
3. durch Einrichtungen der Bundesverwaltung.

§ 60
Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten

(1) Abweichend von § 59 ist das Bundesamt für DNS-Diensteanbieter, Top Level Domain Name Registries, Domain-Name-Registry-Dienstleister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider sowie für Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke nur dann zuständig, wenn diese ihre Hauptniederlassung in der Europäischen Union in der Bundesrepublik Deutschland haben. Ist dies der Fall, so ist das Bundesamt für die Einrichtung in der gesamten Europäischen Union zentral zuständig.

(2) Als Hauptniederlassung in der Europäischen Union im Sinne von Absatz 1 gilt derjenige Mitgliedstaat der Europäischen Union, in dem die Entscheidungen der Einrichtung im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement vorwiegend getroffen werden. Kann ein solcher Mitgliedstaat nicht bestimmt werden oder werden solche Entscheidungen nicht in der Europäischen Union getroffen, so gilt als Hauptniederlassung der Mitgliedstaat, in dem die Cybersicherheitsmaßnahmen durchgeführt werden. Kann ein solcher Mitgliedstaat nicht bestimmt werden, so gilt als Hauptniederlassung der Mitgliedstaat, in dem die betreffende Einrichtung die Niederlassung mit der höchsten Beschäftigtenzahl in der Europäischen Union hat.

(3) Hat eine Einrichtung der in Absatz 1 Satz 1 genannten Einrichtungsart keine Niederlassung in der Europäischen Union, bietet aber Dienste innerhalb der Europäischen Union an, so ist sie verpflichtet, einen Vertreter zu benennen. Der Vertreter muss in einem Mitgliedstaat der Europäischen Union niedergelassen sein, in der die

Einrichtung die Dienste anbietet. Ist der Vertreter in der Bundesrepublik Deutschland niedergelassen, ist das Bundesamt für die Einrichtung zuständig. Hat eine Einrichtung der in Absatz 1 Satz 1 genannten Einrichtungsart in der Europäischen Union keinen Vertreter im Sinne dieses Absatzes benannt, so kann das Bundesamt sich für die betreffende Einrichtung zuständig erklären.

(4) Die Benennung eines Vertreters durch eine Einrichtung der in Absatz 1 Satz 1 genannten Einrichtungsart lässt rechtliche Schritte, die gegen die Einrichtung selbst eingeleitet werden könnten, unberührt.

(5) Hat das Bundesamt ein Amtshilfeersuchen eines anderen Mitgliedstaats der Europäischen Union zu einer Einrichtung der in Absatz 1 Satz 1 genannten Einrichtungsart erhalten, so ist das Bundesamt befugt, innerhalb der Grenzen dieses Ersuchens geeignete Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf die betreffende Einrichtung zu ergreifen, die in der Bundesrepublik Deutschland Dienste anbietet oder eine informationstechnisches System, eine informationstechnische Komponente oder einen informationstechnischen Prozess betreibt. Satz 1 gilt entsprechend bei Amtshilfeersuchen eines anderen Mitgliedstaats der Europäischen Union, der für eine Einrichtung in der gesamten Europäischen Union zuständig ist, wenn die Einrichtung in der Bundesrepublik Deutschland Dienste anbietet oder ein informationstechnisches System, eine informationstechnische Komponente oder einen informationstechnischen Prozess betreibt.

§ 61

Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

(1) Das Bundesamt kann gegenüber einzelnen besonders wichtigen Einrichtungen anordnen, Audits, Prüfungen oder Zertifizierungen von unabhängigen Stellen zur Prüfung der Erfüllung der Verpflichtungen nach § 30 Absatz 1 Satz 1, auch in Verbindung mit § 31 Absatz 1 und 2 Satz 1 und § 32 Absatz 1 bis 3 sowie § 38 Absatz 3 durchführen zu lassen.

(2) Das Bundesamt kann nach Anhörung der betroffenen Einrichtungen und Wirtschaftsverbände fachliche und organisatorische Anforderungen für die prüfenden Stellen festlegen. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamtes.

(3) Das Bundesamt kann auch gegenüber anderen besonders wichtigen Einrichtungen frühestens drei Jahre nach Inkrafttreten dieses Gesetzes die Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in Absatz 1 genannten Verpflichtungen anordnen. Soweit das Bundesamt von seinem Recht nach Absatz 1 Gebrauch gemacht hat, kann es hierbei auch die Übermittlung der Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel sowie die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln die Vorlage eines geeigneten Mängelbeseitigungsplans im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder der sonst zuständigen Aufsichtsbehörde verlangen. Das Bundesamt kann die Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen. Abweichend von Satz 1 kann das Bundesamt gegenüber zugelassenen Krankenhäusern nach § 108 des Fünften Buches Sozialgesetzbuch frühestens fünf Jahre nach Inkrafttreten dieses Gesetzes die Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in Absatz 1 genannten Verpflichtungen anordnen, soweit nicht durch Rechtsverordnung nach § 56 Absatz 6 ein früherer Zeitpunkt bestimmt wird.

(4) Bei der Auswahl, von welchen Einrichtungen das Bundesamt nach Absatz 3 Nachweise anfordert, berücksichtigt das Bundesamt das Ausmaß der Risikoexposition, die Größe der Einrichtung sowie die Eintrittswahrscheinlichkeit und Schwere von möglichen Sicherheitsvorfällen sowie ihre möglichen gesellschaftlichen und wirtschaftlichen Auswirkungen.

(5) Das Bundesamt kann bei besonders wichtigen Einrichtungen die Einhaltung der Anforderungen nach diesem Gesetz überprüfen. Es kann sich bei der Durchführung der Überprüfung eines qualifizierten unabhängigen Dritten bedienen. Die besonders wichtige Einrichtung hat dem Bundesamt und den in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung erhebt das Bundesamt Gebühren und Auslagen bei der jeweiligen besonders

wichtigen Einrichtung nur, sofern das Bundesamt auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach § 30 Absatz 1 begründeten.

(6) Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen im Benehmen mit der zuständigen Aufsichtsbehörde zur Verhütung oder Behebung eines Sicherheitsvorfalls oder eines Mangels erforderliche Maßnahmen nach § 30 Absatz 1 Satz 1 sowie die Vorlage eines geeigneten Mängelbeseitigungsplanes und eines geeigneten Nachweises über die erfolgte Mängelbeseitigung anordnen. Ein Benehmen mit der zuständigen Aufsichtsbehörde kann entfallen, sofern Gefahr im Verzug besteht. Ferner kann das Bundesamt die Berichterstattung zu den nach Satz 1 angeordneten Maßnahmen innerhalb einer angemessenen Frist verlangen.

(7) Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen im Benehmen mit der zuständigen Aufsichtsbehörde Anordnungen zur Umsetzung der in Absatz 1 genannten Verpflichtungen erlassen. Ein Benehmen mit der zuständigen Aufsichtsbehörde kann entfallen, sofern Gefahr im Verzug besteht. Es kann die Umsetzung von im Rahmen einer Sicherheitsprüfung formulierten konkreten Empfehlungen im Einzelfall innerhalb einer angemessenen Frist anordnen.

(8) Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen anordnen,

1. die natürlichen oder juristischen Personen, für die sie Dienste erbringen oder Tätigkeiten ausüben und die potenziell von einer erheblichen Cyberbedrohung betroffen sind, über die Art der Bedrohung und mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten, die diese Personen als Reaktion auf die Bedrohung ergreifen können, und
2. Informationen zu Verstößen gegen die in Absatz 1 genannten Verpflichtungen nach durch das Bundesamt bestimmten Vorgaben öffentlich bekannt zu machen.

(9) Sofern besonders wichtige Einrichtungen den Anordnungen des Bundesamtes nach diesem Gesetz trotz Fristsetzung nicht nachkommen, kann das Bundesamt dies der jeweils zuständigen Aufsichtsbehörde mitteilen. Die zuständige Aufsichtsbehörde kann, wenn ein Zusammenhang zwischen Durchsetzungsmaßnahme und Anordnung besteht, als letztes Mittel

1. die dieser Einrichtung erteilte Genehmigung nach dem jeweiligen Fachrecht vorübergehend ganz oder teilweise aussetzen und
2. unzuverlässigen Geschäftsleitungen die Ausübung der Tätigkeit, zu der sie berufen sind (§ 2 Nummer 13), vorübergehend untersagen.

Die Aussetzung nach Satz 2 Nummer 1 und die Untersagung nach Satz 2 Nummer 2 sind nur solange zulässig, bis die besonders wichtige Einrichtung den Anordnungen des Bundesamtes nachkommt, wegen deren Nichtbefolgung sie ausgesprochen wurden.

(10) Soweit das Bundesamt Maßnahmen gegenüber besonders wichtigen Einrichtungen durchführt, informiert es die zuständige Aufsichtsbehörde des Bundes darüber. Die Information hat unverzüglich zu erfolgen, wenn es sich um Maßnahmen nach Absatz 6 oder 7 handelt, die wegen Gefahr im Verzug ohne Benehmen der zuständigen Aufsichtsbehörde ergangen sind.

(11) Stellt das Bundesamt im Zuge der Beaufsichtigung einer Einrichtung oder Durchsetzung einer Maßnahme fest, dass ein Verstoß gegen die Verpflichtungen dieses Gesetzes eine offensichtliche Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 dieser Verordnung zu melden ist, unterrichtet es unverzüglich die zuständigen Aufsichtsbehörden.

(12) Bei Einrichtungen, die in anderen Mitgliedstaaten der Europäischen Union Dienste erbringen, kann das Bundesamt auch auf Ersuchen der jeweils zuständigen Aufsichtsbehörden des Mitgliedstaats Maßnahmen nach den Absätzen 1 bis 11 ergreifen.

§ 62

Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen

Rechtfertigen Tatsachen die Annahme, dass eine wichtige Einrichtung Verpflichtungen nach § 30 Absatz 1 Satz 1, § 32 Absatz 1 bis 3 und § 38 Absatz 3 nicht oder nicht richtig umsetzt, so kann das Bundesamt deren Einhaltung überprüfen und Maßnahmen nach § 61 treffen.

§ 63

Verwaltungszwang

Sofern das Bundesamt Zwangsgelder verhängt, beträgt deren Höhe abweichend von § 11 Absatz 3 des Verwaltungsvollstreckungsgesetzes bis zu 100 000 Euro.

§ 64

Zuwiderhandlungen durch Institutionen der sozialen Sicherung

Bei Zuwiderhandlungen gegen eine in § 65 Absatz 1 bis 4 genannte Vorschrift, die von Institutionen der Sozialen Sicherung begangen werden, finden die Sätze 2 bis 4 Anwendung. Bei einer in Satz 1 genannten Zuwiderhandlung von Institutionen der Sozialen Sicherung in Trägerschaft des Bundes stellt das Bundesamt das Einvernehmen über die zu ergreifenden Maßnahmen mit der für die Institution der Sozialen Sicherung zuständigen Aufsichtsbehörde her. Bei einer in Satz 1 genannten Zuwiderhandlung von Institutionen der Sozialen Sicherung in Trägerschaft der Länder informiert das Bundesamt die zuständige Aufsichtsbehörde und schlägt geeignete Maßnahmen vor. Die jeweils zuständige Aufsichtsbehörde informiert das Bundesamt über die Einleitung und Umsetzung von Aufsichtsmitteln und sorgt für deren Durchsetzung.

Teil 8

Bußgeldvorschriften

§ 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, auch in Verbindung mit § 16 Absatz 3, § 17 Satz 1, oder § 39 Absatz 1 Satz 5,
   b) § 14 Absatz 2 Satz 1,
   c) den §§ 18, 40 Absatz 5 Satz 1 oder § 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 § 49 Absatz 3 Satz 1 eine dort genannte Vorgabe oder ein dort genanntes Verfahren nicht vorhält,
12. 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,
13. entgegen § 50 Absatz 1 Satz 1 einen Zugang nicht oder nicht rechtzeitig gewährt,
14. 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,
15. entgegen § 53 Absatz 3 Satz 2 oder § 54 Absatz 2 Satz 2 tätig wird oder
16. 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 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15) 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 1 Buchstabe a mit einer Geldbuße bis zu zwei Millionen Euro,

3. in den Fällen der Absätze 1 und 2 Nummer 10 mit einer Geldbuße bis zu einer Million Euro,

4. in den Fällen des Absatzes 2 Nummer 1 Buchstabe c, Nummer 6, 8, 11 bis 15 und des Absatzes 4 mit einer Geldbuße bis zu fünfhunderttausend Euro und

5. in den Fällen des Absatzes 2 Nummer 1 Buchstabe b, Nummer 7 und 16 und des Absatzes 3 mit einer Geldbuße bis zu hunderttausend Euro.

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

(6) Bei einer besonders wichtigen Einrichtung im Sinne des § 28 Absatz 1 Satz 1 mit einem Jahresumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 5 Satz 1 Nummer 1 Buchstabe a 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 Jahresumsatzes geahndet werden.

(7) Bei einer wichtigen Einrichtung im Sinne des § 28 Absatz 2 Satz 1 mit einem Jahresumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 5 Nummer 1 Buchstabe b 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 Jahresumsatzes geahndet werden.

(8) Der Jahresumsatz im Sinne der Absätze 6 und 7 ist der gesamte weltweit getätigte Umsatz des Unternehmens, dem die besonders wichtige Einrichtung oder die wichtige Einrichtung angehört, der in dem Geschäftsjahr erzielt wurde, das dem Verstoß vorangeht.

(9) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesamt.

(10) 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.

Anlage 1

Sektoren besonders wichtiger und wichtiger Einrichtungen

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
1	**Energie**		
1.1		Stromversorgung	
1.1.1			Stromlieferanten nach § 3 Nummer 31c EnWG
1.1.2			Betreiber von Elektrizitätsverteilernetzen nach § 3 Nummer 3 EnWG
1.1.3			Betreiber von Übertragungsnetzen nach § 3 Nummer 10 EnWG
1.1.4			Betreiber von Erzeugungsanlagen nach § 3 Nummer 18d EnWG
1.1.5			Nominierte Strommarktbetreiber nach Artikel 2 Nummer 8 der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5 Juni 2019 über den Elektrizitätsbinnenmarkt (ABl. L 158 vom 14.6.2019, S. 54)
1.1.6			Aggregatoren nach § 3 Nummer 1a EnWG
1.1.7			Betreiber von Energiespeicheranlagen nach § 3 Nummer 15d EnWG
1.1.8			Anbieter von Ausgleichsleistungen nach § 3 Nummer 1b EnWG
1.1.9			Ladepunktbetreiber nach § 2 Nummer 8 LSV
1.2		Fernwärmeversorgung oder Fernkältekälteversorgung	
1.2.1			Betreiber von Fernwärme- oder Fernkälteversorgung im Sinne von § 3 Nummer 19 oder Nummer 20 GEG
1.3		Kraftstoff- und Heizölversorgung	
1.3.1			Betreiber von Erdöl-Fernleitungen
1.3.2			Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
1.3.3			Zentrale Bevorratungsstellen nach Artikel 2 Buchstabe f der Richtlinie 2009/119/EG des Rates vom 14. September 2009 zur Verpflichtung der Mitgliedstaaten, Mindestvorräte an Erdöl und/oder Erdölerzeugnissen zu halten (ABl. L 265 vom 9.10.2009, S. 9)
1.4		Gasversorgung	
1.4.1			Betreiber von Gasverteilernetzen nach § 3 Nummer 8 EnWG

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
1.4.2			Betreiber von Fernleitungsnetzen nach § 3 Nummer 5 EnWG
1.4.3			Betreiber von Gasspeicheranlagen nach § 3 Nummer 6 EnWG
1.4.4			Betreiber von LNG-Anlagen nach § 3 Nummer 9 EnWG
1.4.5			Gaslieferanten nach § 3 Nummer 19b EnWG
1.4.6			Betreiber von Anlagen zur Gewinnung von Erdgas
1.4.7			Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas
1.4.8			Betreiber im Bereich Wasserstofferzeugung, -speicherung und -fernleitung
2	**Transport und Verkehr**		
2.1		Luftverkehr	
2.1.1			Luftfahrtunternehmen nach Artikel 3 Nummer 4 der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72), die für gewerbliche Zwecke genutzt werden
2.1.2			Flughafenleitungsorgane nach Artikel 2 Nummer 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates vom 11. März 2009 über Flughafenentgelte (ABl. L 70 vom 14.3.2009, S. 11), Flughäfen nach Artikel 2 Nummer 1 jener Richtlinie, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU (ABl. L 348, 20.12.2013, S. 1) aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben
2.1.3			Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne von Artikel 2 Nummer 1 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Festlegung des Rahmens für die Schaffung eines einheitlichen europäischen Luftraums (ABl. L 96 vom 31.3.2004, S. 1) bereitstellen
2.2		Schienenverkehr	
2.2.1			Betreiber von Eisenbahninfrastruktur nach § 2 Absatz 6 und 6a AEG einschließlich zentraler Einrichtungen, die den Zugbetrieb vorausschau-

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
			end und bei unerwartet eintretenden Ereignissen disponiert
2.2.2			Eisenbahnverkehrsunternehmen nach § 2 Absatz 3 AEG, einschließlich Betreiber einer Serviceeinrichtung nach § 2 Nummer 9 AEG
2.3		Schifffahrt	
2.3.1			Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen (ABl. L 129 vom 29.4.2004, S. 6) für die Schifffahrt definiert sind, ausschließlich der einzelnen von diesen Unternehmen betriebenen Schiffe
2.3.2			Leitungsorgane von Häfen nach Artikel 3 Nummer 1 der Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Erhöhung der Gefahrenabwehr in Häfen (ABl. L 310 vom 25.11.2005, S. 28), einschließlich ihrer Hafenanlagen nach Artikel 2 Nummer 11 der Verordnung (EG) Nr. 725/2004, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben
2.3.3			Betreiber einer Anlage oder eines Systems zum sicheren Betrieb einer Wasserstraße im Sinne von § 1 Absatz 6 Nummer 1 WaStrG
2.4		Straßenverkehr	
2.4.1			Betreiber einer Anlage oder eines System zur Verkehrsbeeinflussung im Straßenverkehr einschließlich der in § 1 Absatz 4 Nummer 1, 3 und 4 FStrG genannten Einrichtungen, zum Beispiel Verkehrs-, Betriebs- und Tunnelleitzentralen, Entwässerungsanlagen, intelligente Verkehrssysteme und Fachstellen für Informationstechnik und -sicherheit im Straßenbau, sowie der Telekommunikationsnetze der Bundesautobahnen
2.4.2			Betreiber eines intelligenten Verkehrssystems nach § 2 Nummer 1 IVSG.
3	**Finanzwesen**		
3.1		Bankwesen	
3.1.1			Kreditinstitute: Einrichtungen deren Tätigkeit darin besteht, Einlagen oder andere rückzahlbare Gelder des Publikums entgegenzunehmen und Kredite für eigene Rechnung zu gewähren
3.2		Finanzmarktinfrastrukturen	
3.2.1			Handelsplätze im Sinne von § 2 Absatz 22 WpHG
3.2.2			Zentrale Gegenparteien, die zwischen die Gegenparteien der auf einem Markt oder mehreren Märkten gehandelten Kontrakte tritt und somit

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
			als Käufer für jeden Verkäufer bzw. als Verkäufer für jeden Käufer fungiert
4	**Gesundheit**		
4.1.1			Erbringer von Gesundheitsdienstleistungen im Sinne der Richtlinie (EU) 2011/24 des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45)
4.1.2			EU-Referenzlaboratorien nach Artikel 15 der Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates vom 23. November 2022 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU (ABl. L 314 vom 6.12.2022, S. 26)
4.1.3			Unternehmen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel nach § 2 AMG ausüben
4.1.4			Unternehmen, die pharmazeutische Erzeugnisse nach Abschnitt C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen
4.1.5			Unternehmen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch nach Artikel 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates vom 25. Januar 2022 zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und -bewältigung in Bezug auf Arzneimittel und Medizinprodukte (ABl. L 20 vom 31.1.2022, S. 1) („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden
5	**Wasser**		
5.1		Trinkwasserversorgung	
5.1.1			Betreiber von Wasserversorgunsanlagen im Sinne von § 2 Nummer 3 TrinkwV, jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist
5.2		Abwasserbeseitigung	
5.2.1			Unternehmen, die Abwasser nach § 2 Absatz 1 AbwAG sammeln, entsorgen oder behandeln, jedoch unter Ausschluss der Unternehmen, für die das Sammeln, die Entsorgung oder die Behandlung solchen Abwassers ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist.

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
6	**Digitale Infrastruktur**		
6.1.1			Betreiber von Internet Exchange Points
6.1.2			DNS-Dienstanbieter, ausgenommen Betreiber von Root-Nameservern
6.1.3			Top Level Domain Name Registry
6.1.4			Anbieter von Cloud-Computing-Diensten
6.1.5			Anbieter von Rechenzentrumsdiensten
6.1.6			Betreiber von Content Delivery Networks
6.1.7			Vertrauensdienstanbieter
6.1.8			Betreiber öffentlicher Telekommunikationsnetze
6.1.9			Anbieter öffentlich zugänglicher Telekommunikationsdienste
6.1.10			Managed Services Provider
6.1.11			Managed Security Services Provider
7	**Weltraum**		
7.1.1			Betreiber von Bodeninfrastrukturen, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze

Anlage 2

Sektoren wichtiger Einrichtungen

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
1	**Transport und Verkehr**		
1.1		Post- und Kurierdienste	
1.1.1			Anbieter von Postdienstleistungen nach § 3 Nummer 15 PostG, einschließlich Anbieter von Kurierdiensten
2	**Abfallbewirtschaftung**		
2.1.1			Unternehmen der Abfallbewirtschaftung nach § 3 Absatz 14 KrWG, ausgenommen Unternehmen, für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist
3	**Produktion, Herstellung und Handel mit chemischen Stoffen**		
3.1.1			Hersteller und Importeure nach Artikel 3 Nummern 9 und 11 der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates vom 18. Dezember 2006 zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH), zur Schaffung einer Europäischen Chemikalienagentur, zur Änderung der Richtlinie 1999/45/EG und zur Aufhebung der Verordnung (EWG) Nr. 793/93 des Rates, der Verordnung (EG) Nr. 1488/94 der Kommission, der Richtlinie 76/769/EWG des Rates sowie der Richtlinien 91/155/EWG, 93/67/EWG, 93/105/EG und 2000/21/EG der Kommission (ABl. L 396 vom 30.12.2006, S. 1) von chemischen Stoffen und Gemischen im Sinne des Artikels 3 Nummer 1 und 2 der genannten Verordnung, sofern diese in Kategorie 20 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) fallen
4	**Produktion, Verarbeitung und Vertrieb von Lebensmitteln**		
4.1.1			Lebensmittelunternehmen nach Artikel 3 Nummer 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit (ABl. L 31 vom 1.2.2002, S. 1), die im Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
5	**Verarbeitendes Gewerbe/Herstellung von Waren**		
5.1		Herstellung von Medizinprodukten und In-vitro-Diagnostika	
5.1.1			Unternehmen, die Medizinprodukte nach Artikel 2 Nummer 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (ABl. L 117 vom 5.5.2017, S. 1) herstellen, und Unternehmen, die In-vitro-Diagnostika nach Artikel 2 Nummer 2 der Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission (ABl. L 117 vom 5.5.2017, S. 176) herstellen, mit Ausnahme von Unternehmen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch nach Artikel 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates vom 25. Januar 2022 zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und -bewältigung in Bezug auf Arzneimittel und Medizinprodukte (ABl. L 20 vom 31.1.2022, S. 1) („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden
5.2		Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	
5.2.1			Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 26 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
5.3		Herstellung von elektrischen Ausrüstungen	
5.3.1			Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 27 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
5.4		Maschinenbau	
5.4.1			Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
5.5		Herstellung von Kraftwagen und Kraftwagenteilen	
5.5.1			Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 29 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
5.6		Sonstiger Fahrzeugbau	
5.6.1			Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 30 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
6	**Anbieter digitaler Dienste**		
6.1.1			Anbieter von Online-Marktplätzen
6.1.2			Anbieter von Online-Suchmaschinen
6.1.3			Anbieter von Plattformen für Dienste sozialer Netzwerke
7	**Forschung**		
7.1.1			Forschungseinrichtungen

Artikel 2

Änderung des BND-Gesetzes

In § 24 Absatz 5 Satz 2 des BND-Gesetzes vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch Artikel 4 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, werden die Wörter „§ 5 Absatz 7 Satz 2 bis 8 des BSI-Gesetzes“ durch die Wörter „§ 8 Absatz 8 Satz 2 bis 8 des BSI-Gesetzes“ ersetzt.

Artikel 3

Änderung der Sicherheitsüberprüfungsfeststellungsverordnung

In § 1 Nummer 8 der Sicherheitsüberprüfungsfeststellungsverordnung vom 6. Februar 2023 (BGBl. 2023 I Nr. 33), werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 1, Nummer 13 Satz 1 Buchstabe b und c, Nummer 15 und Nummer 18 des BSI-Gesetzes“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 1, 18 Buchstabe b und c, Nummer 22 und 25 des BSI-Gesetzes“ ersetzt.

Artikel 4

Änderung der Besonderen Gebührenverordnung des Bundesministeriums des Innern, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich

Die Anlage (zu § 2 Absatz 1) Abschnitt 7 der besonderen Gebührenverordnung des Bundesministeriums des Innern, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich vom 2. September 2019 (BGBl. I S. 1359), zuletzt geändert durch Artikel 1 der Verordnung vom 10. September 2021 I 4229 (BGBl. I S. 4229), wird wie folgt geändert:

1. In den Nummern 1.1.1; 1.1.1.4.1; 1.1.1.4.2; 1.1.2; 1.1.3; 1.1.4; 1.1.5; 1.2; 1.3; 1.4; 1.5; 1.6; 1.7 werden jeweils die Wörter „§ 3 Absatz 1 Satz 2 Nummer 5 in Verbindung mit § 9 Absatz 2 Satz 1 und Absatz 4 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 8 in Verbindung mit § 52 Absatz 2 Satz 1 und Absatz 4 BSIG“ ersetzt.
2. In Nummer 1.8 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 5 in Verbindung mit § 9 Absatz 7 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 8 in Verbindung mit § 52 Absatz 7 BSIG“ ersetzt.
3. In Nummer 1.9 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 5 in Verbindung mit § 9 Absatz 6 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 8 in Verbindung mit § 52 Absatz 6 BSIG“ ersetzt.
4. In Nummer 1.10 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 8 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 12 BSIG“ ersetzt.
5. In Nummer 2 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 5 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 12 BSIG“ ersetzt.
6. In Nummer 3 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 9 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 13 BSIG“ ersetzt.
7. In Nummer 4 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 12, 13 und 13a BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 16, 18 und 19 BSIG“ ersetzt.

8. In Nummer 5 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 14 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 20 BSIG“ ersetzt.
9. In Nummer 6 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 14a in Verbindung mit § 9c Absatz 5 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 21 in Verbindung mit § 55 Absatz 5 BSIG“ ersetzt.
10. In Nummer 7 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 17 in Verbindung mit § 8a Absatz 2 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 24 in Verbindung mit § 39 BSIG“ ersetzt.
11. In Nummer 8 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 17 in Verbindung mit § 8a Absatz 3 Satz 4 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 24 BSIG in Verbindung mit § 39 Absatz 1“ ersetzt.
12. In Nummer 9 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 18 in Verbindung mit § 5b BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 25 in Verbindung mit § 11 BSIG“ ersetzt.
13. In Nummer 10 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 19 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 26 BSIG“ ersetzt.

Artikel 5

Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes

In § 19 Absatz 4 Satz 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 8 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, werden die Wörter „§ 7d Satz 1 BSI-Gesetz“ durch die Wörter „§ 17 Satz 1 des BSI-Gesetzes“ ersetzt.

Artikel 6

Änderung der Gleichstellungsbeauftragtenwahlverordnung

In § 19 Absatz 9 der Gleichstellungsbeauftragtenwahlverordnung vom 17. Dezember 2015 (BGBl. I S. 2274), die durch Artikel 3 des Gesetzes vom 7. August 2021 geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes“ durch die Wörter „§ 52 des BSI-Gesetzes“ ersetzt.

Artikel 7

Änderung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Artikel 6 Absatz 1 des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021 (BGBl. I S. 1122, 4304), wird wie folgt geändert:

1. Die Nummerbezeichnung „1.“ wird gestrichen und das Wort „und“ am Ende wird durch einen Punkt ersetzt.
2. Nummer 2 wird aufgehoben.

Artikel 8

Änderung der BSI-Zertifizierungs- und -Anerkennungsverordnung

Die BSI-Zertifizierungs- und -Anerkennungsverordnung vom 17. Dezember 2014 (BGBl. I S. 2231), die zuletzt durch Artikel 74 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

1. Die Eingangsformel wird wie folgt gefasst:

   „Auf Grund des § 56 Absatz 1 des BSI-Gesetzes in der Fassung der Bekanntmachung vom … [*einfügen: Datum und Fundstelle dieses Gesetzes*] verordnet das Bundesministerium des Innern und für Heimat nach Anhörung der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz:“.

2. In § 1 werden die Wörter „§ 9 des BSI-Gesetzes“ durch die Wörter „§ 52 des BSI-Gesetzes“ ersetzt.

3. In § 12 Absatz 1 werden die Wörter „§ 9 Absatz 4 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 4 des BSI-Gesetzes“ ersetzt.

4. In § 15 Absatz 1 und § 18 Absatz 1 werden jeweils die Wörter „§ 9 Absatz 5 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 6 des BSI-Gesetzes“ und die Wörter „§ 9 Absatz 4 Nummer 2 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 4 Satz 1 Nummer 2 des BSI-Gesetzes“ ersetzt.

5. § 21 wird wie folgt geändert:

   a) In Absatz 1 werden die Wörter „§ 9 Absatz 6 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 7 des BSI-Gesetzes“ ersetzt.

   b) In Absatz 1 Nummer 2 werden die Wörter „§ 9 Absatz 6 Nummer 2 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 7 Satz 1 Nummer 2 des BSI-Gesetzes“ ersetzt.

   c) In Absatz 4 Satz 1 werden die Wörter „§ 9 Absatz 6 Satz 2 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 7 Satz 2 des BSI-Gesetzes“ ersetzt.

Artikel 9

Änderung der BSI-IT-Sicherheitskennzeichenverordnung

Die BSI-IT-Sicherheitskennzeichenverordnung vom 24. November 2021 (BGBl. I S. 4978), wird wie folgt geändert:

1. Die Eingangsformel wird wie folgt gefasst:

   „Auf Grund des § 56 Absatz 2 des BSI-Gesetzes in der Fassung der Bekanntmachung vom … [einfügen: Datum und Fundstelle dieses Gesetzes] verordnet das Bundesministerium des Innern und für Heimat im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz:“.

2. In § 2 Nummer 4 werden die Wörter „§ 9c Absatz 3 Satz 1 des BSI-Gesetzes“ durch die Wörter „§ 55 Absatz 3 Satz 1 des BSI-Gesetzes“ ersetzt.

3. In § 3 Absatz 1 Satz 1 werden die Wörter „§ 9c Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 55 Absatz 2 des BSI-Gesetzes“ ersetzt.

4. § 5 wird wie folgt geändert:

   a) In Absatz 4 wird die Angabe „§ 9c Absatz 5 BSIG“ durch die Wörter „§ 55 Absatz 5 des BSI-Gesetzes“ ersetzt.

   b) In Absatz 5 Satz 1 Nummer 5 werden die Wörter „§§ 7 oder 7a des BSI-Gesetzes“ durch die Wörter „§ 13 oder 14 des BSI-Gesetzes“ und die Wörter „§ 9c Absatz 8 des BSI-Gesetzes“ durch die Wörter „§ 55 Absatz 8 des BSI-Gesetzes“ ersetzt.

5. In § 6 Absatz 1 werden die Wörter „§ 9 des BSI-Gesetzes“ durch die Wörter „§ 52 des BSI-Gesetzes“ ersetzt.

6. In § 7 Absatz 3 und § 9 Absatz 1 Satz 1 werden die Wörter „§ 9c des BSI-Gesetzes“ durch die Wörter „§ 55 des BSI-Gesetzes“ ersetzt.

7. § 13 wird wie folgt geändert:

   a) In Satz 1 werden die Wörter „§ 9c Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 55 Absatz 2 des BSI-Gesetzes“ ersetzt.

   b) In Satz 2 werden die Wörter „§§ 7 oder 7a des BSI-Gesetzes“ durch die Wörter „§ 13 oder 14 des BSI-Gesetzes“ ersetzt.

8. In § 14 werden die Wörter „§ 10 Absatz 3 Satz 1 des BSI-Gesetzes“ durch die Wörter „§ 56 Absatz 2 des BSI-Gesetzes“ ersetzt.

Artikel 10

Änderung des De-Mail-Gesetzes

In § 18 Absatz 3 Nummer 3 des De-Mail-Gesetzes vom 28. April 2011 (BGBl. I S. 666), das zuletzt durch Artikel 10 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, werden die Wörter „§ 9 Absatz 2 Satz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik“ durch die Wörter „§ 52 Absatz 2 Satz 1 des BSI-Gesetzes“ ersetzt.

Artikel 11

Änderung des E-Government-Gesetz

In § 10 des E-Government-Gesetz vom 25. Juli 2013 (BGBl. I S. 2749), das zuletzt durch Artikel 1 des Gesetzes vom 16. Juli 2021 (BGBl. I S. 2941) geändert worden ist, wird Satz 2 aufgehoben.

Artikel 12

Änderung der Passdatenerfassungs- und Übermittlungsverordnung

In § 4 Absatz 2 der Passdatenerfassungs- und Übermittlungsverordnung vom 9. Oktober 2007 (BGBl. I S. 2312), die zuletzt durch Artikel 4 der Verordnung vom 30. Oktober 2023 (BGBl. 2023 I Nr. 290) geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821)“ durch die Wörter „§ 52 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle dieses Gesetzes]“ ersetzt.

Artikel 13

Änderung der Personalausweisverordnung

In § 3 Absatz 2 der Personalausweisverordnung vom 1. November 2010 (BGBl. I S. 1460), die zuletzt durch Artikel 2 der Verordnung vom 12. April 2024 (BGBl. 2024 I Nr. 125) geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885) geändert worden ist," durch die Wörter „§ 52 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle dieses Gesetzes]" ersetzt.

Artikel 14

Änderung des Hinweisgeberschutzgesetzes

In § 2 Absatz 1 Nummer 3 Buchstabe q des Hinweisgeberschutzgesetzes vom 31. Mai 2023 (BGBl. 2023 I Nr. 140), werden die Wörter „§ 2 Absatz 2 des BSI-Gesetzes" durch die Wörter „§ 2 Nummer 39 des BSI-Gesetzes" und werden die Wörter „Anbietern digitaler Dienste im Sinne des § 2 Absatz 12 des BSI-Gesetzes" durch die Wörter „besonders wichtigen Einrichtungen nach § 28 Absatz 1 des BSI-Gesetzes und wichtigen Einrichtungen nach § 28 Absatz 2 des BSI-Gesetzes, soweit diese den Einrichtungsarten nach Anhang 1 Nummer 6.1.4 oder Anhang 2 Nummern 6.1.1 oder 6.1.2 des BSI-Gesetzes zuzuordnen sind" ersetzt.

Artikel 15

Änderung der Kassensicherungsverordnung

In § 11 Absatz 1 der Kassensicherungsverordnung vom 26. September 2017 (BGBl. I S. 3515), die durch Artikel 2 der Verordnung vom 30. Juli 2021 (BGBl. I S. 3295) geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes" durch die Wörter „§ 52 des BSI-Gesetzes" ersetzt.

Artikel 16

Änderung des Atomgesetzes

In § 44b des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 1 des Gesetzes vom 4. Dezember 2022 (BGBl. I S. 2153) geändert worden ist, werden die Wörter „§ 8b Absatz 1, 2 Nummer 1 bis 3, Nummer 4 Buchstabe a bis c und Absatz 7 des BSI-Gesetzes" durch die Wörter „§ 40 Absatz 1, 3 Nummer 1, 2, 3, 4 Buchstabe a, d und Absatz 6 des BSI-Gesetzes" ersetzt.

Artikel 17

Änderung des Energiewirtschaftsgesetzes

Das Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 1 des Gesetzes vom 14. Mai 2024 (BGBl. 2024 I Nr. 161) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 5b folgende Angabe eingefügt:

   „§ 5c IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz“.

2. Nach § 5b wird folgender § 5c eingefügt:

„§ 5c

IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz

(1) Der Betreiber eines Energieversorgungsnetzes hat einen angemessenen Schutz gegen Bedrohungen für Telekommunikationssysteme sowie elektronische Datenverarbeitungssysteme, die für den sicheren Netzbetrieb notwendig sind, zu gewährleisten. Der angemessene Schutz nach Satz 1 ist auch durch Berücksichtigung erforderlicher Anforderungen bei der Beschaffung von Anlagengütern und Dienstleistungen sicherzustellen. Die Bundesnetzagentur bestimmt im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 in einem Katalog von Sicherheitsanforderungen (IT-Sicherheitskatalog) die Anforderungen an den angemessenen Schutz. Dabei beteiligt die Bundesnetzagentur die Betreiber von Energieversorgungsnetzen und deren Branchenverbände. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf. Ein angemessener Schutz nach Satz 1 liegt vor, wenn die Anforderung des IT-Sicherheitskatalogs eingehalten werden. Die Einhaltung der Anforderungen des IT-Sicherheitskatalogs ist vom Betreiber zu dokumentieren.

(2) Der Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle nach Artikel 1 dieses Gesetzes] in der jeweils geltenden Fassung oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, hat einen angemessenen Schutz gegen Bedrohungen für Telekommunikationssysteme sowie elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. Der angemessene Schutz nach Satz 1 ist auch durch Berücksichtigung erforderlicher Anforderungen bei der Beschaffung von Anlagengütern und Dienstleistungen sicherzustellen. Die Bundesnetzagentur bestimmt im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 in einem IT-Sicherheitskatalog die Anforderungen an den angemessenen Schutz. Dabei beteiligt die Bundesnetzagentur die Betreiber nach Satz 1 und deren Branchenverbände. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf. Für Telekommunikationssysteme sowie elektronische Datenverarbeitungssysteme von Anlagen nach § 7 Absatz 1 des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 16 des Gesetzes vom … [einsetzen: Datum und Fundstelle nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes] geändert worden ist, haben Vorgaben auf Grund des Atomgesetzes Vorrang vor den Anforderungen des IT-Sicherheitskatalogs nach Satz 4. Die für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder sind bei der Erarbeitung des IT-Sicherheitskatalogs nach Satz 4 zu beteiligen. Ein angemessener Schutz nach Satz 1 liegt vor, wenn die Anforderungen des IT-Sicherheitskatalogs eingehalten werden. Die Einhaltung der Anforderungen des IT-Sicherheitskatalogs ist vom Betreiber zu dokumentieren.

(3) Der IT-Sicherheitskatalog nach Absatz 1 Satz 3 und der IT-Sicherheitskatalog nach Absatz 2 Satz 4 sollen jeweils den Stand der Technik einhalten und unter Berücksichtigung der einschlägigen europäischen Normen oder der einschlägigen internationalen Normen sowie der Umsetzungskosten ein Sicherheits-

niveau der informationstechnischen Systeme, Komponenten und Prozesse gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung, ob Maßnahmen dem bestehenden Risiko angemessen sind, sind das Ausmaß der Risikoexposition und die Größe des Betreibers sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen, zu berücksichtigen. Der IT-Sicherheitskatalog nach Absatz 1 Satz 3 und der IT-Sicherheitskatalog nach Absatz 2 Satz 4 umfassen jeweils zumindest Vorgaben für:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationstechnik,
2. die Bewältigung von Sicherheitsvorfällen,
3. die Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und für das Krisenmanagement,
4. die Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit der Informationstechnik,
7. grundlegende Verfahren im Bereich der Cyberhygiene und für Schulungen im Bereich der Sicherheit der Informationstechnik,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
9. die Sicherheit des Personals, Konzepte für die Zugriffskontrolle und das Management von Anlagen,
10. die Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung,
11. den Einsatz von Systemen zur Angriffserkennung nach § 2 Nummer 41 des BSI-Gesetzes,
12. den Einsatz eines Elements oder einer Gruppe von Elementen eines Netz- oder Informationssystems (IKT-Produkt), eines Dienstes, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht (IKT-Dienst) und jeglicher Tätigkeiten, mit denen ein IKT-Produkt oder IKT-Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll (IKT-Prozess) mit Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (ABl. 151 vom 7.6.2019, S. 15).

Die Bundesnetzagentur kann in den IT-Sicherheitskatalogen nähere Bestimmungen zu Format, Inhalt und Gestaltung der nach Absatz 1 Satz 7 oder nach Absatz 2 Satz 10 erforderlichen Dokumentation über die Einhaltung der Anforderungen des jeweiligen IT-Sicherheitskatalogs sowie zur Behebung von Sicherheitsmängeln treffen. Die Bundesnetzagentur kann in den IT-Sicherheitskatalogen auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen treffen.

(4) Der Betreiber eines Energieversorgungsnetzes oder der Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, hat der Bundesnetzagentur die Dokumentation über die Einhaltung der Anforderungen des jeweiligen IT-Sicherheitskatalogs nach Absatz 1 Satz 7 oder nach Absatz 2 Satz 10 zu übermitteln. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. Bei Bedarf kann die Bundesnetzagentur die Vorlage des Mängelbeseitigungsplans von dem Betreiber nach Satz 1 anfordern. Die Bundesnetzagentur kann bei Sicherheitsmängeln, die sich aus dem Mängelbeseitigungsplan ergeben, von dem Betreiber nach Satz 1 die Beseitigung dieser Mängel innerhalb einer durch die Bundesnetzagentur gesetzten Frist verlangen. Der Betreiber nach Satz 1 hat der Bundesnetzagentur und den in deren Auftrag han-

delnden Personen zum Zweck der Überprüfung der Einhaltung der Sicherheitsanforderungen nach Absatz 1 oder Absatz 2 das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung erhebt die Bundesnetzagentur Gebühren und Auslagen nur, sofern die Bundesnetzagentur auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der in den Absätzen 1 und 2 genannten Anforderungen begründen.

(5) Erlangt die Bundesnetzagentur Kenntnis über Hinweise oder Informationen, wonach ein Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, die Sicherheitsanforderungen nach Absatz 2 nicht oder nicht richtig umsetzt, so kann sie von diesem Betreiber Informationen anfordern, um die Einhaltung der Sicherheitsanforderungen nach Absatz 2 zu überprüfen. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. Absatz 4 Satz 3 bis 6 ist entsprechend anzuwenden.

(6) Der Betreiber eines Energieversorgungsnetzes oder der Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, ist verpflichtet, folgende Informationen an eine vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete gemeinsame Meldestelle zu melden:

1. unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall nach § 2 Nummer 11 des BSI-Gesetzes, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf eine rechtswidrige oder eine böswillige Handlung zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte,
2. unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall nach § 2 Nummer 11 des BSI-Gesetzes, eine Meldung über den erheblichen Sicherheitsvorfall, in der die in Nummer 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden,
3. auf Ersuchen des Bundesamtes für Sicherheit in der Informationstechnik eine Zwischenmeldung über relevante Statusaktualisierungen,
4. spätestens einen Monat nach Übermittlung der Meldung des erheblichen Sicherheitsvorfalls nach § 2 Nummer 11 des BSI-Gesetzes eine Abschlussmeldung, die Folgendes enthält:
   a) eine ausführliche Beschreibung des erheblichen Sicherheitsvorfalls nach § 2 Nummer 11 des BSI-Gesetzes, einschließlich seines Schweregrads und seiner Auswirkungen,
   b) Angaben zur Art der Bedrohung beziehungsweise zugrunde liegenden Ursache, die wahrscheinlich den erheblichen Sicherheitsvorfall nach § 2 Nummer 11 des BSI-Gesetzes ausgelöst hat,
   c) Angaben zu den getroffenen und den laufenden Abhilfemaßnahmen,
   d) gegebenenfalls die grenzüberschreitenden Auswirkungen des erheblichen Sicherheitsvorfalls nach § 2 Nummer 11 des BSI-Gesetzes.

§ 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. § 32 Absatz 2 bis 5 und § 36 des BSI-Gesetzes sind entsprechend anzuwenden. Bei Meldungen nach diesem Absatz trifft das Bundesamt für Sicherheit in der Informationstechnik Maßnahmen nach § 36 des BSI-Gesetzes im Benehmen mit der Bundesnetzagentur.

(7) Das Bundesamt für Sicherheit in der Informationstechnik hat die Meldungen nach Absatz 6 und solche Meldungen über Sicherheitsvorfälle nach § 32 des BSI-Gesetzes, bei welchen das Bundesamt für Sicherheit in der Informationstechnik Kenntnis von einer Relevanz für die Energieversorgungssicherheit und Erfüllung der Zwecke und Ziele nach § 1 erlangt, unverzüglich an die Bundesnetzagentur weiterzuleiten. Die Bundesnetzagentur führt unverzüglich eine Bewertung der Auswirkungen des nach Satz 1 übermittelten Si-

cherheitsvorfalls auf die Energieversorgungssicherheit durch und übermittelt ihre Ergebnisse an das Bundesamt für Sicherheit in der Informationstechnik. Die Bundesnetzagentur kann von dem betroffenen Unternehmen die Herausgabe der zur Bewertung der Auswirkungen des Sicherheitsvorfalls auf die Energieversorgungssicherheit notwendigen Informationen, einschließlich personenbezogener Daten, verlangen und ist befugt, zur Bewertung der Auswirkungen des Sicherheitsvorfalls auf die Energieversorgungssicherheit erforderliche personenbezogene Daten zu erheben, zu speichern und zu verwenden. Das betroffene Unternehmen hat der Bundesnetzagentur die zur Bewertung der Auswirkungen des Sicherheitsvorfalls auf die Energieversorgungssicherheit notwendigen Informationen, einschließlich personenbezogener Daten, zu übermitteln. Die Bundesnetzagentur kann bei der Durchführung der Bewertung nach Satz 2 die Betreiber von Übertragungs-, von Fernleitungs- sowie von Verteilnetzen einbeziehen und ist befugt, ihnen die hierzu erforderlichen personenbezogenen Daten zu übermitteln. Die Betreiber von Übertragungs-, von Fernleitungs- sowie von Verteilnetzen sind befugt, die ihnen nach Satz 5 zum dort genannten Zweck übermittelten personenbezogenen Daten zu erheben, zu speichern und zu verwenden. Nach Erstellung der Bewertung sind die hierzu verwendeten personenbezogenen Daten von der Bundesnetzagentur und den Betreibern von Übertragungs-, von Fernleitungs- sowie von Verteilnetzen unverzüglich zu löschen. Das Bundesamt für Sicherheit in der Informationstechnik berücksichtigt die Bewertung der Bundesnetzagentur bei der Erfüllung der Aufgaben nach § 40 Absatz 3 Nummer 2 des BSI-Gesetzes. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben jeweils sicherzustellen, dass die unbefugte Offenbarung der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Zugang zu den Akten des Bundesamtes für Sicherheit in der Informationstechnik sowie zu den Akten der Bundesnetzagentur in Angelegenheiten nach den Absätzen 1 bis 6 sowie dieses Absatzes wird nicht gewährt. § 29 des Verwaltungsverfahrensgesetzes bleibt unberührt.

(8) Der Betreiber eines Energieversorgungsnetzes oder einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, ist verpflichtet, spätestens drei Monate, nachdem er erstmals oder erneut als eine der vorgenannten Einrichtungen gilt, dem Bundesamt für Sicherheit in der Informationstechnik über eine gemeinsam vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit die Angaben nach § 33 Absatz 1 Nummer 1 bis 4 des BSI-Gesetzes zu übermitteln. Der Betreiber eines Energieversorgungsnetzes, der nicht eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder nicht eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist, ist verpflichtet, spätestens bis zum Ablauf des … [einsetzen: Datum desjenigen Tages des dritten auf den Monat des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes folgenden Kalendermonats, dessen Zahl mit der des Tages der des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes übereinstimmt, oder, wenn es einen solchen Kalendertag nicht gibt, Datum des ersten Tages des darauffolgenden Kalendermonats] dem Bundesamt für Sicherheit in der Informationstechnik über eine gemeinsam vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit die Angaben nach § 33 Absatz 1 Nummer 1 bis 4 des BSI-Gesetzes zu übermitteln. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. § 33 Absatz 2, 4 und 5 des BSI-Gesetzes ist entsprechend anzuwenden. Das Bundesamt für Sicherheit in der Informationstechnik übermittelt die Registrierungen nach den Sätzen 1 und 2 einschließlich der damit verbundenen Kontaktdaten und jede Änderung der Registrierungen unverzüglich an die Bundesnetzagentur. Die Registrierungen nach den Sätzen 1 und 2 kann das Bundesamt für Sicherheit in der Informationstechnik auch selbst vornehmen und eine Kontaktstelle benennen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Nimmt das Bundesamt für Sicherheit in der Informationstechnik eine solche Registrierung selbst vor, informiert es sowohl den betreffenden Betreiber als auch die Bundesnetzagentur darüber und übermittelt die damit verbundenen Kontaktdaten. Jeder Betreiber hat sicherzustellen, dass er über die benannte oder durch das Bundesamt für Sicherheit in der Informationstechnik festgelegte Kontaktstelle jederzeit erreichbar ist. Die Übermittlung von Informationen durch das Bundesamt für Sicherheit in der Informationstechnik nach § 40 Absatz 3 Nummer 4 Buchstabe a des BSI-Gesetzes erfolgt an diese Kontaktstelle.

(9) Geschäftsleitungen eines Betreibers eines Energieversorgungsnetzes oder eines Betreibers einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein

Energieversorgungsnetz angeschlossen ist, sind verpflichtet, die Sicherheitsanforderungen nach Absatz 1 oder Absatz 2 umzusetzen und ihre Umsetzung zu überwachen. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt.

(10) Geschäftsleitungen, die ihre Pflichten nach Absatz 9 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.

(11) Die Geschäftsleitungen eines Betreibers eines Energieversorgungsnetzes oder eines Betreibers einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt.

(12) Die Bundesnetzagentur legt bis zum Ablauf des … [einsetzen: Datum desjenigen Tages des ersten auf den Monat des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes folgenden Kalendermonats, dessen Zahl mit der des Tages des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes übereinstimmt, oder, wenn es einen solchen Kalendertag nicht gibt, Datum des ersten Tages des darauffolgenden Kalendermonats] im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Allgemeinverfügung im Wege einer Festlegung nach § 29 Absatz 1 in einem Katalog von Sicherheitsanforderungen für das Betreiben von Energieversorgungsnetzen und Energieanlagen fest,

1. welche Komponenten kritische Komponenten nach § 2 Nummer 23 Buchstabe c Doppelbuchstabe aa des BSI-Gesetzes sind oder
2. welche Funktionen kritisch bestimmte Funktionen nach § 2 Nummer 23 Buchstabe c Doppelbuchstabe bb des BSI-Gesetzes sind.

Der Betreiber eines Energieversorgungsnetzes, das eine kritische Anlage nach § 2 Nummer 22 des BSI-Gesetzes ist, oder der Betreiber einer Energieanlage, die eine kritische Anlage nach § 2 Nummer 22 des BSI-Gesetzes ist, hat die Vorgaben des Katalogs spätestens sechs Monate nach dessen in der Allgemeinverfügung bestimmten Inkrafttreten zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden. Der Katalog wird mit den IT-Sicherheitskatalogen nach den Absätzen 1 und 2 verbunden.“

3. § 11 Absatz 1a bis 1g wird aufgehoben.
4. § 59 Absatz 1 Nummer 1a wird wie folgt gefasst:

   „1a. die Festlegungen nach § 5c Absatz 1, 2 sowie 12,“.
5. In § 91 Absatz 1 Satz 1 Nummer 4 wird nach den Wörtern „Amtshandlungen auf Grund der §§“ die Angabe „5c Absatz 4,“ eingefügt.
6. § 95 wird wie folgt geändert:
   a) Absatz 1 wird wie folgt geändert:
      aa) Die Nummern 2a und 2b werden aufgehoben.
      bb) Nach Nummer 3a werden die folgenden Nummern 3b bis 3d eingefügt:
         „3b. entgegen § 5c Absatz 1 Satz 1 oder Absatz 2 Satz 1 einen dort genannten Schutz nicht gewährleistet,
         3c. entgegen § 5c Absatz 1 Satz 7 oder Absatz 2 Satz 10 die Einhaltung der Anforderungen des IT-Sicherheitskatalogs nicht, nicht richtig oder nicht vollständig dokumentiert,

3d. entgegen § 5c Absatz 6 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,“.

cc) Die bisherigen Nummern 3b bis 3d werden die Nummern 3e bis 3g.

dd) Die bisherigen Nummern 3f bis 3i werden die Nummern 3h bis 3k.

b) Nach Absatz 2 werden die folgenden Absätze 2a bis 2d eingefügt:

„(2a) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 3b bis 3d geahndet werden:

1. bei besonders wichtigen Einrichtungen nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes mit einer Geldbuße bis zu zehn Millionen Euro,
2. bei wichtigen Einrichtungen nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes mit einer Geldbuße bis zu sieben Millionen Euro und
3. in den übrigen Fällen mit einer Geldbuße bis zu einer Million Euro.

(2b) Bei einer besonders wichtigen Einrichtung im Sinne des § 28 Absatz 1 Satz 1 des BSI-Gesetzes mit einem Jahresumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 2a Nummer 1 eine Ordnungswidrigkeit nach Absatz 1 Nummer 3b, 3c und 3d mit einer Geldbuße bis zu 2 Prozent des Jahresumsatzes geahndet werden.

(2c) Bei einer wichtigen Einrichtung im Sinne des § 28 Absatz 2 Satz 1 des BSI-Gesetzes mit einem Jahresumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 2a Nummer 2 eine Ordnungswidrigkeit nach Absatz 1 Nummer 3b, 3c und 3d mit einer Geldbuße bis zu 1,4 Prozent des Jahresumsatzes geahndet werden.

(2d) § 65 Absatz 8 des BSI-Gesetzes ist entsprechend anzuwenden.“

c) In Absatz 5 wird die Angabe „Nummer 2b“ durch die Angabe „Nummer 3d“ ersetzt.

Artikel 18

Änderung des Messstellenbetriebsgesetzes

In § 24 Absatz 2 des Messstellenbetriebsgesetzes vom 29. August 2016 (BGBl. I S. 2034), das zuletzt durch Artikel 7 des Gesetzes vom 8. Mai 2024 (BGBl. 2024 I Nr. 151) geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821)“ durch die Wörter „§ 52 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle nach Artikel 1 dieses Gesetzes] in der jeweils geltenden Fassung“ ersetzt.

Artikel 19

Änderung des Energiesicherungsgesetzes

Das Energiesicherungsgesetz vom 20. Dezember 1974 (BGBl. I S. 3681), das zuletzt durch Artikel 1 des Gesetzes vom 23. Juni 2023 (BGBl. 2023 I Nr. 167) geändert worden ist, wird wie folgt geändert:

1. Dem § 10 Absatz 1 wird folgender Satz angefügt:

„Soweit Daten im Sinne des Satzes 3 für Maßnahmen nach § 1 der Gassicherungsverordnung vom 26. April 1982 (BGBl. I S. 517), die zuletzt durch Artikel 1 der Verordnung vom 31. März 2023 (BGBl. 2023 Nr. 94) geändert worden ist, und für Solidaritätsmaßnahmen nach § 2a von der Bundesnetzagentur erlangt werden, übermittelt diese die Daten auf deren Ersuchen und, soweit dies für die Erfüllung von deren Aufgaben erforderlich ist, an die Bundesanstalt für Finanzdienstleistungsaufsicht.“

2. In § 17 Absatz 1, § 18 Absatz 2 Satz 1 Nummer 1 und § 29 Absatz 1 Satz 1 werden jeweils die Wörter „Kritische Infrastrukturen“ durch die Wörter „kritische Anlagen“ und die Wörter „§ 2 Absatz 10 des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 22 des BSI-Gesetzes“ ersetzt.

Artikel 20

Änderung des Wärmeplanungsgesetzes

In § 11 Absatz 4 Satz 1 des Wärmeplanungsgesetzes vom 20. Dezember 2023 (BGBl. 2023 I Nr. 394), werden die Wörter „Kritischen Infrastrukturen“ durch die Wörter „kritischen Anlagen“ und die Wörter „§ 2 Absatz 10 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist“ durch die Wörter „§ 2 Nummer 22 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle nach Artikel 1 dieses Gesetzes] in der jeweils geltenden Fassung“ ersetzt.

Artikel 21

Änderung des Fünften Buches Sozialgesetzbuch

Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 3 des Gesetzes vom 30. Mai 2024 (BGBl. 2024 I Nr. 173) geändert worden ist, wird wie folgt geändert:

1. § 391 wird wie folgt geändert:
   a) In Absatz 4 werden die Wörter „§ 8a Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 30 Absatz 8 des BSI-Gesetzes“ ersetzt.
   b) In Absatz 5 werden die Wörter „Kritischer Infrastrukturen“ durch die Wörter „kritischer Anlagen“ und die Wörter „§ 8a des BSI-Gesetzes“ durch die Wörter „den §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.
2. § 392 wird wie folgt geändert:
   a) In Absatz 3 werden die Wörter „§ 8a Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 30 Absatz 8 des BSI-Gesetzes“ ersetzt.
   b) In Absatz 5 werden die Wörter „Kritischer Infrastrukturen“ durch die Wörter „kritischer Anlagen“ und die Wörter „§ 8a des BSI-Gesetzes“ durch die Wörter „den §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.

Artikel 22

Änderung der Digitale Gesundheitsanwendungen-Verordnung

In Anlage 1 der Digitale Gesundheitsanwendungen-Verordnung vom 8. April 2020 (BGBl. I S. 768), die zuletzt durch Artikel 4 des Gesetzes vom 22. März 2024 (BGBl. 2024 I Nr. 101) geändert worden ist, werden in dem Abschnitt „Datensicherheit“, Unterabschnitt „Basisanforderungen, die für alle digitalen Gesundheitsanwendungen gelten“ in Nummer 5 in der Spalte „Anforderung“ die Wörter „§ 8 Absatz 1 Satz 1 des BSI-Gesetzes“ durch die Wörter „§ 44 Absatz 1 Satz 1 des BSI-Gesetzes“ ersetzt.

Artikel 23

Änderung des Sechsten Buches Sozialgesetzbuch

Das Sechste Buch Sozialgesetzbuch – Gesetzliche Rentenversicherung – in der Fassung der Bekanntmachung vom 19. Februar 2002 (BGBl. I S. 754, 1404, 3384), das zuletzt durch Artikel 1 des Gesetzes vom 30. Mai 2024 (BGBl. 2024 I Nr. 173) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:
   a) Nach der Angabe zu § 145 wird folgende Angabe eingefügt:

      „Achter Unterabschnitt

      Sicherheit in der Informationstechnik“.

   b) Die Angabe zu § 146 wird wie folgt gefasst:

      „§ 146 Verbindliche Entscheidungen zur Sicherheit der Informationstechnik“.
2. § 138 Absatz 1 Satz 2 wird wie folgt geändert:
   a) In Nummer 15 wird das Wort „und“ am Ende durch ein Komma ersetzt.
   b) In Nummer 16 wird der Punkt am Ende durch das Wort „und“ ersetzt.
   c) Folgende Nummer 17 wird angefügt:

      „17. Koordinierung einer an den Zielen von Wirtschaftlichkeit und Sicherheit ausgerichteten Informationstechnik der Rentenversicherung.“
3. Nach § 145 wird folgende Überschrift eingefügt:

   „Achter Unterabschnitt

   Sicherheit in der Informationstechnik“.

4. § 146 wird wie folgt gefasst:

   „§ 146

   Verbindliche Entscheidungen zur Sicherheit der Informationstechnik

   Die Deutsche Rentenversicherung Bund hat in Wahrnehmung der ihr nach § 138 Absatz 1 Satz 2 Nummer 17 zugewiesenen Aufgaben bis 30. Juni 2025 folgende verbindliche Entscheidungen herbeizuführen:

   1. zur Festlegung von einheitlichen Grundsätzen für die Informationstechnik und Informationssicherheit der Rentenversicherung,
   2. zum Betrieb der informationstechnischen Infrastruktur und des Netzwerkes der Rentenversicherung,
   3. zur Entwicklung rentenversicherungsbezogener Anwendungen und
   4. zur Festlegung eines Beschaffungskonzepts.

Satz 1 gilt im Verhältnis zur Deutschen Rentenversicherung Knappschaft-Bahn-See mit der Maßgabe, dass notwendige Abweichungen wegen der dieser übertragenen weiteren gesetzlichen Aufgaben und ihrer spezifischen Leistungen zulässig sind.“

Artikel 24

Änderung der Verordnung zum Barrierefreiheitsstärkungsgesetz

In § 2 Nummer 3 der Verordnung zum Barrierefreiheitsstärkungsgesetz vom 15. Juni 2022 (BGBl. I S. 928) werden die Wörter „§ 2 Absatz 2 Satz 4 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist“ durch die Wörter „§ 2 Nummer 39 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle dieses Gesetzes]“.

Artikel 25

Änderung des Elften Buches Sozialgesetzbuch

§ 103a des Elften Buch Sozialgesetzbuch – Soziale Pflegeversicherung – (Artikel 1 des Gesetzes vom 26. Mai 1994, BGBl. I S. 1014, 1015), das zuletzt durch Artikel 4 des Gesetzes vom 30. Mai 2024 (BGBl. 2024 I Nr. 173) geändert worden ist, wird wie folgt geändert:

1. In Absatz 3 werden die Wörter „§ 8a Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 30 Absatz 8 des BSI-Gesetzes“ ersetzt.
2. In Absatz 5 werden die Wörter „Kritischer Infrastrukturen“ durch die Wörter „kritischer Anlagen“ und die Wörter „§ 8a des BSI-Gesetzes“ durch die Wörter „den §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.

Artikel 26

Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 35 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 168 wie folgt gefasst:

   „§ 168 Meldung eines Sicherheitsvorfalls“.

2. § 3 wird wie folgt geändert:

   a) Nummer 53 wird wie folgt gefasst:

      „53. „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigt;“.

   b) In Nummer 79 wird der Punkt am Ende durch ein Semikolon ersetzt.

   c) Folgende Nummer 80 wird angefügt:

      „80. „Netz- und Informationssystem“

         a) ein Telekommunikationsnetz im Sinne von Nummer 65,

b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder

c) digitale Daten, die von den in den Buchstaben a und b genannten Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden."

3. § 165 wird wie folgt geändert:

a) Absatz 2 Satz 3 wird durch die folgende Sätze ersetzt:

„Bei diesen Maßnahmen ist unter Berücksichtigung des Stands der Technik, der einschlägigen europäischen und internationalen Normen sowie der Umsetzungskosten ein Sicherheitsniveau der Netz- und Informationssysteme zu gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung, ob Maßnahmen dem bestehenden Risiko angemessen sind, sind das Ausmaß der Risikoexposition und die Größe des Betreibers oder des Anbieters sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen."

b) Nach Absatz 2 werden die folgenden Absätze 2a bis 2d eingefügt:

„(2a) Maßnahmen nach Absatz 2 von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Widerherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Maßnahmen nach Absatz 2 im Bereich der Sicherheit von Netzen und Diensten,
7. Grundlegende Verfahren und Schulungen im Bereich der Sicherheit von Netzen und Diensten,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

(2b) Die Geschäftsleitungen von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, sind verpflichtet, die von diesen Einrichtungen nach Absatz 2 zu ergreifenden Maßnahmen umzusetzen und ihre Umsetzung zu überwachen.

(2c) Geschäftsleitungen, die ihre Pflichten nach Absatz 2b verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Re-

geln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.

(2d) Die Geschäftsleitungen von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können."

c) In Absatz 3 Satz 1 werden die Wörter „§ 2 Absatz 9b des BSI-Gesetzes" durch die Wörter „§ 2 Nummer 41 des BSI-Gesetzes" ersetzt.

d) In Absatz 4 werden die Wörter „§ 2 Absatz 13 des BSI-Gesetzes" durch die Wörter „§ 2 Nummer 23 des BSI-Gesetzes" ersetzt.

e) In Absatz 11 Satz 1 werden die Wörter „Artikel 9 der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1; L 33 vom 7.2.2018, S. 5)" durch die Wörter „Artikel 10 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 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80)" ersetzt.

4. In § 167 Absatz 1 Satz 1 Nummer 2 werden die Wörter „§ 2 Absatz 13 Satz 1 Nummer 3 Buchstabe b des BSI-Gesetzes" durch die Wörter „§ 2 Nummer 23 Buchstabe c Doppelbuchstabe bb des BSI-Gesetzes" und die Wörter „§ 2 Absatz 13 des BSI-Gesetzes" durch die Wörter „§ 2 Nummer 23 des BSI-Gesetzes" ersetzt.

5. § 168 wird wie folgt geändert:

a) Die Überschrift wird wie folgt gefasst:

„§ 168

Meldung eines Sicherheitsvorfalls".

b) Die Absätze 1 bis 3 werden wie folgt gefasst:

„(1) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, übermittelt der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik:

1. unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;

2. unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Meldung über den Sicherheitsvorfall, in der die in Nummer 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;

3. auf Ersuchen der Bundesnetzagentur oder dem Bundesamt für Sicherheit in der Informationstechnik eine Zwischenmeldung über relevante Statusaktualisierungen;

4. spätestens einen Monat nach Übermittlung der Meldung des erheblichen Sicherheitsvorfalls gemäß Nummer 2, vorbehaltlich Absatz 2, eine Abschlussmeldung, die Folgendes enthält:

   a) eine ausführliche Beschreibung des erheblichen Sicherheitsvorfalls, einschließlich seines Schwergrads und seiner Auswirkungen;

   b) Angaben zur Art der Bedrohung beziehungsweise zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;

   c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;

   d) Gegebenenfalls die grenzüberschreitenden Auswirkungen des erheblichen Sicherheitsvorfalls.

§ 42 Absatz 4 und § 43 Absatz 4 des Bundesdatenschutzgesetzes gelten entsprechend.

(2) Dauert der erhebliche Sicherheitsvorfall im Zeitpunkt des Absatzes 1 Nummer 4 noch an, legt der Betroffene statt einer Abschlussmeldung zu diesem Zeitpunkt eine Fortschrittsmeldung und eine Abschlussmeldung innerhalb eines Monats nach Abschluss der Bearbeitung des erheblichen Sicherheitsvorfalls vor.

(3) Ein Sicherheitsvorfall gilt als erheblich, wenn

1. er schwerwiegende Betriebsstörungen oder finanzielle Verluste für den betreffenden Betreiber öffentlicher Telekommunikationsnetze oder Anbieter öffentlich zugänglicher Telekommunikationsdienste verursacht hat oder verursachen kann oder

2. er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.“

c) In Absatz 4 wird das Wort „Mitteilungsverfahrens“ durch das Wort „Meldeverfahrens“ ersetzt.

d) Nach Absatz 4 wird folgender Absatz 5 eingefügt:

„(5) Die Bundesnetzagentur übermittelt den nach Absatz 1 Satz 1 Verpflichteten unverzüglich und nach Möglichkeit innerhalb von 24 Stunden nach der frühen Erstmeldung nach Absatz 1 Satz 1 Nummer 1 eine Bestätigung über den Eingang der Meldung. Das Bundesamt für Sicherheit in der Informationstechnik kann auf Ersuchen der nach Absatz 1 Satz 1 Verpflichteten zusätzliche technische Unterstützung, Orientierungshilfen oder operative Beratung zu Abhilfemaßnahmen leisten. Das Bundesamt für Sicherheit in der Informationstechnik informiert die Bundesnetzagentur über Maßnahmen nach Satz 2.“

e) Der bisherige Absatz 5 wird Absatz 6 und wird wie folgt gefasst:

„(6) Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Agentur der Europäischen Union für Cybersicherheit über den Sicherheitsvorfall. Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Sicherheitsvorfall zu verhindern oder zu bewältigen, oder liegt die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann die Bundesnetzagentur nach Anhörung der nach Absatz 1 Satz 1 Verpflichteten die Öffentlichkeit unterrichten oder die nach Absatz 1 Satz 1 Verpflichteten zu dieser Unterrichtung verpflichten.“

f) Der bisherige Absatz 6 wird Absatz 7 und die Wörter „§ 8e des BSI-Gesetzes“ werden durch die Wörter „§ 42 des BSI-Gesetzes“ ersetzt.

g) Der bisherige Absatz 7 wird Absatz 8.

6. In § 174 Absatz 3 Nummer 8 und Absatz 5 Nummer 8 werden die Wörter „Bereichen des § 2 Absatz 10 Satz 1 Nummer 1 des BSI-Gesetzes“ durch die Wörter „Sektoren des § 2 Nummer 24 des BSI-Gesetzes“ ersetzt.

7. In § 214 Absatz 3 werden die Wörter „Kritische Infrastrukturen“ durch die Wörter „kritische Anlagen“ und die Wörter „§ 2 Absatz 10 des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 22 des BSI-Gesetzes“ ersetzt.

8. In § 228 Absatz 2 Nummer 39 werden die Wörter „eine Mitteilung“ durch die Wörter „eine Meldung oder Mitteilung“ ersetzt.

Artikel 27

Änderung der Krankenhausstrukturfonds-Verordnung

Die Krankenhausstrukturfonds-Verordnung vom 17. Dezember 2015 (BGBl. I S. 2350), die zuletzt durch Artikel 6 des Gesetzes vom 20. Dezember 2022 (BGBl. I S. 2793) geändert worden ist, wird wie folgt geändert:

1. In § 11 Absatz 1 Nummer 4 Buchstabe a werden nach den Wörtern „Anhangs 5 Teil 3 der BSI-Kritisverordnung“ die Wörter „vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 1 der Verordnung vom 29. November 2023 (BGBl. 2023 I Nr. 339) geändert worden ist,“ eingefügt und werden die Wörter „an die Vorgaben von § 8a des BSI-Gesetzes“ durch die Wörter „an die Anforderungen der §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.
2. In § 14 Absatz 2 Nummer 8 werden die Wörter „an die Vorgaben von § 8a des BSI-Gesetzes“ durch die Wörter „an die Anforderungen der §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.

Artikel 28

Änderung der Außenwirtschaftsverordnung

§ 55a Absatz 1 der Außenwirtschaftsverordnung vom 2. August 2013 (BGBl. I S. 2865), die zuletzt durch Artikel 3 des Gesetzes vom 27. Februar 2024 (BGBl. 2024 I Nr. 71) geändert worden ist, wird wie folgt geändert:

1. In Nummer 1 werden die Wörter „Kritischen Infrastruktur“ durch die Wörter „kritischen Anlage“ ersetzt.
2. In Nummer 2 werden die Wörter „§ 2 Absatz 13 des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 23 des BSI-Gesetzes“ und die Wörter „Kritischen Infrastrukturen“ durch die Wörter „kritischen Anlagen“ ersetzt.

Artikel 29

Änderung des Vertrauensdienstegesetzes

§ 2 Absatz 3 des Vertrauensdienstegesetzes vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist, wird aufgehoben.

Artikel 30

Weitere Änderung des BSI-Gesetzes

Das BSI-Gesetz, das durch Artikel 1 dieses Gesetzes neu gefasst worden ist, wird wie folgt geändert:

1. § 2 wird wie folgt geändert:
   a) Nummer 22 wird wie folgt gefasst:

      „22. „kritische Anlage“ eine Anlage im Sinne von § 2 Nummer 3 des Dachgesetzes zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz);“.

b) In Nummer 23 wird die Angabe „Nummer 24“ durch die Wörter „§ 4 Absatz 1 des KRITIS-Dachgesetzes“ ersetzt.

c) Nummer 24 wird aufgehoben.

2. In § 12 Absatz 1 Satz 2 wird die Angabe „§ 2 Nummer 24“ durch die Wörter „§ 4 Absatz 1 des KRITIS-Dachgesetzes“ ersetzt.

3. § 28 Absatz 7 wird aufgehoben.

4. In § 33 Absatz 2 Satz 1 und § 41 Absatz 2 Satz 1, Absatz 3 Satz 4, Absatz 4 Satz 1, Absatz 6 Satz 1 und Absatz 7 wird jeweils die Angabe „§ 56 Absatz 4“ durch die Wörter „§ 5 Absatz 1 in Verbindung mit § 4 Absatz 3 des KRITIS-Dachgesetzes“ ersetzt.

5. § 56 Absatz 4 wird aufgehoben.

6. In § 65 Absatz 1 und Absatz 2 Nummer 6 und 10 werden jeweils die Wörter „§ 56 Absatz 4 Satz 1“ durch die Wörter „§ 5 Absatz 1 in Verbindung mit § 4 Absatz 3 des KRITIS-Dachgesetzes“ ersetzt.

Artikel 31

Weitere Änderung des Telekommunikationsgesetzes

In § 174 Absatz 3 Nummer 8 und Absatz 5 Nummer 8 des Telekommunikationsgesetzes vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 26 dieses Gesetzes geändert worden ist, werden jeweils die Wörter „§ 2 Nummer 24 des BSI-Gesetzes“ durch die Wörter „§ 4 Absatz 1 des KRITIS-Dachgesetzes“ ersetzt.

Artikel 32

Weitere Änderung der Außenwirtschaftsverordnung

In § 55a Absatz 1 Nummer 1 und 2 der Außenwirtschaftsverordnung vom 2. August 2013 (BGBl. I S. 2865; 2021 I S. 4304), die zuletzt durch Artikel 28 dieses Gesetzes geändert worden ist, werden die Wörter „im Sinne des BSI-Gesetzes“ durch die Wörter „gemäß § 2 Nummer 3 des KRITIS-Dachgesetzes“ ersetzt.

Artikel 33

Inkrafttreten, Außerkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach der Verkündung in Kraft. Gleichzeitig tritt das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821) außer Kraft.

(2) Die Artikel 30, 31 und 32 treten an dem Tag in Kraft, an dem die Rechtsverordnung nach § 5 Absatz 1 in Verbindung mit § 4 Absatz 3 des Dachgesetzes zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz) in Kraft tritt, aber nicht vor dem Inkrafttretenstermin nach Absatz 1. Das Bundesministerium des Innern und für Heimat gibt den Tag des Inkrafttretens im Bundesgesetzblatt bekannt.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Die moderne Wirtschaft Deutschlands ist für ihr Funktionieren, die Generierung von Wohlstand und Wachstum und auch für ihre Adaptionsfähigkeit auf geänderte wirtschaftspolitische und geopolitische Rahmenbedingungen angewiesen auf funktionierende und resiliente Infrastruktur, sowohl im physischen als auch im digitalen Bereich. Diese Faktoren haben in den vergangenen Jahren erheblich an Bedeutung gewonnen. Unternehmen sehen sich nicht nur in ihrem wirtschaftlichen Tun, sondern auch in dessen praktischer Absicherung vor eine Vielzahl von Herausforderungen gestellt. Europaweit und global vernetzte Prozesse führen ebenso wie die zunehmende Digitalisierung aller Lebens- und somit auch Wirtschaftsbereiche zu einer höheren Anfälligkeit gegenüber externen, vielfach nicht steuerbaren Faktoren. Informationstechnik in kritischen Anlagen sowie in bestimmten Unternehmen spielt dabei eine zentrale Rolle. Ihre Sicherheit und Resilienz bilden auch die Grundlage für die Versorgungssicherheit, von der Versorgung mit Strom und Wasser bis hin zur Entsorgung von Siedlungsabfällen. Gleiches gilt für das Funktionieren der Marktwirtschaft in Deutschland und dem Binnenmarkt der Europäischen Union. Die Vernetzung und enge Verzahnung gerade der Wirtschaft innerhalb Deutschlands und der Europäischen Union resultieren in Interdependenzen bei der Cybersicherheit. Die vor diesem Hintergrund gestiegenen Cybersicherheitsanforderungen an juristische und natürliche Personen, die wesentliche Dienste erbringen oder Tätigkeiten ausüben, 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.

Mit der NIS-2-Richtlinie wurden Maßnahmen festgelegt, mit denen in der gesamten Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll, um so das Funktionieren des Binnenmarkts zu verbessern. Zu diesem Zweck wird in der NIS-2-Richtlinie die Pflicht für alle Mitgliedstaaten festgelegt, nationale Cybersicherheitsstrategien zu verabschieden sowie zuständige nationale Behörden, Behörden für das Cyberkrisenmanagement, zentrale Anlaufstellen für Cybersicherheit (zentrale Anlaufstellen) und Computer-Notfallteams (CSIRT) zu benennen oder einzurichten. Ferner werden Pflichten in Bezug auf das Cybersicherheitsrisikomanagement sowie Berichtspflichten für Einrichtungen der in den Anhang I oder II der NIS-2-Richtlinie aufgeführten Arten sowie für Einrichtungen, die nach Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden festgelegt. Des Weiteren sieht die NIS-2-Richtlinie Vorschriften und Pflichten zum Austausch von Cybersicherheitsinformationen sowie Aufsichts- und Durchsetzungspflichten für die Mitgliedstaaten vor.

Die Vorgaben der NIS-2-Richtlinie sind gestützt auf Artikel 114 AEUV und dienen der Harmonisierung des Binnenmarkts der Europäischen Union. Die Umsetzung der Vorgaben erfolgt mithin – neben weiteren im Vorblatt des Gesetzesentwurfs dargestellten Erwägungen – insbesondere auch um Verzerrungen im Binnenmarkt zu beseitigen und zu vermeiden. Denn die Cybersicherheitsanforderungen würden sich sonst von Mitgliedstaat zu Mitgliedstaat erheblich unterscheiden. Solche Unterschiede hinsichtlich Cybersicherheitsanforderungen und Aufsicht würden zusätzliche Kosten bei den Wirtschaftsteilnehmern verursachen und negative Auswirkungen auf das grenzüberschreitende Angebot von Waren oder Dienstleistungen haben.

Infolge des völkerrechtswidrigen russischen Angriffskriegs auf die Ukraine hat sich nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im Bericht zur Lage der IT-Sicherheit in Deutschland 2023 die IT-Sicherheitslage insgesamt zugespitzt. Im Bereich der Wirtschaft zählen hierbei Ransomware-Angriffe, Ausnutzung von Schwachstellen, offene oder falsch konfigurierte Online-Server sowie Abhängigkeiten von der IT-Lieferkette und in diesem Zusammenhang auch insbesondere Cyberangriffe über die Lieferkette (sogenannte Supply-Chain-Angriffe) zu den größten Bedrohungen. Zusätzlich zu den bereits bekannten Bedrohungen entstanden in Folge des russischen Angriffskriegs auf die Ukraine und der damit einhergehenden „Zeiten-

wende“ auch neue Bedrohungen oder die Einschätzungen zu bereits bekannten Bedrohungen mussten aufgrund veränderter Rahmenbedingungen geändert werden. Beispiele hierfür bestehen im Bereich Hacktivismus, insbesondere mittels Distributed-Denial-of-Service (DdoS)-Angriffen oder auch durch in Deutschland erfolgte Kollateralschäden in Folge von Cyber-Sabotage-Angriffen im Rahmen des Krieges. Zudem haben auch Störungen und Angriffe im Bereich der Lieferketten sowohl aus den Bereichen Cybercrime als auch im Rahmen des Krieges zuletzt zugenommen. Diese Phänomene treten nicht mehr nur vereinzelt auf, sondern sind insgesamt Teil des unternehmerischen Alltags geworden. Eine Erhöhung der Resilienz der Wirtschaft gegenüber den Gefahren der digitalen Welt ist daher eine zentrale Aufgabe für die beteiligten Akteure in Staat, Wirtschaft und Gesellschaft, um den Wirtschaftsstandort Deutschland und den Binnenmarkt der Europäischen Union insgesamt robust und leistungs- und funktionsfähig zu halten.

Für das Informationssicherheitsmanagement in der Bundesverwaltung haben sich die bisherigen Steuerungsinstrumente auf überwiegend untergesetzlicher Basis als nicht ausreichend effektiv erwiesen, um eine flächendeckend wirksame Steigerung des Sicherheitsniveaus zu erreichen. Dies haben insbesondere Sachstandserhebungen zum Umsetzungsplan Bund sowie Prüfungen des Bundesrechnungshofs (BRH) bestätigt. Vor dem Hintergrund der durch aktuelle geopolitische Entwicklungen („Zeitenwende“) abermals verschärften Bedrohungslage hat sich das Risiko für staatliche Einrichtungen zudem weiter erhöht, durch Gefährdungen aus dem Cyberraum in ihrer Handlungsfähigkeit eingeschränkt zu werden.

Entsprechend der unionsrechtlichen Vorgaben wird der mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I 2015 S. 1324) und dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021 (BGBl. I 2021, S. 1122) geschaffene Ordnungsrahmen durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz auf den Bereich bestimmter Unternehmen erweitert, zusätzlich werden entsprechende Vorgaben für die Bundesverwaltung eingeführt. Aufgrund des großen Umfangs des Vorhabens, wird es mit einer Novellierung des BSI-Gesetzes verbunden. In diesem Zusammenhang wird auch der Auftrag aus dem Koalitionsvertrag für die 20. Legislaturperiode, Zeile 438, aufgriffen, das IT-Sicherheitsrecht weiterzuentwickeln.

Dieser Entwurf steht im Kontext der Bestrebungen der Europäischen Union und ihrer Mitgliedstaaten zur Erhöhung der Wirtschaftssicherheit und Verbesserung der Resilienz als Antwort auf neue geopolitische Rahmenbedingungen. Mit der am 20. Juni 2023 veröffentlichten Europäischen Strategie für wirtschaftliche Sicherheit identifiziert die Europäische Kommission das Risiko für die Sicherheit kritischer Infrastruktur vor physischen und Cyberangriffen als eines von vier Hauptrisiken für die europäische Volkswirtschaft.

Dieser Entwurf steht außerdem im Kontext der gefährdeten rechtzeitigen Erreichung der Ziele der Resolution der Generalversammlung der Vereinten Nationen vom 25. September 2015 „Transformation unserer Welt: die UN-Agenda 2030 für nachhaltige Entwicklung“. Der Entwurf soll insbesondere zur Erreichung des Nachhaltigkeitsziels 9 der UN-Agenda 2030 beitragen, eine hochwertige, verlässliche und widerstandsfähige Infrastruktur aufzubauen.

II. Wesentlicher Inhalt des Entwurfs

Die unionsrechtlichen Vorgaben der NIS-2-Richtlinie werden im Rahmen einer Novellierung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) sowie einzelner Fachgesetze umgesetzt. Des Weiteren wird das Informationssicherheitsmanagement in der Bundesverwaltung gestärkt. Die Neuregelung hinsichtlich der im Anwendungsbereich erfassten Unternehmen erfolgt insbesondere zur Stärkung der Resilienz der Wirtschaft, welche vor dem Hintergrund der gesteigerten Cyberbedrohungslage und den Implikationen der „Zeitenwende“ notwendig geworden ist. Im Einzelnen

– Einführung der vorgegebenen Einrichtungskategorien besonders wichtige und wichtige Einrichtungen, die eine signifikante Ausweitung des bisher auf Betreiber Kritischer Infrastrukturen, Anbieter digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse beschränkten Anwendungsbereichs, vorsieht.

– Weiterführung der Einrichtungskategorie KRITIS als zusätzliche Kategorie für Unternehmen, die besonders schützenswert sind, mit entsprechenden Anforderungen.

- Der Katalog der Mindestsicherheitsanforderungen des Artikel 21 Absatz 2 NIS-2-Richtlinie wird in das BSI-Gesetz übernommen, wobei in der Intensität der jeweiligen Maßnahme aus Gründen der Verhältnismäßigkeit zwischen den Kategorien ausdifferenziert wird.
- Gesetzliche Verankerung wesentlicher nationaler Anforderungen an das Informationssicherheitsmanagement des Bundes und Abbildung der zugehörigen Rollen und Verantwortlichkeiten.
- Harmonisierung der Anforderungen an Einrichtungen der Bundesverwaltung aus nationalen und unionsrechtlichen Vorgaben, um ein insgesamt kohärentes und handhabbares Regelungsregime zu gewährleisten.
- Einführung eines dreistufigen Melderegimes, wodurch der bürokratische Aufwand für die Einrichtungen im Rahmen des Umsetzungsspielraums minimiert und mögliche Synergien mit weiteren Meldepflichten – insbesondere zum Störungs-Monitoring des geplanten Dachgesetzes zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz) – gesucht und genutzt werden.
- Ergänzung des Instrumentariums des BSI bei der Aufsicht: Es wird ein der EU-Datenschutz-Grundverordnung nachempfundener Bußgeldrahmen umgesetzt, der einerseits zwischen KRITIS und besonders wichtigen Einrichtungen sowie andererseits wichtigen Einrichtungen unterscheidet.
- Umsetzung einer Ausschlussklausel für Unternehmen, die einen besonderen Bezug zum Sicherheits- und Verteidigungsbereich aufweisen. Für solche Einrichtungen gelten dann die jeweils einschlägigen Vorgaben für den Sicherheits- bzw. Verteidigungsbereich.
- Etablierung eines CISO Bund als zentralem Koordinator für Maßnahmen zur Informationssicherheit in Einrichtungen der Bundesverwaltung und zur Unterstützung der Ressorts bei der Umsetzung der Vorgaben für das Informationssicherheitsmanagement.
- Weiterentwicklung der BSI-KritisV, sodass eine Erfassung von Einrichtungen unterhalb der Size-Cap-Rule, für die die NIS-2-Richtlinie als Sonderfall eine Identifizierung anhand von Kritikalitätskriterien vorsieht, erfolgen kann.

III. Alternativen

Keine.

IV. Gesetzgebungskompetenz

Für die Novellierung des BSI-Gesetzes in Artikel 1, die Änderung des BSI-Gesetzes in Artikel 30, die Änderung des IT-Sicherheitsgesetzes 2.0 in Artikel 7, die Änderung des EnWG in Artikel 17, die Änderung des Energiesicherungsgesetzes in Artikel 19 und die Änderung des Telekommunikationsgesetzes in Artikel 26, die den rein technischen Schutz der Informationstechnik von und für kritische Anlagen und besonders wichtige Einrichtungen und wichtige Einrichtungen betreffen, folgt die Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 7 (Telekommunikation) des Grundgesetzes (GG) sowie aus Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft, einschließlich gefahrenabwehrrechtlicher Annexkompetenz) in Verbindung mit Artikel 72 Absatz 2 GG und Artikel 74 Absatz 1 Nummer 12 GG (Sozialversicherung einschließlich der Arbeitslosenversicherung).

Eine bundesgesetzliche Regelung dieser Materie ist zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Eine Regelung durch den Landesgesetzgeber würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die sowohl im Interesse des Bundes als auch der Länder nicht hingenommen werden können. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Behandlungen gleicher Lebenssachverhalte, z. B. unterschiedliche Voraussetzungen für die Vergabe von Sicherheitszertifikaten, erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten. Internationale Abkommen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten und zum Austausch über eine zentrale Anlaufstelle gemäß Artikel 8 Absatz 3 der NIS-2-Richtlinie erfordern eine bundesgesetzliche Regelung. Die Voraussetzungen des Artikel 72 Absatz 2 GG sind auch im Hinblick auf die neuen Regelungen für die KRITIS-Betreiber erfüllt. Betreiber kritischer Anlagen sowie besonders wichtige Einrichtun-

gen und wichtige Einrichtungen stellen wesentliche Teile der Wirtschaft in Deutschland dar, deren Cybersicherheitsniveau vor dem Hintergrund der gestiegenen Bedrohungslage („Zeitenwende“) es anzuheben gilt. Die Anhebung des Cybersicherheitsniveaus wesentlicher Teile der Wirtschaft in Deutschland in Form einer bundesgesetzlichen Regelung ist auch zur Herstellung zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Regionale Unterschiede im Cybersicherheitsniveau der Unternehmen hätten erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge.

Für Regelungen in Artikel 1 und 30 zum Schutz der Bundesverwaltung steht dem Bund eine Gesetzgebungskompetenz kraft Natur der Sache zu.

Die Zuständigkeit des Bundes für Regelungen zur bundesweiten Information einschließlich eventueller Empfehlungen und Warnungen von Verbraucherinnen und Verbrauchern auf dem Gebiet der Informationssicherheit folgt mit Blick auf die gesamtstaatliche Verantwortung der Bundesregierung ebenfalls aus der Natur der Sache (Staatsleitung), denn Fragen zur Sicherheit in der Informationstechnik haben bei stetig zunehmender Digitalisierung und Vernetzung aller Lebensbereiche regelmäßig überregionale Auswirkungen.

Der Bund hat darüber hinaus die ausschließliche Gesetzgebungskompetenz nach Artikel 73 Absatz 1 Nummer 8 GG für die Rechtsverhältnisse der im Dienst des Bundes und der bundesunmittelbaren Körperschaften des öffentlichen Rechts stehenden Personen.

Die Gesetzgebungskompetenz des Bundes für die Regelungen der Bußgeldvorschriften und Ordnungswidrigkeiten im Artikel 1 folgt aus Artikel 74 Absatz 1 Nummer 1 GG (Strafrecht).

Die Gesetzgebungskompetenz des Bundes für die Änderung des Sechsten Buches Sozialgesetzbuch im Artikel 23 ergibt sich aus Artikel 74 Absatz 1 Nummer 12 GG.

Die Gesetzgebungskompetenzen des Bundes für die Folgeänderungen zum BSI-Gesetz entsprechen denjenigen für Artikel 1.

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union vereinbar. Er dient in weiten Teilen der Umsetzung der NIS-2-Richtlinie, zur Novellierung des BSI-Gesetzes (Artikel 1) im Einzelnen:

– Bei der Beibehaltung der Identifizierung von kritischen Anlagen (ehemals Kritische Infrastrukturen) und der Regulierung ihrer Betreiber wird eine bestehende Regelung beibehalten, die nicht von der Vorgabe der NIS-2-Richtlinie umfasst ist.

– Die von der NIS-2-Richtlinie vorgegebenen Einrichtungskategorien wesentliche und wichtige Einrichtungen werden mit den neu eingeführten Einrichtungskategorien der besonders wichtigen und wichtigen Einrichtungen umgesetzt.

– Bei der Regulierung der Einrichtungen der Bundesverwaltung (Teil 2 Kapitel 3) handelt es sich insoweit um Regelungen zur Umsetzung der NIS-2-Richtlinie, als eine Einrichtung der Bundesverwaltung Teil der Zentralregierung im Sinne von Artikel 2 Absatz 2 Buchstabe f Ziffer i der NIS-2-Richtlinie ist. Unter den Begriff Zentralregierung im Sinne der NIS-2-Richtlinie 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 Bundeskanzleramt, jeweils ohne nachgeordneten Bereich, gefasst. Zudem handelt es sich um Regelungen, die für die Einrichtungen der Bundesverwaltung abweichend zu den Regelungen für (besonders) wichtige Einrichtungen getroffen werden, als auch um bestehende Regelungen des BSI-Gesetzes sowie ergänzende nationale Regelungen.

Der Gesetzentwurf ist mit völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, vereinbar.

VI. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Der Gesetzesentwurf trägt zur Rechtsvereinfachung bei, indem er das bestehende BSI-Gesetz novelliert. Das BSI-Gesetz wird neu geordnet und gegliedert, wodurch dem Rechtsanwender die Arbeit erleichtert wird. Des Weiteren trägt der Gesetzesentwurf zur Verwaltungsvereinfachung bei, indem er die Rechte und Pflichten des Bundesamtes insbesondere gegenüber anderen Aufsichtsbehörden schärft und somit die Verantwortlichkeiten weiter konkretisiert. Durch ein gemeinsames Meldeportal mit anderen Aufsichtsbehörden sollen Synergien bei den Meldepflichten der erfassten Betreiber und Einrichtungen genutzt und der Bürokratieaufwand minimiert werden. Schließlich wird durch die gesetzliche Verankerung bisheriger untergesetzlicher Regelungen des Informationssicherheitsmanagements die IT-Sicherheit der öffentlichen Bundesverwaltung weiter gestärkt werden.

2. Nachhaltigkeitsaspekte

Der Gesetzentwurf steht im Einklang mit dem Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Deutschen Nachhaltigkeitsstrategie, die der Umsetzung der UN-Agenda 2030 für nachhaltige Entwicklung der Vereinten Nationen dient. Indem der Entwurf in weiten Teilen die NIS-2-Richtlinie umsetzt, welche die erforderlichen Cybersicherheitsanforderungen an juristische und natürliche Personen regelt, die wesentliche Dienste oder Tätigkeiten erbringen, leistet er einen Beitrag zur Verwirklichung von Nachhaltigkeitsziel 9 „Eine widerstandsfähige Infrastruktur aufbauen, inklusive und nachhaltige Industrialisierung fördern und Innovationen unterstützen“. Dieses Nachhaltigkeitsziel verlangt mit seiner Zielvorgabe 9.1, eine hochwertige, verlässliche, nachhaltige und widerstandsfähige Infrastruktur aufzubauen, einschließlich regionaler und grenzüberschreitender Infrastruktur, um die wirtschaftliche Entwicklung und das menschliche Wohlergehen zu unterstützen. Der Entwurf fördert die Erreichung dieser Zielvorgabe, indem er die Sicherheit in der Informationstechnik bei kritischen Anlagen verbessert, die insbesondere der Versorgung der Bevölkerung mit lebens-wichtigem Wasser und Energie dienen.

Im Sinne des systemischen Zusammendenkens der Nachhaltigkeitsziele leistet der Entwurf gleichzeitig einen Beitrag zur Erreichung von Ziel 16, welches in seiner Zielvorgabe 16.6 verlangt, leistungsfähige, rechenschaftspflichtige und transparente Institutionen auf allen Ebenen aufzubauen. Der Entwurf fördert die Erreichung dieser Zielvorgabe, indem er insbesondere das Informationssicherheitsmanagement in der Bundesverwaltung stärkt und die Bedeutung des Bundesamtes für Sicherheit in der Informationstechnik stärkt.

Der Entwurf trägt damit gleichzeitig zur Erreichung weiterer Nachhaltigkeitsziele der UN-Agenda 2030 bei, nämlich

Ziel 3: „Ein gesundes Leben für alle Menschen jeden Alters gewährleisten und ihr Wohlergehen fördern“, indem er die Lebensqualität durch die Schaffung eines hohen Niveaus an Cyber-Sicherheit stärkt und die Versorgungssicherheit für die Bürgerinnen und Bürger zu gewährleistet,

Ziel 8: „Dauerhaftes, inklusives und nachhaltiges Wirtschaftswachstum, produktive Vollbeschäftigung und menschenwürdige Arbeit für alle fördern“ und

Ziel 11: „Städte und Siedlungen inklusiv, sicher, widerstandsfähig und nachhaltig gestalten“.

Damit berücksichtigt der Entwurf die Querverbindungen zwischen den Zielen für nachhaltige Entwicklung und deren integrierenden Charakter, der für die Erfüllung von Ziel und Zweck der UN-Agenda 2030 von ausschlaggebender Bedeutung ist. Der Entwurf folgt den Nachhaltigkeitsprinzipien der DNS „(1.) Nachhaltige Entwicklung als Leitprinzip konsequent in allen Bereichen und bei allen Entscheidungen anwenden“, „(2.) Global Verantwortung wahrnehmen“, „(4.) Nachhaltiges Wirtschaften stärken“, „(5.) Sozialen Zusammenhalt in einer offenen Gesellschaft wahren und verbessern“.

3. Haushaltsausgaben ohne Erfüllungsaufwand

a. Gesamtaufstellung

Zusätzliche Haushaltsausgaben ohne Erfüllungsaufwand infolge des Gesetzes sind für Länder und Gemeinden nicht zu erwarten. Die zusätzlichen Haushaltsausgaben ohne Erfüllungsaufwand infolge des Gesetzes für den Bund insgesamt ergeben sich wie folgt.

Gesamtaufstellung Haushaltsausgaben Bund:

	Haushaltsausgaben in TEUR			
Haushaltsjahr	**2026**	**2027**	**2028**	**2029**
Summe pro Haushaltsjahr	192.364	192.161	209.735	216.289
Gesamtsumme im Finanzplanzeitraum	810.549			

Gesamtaufstellung Planstellen und Stellen Bund:

	Planstellen und Stellen			
Haushaltsjahr	**2026**	**2027**	**2028**	**2029**
Höherer Dienst (hD)	218,37	303,96	388,07	418,67
Gehobener Dienst (gD)	365,95	439,9	496,4	515,2
Mittlerer Dienst (mD)	56,13	81,63	93,43	100,33
Gesamtsumme Planstellen und Stellen im Finanzplanzeitraum	1.034,2			

Gesamtaufstellung Haushaltsausgaben Sozialversicherungsträger:

Haushaltsausgaben	**Haushaltsausgaben in TEUR in Summe pro Haushaltsjahr**				**Gesamtsumme im Finanzplanzeitraum in TEUR**
Epl. / Haushaltsjahr	**2026**	**2027**	**2028**	**2029**	
Sozialversicherungsträger	2.482	2.482	2.482	2.482	9.928
davon einmalige Ausgaben:	0	0	0	0	0
davon jährliche Ausgaben:	2.482	2.482	2.482	2.482	9.928

b. Haushaltsausgaben nach Einzelplänen einschließlich Wirtschaftsplänen

Die unter A.VI.3.a. genannten Gesamthaushaltsausgaben entfallen wie folgt auf die Einzelpläne:

Haushaltsausgaben	**Haushaltsausgaben in TEUR in Summe pro Haushaltsjahr**				**Gesamtsumme im Finanzplanzeitraum in TEUR**
Epl. / Haushaltsjahr	**2026**	**2027**	**2028**	**2029**	
Gesamtdarstellung **04** (Bundeskanzleramt, Presse- und Informationsamt der Bundesregierung und Beauftragte der Bundesregie-rung für Kultur und Medien)					

Haushaltsausgaben	**Haushaltsausgaben in TEUR in Summe pro Haushaltsjahr**				**Gesamtsumme im Finanzplanzeitraum in TEUR**
Epl. / Haushaltsjahr	**2026**	**2027**	**2028**	**2029**	
06 (Bundesministerium des Innern und für Heimat)	84.569,122	85.556,655	105.706,849	112.197,524	388.030,15
davon einmalige Ausgaben:	23.986,8	0	0	0	23.986,8
davon jährliche Ausgaben:	60.582,342	85.556,655	105.706,849	112.197,524	360.043,370
09 (Bundesministerium für Wirtschaft und Klimaschutz)	14.231	9.489	9.363	9.426,3	42.509,3
davon einmalige Ausgaben:	6.782	294	29	19,76	7.124,76
davon jährliche Ausgaben:	7.449	9.195	9.334	9.406,54	35.384,5
08 (Bundesministerium der Finanzen)	1.934	3.408	2.608	2.608	10.558
davon einmalige Ausgaben:	900	0	0	0	900
davon jährliche Ausgaben:	1.034	3.408	2.608	2.608	9.658
05 (Auswärtiges Amt)	10.714	15.594	14.828	14.828	55.964
davon einmalige Ausgaben:	1.791	766	0	0	2557
davon jährliche Ausgaben:	8.923	14.828	14.828	14.828	53.407
07 (Bundesministerium der Justiz)	5.067	2.496	2.496	2.496	12.555
davon einmalige Ausgaben:	2.571	0	0	0	2.571
davon jährliche Ausgaben:	2.496	2.496	2.496	2.496	9.984
11 (Bundesministerium für Arbeit und Soziales)	5.232	5.232	5.232	5.232	20.928
davon einmalige Ausgaben:	0	0	0	0	0
davon jährliche Ausgaben:	5.232	5.232	5.232	5.232	20.928
14 (Bundesministerium der Verteidigung)	0	0	0	0	0
10 (Bundesministerium für Ernährung und Landwirtschaft)	2.127	1.572	1.521	1.521	6.741
davon einmalige Ausgaben:	605,5	56	0	0	661,5
davon jährliche Ausgaben:	1521	1.521	1.521	1.521	6.084
17 (Bundesministerium für Familie, Senioren, Frauen und Jugend)	2.240	2.180	2.180	2.180	8.780
davon einmalige Ausgaben:					

Haushaltsausgaben	**Haushaltsausgaben in TEUR in Summe pro Haushaltsjahr**				**Gesamtsumme im Finanzplanzeitraum in TEUR**
Epl. / Haushaltsjahr	**2026**	**2027**	**2028**	**2029**	
davon einmalige Ausgaben:	60	0	0	0	60
davon jährliche Ausgaben:	2.180	2.180	2.180	2.180	8.720
15 (Bundesministerium für Gesundheit)	6.864	6.864	6.864	6.864	27.456
davon einmalige Ausgaben:	0	0	0	0	0
davon jährliche Ausgaben:	6.864	6.864	6.864	6.864	27.456
12 (Bundesministerium für Digitales und Verkehr)	2.257	2.140	1.620	1.620	7.637
davon einmalige Ausgaben:	174,2	57,5	58	58	347,7
davon jährliche Ausgaben:	2.082	2.082	1.562	1.562	7.288,8
16 (Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz)	5.469	5.136	5.136	5.136	20.877
davon einmalige Ausgaben:	0	0	0	0	0
davon jährliche Ausgaben:	5.469	5.136	5.136	5.136	20.877
30 (Bundesministerium für Bildung und Forschung)	85	53	53	53	244
davon einmalige Ausgaben:	0	0	0	0	0
davon jährliche Ausgaben:	85	53	53	53	244
23 (Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung)	2.008	3.709	3.401	3.401	12.519
davon einmalige Ausgaben:	0	0	0	0	0
davon jährliche Ausgaben:	2.008	3.709	3.401	3.401	12.519
25 (Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen)	1.355	495	495	495	2.840
davon einmalige Ausgaben:	0	0	0	0	0
davon jährliche Ausgaben:	1.355	495	495	495	2.840
21 (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)	1.140	1.140	1.140	1.140	4.560
davon einmalige Ausgaben:	0	0	0	0	0

Haushaltsausgaben	**Haushaltsausgaben in TEUR in Summe pro Haushaltsjahr**				**Gesamtsumme im Finanzplanzeitraum in TEUR**
Epl. / Haushaltsjahr	**2026**	**2027**	**2028**	**2029**	
davon jährliche Ausgaben:	1.140	1.140	1.140	1.140	1.140

c. Planstellen und Stellen nach Einzelplänen

Die Planstellen und Stellen in der unter A.VI.3.a. genannten Gesamtaufstellung Planstellen und Stellen entfallen wie folgt auf die Einzelpläne:

Planstellen und Stellen					
Einzelplan	**Haushaltsjahr**	**2026**	**2027**	**2028**	**2029**
Gesamtdarstellung **04** (Bundeskanzleramt, Presse- und Informationsamt der Bundesregierung und Beauftragte der Bundesregierung für Kultur und Medien) **06** (Bundesministerium des Innern und für Heimat)	697,69 Planstellen / Stellen	313,19	491,99	641,79	697,69
	hD	121,42	212,42	295,42	325,42
	gD	160,75	223,25	278,25	297,25
	mD	31,02	56,32	68,12	75,02
09 (Bundesministerium für Wirtschaft und Klimaschutz)	56,32 Planstellen / Stellen	48,6	55,31	55,92	56,32
	hD	12,8	15,39	15,5	16,1
	gD	31,5	35,4	35,9	35,7
	mD	4,32	4,52	4,52	4,52
08 (Bundesministerium der Finanzen)	7 Planstellen / Stellen	4	7	7	7
	hD	0	1	1	1
	gD	3	5	5	5
	mD	1	1	1	1
05 (Auswärtiges Amt)	95,8 Planstellen / Stellen	95,8	95,8	95,8	95,8
	hD	23,7	23,7	23,7	23,7
	gD	68,9	68,9	68,9	68,9
	mD	3,21	3,21	3,21	3,21
07 (Bundesministerium der Justiz)	30 Planstellen / Stellen	30	18	18	18
	hD	14	5	5	5
	gD	11,5	9	9	9

Planstellen und Stellen					
Einzelplan	**Haushaltsjahr**	**2026**	**2027**	**2028**	**2029**
	mD	4,5	4	4	4
11 (Bundesministerium für Arbeit und Soziales)	27 Planstellen / Stellen	27	27	27	27
	hD	6,5	6,5	6,5	6,5
	gD	20,5	20,5	20,5	20,5
	mD	0	0	0	0
14 (Bundesministerium der Verteidigung)	0 Planstellen / Stellen	0	0	0	0
	hD	0	0	0	0
	gD	0	0	0	0
	mD	0	0	0	0
10 (Bundesministerium für Ernährung und Landwirtschaft)	8,98 Planstellen / Stellen	8,73	8,98	8,98	8,98
	hD	2,43	2,5	2,5	2,5
	gD	6,3	6,48	6,48	6,48
	mD	0	0	0	0
17 (Bundesministerium für Familie, Senioren, Frauen und Jugend)	13,2 Planstellen / Stellen	13,2	13,2	13,25	13,25
	hD	7,2	7,2	7,2	7,2
	gD	5,75	5,75	5,75	5,75
	mD	0,25	0,25	0,25	0,25
15 (Bundesministerium für Gesundheit)	23,3 Planstellen / Stellen	23,3	23,3	23,3	23,3
	hD	9,1	9,1	9,1	9,1
	gD	11,2	11,2	11,2	11,2
	mD	3	3	3	3
12 (Bundesministerium für Digitales und Verkehr)	35,8 Planstellen / Stellen	35,8	35,8	35,8	35,8
	hD	6,9	6,9	6,9	6,9
	gD	25,12	25,12	25,12	25,12
	mD	3,8	3,8	3,8	3,8
16 (Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz)	28,35 Planstellen / Stellen	19,63	28,35	28,35	28,35
	hD	6,42	8,25	8,25	8,25

Planstellen und Stellen					
Einzelplan	**Haushaltsjahr**	**2026**	**2027**	**2028**	**2029**
	gD	12,21	18,6	18,6	18,6
	mD	1	1,5	1,5	1,5
30 (Bundesministerium für Bildung und Forschung)	0,54 Planstellen / Stellen	0,54	0,16	0,16	0,16
	hD	0	0	0	0
	gD	0,54	0,16	0,16	0,16
	mD	0	0	0	0
23 (Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung)	12 Planstellen / Stellen	9	10	12	12
	hD	2	2	3	3
	gD	3	4	5	5
	mD	4	4	4	4
25 (Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen)	5,6 Planstellen / Stellen	5,6	5	5	5
	hD	2,9	1	1	1
	gD	2,7	4	4	4
	mD	0	0	0	0
21 (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)	6 Planstellen / Stellen	6	6	6	6
	hD	3	3	3	3
	gD	3	3	3	3
	mD	0	0	0	0

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden. Dies gilt ebenso für den unter A.IV.4.c dargestellten Erfüllungsaufwand, sofern dieser haushaltswirksam wird.

d. Auswirkungen auf Sozialversicherungsträger

Haushaltsausgaben	**Haushaltsausgaben in TEUR in Summe pro Haushaltsjahr**				**Gesamtsumme im Finanzplanzeitraum in TEUR**
Epl. / Haushaltsjahr	**2026**	**2027**	**2028**	**2029**	
Sozialversicherungsträger	4.142	4.142	4.142	4.142	16.568
davon einmalige Ausgaben:	0	0	0	0	0
davon jährliche Ausgaben:	4.142	4.142	4.142	4.142	16.568
Bundesagentur für Arbeit	1.517	1.517	1.517	1.517	6.068

Haushaltsausgaben	**Haushaltsausgaben in TEUR in Summe pro Haushaltsjahr**				**Gesamtsumme im Finanzplanzeitraum in TEUR**
Epl. / Haushaltsjahr	**2026**	**2027**	**2028**	**2029**	
SVLFG	940	940	940	940	3760
Rentenservice Deutsche Post	25	25	25	25	100
DRV Bund	1.660	1.660	1.660	1.660	6.640

Planstellen und Stellen					
	Haushaltsjahr	**2026**	**2027**	**2028**	**2029**
Sozialversicherungsträger	31,35 Planstellen	31,35	31,35	31,35	31,35
Bundesagentur für Arbeit	hD	2	2	2	2
SVLFG		0	0	0	0
Rentenservice Deutsche Post		0	0	0	0
DRV Bund		5	5	5	5
Bundesagentur für Arbeit	gD	5	5	5	5
SVLFG		2	2	2	2
Rentenservice Deutsche Post		0,35	0,35	0,35	0,35
DRV Bund		17	17	17	17
Bundesagentur für Arbeit	mD	0	0	0	0
SVLFG		0	0	0	0
Rentenservice Deutsche Post		0	0	0	0
DRV Bund		0	0	0	0

4. Erfüllungsaufwand

a. Erfüllungsaufwand für die Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

b. Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft erhöht sich der jährliche Erfüllungsaufwand um rund 2,2 Milliarden Euro. Insgesamt entsteht einmaliger Aufwand von rund 2,1 Milliarden Euro. Dieser ist fast ausschließlich der Kategorie Einführung oder Anpassung digitaler Prozessabläufe zuzuordnen.

Davon entfallen rund 1,9 Millionen Euro auf Bürokratiekosten aus Informationspflichten.

Die Belastungen sind nicht im Rahmen der One in, one out-Regel der Bundesregierung zu kompensieren, da diese Änderungen aus einer 1:1-Umsetzung der verbindlichen Mindestvorgaben der Richtlinie (EU) 2022/2555 resultieren.

aa. Wesentliche Rechtsänderungen

Vorgabe 4.2.1 (Weitere Vorgabe): Einhaltung eines Mindestniveaus an IT-Sicherheit (Besonders wichtige und wichtige Einrichtungen); §§ 30, 31 und 38 Absatz 1 in Verbindung mit § 28 BSIG-E, § 5c Absatz 1 und 2 EnWG-E , § 165 Absätze 2 und 2a TKG

Veränderung des jährlichen Erfüllungsaufwands:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
2 950	2 752	52,30	60 000	424 592	177 000
17 900	1 100	52,30	24 000	1 029 787	429 600
Änderung des Erfüllungsaufwands (in Tsd. Euro)				2 060 979	

Einmaliger Erfüllungsaufwand: 2,1 Milliarden Euro

Bereits heute sind Betreiber kritischer Infrastrukturen und Anbieter digitaler Dienste verpflichtet, ein Mindestniveau an IT-Sicherheit zu gewährleisten (vgl. §§ 8a und 8c BSIG, § 11 Absatz 1a ff. EnWG und § 165 TKG). Der Regelungsentwurf führt mit §§ 30, 31 und 38 Absatz 1 in Verbindung mit § 28 BSIG-E sowie mit § 5c Absatz 1 und 2 EnWG und mit § 165 Absatz 2 und 2a TKG vergleichbare Normen fort, in deren Anwendungsbereich deutlich mehr Unternehmen fallen werden. Demnach sollen künftig alle besonders wichtigen und wichtigen Einrichtungen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen, um für ihre Diensteerbringung relevante IT-bezogene Störungen zu vermeiden (§ 30 Absatz 1 BSIG-E). Hinsichtlich der Verhältnismäßigkeit wird in der Gesetzesbegründung zum § 30 BSIG-E, in § 5c Absatz 3 EnWG-E oder in § 165 Absatz 2 TKG-E auf die Bewertungskriterien etablierte IT-Standards, Umsetzungskosten und bestehende Risiken verwiesen. Letztere werden bestimmt durch die Risikoexposition, die Größe der Einrichtung bzw. des Betreibers sowie der Eintrittswahrscheinlichkeit und die Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen. Folglich werden erforderliche Maßnahmen zum Risikomanagement, die besonders wichtige Einrichtungen ergreifen müssen, umfangreicher sein als Maßnahmen, die wesentliche Einrichtungen ergreifen müssen. Geschäftsleiter sind verpflichtet die Risikomaßnahmen zu billigen und zu überwachen (vgl. § 38 Absatz 1 BSIG-E).

Auf Basis von Angaben des BMWK und Daten des Unternehmensregisters des StBA kann angenommen werden, dass in Deutschland künftig rund 8 250 Unternehmen als besonders wichtige und rund 21 600 Unternehmen als wichtige Einrichtungen zu klassifizieren sind, die dem Normadressat der Wirtschaft zuzurechnen sind – darunter auch kommunale Eigenbetriebe oder Landesbetriebe sowie juristische Personen des öffentlichen Rechts, die nicht in dem Sektor „öffentliche Verwaltung“ tätig sind (vgl. Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates, Anhang 1). Unter den besonders wichtigen Einrichtungen sind 4 693 Anbieter digitaler Dienste und Betreiber kritischer Anlagen, die bereits heute nach geltender Rechtslage entsprechende Maßnahmen implementieren müssen (vgl. Online-Datenbank des Erfüllungsaufwands des StBA (OnDEA), ID 2015030909595401, 2017052913283301, 2020093009264301 und 2020093009264401). Folglich konstituiert die Rechtsänderung nur für die übrigen rund 3 550 besonders wichtigen Einrichtungen – und für die wichtigen Einrichtungen – vollständig neue rechtliche Verpflichtungen. Zu beachten ist, dass auch von diesen potenziell betroffenen Unternehmen bereits heute ein Teil die geforderten Sicherheitsmaßnahmen ergreift. Laut einer Studie sahen sich im Jahr 2023 17 Prozent der befragten Unternehmen als sehr gut gegen Cyberangriffe aufgestellt (vgl. eco – Verband der Internetwirtschaft e. V. (2023): www.eco.de/presse/eco-it-sicherheitsumfrage-2023-viele-unternehmen-unterschaetzen-noch-immer-bedrohungslage/). Mangels anderer Daten wird auf Basis dieser Studie angenommen, dass rund 17 Prozent der betroffenen Unternehmen bereits heute ausreichende Maßnahmen im Sinne des Umsetzungsgesetzes treffen. Folglich geht die nachfolgende Kalkulation davon aus, dass rund 2 950 (= 0,83 * 3 550) besonders wichtigen Einrichtungen und rund 17 900 (= 0,83 * 21 600) wichtigen Einrichtungen Erfüllungsaufwand entsteht.

Für die unternehmensbezogenen Personal- und Sachkosten werden Daten des StBA herangezogen, die im Rahmen der Nachmessung des Erfüllungsaufwands des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme und des Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 mittels einer Befragung von Betreibern kritischer Infrastrukturen Ende des Jahres 2020 ermittelt wurden. Demnach beträgt der auf diese Gesetze zurückzuführende zusätzliche Personalaufwand der Betreiber kritischer Infrastrukturen für die Einhaltung eines Mindestniveaus an IT-Sicherheit durchschnittlich 2 752 Stunden und 60 000 Euro Sachkosten (vgl. OnDEA, ID

2015030909595401 und 2017052913283301). Mit Blick auf die Implementierung verhältnismäßiger Maßnahmen wird dieser Aufwand auch für die betroffenen besonders wichtigen Einrichtungen angenommen. Für wichtige Einrichtungen fällt entsprechend den Bewertungskriterien der Verhältnismäßigkeit ein geringerer Aufwand an. Mangels verfügbarer Daten wird angenommen, dass dieser Aufwand im Durchschnitt 60 Prozent geringer ist, also einem Personaleinsatz von rund 1 100 Stunden und Sachkosten in Höhe von 24 000 Euro entspricht. Da anhand der Daten des BMWK und des StBA abgeschätzt werden kann, dass 13 Prozent der wichtigen Einrichtungen auf große und 87 Prozent auf mittlere Unternehmen entfallen, entspricht der gemittelte Aufwand in Höhe von 1 100 Stunden und 24 000 Euro einer Konstellation, in der der Aufwand großer wichtiger Einrichtungen 70 Prozent der Aufwände der besonders wichtigen Einrichtungen und der Aufwand mittlerer wichtiger Einrichtungen 35 Prozent der Aufwände der besonders wichtigen Einrichtungen entspricht.

Werden die oben dargestellten Parameter angewendet, lässt sich bei einem mittleren Lohnsatz von 52,30 pro Stunde (vgl. Leitfaden zur Ermittlung und Darstellung des Erfüllungsaufwands (nachfolgend: Leitfaden), Abschnitt 7, Gesamtwirtschaft A-S ohne O; mittleres Qualifikationsniveau mit 25 Prozent, hohes Qualifikationsniveau mit 75 Prozent; sowie OnDEA ID 2015030909595401 und 2017052913283301) schätzen, dass den besonders wichtigen Einrichtungen bzw. den wichtigen Einrichtungen ein jährlicher Erfüllungsaufwand von rund 600 Millionen Euro bzw. 1,5 Milliarden Euro entsteht.

Hinsichtlich des einmaligen Aufwands liegen keine Anhaltspunkte für eine Schätzung vor. Es wird vereinfachend angenommen, dass für die Implementierung neuer bzw. für die Anpassung der bestehenden IT-Infrastruktur zur Einhaltung des geforderten Mindestniveaus an IT-Sicherheit zusätzlich einmaliger Aufwand anfällt, welcher der Höhe des jährlichen Aufwands eines Jahres entspricht. Die umfassende Befragung der Bundesverwaltung ergab in etwa ein ähnliches Größenverhältnis zwischen dem jährlichen und dem einmaligen Aufwand (vgl. Vorgabe 4.3.1). Insofern ist von einem einmaligen Erfüllungsaufwand der Kostenkategorie „Einführung und Anpassung digitaler Prozessabläufe“ von knapp 2,1 Milliarden Euro auszugehen.

Da der Regelungsentwurf der Umsetzung der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und Rates dient, ist der nationalen Ausgestaltung zur Erhöhung der Sicherheit informationstechnischer Systeme enge Grenzen gesetzt. Der Zielsetzung des „Konzepts zur Erhöhung der Transparenz über den Umstellungsaufwand für die Wirtschaft und zu dessen wirksamer und verhältnismäßiger Begrenzung“ ist insofern Rechnung getragen, als dass das Umsetzungsgesetz nicht über den Regelungsgehalt der Richtlinie hinausgeht. Aber bereits bei der Ausarbeitung der EU-Richtlinie hat sich auch die Bundesregierung im Sinne des Konzepts erfolgreich im Rahmen der Trilogverhandlungen für aufwandsärmere Lösungen eingesetzt. So sah der Richtlinienvorschlag der Europäischen Kommission (EU-KOM) – anders als die nun geltende Richtlinie – keine differenzierten Regelungen für besonders wichtigen und wichtigen Einrichtungen vor. Im Sinne des Artikels 21 und des Erwägungsgrunds 15 wird mit Blick auf die zu ergreifenden Maßnahmen nun im Umsetzungsgesetz der Ansatz der Verhältnismäßigkeit normiert, wodurch wichtige Einrichtungen monetär weniger stark belastet werden wie die besonders wichtigen Einrichtungen. Der Vorschlag der EU-KOM sah zudem vor, dass bei einer hinreichenden öffentlichen Beteiligung an einer Einrichtung, selbige auch dann in den Anwendungsbereich fällt, wenn es sich um ein kleines oder Kleinstunternehmen handelt. Da das Kriterium der öffentlichen Beteiligung keine Relevanz mehr hat, fallen diese (mit wenigen Ausnahmen durch die Konkretisierungen in Artikel 2) nun nicht mehr in den Anwendungsbereich. Schließlich wurde im Vergleich zu dem Richtlinienvorschlag in der geltenden EU-Richtlinie der Anwendungsbereich in einige Sektoren enger gefasst – insbesondere für Lebensmittelunternehmen.

Vorgabe 4.2.2 (Informationspflicht): Sicherheitsvorfälle (Meldung-, Unterrichtungs- und Auskunftspflichten); §§ 32, 35 und 40 Absatz 5 in Verbindung mit § 28 BSIG-E, § 5c Absatz 6 und 7 EnWG-E, § 168 Absatz 1 bis 3 TKG-E

Veränderung des jährlichen Erfüllungsaufwands:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
2 400	6,75	58,40	0	946	0
450	2,25	58,40	0	59	0
2 85	1,00	58,40	0	17	0
Änderung des Erfüllungsaufwands (in Tsd. Euro)				1 022	

Der Regelungsentwurf sieht im Zusammenhang mit Sicherheitsvorfällen Meldepflichten besonders wichtiger und wichtiger Einrichtungen gegenüber einer Meldestelle, in bestimmten Fällen eine Unterrichtungspflicht und auf Verlangen eine Auskunftspflicht vor (vgl. §§ 32, 35 und 40 Absatz 5 BSIG-E, § 5c Absatz 6 und 7 EnWG-E, § 168 Absatz 1 bis 3 TKG-E). Bereits heute existiert für Betreiber kritischer Infrastrukturen (vgl. § 8b Absatz 4 BSIG, § 44b AtG), Unternehmen im besonderen öffentlichen Interesse (vgl. § 8f Absatz 7 und 8 BSIG), Anbieter digitaler Dienste (vgl. § 8c Absatz 3 BSIG) und für Unternehmen der Sektoren Telekommunikation und Energie (vgl. § 11 Absatz 1c EnWG, § 168 TKG) eine Meldepflicht von Sicherheitsvorfällen. Erfüllungsaufwand entsteht, da (a) mehr Unternehmen melde- und auskunftspflichtig werden, (b) die Meldepflicht an sich aufgrund des künftig mehrstufigen Verfahrens auch für bereits meldepflichtige Unternehmen aufwendiger wird und (c) die Unterrichtungspflicht neu eingeführt werden.

Die Anzahl der gemeldeten Sicherheitsvorfälle betrug im Berichtsjahr 2021/2022 rund 450 (vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2022, S. 68, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8). Geht man von einem ähnlichen Meldeaufkommen der neu hinzukommenden 25 157 (= 29 850 – 4 693) meldepflichtigen Unternehmen pro Jahr aus, ist mit zusätzlichen 2 400 gemeldeten Sicherheitsvorfälle zu rechnen.

Der fallbezogene Zeitaufwand beträgt rund 4,5 Stunden für Meldungen nach geltender Rechtslage (vgl. OnDEA, ID 2017052913283701 und 2015030909595201). Aufgrund des mehrstufiges Meldeverfahren wird vereinfacht ein Aufschlag von 50 Prozent angesetzt, so dass von einer Gesamtdauer von 6,75 Stunden je Sicherheitsvorfall bzw. 16 200 Stunden (=6,75*2 400) für die neuen meldepflichtigen Unternehmen insgesamt ausgegangen wird. Für die bisher meldepflichtigen Unternehmen erhöht sich der Zeitaufwand um 2,25 Stunden pro Meldung bzw. zusammen rund 1 000 zusätzliche Stunden. Für die Unterrichtungs- und Auskunftspflicht wird vereinfacht angenommen, dass in nicht mehr als 10 Prozent aller rund 2 850 gemeldeten Sicherheitsvorfälle ein zusätzlicher Zeitaufwand von rund einer Stunde anfällt, also zusammen maximal 285 Stunden.

Bei einem gesamten zeitlichen Aufwand von rund 17 500 Stunden und einem Lohnsatz von 58,40 Euro je Stunde (vgl. Leitfaden, Anhang 7, Gesamtwirtschaft (A-S ohne O), hohes Qualifikationsniveau) beträgt der jährliche Erfüllungsaufwand insgesamt rund einer Million Euro.

Vorgabe 4.2.3 (Informationspflicht): Registrierungspflichten für besonders wichtige und wichtige Einrichtungen sowie bestimmte Einrichtungsarten; §§ 33 und 34 in Verbindung mit § 28 BSIG-E, § 5c Absatz 8 EnWG-E

Veränderung des jährlichen Erfüllungsaufwands: 48 000 Euro

Einmaliger Erfüllungsaufwand: 361 000 Euro

Durch den Regelungsentwurf wird die bestehende Registrierungspflicht (vgl. §§ 8b und 8f BSIG) auf alle besonders wichtigen und wichtigen Einrichtungen sowie für bestimmte Einrichtungsarten ausgeweitet. Durch die erstmalige Übermittlung der Informationen entsteht einmaliger Erfüllungsaufwand. Jährlicher Erfüllungsaufwand entsteht aus der Pflicht, Änderungen der registerpflichtigen Angaben melden zu müssen (vgl. §§ 33 und 34 in Verbindung mit § 28 BSIG-E sowie § 5c Absatz 8 EnWG).

Unter der Annahme, dass heute bereits insgesamt rund 6 000 Betreiber kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse registriert sind, werden in Deutschland künftig zusätzlich rund 23 850 besonders wichtige und wichtige Einrichtungen in den Anwendungsbereich der Rechtsänderungen fallen. Für das erstmalige Zusammenstellen sowie die Übermittlung der Informationen wird gemäß Anhang 5 des Leitfadens ein Zeitaufwand von einmalig 25 Minuten angenommen (Standardaktivitäten 1, 2 und 3 in mittlerer Komplexität sowie 5, 7 und 8 in einfacher Komplexität). Bei einem Lohnsatz von 36,30 Euro pro Stunde (vgl. Leitfaden, Anhang 7, Gesamtwirtschaft A-S ohne O; mittleres Qualifikationsniveau) entsteht einmaliger Erfüllungsaufwand der Kategorie einmalige Informationspflicht in Höhe von rund 361 000 Euro. Unter der Annahme, dass das BSI eine elektronisches Registrierungsverfahren implementiert, entstehen keine weiteren Sachkosten aus der Datenübermittlung.

Die (besonders) wichtigen Einrichtungen haben die zuständige Behörde über etwaige Änderungen zu informieren (vgl. §§ 33 Absatz 5, 34 Absatz 2 BSIG-E). Es wird davon ausgegangen, dass sich pro Jahr in einem Drittel der Einrichtungen mindestens eine Angabe ändert (= rund 7 950 Fälle). Bei einem fallbezogenen Zeitaufwand von 10

Minuten (vgl. Leitfaden, Anhang 5, Standardaktivitäten 2, 3, 5, 7 und 8 in einfacher Komplexität) und einem Lohnsatz von 36,30 Euro je Stunde entsteht jährlicher Erfüllungsaufwand von rund 48 000 Euro.

Vorgabe 4.2.4 (Weitere Vorgabe): Regelmäßige Schulungen (Besonders wichtige und wichtige Einrichtungen); § 38 Absatz 3 in Verbindung mit § 28 BSIG-E

Veränderung des jährlichen Erfüllungsaufwands:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
150 000	4	58,40	100	35 040	15 000
3 000 000	1	36,30	0	108 900	
Änderung des Erfüllungsaufwands (in Tsd. Euro)				158 940	

Die Regelungsentwurf sieht vor, dass Geschäftsleiter aller adressierten Einrichtungen regelmäßig Cybersicherheitsschulungen absolvieren müssen; die übrigen Mitarbeitenden sollen regelmäßig an solchen Schulungen teilnehmen (vgl. § 38 Absatz 3 BISG-E).

Das Umsetzungsgesetz (vgl. Gesetzesbegründung) und die NIS-2-Richtlinie (vgl. Artikel 20 Absatz 2) machen hier nur allgemeine Forderungen von Schulungen zum Erwerb allgemeiner Kenntnisse und Fähigkeiten, um unter anderem Risiken im Bereich der Cybersicherheit zu erkennen und zu bewerten. So sollen die Schulungen zwar regelmäßig absolviert werden, eine konkrete Periodizität wird allerdings nicht vorgegeben. Zusätzlich ist unklar, wer im Unternehmen konkret zu den Geschäftsleitern zählt. Schließlich ist nicht zu erkennen, wie umfangreich die speziellen Cybersicherheitsschulungen sein müssen. Theoretisch können das Kurzschulungen von wenigen Stunden sein, oder aufgrund der komplexen Thematik mehrtägige Seminare.

Es wird geschätzt, dass jährlich rund 298 500 Geschäftsleiter Schulungen absolvieren. Dies liegt der freien Annahme zu Grunde, dass einmal im Jahr zehn leitende Beschäftigte je Unternehmen an einer solchen Schulung teilnehmen (29 850 Unternehmen * 10). Es ist jedoch davon auszugehen, dass Unternehmen aus eigenem Interesse zum Teil bereits heute ihren führenden Mitarbeitenden Cybersicherheitsschulungen anbieten. Es wird daher angenommen, dass dies für 50 Prozent der Unternehmen zutrifft, sodass davon auszugehen ist, dass sich für rund 150 000 leitende Beschäftigte eine Veränderung des Status Quos ergibt.

Des Weiteren wird frei angenommen, dass es sich im Durchschnitt um eine halbtägige Schulung handelt (4 Stunden). Bei einem Lohnsatz von 58,40 Euro je Stunde (vgl. Leitfaden, Anhang 7, Gesamtwirtschaft (A-S ohne O), hohes Qualifikationsniveau) betragen die jährlichen Personalkosten knapp 35 Millionen Euro. Werden je teilnehmender Person zusätzliche Schulungskosten für von externen Dozenten durchgeführte Schulungen in Höhe von 100 Euro angenommen, fallen zusätzlich jährliche Sachkosten in Höhe von 15 Millionen Euro an. Es sei darauf hingewiesen, dass es bereits kostenlose Online-Schulungen zum Thema IT-Sicherheit gibt. Sollten diese für die gesetzlichen Anforderungen an Geschäftsleiter hinreichend sein, würden die Sachkosten entsprechend bedeutend geringer ausfallen.

Hinsichtlich der Schulung der Mitarbeitenden wird angenommen, dass Schulungen für alle bzw. einen Großteil der in den als besonders wichtig und wichtig klassifizierten Einrichtungen angestellten Personen angeboten werden sollen. Anhand von Daten des StBA wurde errechnet, dass die durchschnittliche Zahl der Beschäftigten in großen und mittleren Unternehmen bei über 200 liegt. Es wird vereinfacht davon ausgegangen, dass in jedem der rund 29 850 Einrichtungen im Mittel 200 Beschäftigte eine Cybersicherheitsschulung absolvieren. Wie bei den Geschäftsleitern wird davon ausgegangen, dass rund 50 Prozent der Unternehmen ihren Mitarbeitenden bereits heute die Teilnahme an entsprechenden Cybersicherheitsschulungen ermöglichen, so dass schließlich von rund drei Millionen zu schulenden Personen auszugehen ist. Zudem wird angenommen, dass die Schulungen weniger zeitaufwändig sind als die, welche durch die Mitglieder der Leitungsorgane absolviert werden. In diesem Szenario wird davon ausgegangen, dass pro Jahr im Durchschnitt eine einstündige Schulung oder Selbstlerneinheit absolviert wird und dass überwiegend auf kostenfreie Angebote, die es bereits heute gibt, zurückgegriffen wird (vgl. BSI, IT-Grundschutz-Schulungen, www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/it-grundschutzschulung_node.html). Unter den dargestellten Annahmen entsteht bei einem Lohnsatz von 36,30 Euro je

Stunde (Lohnkosten der Gesamtwirtschaft A-S ohne O; durchschnittliches Qualifikationsniveau) zusätzlicher jährlicher Erfüllungsaufwand in der Höhe von rund 109 Millionen Euro.

Insgesamt summiert sich der jährliche Erfüllungsaufwand für Schulungen von Geschäftsleitern und Mitarbeitenden auf rund 159 Millionen Euro.

Vorgabe 4.2.5 (Informationspflicht): Nachweis über Erfüllung von Anforderungen zur IT-Sicherheit (Besonders wichtige und wichtige Einrichtungen); § 61 Absatz 3 und 4 sowie § 62 in Verbindung mit § 28 BSIG-E

Veränderung des jährlichen Erfüllungsaufwands:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
24	282	56,94	19 300	385	463
Änderung des Erfüllungsaufwands (in Tsd. Euro)				849	

Das BSI kann von einer Auswahl besonders wichtiger Einrichtungen Nachweise zur Einhaltung von Anforderungen zur IT-Sicherheit anfordern. Zur Bestimmung nachweispflichtiger Einrichtungen soll es bestimmte Kriterien wie das Ausmaß der Risikoexposition heranziehen (vgl. § 64 Absatz 3 und 4 BSIG-E). Von wichtigen Einrichtungen kann das BSI ebenfalls Nachweise verlangen, sofern Annahmen die Tatsache rechtfertigen, dass diese die gesetzlichen Anforderungen zur IT-Sicherheit nicht oder nicht richtig umsetzen. Für Betreiber kritischer Anlagen wird eine bereits bestehende obligatorische Nachweispflicht in den § 39 BSIG-E überführt.

Auf Basis der bisherigen Vollzugspraxis schätzt das Bundesministerium des Innern und für Heimat (BMI), dass das BSI pro Jahr von rund 24 (besonders) wichtigen Einrichtungen Nachweise verlangen wird. Die bestehende Nachweispflicht für Betreiber kritischer Anlagen verursacht laut OnDEA (ID 2015030909595501 und 2020093009264402) einen durchschnittlichen Zeitaufwand von im Mittel 282 Stunden und Sachkosten von 19 300 Euro. Bei einem mittleren Lohnsatz von 56,94 Euro je Stunde (vgl. Leitfaden, Abschnitt 7, Gesamtwirtschaft A-S ohne O; mittleres Qualifikationsniveau mit 6 Prozent, hohes Qualifikationsniveau mit 94 Prozent; sowie OnDEA ID 2015030909595501 und 2020093009264402) ergibt sich für die geschätzt 24 nachweispflichtigen Einrichtungen ein jährlicher Erfüllungsaufwand von rund 849 000 Euro.

bb. Weitere Rechtsänderungen

Der Regelungsentwurf umfasst zahlreiche Rechtsänderungen ohne bzw. ohne wesentliche Auswirkungen auf den Erfüllungsaufwand (vgl. Tabelle, „formelle Änderung“ bzw. „geringfügig“). Zum einen werden bestehende Vorgaben in den künftigen Fassungen des BSIG, des EnWG und des TKG fortgesetzt, so dass keine Entlastungen aufgrund wegfallender Vorgaben zu verzeichnen sind. Zum anderen kann es bei diesen Vorgaben nach der künftigen Rechtslage zu geringfügigen Erhöhungen der Aufwände kommen, da der Geltungsbereich des BSIG ausgeweitet wird. Solche geringfügigen Erhöhungen resultieren zum Beispiel aus den §§ 7, 12, 17 und 41 BSIG-E (Begründung zur Geringfügigkeit siehe BR-Drs. 16/21, S. 34), § 64 Absatz 5 BSIG-E (bei der Nachmessung des Erfüllungsaufwands des IT-Sicherheitsgesetzes und des Gesetzes zur Umsetzung der NIS-Richtlinie gab das BSI an, nur wenige Prüfungen durchgeführt zu haben) oder § 33 Absatz 3 BSIG-E (laut BSI ist die Angabe einer Funktionspostfachs ausreichend, vgl. www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Kontaktstelle-benennen/kontaktstelle-benennen_node.html).
Rechtsänderungen mit Erfüllungsaufwänden sind im vorherigen Abschnitt erörtert (vgl. Tabelle, Vorgabe 4.2.X).

Bezeichnung der Vorgabe	Paragraf		ID des StBA	Erfüllungsaufwand
	bisher	künftig		
BSIG (Artikel 1)				
Bereitstellung von Unterlagen und Datenträgern	§ 4a	§ 7 Absatz 1	2021012507333201	geringfügig
Bestandsdatenauskunft	§ 5c	§ 12	2021012507393701	geringfügig
Auskunftspflicht (Hersteller von informationstechnischen Produkten und Systemen) gegenüber dem Bundesamt	§ 7a Absatz 2	§ 14 Absatz 2	2021011810433601	formelle Änderung
Maßnahmen (Anbieter von Telekommunikationsdiensten) im Zusammenhang mit den Anordnungen des	§ 7c	§ 16	2021011810483101	formelle Änderung

Bezeichnung der Vorgabe	Paragraf bisher	Paragraf künftig	ID des StBA	Erfüllungsaufwand
Bundesamtes zur Abwehr konkreter erheblicher Gefahren				
Aufwand im Zusammenhang mit Anordnungen des Bundesamtes (BSI) gegenüber Anbietern von digitalen Diensten	§ 7d	§ 17	2021012507494901	geringfügig
Einhaltung eines Mindestniveaus an IT-Sicherheit (Kritische Infrastrukturen)	§ 8a i. V. m. § 8c	§ 31 Absatz 1	2015030909595401	s. Vorgabe 4.2.1
Einhaltung eines Mindestniveaus an IT-Sicherheit (Anbieter digitaler Dienste)	§ 8c Absatz 1	§ 31 Absatz 1	2017052913283301	s. Vorgabe 4.2.1
Verpflichtender Einsatz von Systemen zur Angriffserkennung bei Betreibern kritischer Infrastrukturen	§ 8a Absatz 1a	§ 31 Absatz 2	2021011810531701	s. Vorgabe 4.2.1
Meldung erheblicher IT-Sicherheitsvorfälle an das BSI (Kritische Infrastrukturen)	§ 8b Absatz 4	§ 32	2015030909595201	s. Vorgabe 4.2.2
Meldung erheblicher IT-Sicherheitsvorfälle an das BSI (Anbieter digitaler Dienste)	§ 8c Absatz 3	§ 32	2017052913283701	s. Vorgabe 4.2.2
Pflicht von Unternehmen im besonderen öffentlichen Interesse bestimmte Störungen ihrer informationstechnischen Systeme, Komponenten und Prozesse unverzüglich dem BSI zu melden	§ 8f Absatz 7 und 8	§ 32	2021012507215301	s. Vorgabe 4.2.2
Registrierung der Kritischen Infrastruktur und Benennung einer Kontaktstelle	§ 8b Absatz 3	§ 33 Absatz 1	2015030909595901	s. Vorgabe 4.2.3
Betreiben einer Kontaktstelle	§ 8b Absatz 3	§ 33 Absatz 3	2015030909595701	geringfügig
Nachweis der Erfüllung der Mindestanforderungen durch Sicherheitsaudits (Kritische Infrastrukturen)	§ 8a Absatz 3	§ 39 Absatz 1	2015030909595501	formelle Änderung
Nachweis über Maßnahmen zur Wahrung der Sicherheit von Netz- und Informationssystemen (Anbieter digitaler Dienste)	§ 8c Absatz 4	§ 39 Absatz 1	2020093009355901	formelle Änderung
Pflicht von Unternehmen im besonderen öffentlichen Interesse zur Vorlage einer Selbsterklärung zur IT-Sicherheit gegenüber dem BSI	§ 8f Absatz 1	§ 39 Absatz 1	2021012506571401	formelle Änderung
Bereitstellung von Information im Rahmen der amtlichen Prüfung	§ 8f Absatz 9	§ 39 Absatz 1 und § 64 Absatz 5	2021012507544601	formelle Änderung
Übermittlungspflicht an BSI von KRITIS und UBI zur Bewältigung von erheblichen IT-Störungen	§ 8b Absatz 4a	§ 40 Absatz 5	2021012506532301	s. Vorgabe 4.2.2
Anzeige des Einsatzes kritischer Komponenten für die eine gesetzliche Zertifizierungspflicht besteht gegenüber dem BMI	§ 9b Absatz 1	§ 41 Absatz 1	2021012507595001	geringfügig
Garantieerklärung des Herstellers gegenüber dem Betreiber der Kritischen Infrastruktur	§ 9b Absatz 3	§ 41 Absatz 2	2021012508035801	geringfügig
Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen	§ 4b Absatz 2	§ 5 Absatz 4	2021012507365101	formelle Änderung
Antrag auf Erteilung eines Sicherheitszertifikats	§ 9 Absatz 2	§ 54 Absatz 2	200609271412501x	formelle Änderung
Antrag der Konformitätsbewertungsstellen auf Erteilung einer Befugnis, als solche tätig zu werden	§ 9a Absatz 2	§ 55 Absatz 2	2021012507302801	formelle Änderung
Vor-Ort-Begleitung bei Prüfungen des BSI	§ 8a Absatz 4	§§ 64 und 65	2017052913282901	geringfügig
EnWG (Artikel 16)				
Einhaltung eines Mindestniveaus an IT-Sicherheit (Energie)	§ 11 Absatz 1a und 1b	§ 5c Absatz 1 und 2	2020093009264301	s. Vorgabe 4.2.1
Dokumentation der Einhaltung der Sicherheitsanforderungen an die IT-Sicherheit (Energie)	§ 11 Absatz 1b	§ 5c Absatz 1 und 2	2020093009264402	formelle Änderung
Meldung erheblicher IT-Sicherheitsvorfälle an das BSI (Energie)	§ 11 Absatz 1c	§ 5c Absatz 6 und 7	2020093009264501	s. Vorgabe 4.2.2
TKG (Artikel 23)				

Bezeichnung der Vorgabe	Paragraf		ID des StBA	Erfüllungsaufwand
	bisher	künftig		
Einhaltung eines Mindestniveaus an IT-Sicherheit (Telekommunikation)	§ 165 Absatz 2	§ 165 Absatz 2 und 2a	2020093009264401	s. Vorgabe 4.2.1
Meldung erheblicher IT-Sicherheitsvorfälle an das BSI (Telekommunikation)	§ 168 Absatz 1 – 3	§ 168 Absatz 1 bis 3	2011101812110109	s. Vorgabe 4.2.2

KMU-Test

Ein KMU-Test ist für den Gesetzentwurf durchgeführt worden. Das Regelungsvorhaben betrifft kleine und mittlere Unternehmen, da diese unter § 28 Absatz 2 BSIG E fallen können. Es ist damit zu rechnen, dass voraussichtlich rund 20 900 Unternehmen als wichtige Einrichtungen erfasst werden. Belastungen für mittlere Unternehmen könnten sich aus einer anfänglich fehlenden Routine bei der Umsetzung obengenannter Vorschriften ergeben. Weiterhin ist damit zu rechnen, dass unter Umständen fachspezifische Expertise bei kleineren Unternehmen noch im Aufbau sein wird.

Der Regelungsentwurf dient der Umsetzung der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und Rates, weshalb Abweichungen bei der nationalen Ausgestaltung lediglich eng begrenzt möglich sind. Jedoch ist zu bedenken, dass Differenzierungen im Rahmen der Angemessenheit der Maßnahmen gesetzlich Niederschlag gefunden haben (s. vorgenannte Ausführungen). Das Regelungsvorhaben gleicht auferlegte Belastungen durch die Häufigkeit, der einer Pflicht nachgekommen werden muss, variierend nach der Einrichtungsart aus.

c. Erfüllungsaufwand für die Verwaltung

Der Bundesverwaltung entsteht Erfüllungsaufwand als Adressat von Vorgaben des Regelungsentwurfs zur Wahrung der Sicherheit in der Informationstechnik (vgl. Vorgaben 4.3.1 bis 4.3.4), wobei Vorgabe 4.3.1 mit Ausnahme des BMVg von den Ressorts und dem Bundeskanzleramt und die Vorgaben 4.3.2 bis 4.3.4 auch von den Geschäftsbereichsbehörden, Bundesgerichten und sonstigen Bundesbehörden zu erfüllen sind.

Zudem entsteht einigen Behörden weiterer Erfüllungsaufwand, da ihnen durch mehrere Vorgaben neue Aufgaben im Verwaltungsvollzug zugewiesen werden (vgl. Vorgaben 4.3.5 bis 4.3.12).

Um den Erfüllungsaufwand des Bundes abschätzen zu können, hat das BMI zusammen mit dem StBA eine schriftliche Befragung der Bundesverwaltung durchgeführt. Teilweise erhielt das StBA aggregierte Schätzungen von Ressorts zum gesamten Geschäftsbereich, teilweise erhielt es Einzelschätzungen zu einzelnen Behörden.

Aufgrund des prognostischen Charakters betonen viele beteiligte Stellen, dass die Angaben mit zum Teil großen Unsicherheiten behaftet sind.

Im Folgenden wird die Schätzung des Erfüllungsaufwands der Bundesverwaltung für die einzelnen Vorgaben dargestellt. Die Darstellung ist stark aggregiert, da Einzeldaten zur notwendigen Aufrüstung der IT-Sicherheit von Einrichtungen der Bundesverwaltung als sensibel einzustufen sind. Die qualitative Beschreibung ist eine stark verkürzte aber sinngemäße Synthese der entsprechenden Erläuterungen der beteiligten Stellen.

In der Übergangsphase direkt nach in Krafttreten des Gesetzes fallen bei verschiedenen Vorgaben einmalige Tätigkeiten unter anderem für die Implementierung neuer Prozesse an. Daraus entstehender Aufwand wird als einmaliger Erfüllungsaufwand ausgewiesen. Sich anschließende dauerhafte Tätigkeiten und daraus resultierende Aufwände werden als jährlicher Erfüllungsaufwand dargestellt.

aa. Wesentliche Rechtsänderungen

aaa. Vorgaben für Einrichtungen der Bundesverwaltung zur Wahrung der IT-Sicherheit

Die Behörden schätzen ihren dauerhaften Personalbedarf aus den Vorgaben (4.3.1 bis 4.3.4) zur Wahrung der IT-Sicherheit auf zusammen rund 381 Stellen, wodurch Personal-kosten in Höhe von rund 31,7 Millionen Euro entstehen werden. Die jährlichen Sachkosten schätzen sie auf zusammen rund 30 Millionen Euro. Den einmaligen Erfüllungsaufwand beziffern sie auf insgesamt 27 Millionen Euro.

Vorgabe 4.3.1: Maßnahmen zur Gewährleistung der Informationssicherheit; § 43 Absatz 1, 3 und 4 Satz 2, §§ 44 bis 46 und 50 in Verbindung mit §§ 29 und 37 Absatz 1 sowie § 46 Absatz 4 BSIG-E

Veränderung des jährlichen Erfüllungsaufwands des Bundes:

Fallzahl*	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
11,0 (mD)	1 600	33,80	0	595	0
108,8 (gD)	1 600	46,50	0	8095	0
47,4 (hD)	1 600	70,50	0	5347	0
1	0	0	14 364 065	0	14 364
Änderung des Erfüllungsaufwands (in Tsd. Euro)				28 400	

* mD ~ mittlerer Dienst, gD ~ gehobener Dienst, hD ~ höherer Dienst

Einmaliger Erfüllungsaufwand des Bundes:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
5,8 (mD)	1 600	33,80	0	314	0
49,9 (gD)	1 600	46,50	0	3 713	0
21,7 (hD)	1 600	70,50	0	2 448	0
1	0	0	9 832 553		
Erfüllungsaufwand (in Tsd. Euro)				16 307	

Einrichtungen der Bundesverwaltung im Sinne des § 29 BSIG-E müssen hinsichtlich des IT-Betriebs künftig gemäß § 43 Absatz 1 BSIG-E die Voraussetzungen zur Gewährleistung der Informationssicherheit schaffen. Hierzu soll das BSI durch den IT-Grundschutz und durch Mindeststandards für die Sicherheit in der Informationstechnik des Bundes die zu erfüllenden Anforderungen festlegen (vgl. § 44 BSIG-E). Eine grundsätzliche Pflicht zur Umsetzung von Mindeststandards für die Sicherheit der Informationstechnik existiert bereits nach geltendem Recht (vgl. § 8 BSIG) und wurde zuletzt auf IT-Dienstleister, soweit sie IT-Dienstleistungen für die Kommunikationstechnik des Bundes erbringen, ausgeweitet (vgl. BT-Drs. 19/26106, S. 78 und OnDEA unter anderem ID 2021012607002101).

Die Einrichtungen der Bundesverwaltungen schätzen den gesamten Personalbedarf dauerhaft auf zusammen 167 Stellen und einmalig auf 77 Stellen, wodurch jährliche Personalkosten von rund 14 Millionen Euro und einmalig von sechs Millionen Euro entstehen.

Der Personalaufwand entsteht unter anderem aus folgenden Tätigkeiten: Etablierung und Durchführung eines Risikomanagements in der Informationssicherheit, Erstellung und ständige Aktualisierung von Sicherheitskonzepten, Sicherheitsvorfallmanagement, Sicherstellung der Einhaltung der Vorgaben der Informationssicherheit bei Dienstleistern sowie bei der Beschaffung, Entwicklung und Wartung von IT-Systemen, erweitertes Reporting, Ausbau und Wahrnehmung der Fachaufsicht.

Jährliche und einmalige Sachkosten werden von den Einrichtungen der Bundesverwaltung auf rund 14 Millionen Euro und zehn Millionen Euro geschätzt. Neben einzelnen Positionen wie dem Aufwand zum Erwerb und dem Aufrechterhalten der Fachkunde des Informationssicherheitsbeauftragten und dessen Vertretung entstehen Sachkosten vor allem für den Ausbau und den Betrieb der zusätzlich notwendigen IT-Infrastruktur sowie die Beanspruchung von Dienstleitungen Dritter.

Bedeutsame Positionen der Infrastrukturkosten umfassen: Zusätzliche Hardware, Support und Wartung von Hardware sowie Software und Lizenzen, Ertüchtigung und Dauerbetrieb paralleler Infrastrukturen und redundanter Betriebsumgebungen sowie Kommunikationsstrukturen.

Teilweise signifikanten Aufwand für Beratungsleistungen schätzen Behörden mit dem Verweis auf den allgemeinen Fachkräftemangel und den vergleichsweisen attraktiven Gehältern der Privatwirtschaft. Allgemein sollen entsprechend der Anforderungen des Umsetzungsgesetzes Aufträge und Dienstleistungen in verschiedenen Bereichen der Informationstechnik erbracht werden. Im Einzelnen sollen zum Beispiel BSI zertifizierte externe Beraterinnen und Berater beauftragt werden, die unter anderem für IS-Penetrationstets (und Bewertung der Mängel) und für die besondere Expertise bei der Sicherheitsberatung zu kritischen Geschäftsprozessen sowie IT-Verfahren zum Einsatz kommen. Ebenso sollen Coachings, Unterstützungsleistungen unter anderem für die Erstellung des Sicherheitskonzeptes und für die Überprüfung von IT-Dienstleistern und Unterstützungsleistung von Dritten für das Notfallmanagement eingekauft werden.

Der Erfüllungsaufwand beträgt jährlich 28 Millionen Euro und einmalig 16 Millionen Euro.

Vorgabe 4.3.2: Sicherheitsvorfälle (Meldung; Gegenmaßnahmen; Unterrichtungspflichten); §§ 10, 32, 35 und 36 in Verbindung mit §§ 29, 37, 43 Absatz 5 und 6 sowie § 46 Absatz 4 BSIG-E

Veränderung des jährlichen Erfüllungsaufwands des Bundes:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
12,9 (mD)	1 600	33,80	0	697	0
87,7 (gD)	1 600	46,50	0	6506	0
26,6 (hD)	1 600	70,50	0	3001	0
1	0	0	8 928 570	0	8 929
Änderung des Erfüllungsaufwands (in Tsd. Euro)				19 603	

Einmaliger Erfüllungsaufwand des Bundes:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
0,2 (mD)	1 600	33,80	0	11	0
2,1 (gD)	1 600	46,50	0	156	0
8,2 (hD)	1 600	70,50	0	925	0
1	0	0	4 138 693	0	4 139
Erfüllungsaufwand (in Tsd. Euro)				5 231	

Einrichtungen der Bundesverwaltung müssen erhebliche Sicherheitsvorfälle an das BSI melden (vgl. § 32 in Verbindung mit § 29 Absatz 2 BSIG-E). Mit Ausnahmen des Geschäftsbereichs des Bundesressort Verteidigung müssen sie im Falle einer Anordnung des BSI Maßnahmen zur Abwendung oder Behebung von Sicherheitsvorfällen ergreifen (vgl. § 10 in Verbindung mit § 29 Absatz 2 und 3 BSIG-E) und bei einer Anweisung des BSI Empfängerinnen und Empfängern ihrer Dienste über erhebliche Sicherheitsvorfälle unterrichten (vgl. § 35 in Verbindung mit § 29 Absatz 2 und 3 BSIG-E).

Insgesamt werden vermutlich einmalig 10,5 Stellen und dauerhaft 127,2 Stellen für die Erfüllung der Vorgaben zu Sicherheitsvorfällen eingesetzt, wodurch Personalkosten von einmalig 1,1 Millionen Euro und jährlich 10,2

Millionen Euro entstehen werden. Bearbeitungsaufwand entsteht voraussichtlich insbesondere für die Umsetzung der Anordnungen von Maßnahmen zur Abwendung und Behebung von Sicherheitsvorfällen. Zeitaufwand bedeuten ebenfalls die Meldungen selbst wie auch das Berichtswesen über die Umsetzung der Anordnungen an das BSI.

Sachkosten werden einmalig auf rund 4,1 Millionen Euro und jährlich auf rund 8,9 Millionen Euro geschätzt. Diese fallen an für das Incident und IT-Sicherheitsvorfall Management, Notfallmanagement und die materialbezogene Umsetzung von Sicherheitsmaßnahmen zur Abwendung und Behebung von Sicherheitsvorfällen. Zum Teil rechnen Behörden auch mit dem Einsatz externer Expertenteams.

Der Erfüllungsaufwand beträgt einmalig 5,2 Millionen Euro und jährlich 19,1 Millionen Euro.

Vorgabe 4.3.3: Regelmäßige Schulungen; § 43 Absatz 2 und § 44 Absatz 1 in Verbindung mit §§ 29, 37 und 46 Absatz 4 BSIG-E

Veränderung des jährlichen Erfüllungsaufwands des Bundes:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
4,4 (mD)	1 600	33,80	0	238	0
17,6 (gD)	1 600	46,50	0	1 309	0
9,7 (hD)	1 600	70,50	0	1 094	0
1	0	0	2 500 752	0	2 501
Änderung des Erfüllungsaufwands (in Tsd. Euro)				5 142	

Einmaliger Erfüllungsaufwand des Bundes:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
0,0 (mD)	1 600	33,80	0	0	0
2,8 (gD)	1 600	46,50	0	208	0
0,6 (hD)	1 600	70,50	0	68	0
1	0	0	663 000	0	663
Erfüllungsaufwand (in Tsd. Euro)				939	

Einrichtungsleitungen der Bundesbehörden sollen regelmäßig Cybersicherheitsschulungen absolvieren (vgl. § 43 Absatz 2 BISG-E). Gemäß Artikel 20 Absatz 2 der NIS-2-Richtlinie erstreckt sich die Schulungspflicht auch auf alle Mitarbeitende – dies wird im nationalen Recht durch § 44 Absatz 1 BSIG-E sichergestellt (vgl. Gesetzesbegründung).

Für den Besuch von Fortbildung sowie die teilweise Erarbeitung von Lehrmaterial schätzen die Bundesbehörden den Personalaufwand initial auf insgesamt rund 3,4 Stelle und dauerhaft auf rund 31,7 Stellen. Sachkosten für Lehrmaterial, Schulungen und die teilweise geplante Einbindung von externen Lehrkräften sowie Expertinnen und Experten schätzen sie einmalig auf 663 000 Euro und laufend auf 2,5 Millionen Euro. Der Erfüllungsaufwand beträgt einmalig 939 000 Euro und jährlich 5,1 Millionen Euro.

Vorgabe 4.3.4: Wesentliche Digitalisierungsvorhaben und Kommunikationsinfrastrukturen; § 47 BSIG-E in Verbindung mit §§ 29, 37 und 46 Absatz 4 BSIG-E

Veränderung des jährlichen Erfüllungsaufwands des Bundes:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
4,3 (mD)	1 600	33,80	0	233	0
28,1 (gD)	1 600	46,50	0	2 091	0
22,4 (hD)	1 600	70,50	0	2 527	0
1	0	0	4 579 962	0	4 580
Änderung des Erfüllungsaufwands (in Tsd. Euro)				9 430	

Einmaliger Erfüllungsaufwand des Bundes: 4,7 Millionen Euro.

Für die Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes sind eigene Informationssicherheitsbeauftragte zu bestellen. Zur Gewährleistung der Informationssicherheit bei solchen Vorhaben sind bedarfsgerechte Mittel für die Informationssicherheit einzusetzen (vgl. § 47 BSIG-E).

Die Anzahl wesentlicher Digitalisierungsvorhaben und Kommunikationsinfrastrukturen variiert zwischen den Behörden stark. Eine Vielzahl an Behörden sieht hier aufgrund fehlender Vorhaben keinen Aufwand. Einige Behörden wie das Umweltbundesamt, die Generalzolldirektion, das Auswärtige Amt oder das Statistische Bundesamt rechnen dauerhaft mit mehreren Vorhaben. Zur Sicherstellung der Informationssicherheit der Projekte rechnen solche Behörden nicht selten mit – auch laufbahnübergreifend – einer Stelle je Vorhaben.

In der Summe schätzen die Bundesbehörden den Stellenbedarf dauerhaft auf 55 Stellen, wodurch jährliche Personalkosten von4,9 Millionen Euro entstehen. Die Sachkosten schätzen sie jährlich auf 4,6 Millionen Euro und einmalig auf rund 4,7 Millionen Euro. Diese entstehen hauptsächlich durch die Inanspruchnahme der Dienstleistungen Dritter (z. B. für die Erstellung und Initialisierung der Sicherheitsleitlinien zu wesentlichen Digitalisierungsvorhaben sowie für externe Betriebsunterstützung in Ermangelung von verfügbarem qualifiziertem Personal) und den Ausbau und Betrieb zusätzlicher IT-Infrastruktur.

Der Erfüllungsaufwand beträgt einmalig 4,7 Millionen Euro und jährlich 9,4 Millionen Euro.

Bbb. Vorgaben zum Vollzug

Durch das Umsetzungsgesetz wird im BSIG der Aufgabenbereich der betroffenen Vollzugsbehörden neu strukturiert. Wesentlicher neuer Aufwand entstehen BSI, BBK, BnetzA, BfDI und BMI. Dieser entsteht vor allem durch die stark zunehmende Anzahl der zu beaufsichtigen Einrichtungen. Derzeit kann nur schwer abgeschätzt werden, wie hoch der zusätzliche Personalbedarf der betroffenen Vollzugbehörden tatsächlich sein wird. Die Behörden schätzen ihren dauerhaften Personalbedarf auf zusammen rund 539 Stellen, wodurch jährliche Personalkosten in Höhe von rund 50 Millionen Euro entstehen werden. Die jährlichen bzw. einmaligen Sachkosten schätzen sie auf zusammen rund 10 Millionen Euro bzw. 11 Millionen Euro.

Allein auf das BSI entfallen rund 476 Stellen (neben 16 weiteren Stellen die bei den Vorgaben 4.3.1 bis 4.3.4 berücksichtigt sind). Im Vergleich dazu werden derzeit allein im BSI aufgrund der vorangegangenen Regelungsvorhaben IT-Sicherheitsgesetz, Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 und zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme rund 645 Stellen für die Wahrnehmung bestehender Aufgabe der Sicherheit in der Informationstechnik gemäß §§ 3 ff. BSIG eingesetzt.

Viele der Behörden, die bereits heute in relativ geringem Umfang am Vollzug das BSIG mitwirken, haben auf keine wesentlichen Veränderungen ihres Vollzugsaufwands hingewiesen. Diese Rechtsänderungen können im Sinne des Erfüllungsaufwands als formelle Rechtsänderungen gesehen werden (vgl. Unterabschnitt b).

Vorgabe 4.3.5: Grundsatzaufgaben und Befugnisse (BSI, BfDI); §§ 3 bis 19 in Verbindung mit §§ 20 bis 27 BSIG-E

Veränderung des jährlichen Erfüllungsaufwands des Bundes:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
26,0 (mD)	1 600	33,80	0	1 406	0
96,0 (gD)	1 600	46,50	0	7 142	0
187,0 (hD)	1 600	70,50	0	21 094	0
1		0	3 943 000	0	3 943
Änderung des Erfüllungsaufwands (in Tsd. Euro)				33 585	

Einmaliger Erfüllungsaufwand des Bundes: 2,5 Millionen Euro

Die „Grundsatzaufgaben“ und Befugnisse im Bereich der bundesrechtlich geregelten Sicherheit in der Informationstechnik ergeben sich künftig aus den §§ 3 bis 19 in Verbindung mit §§ 20 bis 27 BSIG-E. Bereits heute nimmt das BSI umfassende Aufgaben in diesem Bereich wahr (vgl. §§ 3 BISG; OnDEA, u. a. ID 2015030910484001, 2021012608550401). Mit der Umsetzung der NIS-2-Richtlinie werden diese Aufgaben des BSI ausgeweitet. So fallen zum Beispiel künftig alle Einrichtungen der Bundesverwaltung in den Anwendungsbereich des BSIG, wodurch insbesondere der Aufwand aus Tätigkeiten zur Wahrung des Schutzes der gesamten Kommunikationstechnik des Bundes zunimmt (vgl. §§ 7 und 8 BSIG-E). Mit Blick auf datenschutzrechtliche Belange wird das BSI bei der Wahrnehmung seiner Aufgaben nach dem BSIG durch den BfDI unterstützt. Der BfDI sieht durch die erhebliche Erweiterung des Wirkungskreises des BSI und die Erweiterung seiner Aufgaben auf weitaus mehr Behörden höheren Beratungs- und Kontrollaufwand des BfDI gegenüber dem BSI.

Insgesamt beziffert der BfDI seinen dauerhaften Mehraufwand mit vier Stellen (je zwei Stellen im gehobenen und höheren Dienst) und das BSI mit 305 Stellen (rund 26, 94 bzw. 185 Stellen im mittleren, gehobenen bzw. höheren Dienst). Behördenübergreifend entstehen dadurch jährliche Personalkosten von rund 33,6 Millionen Euro. Im Einzelnen ergibt sich der Bedarf aus Tätigkeiten wie: Beratung und Kontrolle zur Sicherung der datenschutzkonformen Umsetzung des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes, Erstellung, Abstimmung und regelmäßige Anpassung von Vorgaben zur Definition erheblicher Sicherheitsvorfälle auf Grund der Dynamik der Entwicklung bei Cyber-Angriffen . Für Einsätze von BSI Computernotfallteams zur Unterstützung anderer Teams im Unionsgebiet müssen entsprechend einsatzfähige Teams vorgesehen und vorgehalten werden; dadurch können die im Gesetz vorgesehenen Leistungen zur gegenseitigen Unterstützung innerhalb der Union zusätzlich zu den bestehenden Einsätzen im nationalen Rahmen erbracht werden. Zudem fällt auf Aufwand an für Peer Reviews, die operative Koordination, zentrale Anlaufstelle CSIRT, Unterrichtung von Einrichtungen umfangreiche Vorfallsunterstützung, MIRT-Beratung Warnanlässe, Dauerdienste, Unterrichtung durch LZ/WG, Onlineportal mit WG23, Scans nach Schwachstellen).

Für die Implementierung und den Betrieb der mit den zusätzlichen Aufgaben verbundenen neuen Verfahrensabläufe und zusätzlicher IT-Ausstattung (z. B. Ausbau der Detektionsinfrastruktur, Fortschreibung bzw. Erweiterung des Schulungskonzepts für KRITIS-Prüfer, Prüfungen, Öffentlichkeitsarbeit) veranschlagen die Behörden zusammen jährliche bzw. einmalige Sachkosten von rund vier Millionen bzw. 2,5 Millionen Euro.

Der Erfüllungsaufwand beträgt einmalig 2,5 Millionen Euro und jährlich 33,6 Millionen Euro.

Vorgabe 4.3.6: Bearbeitung von Meldungen erheblicher Sicherheitsvorfälle (BSI und BBK); §§ 32, 35, 36 sowie 40 Absatz 3 und 4 BSIG-E

Veränderung des jährlichen Erfüllungsaufwands des Bundes:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
12,0 (mD)	1 600	33,80	0	649	0
49,0 (gD)	1 600	46,50	0	3 646	0
49,0 (hD)	1 600	70,50	0	5 527	0
1	0	0	1 119 450	0	1 119
Änderung des Erfüllungsaufwands (in Tsd. Euro)				10 941	

Einmaliger Erfüllungsaufwand des Bundes: 508 000 Euro

Bereits heute ist das BSI zentrale Anlaufstelle für Meldungen von Betreibern Kritischer Infrastrukturen zu erheblichen Sicherheitsvorfällen (vgl. § 8b Absatz 3 BSIG). Künftig werden in den §§ 32, 35, 36 sowie 40 Absatz 4 und 5 BSIG-E diesbezügliche Vollzugsaufgaben des BSI und des BBK geregelt. Seitens der Behörden ist allein aufgrund der deutlichen Ausweitung der meldepflichtigen Einrichtungen mit erheblichem Mehraufwand zu rechnen. Zusätzlich wird der Aufwand pro Meldung im Mittel aufwendiger, da nun ein mehrstufiges Meldeverfahren eingeführt wird (vgl. § 32 BSIG-E, Vorgab 4.2.2). Das BSI kann in bestimmten Fällen Anweisungen zur Unterrichtung von Diensteempfängern erteilen (vgl. § 35 BSIG-E) und es bietet in strafrechtsrelevanten Fällen Orientierungshilfen für die Meldung an Strafvollzugsbehörden (vgl. § 36 BSIG-E). Zudem kann das BSI bestimmte Informationen von Betreibern verlangen und in bestimmten Fällen unterliegt es selbst einer Unterrichtungspflicht gegenüber Mitgliedstaaten der Europäischen Union (vgl. § 40 Absatz 3 und 4 BSIG-E). Das BBK sieht einen Mehraufwand aufgrund der Einrichtung und des Betriebs des Meldeverfahrens. Zudem entsteht ein Mehraufwand, da Prüfungen bezüglich des IT-SiG 2.0 auf etwaige Konflikte mit § 12 Absatz 1 KRITIS-DachG-E Meldewesen durchgeführt werden müssen.

Insgesamt beziffert das BBK seinen dauerhaften Mehraufwand auf sechs Stellen (je zwei Stellen im mittleren, gehobenen und höheren Dienst); das BSI erwartet, dass laufbahnübergreifend zusätzliche 104 Stellen erforderlich sein werden (10, 47bzw. 47 Stellen im mittleren, gehobenen bzw. höheren Dienst). Behördenübergreifend entstehen dadurch jährliche Personalkosten von rund 9,8 Millionen Euro. Zusätzlich entstehen laut BBK und BSI für die Einrichtung und den Betrieb des Benachrichtigungstools, Ausbau des Meldewesens, neue Notebooks und den Skalierenden Betrieb der Kommunikations- und Unterstützungsmaßnahmen einmalige bzw. jährliche Sachkosten von 508 000 Euro bzw. 1,1 Millionen Euro.

Vorgabe 4.3.7: Einrichtung und Betrieb eines Registers für (besonders) wichtige Einrichtungen, bestimmte Einrichtungsarten sowie für Einrichtungen der Bundesverwaltung (BSI und BBK); §§ 33, 34 und 43 Absatz 4 BSIG-E

Veränderung des jährlichen Erfüllungsaufwands des Bundes:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
7,0 (mD)	1 600	33,80	0	379	0
12,0 (gD)	1 600	46,50	0	893	0
7,0 (hD)	1 600	70,50	0	790	0
1	0	0	1 950	0	2
Änderung des Erfüllungsaufwands (in Tsd. Euro)				2 063	

Einmaliger Erfüllungsaufwand des Bundes: 8 000 Euro

Dem BSI und BBK entstehen Erfüllungsaufwand aus der Registrierungspflicht für (besonders) wichtige Einrichtungen, bestimmte Einrichtungsarten und Einrichtungen der Bundesverwaltung (vgl. §§ 33, 34 und 43 Absatz 4 in BSIG-E). Bereits heute verarbeitet und pflegt das BSI entsprechende Angaben von Betreibern kritischer Infrastrukturen und von Unternehmen im besonderen öffentlichen Interesse (vgl. § 8b Absatz 3 und 8f Absatz 5 BSIG).

Durch die neuen Regelungen bedarf es laut BBK der Etablierung und dauerhaften Durchführung eines angepassten Registrierungsverfahrens. Zudem entsteht Mehraufwand, da Prüfungen bezüglich des IT-SiG 2.0 auf etwaige Konflikte mit § 6 Absatz 1 KRITIS-DachG-E Registrierung durchgeführt werden müssen. Aufgrund der Ausweitung des Normadressatenkreises erwarten das BSI Mehraufwand insbesondere durch die Verarbeitung eingehender Registrierungen, Anfragenbearbeitung und Stammdatenpflege von besonders wichtigen und wichtigen Einrichtungen. Zudem obliegt ihm die Fachadministration der IT-Systeme. BSI und BBK schätzen den zusätzlichen Personalbedarf auf insgesamt 26 Stellen (sechs im BBK und 20 im BSI), wodurch dauerhafte Personalkosten von rund zwei Millionen Euro entstehen. Zudem entstehen für die erstmalige Anschaffung und den dauerhaften Ersatz von Notebooks geringe Sachkosten.

Vorgabe 4.3.8: Zentrale Melde- und Anlaufstelle (BSI, BBK, BnetzA); § 40 BSIG-E

Veränderung des jährlichen Erfüllungsaufwands des Bundes:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
3,0 (mD)	1 600	33,80	0	162	0
14,0 (gD)	1 600	46,50	0	1 042	0
26,5 (hD)	1 600	70,50	0	2 989	0
1	0	0	2 925	0	3
Änderung des Erfüllungsaufwands (in Tsd. Euro)				4 196	

Einmaliger Erfüllungsaufwand des Bundes: 11 700 Euro

In § 40 BSIG-E wird die bisher in § 8b BSIG normierte Aufgabe des BSI als zentrale Melde- und Anlaufstelle mit Unterstützung des BBK fortgeführt. Aufgrund der deutlichen Ausweitung des Anwendungsbereichs des BSIG entsteht den Behörden zusätzlicher Aufwand: Insbesondere für die Sammlung von Informationen zur IT-bezogenen Gefahrenabwehr sowie deren fachlichen Auswertung mit Blick auf die Auswirkungen auf kritische Dienstleistungen, Prüfungen bezüglich des IT-SiG 2.0 auf etwaige Konflikte zu Vorfallsmeldungen und Bearbeitungen nach § 12 Absatz 5 bis 8 KRITIS-DachG-E, Anpassung der Prozessabläufe der Meldestelle auch unter Berücksichtigung von KRITS-DachG-E. Im Telekommunikationssektor zählt auch die Bundesnetzagentur als Melde- und Anlaufstelle. Diese muss zur Zusammenarbeit eine Stelle einrichten, welche als Ansprechpartnerin dem BSI zur Verfügung steht und bei Bedarf die notwendigen Informationen auswertet und unverzüglich zur Verfügung stellt.

BSI, BBK und BnetzA schätzen den zusätzlichen Personalbedarf auf insgesamt 44 Stellen (sieben im BBK, rund 33 im BSI und vier in der BnetzA), wodurch dauerhafte Personalkosten von rund 4,2 Millionen Euro entstehen. Zudem entstehen für die erstmalige Anschaffung und den dauerhaften Ersatz von Notebooks geringe Sachkosten.

Vorgabe 4.3.9: Verschiedene Vollzugsaufgaben im Bereich der IT-Sicherheit – Bund (BMI, BSI und BBK); § 30 Absatz 9, §§ 39, 48 , 58, 61 bis 64 und 65 BSIG-E

Veränderung des jährlichen Erfüllungsaufwands des Bundes:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
4,0 (mD)	1 600	33,80	0	216	0
10,8 (gD)	1 600	46,50	0	804	0
13,0 (hD)	1 600	70,50	0	1 466	0
1	0	0	2 535 425	0	2 535
Änderung des Erfüllungsaufwands (in Tsd. Euro)				5 022	

Einmaliger Erfüllungsaufwand des Bundes: 11 700 Euro

Neben den bisher genannten Aufgabenbereichen werden dem BMI, BSI und dem BBK durch den Regelungsentwurf weitere Aufgabe übertrageben. Hierzu zählen die Bearbeitung von Anträgen zur Eignungsfeststellung branchenspezifischer Standards (vgl. § 30 Absatz 9 BSIG-E), die Bearbeitung und Prüfung von Nachweisen über die Erfüllung der gesetzlichen Anforderungen zur IT-Sicherheit (vgl. § 39 BSIG-E), das Ergreifen von Aufsichts- und Durchsetzungsmaßnahmen (vgl. §§ 61 bis 64 BSIG-E) und die Durchführung von Ordnungswidrigkeitenverfahren (vgl. 65 BSIG-E).

Behördenübergreifend schätzen die betroffenen Behörden für die verschiedenen Aufgaben den Personalbedarf auf rund 28 Stellen (rund acht, sechs bzw. 14 Stellen beim BMI, BBK bzw. beim BSI), wodurch dauerhaft Personalkosten in Höhe von 2,5 Millionen Euro entstehen. Zusätzlich fallen jährliche Sachkosten von 2,5 Millionen Euro an – laut BSI vor allem für Studien –, und geringe einmalige Sachkosten.

Vorgabe 4.3.10: Verschiedene Vollzugsaufgaben im Bereich der IT-Sicherheit – Länder; § 40 Absatz 3 Nummer 2 und § 61 Absatz 9 Nummer 2 BSIG-E

Veränderung des jährlichen Erfüllungsaufwands der Länder: 85 000 Euro

Zwei Rechtsänderungen beeinflussen grundsätzlich den Vollzugsaufwand der Länder:

Wesentliche Informationen für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik hat das BSI zuständigen Landesbehörden zu übermitteln, die dann gemeinsam mit anderen Behörden die Relevanz analysieren (vgl. § 40 Absatz 3 Nummer 2 BSIG-E). In der Vergangenheit gab es zu Betreibern kritischer Infrastrukturen und Anbietern digitaler Dienste pro Jahr 15 dieser Meldungen. Aufgrund der Ausweitung des Anwendungsbereichs auf besonders wichtige und wichtige Einrichtungen kann vorsichtig geschätzt werden (vgl. Vorgabe 4.2.1), dass sich die Anzahl der relevanten Meldungen um das Fünffache ansteigt, also zusätzlich 75 Fälle. Für die Entgegennahme und Analyse einer Meldung werden gemäß Leitfaden als fallbezogener Zeitaufwand zwei Arbeitstage angesetzt (vgl. Leitfaden, Anhang 9, Standardaktivitäten 1 und 2 in einfacher Komplexität, 4, 8, 9 und 14 in mittlerer Komplexität und 5 in hoher Komplexität). Angenommen wird eine Bearbeitung durch den höheren Dienst, so dass bei einem Lohnsatz von 70,50 Euro pro Stunde ein gesamter jährlicher Zusatzaufwand von 85 000 Euro entsteht.

Schließlich kann die zuständige Landesbehörde in bestimmten Fällen der Geschäftsleitung die Ausübung seiner Tätigkeit vorübergehend untersagen (vgl. § 61 Absatz 9 Nummer 2 BSIG-E). Es kann davon ausgegangen werden, dass dieses Mittel als Ultima Ratio äußerst selten vorkommen wird und in der Regel die übrigen Aufsichtsmaßnahmen ausreichend sind. Insofern wird der Erfüllungsaufwand aufgrund der Ausweitung des Anwendungsbereichs als vernachlässigbar gering eingestuft.

Vorgabe 4.3.11: Grundsatzaufgaben zur IT-Sicherheit im Energiesektor (BnetzA); §§ 5c und 95 EnWG-E

Veränderung des jährlichen Erfüllungsaufwands des Bundes:

Fallzahl*	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
0,8 (mD)	1 600	33,80	0	43	0
4,8 (gD)	1 600	46,50	0	357	0
5,2 (hD)	1 600	70,50	0	587	0
Änderung des Erfüllungsaufwands (in Tsd. Euro)				987	

Im Energiesektor werden die Vorschriften zur IT-Sicherheit für Betreiber von Energieversorgungsnetzen und Energieanlagen aus § 11 Absatz 1a bis 1g EnWG in dem § 5c EnWG-E neu gefasst. Der BnetzA entsteht insofern neuer Aufwand, da die bestehenden IT-Sicherheitskataloge und Vorgaben zu Risikobehandlungsplänen und zur Beseitigung von Sicherheitsmängeln ausgeweitet werden. Sie muss neue Schulungskonzepte entwickeln und pflegen, energiesystemische Bewertungen von BSI-Meldung vornehmen und diese Ergebnisse an das BSI übermitteln, Jahresberichte über Sicherheitsvorfälle erstellen und zusätzliche Ordnungswidrigkeitenverfahren durchführen. Insgesamt rechnet die BnetzA laufbahnübergreifen mit einem zusätzlichen Personalbedarf von 10,8 Stellen, wodurch ein jährlicher Erfüllungsaufwand von knapp einer Million Euro entsteht.

Vorgabe 4.3.12: Grundsatzaufgaben zur IT-Sicherheit im Telekommunikationssektor (BnetzA); §§ 165 und 168 TKG-E

Veränderung des jährlichen Erfüllungsaufwands des Bundes:

Fallzahl*	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
1,0 (mD)	1 600	33,80	0	54	0
10,0 (gD)	1 600	46,50	0	744	0
1,0 (hD)	1 600	70,50	0	113	0
1	0	0	2 000 000	0	2 000
Änderung des Erfüllungsaufwands (in Tsd. Euro)				2 911	

Einmaliger Erfüllungsaufwand des Bundes: 8 Millionen Euro

Im Telekommunikationssektor werden für Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste gemäß § 165 TKG-E Maßnahmen in Form von Konzepten, Lieferkettenangaben, Verschlüsselungsverfahren und Bewertungen von Maßnahmen, welche von besonders wichtigen und wichtigen Einrichtungen zu erfüllen sind, erweitert. Diese werden turnusmäßig alle zwei Jahre von der BnetzA überprüft. Zusätzlich müssen regelmäßig Fortbildungen und Ausbildungen durchgeführt werden, um sich in dem Bereich auf den neusten Stand zu bringen. Der § 168 TKG-E wird erweitert, da nun eine Erstmeldung und ein abschließender Bericht vorgesehen wird. Die Berichte müssen ausgewertet und bewertet werden, kommen die Verpflichteten ihren Aufgaben in der Zeit nicht nach, muss ein Ordnungswidrigkeitenverfahren durchgeführt werden. Die BnetzA schätzt den zusätzlichen Personalaufwand dauerhaft auf zwölf Stellen, wodurch jährliche Kosten von 911 000 Euro entstehen.

Zusätzlich fallen laut BnetzA Sachkosten in Umfang von acht Millionen Euro einmalig und zwei Millionen Euro jährlich an, da aufgrund der zum Teil hoch sensiblen Daten, die von den Erbringern von Telekommunikationsdiensten gemeldet werden, eine noch nicht vorhandene VS-Registratur eingerichtet und betrieben werden muss.

bb. Weitere Rechtsänderungen

Wie bei der Wirtschaft wird angenommen, dass der Aufwand für die Registrierung (vgl. § 33 in Verbindung mit § 29 BSIG-E) vernachlässigbar geringen Aufwand verursachen wird. Daneben werden zahlreiche Vorgabe von der aktuell geltenden Fassung in die künftige Fassung des BSIG bzw. EnWG überführt, ohne dass die betroffenen

Behörden Veränderungen beim Erfüllungsaufwand sehen (vgl. Tabelle, „formelle Änderung“). Rechtsänderungen mit Erfüllungsaufwänden sind im vorherigen Abschnitt erörtert (vgl. Tabelle, Vorgabe 4.3.X).

Bezeichnung der Vorgabe	Paragraf		ID des StBA	Erfüllungsaufwand
	bisher	künftig		
BSIG (Artikel 1)				
Fachaufsicht über das BSI	§ 1	§ 1	2017052913284101	formelle Änderung
Unterrichtung des Innenausschusses über die Anwendung des BSIG (BMI)	§ 13 Absatz 3	§ 58 Absatz 3	2023121812242201	formelle Änderung
Ordnungswidrigkeitsverfahren (BSI)	§ 14	§ 65	2021012613125701	Vorgabe 4.3.10
Mitwirken bei Ordnungswidrigkeitsverfahren des BSI (BMG)	§ 14	§ 65	2021012707301701	formelle Änderung
Einvernehmensverfahren der für die Institutionen der sozialen Sicherung zuständigen Aufsichtsbehörden (BMAS und BAS) mit BSI über zu ergreifende Maßnahmen	§ 14a	§ 64	2021102813021101	formelle Änderung
Bestimmung von KRITIS-Betreibern	§ 2 Absatz 10 i. V. m. § 10 Absatz 1	§ 28 Absatz 6 und 7	2023121812504101	formelle Änderung
Gewährleistung der IT-Sicherheit bei der Kommunikation zwischen Behörden und öffentlichen Netzen (ITZBund)	§ 2 Absatz 3	§ 7 i. V. m. § 2 Absatz 1 Nummer 20	2021110314194701	Vorgabe 4.3.6
Mitwirken bei der Förderung der Sicherheit in der Informationstechnik durch BSI (BMFSFJ)	§ 3 Absatz 1	§ 3 Absatz 1	2021012707534101	formelle Änderung
Mitwirken bei der Förderung der Sicherheit in der Informationstechnik durch BSI (BzKJ)	§ 3 Absatz 1	§ 3 Absatz 1	2021012708221801	formelle Änderung
Mitwirken bei der Förderung der Sicherheit in der Informationstechnik durch BSI (BAFzA)	§ 3 Absatz 1	§ 3 Absatz 1	2021012709053401	formelle Änderung
Beratung, Information, Empfehlung und Warnung in Fragen der Sicherheit in der Informationstechnik (BSI)	§ 3 Absatz 1 Nummer 14, 14a und 19	§ 3 Absatz 1	2015030910484001	Vorgabe 4.3.6
Beratung, Kontrolle und Prüfung datenschutzrechtlicher Vorgaben bei der Umsetzung der Prüf-, Abfrage- und Kontrollbefugnisse des BSI (BfDI)	§ 3 Absatz 1 Satz 2 Nummer 12	§ 3 Absatz 1	2021012706485901	Vorgabe 4.3.6
Kontrolle der Kommunikationstechnik des Bundes durch das Bundesamt (BSI)	§ 4a	§ 7	2021012608550401	Vorgabe 4.3.6
Mitwirken bei Kontrolle der Kommunikationstechnik des Bundes durch das BSI (Bundesbehörden)	§ 4a	§ 7	2021012707130301	Vorgabe 4.3.6
Allgemeine Meldestelle für die Sicherheit in der Informationstechnik (BSI)	§ 4b	§ 5 Absatz 1	2021012609014501	Vorgabe 4.3.6
Mitwirken bei der Allgemeinen Meldestelle für die Sicherheit in der Informationstechnik beim BSI (Bundesbehörden)	§ 4b	§ 5 Absatz 1	2021012707162401	formelle Änderung
Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes (BSI)	§ 5	§ 8	2021012609055001	Vorgabe 4.3.6
Mitwirken bei der Verarbeitung eigener behördeninterner Protokollierungsdaten durch das BSI (Bundesbehörden)	§ 5a	§ 9	2021012606533701	formelle Änderung
Verarbeitung behördeninterner Protokollierungsdaten (BSI)	§ 5a	§ 9	2021012609332401	Vorgabe 4.3.6
Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen (BSI)	§ 5b	§ 11	2021012609372701	Vorgabe 4.3.6
Bestandsdatenabfrage (BSI)	§ 5c	§ 12	2021012609432501	Vorgabe 4.3.6
Aufgaben im Rahmen der Einschränkung von Informationspflichten (BSI)	§ 6a	§ 21	2019011110030201	Vorgabe 4.3.6
Technische Untersuchungen durch das Bundesamt (BSI)	§ 7a	§ 14 Absatz 1	2021012610373001	Vorgabe 4.3.6
Umsetzung von Maßnahmen zur Sicherheit der Informationstechnik (BMAS)	§ 7a	§ 14	2021102713464901	formelle Änderung

Bezeichnung der Vorgabe	Paragraf		ID des StBA	Erfüllungsaufwand
	bisher	künftig		
Mitwirken bei der Untersuchung der Sicherheit in der Informationstechnik durch BSI (BfDI)	§ 7a Absatz 3	§ 14 Absatz 3	2021012706565501	Vorgabe 4.3.6
Mitwirken bei der Untersuchung der Sicherheit in der Informationstechnik durch BSI (BMG)	§ 7a Absatz 3	§ 14 Absatz 3	2021012707245801	formelle Änderung
Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden (BSI)	§ 7b	§ 15	2021012610415601	Vorgabe 4.3.6
Einvernehmen mit dem BfDI vor einer Anordnung durch das Bundesamt (BSI)	§ 7c Absatz 1	§ 16 Absatz 1	2021012707021901	Vorgabe 4.3.6
Festlegung von Mindeststandards für die Sicherheit der Informationstechnik des Bundes BSI	§ 8	§ 44	2021012611515101	Vorgabe 4.3.6
Festlegung und Einhaltung einvernehmlicher IT-Mindeststandards und Beteiligung des BSI bei wesentlichen Digitalisierungsvorhaben (Bundesbehörden)	§ 8 Absatz 1, 1a und 4	§§ 44 i. V. m. § 47	2021012607002101	formelle Änderung
Prüfung branchenspezifischer Sicherheitsstandards (BSI)	§ 8a	§ 30 Absatz 9	2023121812331001	Vorgabe 4.3.6
Umsetzung von organisatorischen und technischen Vorkehrungen (AA)	§ 8a Absatz 1a	§ 31 Absatz 2	2021102814224601	formelle Änderung
Mitwirken bei der Prüfung branchenspezifischer Sicherheitsstandards (BBK)	§ 8a Absatz 2	§ 30 Absatz 9	2015030910484201	formelle Änderung
Mitwirken bei der Aufgabenerfüllung der Meldestelle (BfV)	§ 8b Absatz 2 Nummer 4 b	§ 40 Absatz 3 Nummer 5	2015030910484401	formelle Änderung
Mitwirken bei der Aufgabenerfüllung der Meldestelle (BND)	§ 8b Absatz 2 Nummer 4 b	§ 40 Absatz 3 Nummer 5	2015030910484501	formelle Änderung
Bewertung und Bewältigung erheblichen Sicherheitsvorfälle (BSI)	§ 8b Absatz 4a	§ 40 Absatz 5	2021012611561201	Vorgabe 4.3.7
Mitwirken bei der Bewältigung erheblichen Sicherheitsvorfälle (Bundesbehörden)	§ 8b Absatz 4a	§§ 36 und 40 Absatz 5	2021012710391601	Vorgabe 4.3.7
Mitwirken bei der Bewältigung erheblichen Sicherheitsvorfälle (ITZBund)	§ 8b Absatz 4a	§§ 36 und 40 Absatz 5	2021110314022901	Vorgabe 4.3.7
Bearbeitungen von Selbsterklärungen (BSI)	§ 8f	§§ 33 und 34	2021012611593401	Vorgabe 4.3.3
Nationale Behörde für die Cybersicherheitszertifizierung (BSI)	§ 9a	§ 54	2021012612594401	formelle Änderung
Mitwirken bei der Prüfung zur Untersagung des Einsatzes kritischer Komponenten (BMI)	§ 9b	§ 41 Absatz 3	2021012613034601	formelle Änderung
Mitwirken bei der Prüfung der Garantieerklärung und Untersagung kritischer Komponenten (BND)	§ 9b Absatz 3 & 4	§ 41 Absatz 3 & 4	2021110409335901	formelle Änderung
Untersagung des Einsatzes kritischer Komponenten oder Erlass sonstiger Anordnungen (BMI)	§ 9b Absatz 4	§ 41 Absatz 4	2021012508360401	formelle Änderung
Mitwirken bei der Untersagung kritischer Komponenten (BMG)	§ 9b Absatz 4	§ 41 Absatz 4	2021012707270601	formelle Änderung
Mitwirken bei der Untersagung kritischer Komponenten (BMAS)	§ 9b Absatz 4	§ 41 Absatz 4	2021102714324301	formelle Änderung
Mitwirken bei der Untersagung kritischer Komponenten (AA)	§ 9b Absatz 4	§ 41 Absatz 4	2021110111334101	formelle Änderung
Vergabe des IT-Sicherheitskennzeichens durch das Bundesamt (BSI)	§ 9c	§ 55	2021012613071901	formelle Änderung
Anpassungen der IT-Sicherheit (GDZ)	§§ 4a, 4b, 8, 8b Absatz 4a	§ 5 Absatz 3	2021110111534201	Vorgabe 4.3.1
Aufgaben im Rahmen der Einschränkung von Betroffenenrechten (BSI)	§§ 6b bis 6f	§§ 23 bis 27	2019011110030202	Vorgabe 4.3.6
EnWG (Artikel 15)				
Bearbeitung der Nachweise von kritischen Unternehmen über die Erfüllung der von BSI festgelegten Anforderungen (BnetzA)	§ 11 Absatz 1e	§ 5c Absatz 4	2021110811522901	formelle Änderung
Festlegung von Sicherheitsanforderungen (BnetzA)	§ 11 Absatz 1g	§ 5c	2022063010393601	formelle Änderung

5. Weitere Kosten

Keine.

6. Weitere Gesetzesfolgen

Durch den Gesetzesentwurf wird die Versorgungssicherheit für Verbraucherinnen und Verbraucher erhöht. Die bestehenden Regelungen des BSI-Gesetzes zum Verbraucherschutz werden nicht berührt.

Die Regelungen des Gesetzentwurfs sind inhaltlich geschlechtsneutral aufgrund der vorrangig gegebenen unmittelbaren Betroffenheit der Zielgruppe des Regelungsvorhabens und damit ohne Gleichstellungsrelevanz. Die weitere Stärkung und Förderung der Cyber- und Informationssicherheit betrifft jedoch sowohl mittel- als auch unmittelbar Frauen und Männer. § 4 Absatz 3 Satz 1 des Bundesgleichstellungsgesetzes bestimmt, dass Rechts- und Verwaltungsvorschriften des Bundes die Gleichstellung von Frauen und Männern auch sprachlich zum Ausdruck bringen sollen. Dies wurde in der Entwicklung der Gesetzesformulierung unter Einbeziehung bereits gegebener Diktion berücksichtigt.

Die Regelungen entsprechen zudem den Anforderungen des „Gleichwertigkeits-Checks“. Der Gesetzentwurf dient der Förderung der Versorgung in den digitalen Infrastrukturen und der Erreichbarkeit von Dienstleistungen und Verwaltungsleistungen. Auch wird dem Schutz einer Daseinsvorsorge mit ihren unterschiedlichen Bereichen, die eine wesentliche Voraussetzung für gleichwertige Lebensverhältnisse der Menschen und den gesellschaftlichen Zusammenhalt Rechnung getragen. Auswirkungen auf die vorhandene Siedlungs- und Raumstruktur oder demographische Belange sind nicht zu erwarten.

VII. Exekutiver Fußabdruck

Der Inhalt des Gesetzentwurfs hat sich durch Vorträge von Interessenvertreterinnen und Interessenvertretern sowie von der Bundesregierung beauftragten Dritten nicht wesentlich geändert.

VIII. Befristung; Evaluierung

Das Gesetz ist nicht mit einer Befristung versehen.

Gemäß Artikel 40 der NIS-2-Richtlinie nimmt die Europäische Kommission eine eigene Evaluierung der Richtlinie vor. Demzufolge prüft die Europäische Kommission bis zum 17. Oktober 2027 – und danach alle 36 Monate – regelmäßig die Anwendung der NIS-2-Richtlinie und berichtet dem Europäischen Parlament und dem Rat.

Unter Berücksichtigung der Ergebnisse der Europäischen Kommission soll eine umfassende Evaluierung der Maßnahmen dieses Gesetzes spätestens nach fünf Jahren erfolgen. Dabei soll evaluiert werden, ob eine Erhöhung des gemeinsamen Cybersicherheitsniveaus in Deutschland erreicht wurde. Als Kriterium kann auf die ergriffenen Cybersicherheitsmaßnahmen der von diesem Gesetz erfassten Einrichtungen abgestellt werden. Informationen können aus der Berichterstattung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie aus freiwilligen Umfragen bei den betroffenen Einrichtungen gewonnen werden.

Nach spätestens drei Jahren soll eine umfassende Evaluierung von § 28 Absatz 6 des BSI-Gesetzes erfolgen. Dabei soll insbesondere evaluiert werden, ob durch die Ausnahme von KRITIS-Betreibern im Finanzsektor von der Meldepflicht nach § 32 wesentliche Informationen für ein umfassendes Lagebild gefehlt haben.

B. Besonderer Teil

Zu Artikel 1 (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen)

Die Änderung der Gesetzesüberschrift durch die Ergänzung „und über die Sicherheit in der Informationstechnik von Einrichtungen“ soll dem Umstand Rechnung tragen, dass es sich nicht um ein reines Errichtungsgesetz einer Bundesbehörde handelt.

Die Schaffung einer (amtlichen) Inhaltsübersicht erfolgt aufgrund des gestiegenen Umfangs des Gesetzes sowie Strukturierung des Gesetzes in Teile und Kapitel zur besseren Übersicht für den Rechtsanwender.

Zu Teil 1 (Allgemeine Vorschriften)

Zu § 1 (Bundesamt für Sicherheit in der Informationstechnik)

§ 1 führt den bisherigen § 1 fort.

Zu § 2 (Begriffsbestimmungen)

Die Begriffsbestimmungen werden zur Steigerung der Übersichtlichkeit in Nummern anstatt von einzelnen Absätzen gestaltet, welche alphabetisch sortiert werden. Dies war infolge der Einführung zahlreicher neuer Begriffsbestimmungen, bedingt durch die Vorgaben der NIS-2-Richlinie, erforderlich geworden. Eine thematische Sortierung scheidet aufgrund der großen Anzahl der Begriffe aus, eine Übersichtlichkeit für den Rechtsanwender könnte dann nicht mehr gewährleistet werden.

Zu Nummer 1

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 5 der NIS-2-Richtlinie. Die Legaldefinition eines Beinahevorfalls ist hier bewusst weit gefasst, da grundsätzlich vielfältige Vorfälle im Kontext der Cybersicherheit als Beinahevorfall gewertet werden können. Demnach kann beispielsweise eine professionell gestaltete Phishingmail, die nur aufgrund entsprechender besonders intensiver Sensibilisierung der Mitarbeiter oder aufgrund einer erhöhten Aufmerksamkeit der Belegschaft als solche erkannt wurde, durchaus als Beinahevorfall gewertet werden, wenn diese unter sonst üblichen Bedingungen nicht erkannt worden wäre. Nicht als Beinahevorfall anzusehen sind jedoch regelmäßige und alltägliche Störungen und Belästigungen wie Spam E-Mails oder offenkundig auch für ungeschultes Personal als Phishingmail erkennbare E-Mails.

Die Begriffsbestimmung enthält die Trias Verfügbarkeit, Integrität und Vertraulichkeit der bisherigen Begriffsbestimmung des § 2 Absatz 2 Satz 4 BSI-Gesetz (Sicherheit in der Informationstechnik). Der Begriff Authentizität stellt im deutschen Recht einen Unterfall der Integrität dar, daher erfolgt anders als z. B. in Artikel 6 Nummer 5 der NIS-2-Richtlinie keine ausdrückliche Nennung des Begriffs.

Zu Nummer 2

Die Begriffsbestimmung dient der Umsetzung von Artikel 28 Absatz 5 der NIS-2-Richtlinie und definiert den „berechtigten Zugangsnachfrager“ für die Zwecke des § 50.

Zu Nummer 3

Der Sektor Weltraum umfasst insbesondere Einrichtungen, deren Funktionsfähigkeit für die Erbringung verschiedener kritischen Dienstleistungen zwingend erforderlich sind. Dazu werden die Begriffe „Bodeninfrastruktur“ und „weltraumgestützte Dienste“ (Nummer 45) definiert. Bodeninfrastruktur umfasst dabei Einrichtungen wie etwa Satellitenkontrollzentren und Bodenstationen während weltraumgestützte Dienste zum Beispiel Globale Navigationssatellitensysteme (GNSS) oder hochgenaue Zeitservices umfassen. Von der Kontrolle in der Begriffsbestimmung „Bodeninfrastruktur“ umfasst sind insbesondere die Kommunikation, Beobachtung und Steuerung.

Zu Nummer 4

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 30 der NIS-2-Richtlinie.

Zu Nummer 5

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 32 der NIS-2-Richtlinie. Die Bereitstellung digitaler Inhalte und Dienste für Internetnutzer im Auftrag von Inhalte- und Diensteanbietern umfasst insbesondere das sogenannte Caching. Bei dem Wort „Zustellung“ ist eine tatsächliche und keine formelle Zustellung gemeint.

Zu Nummer 6

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 10 der NIS-2-Richtlinie.

Zu Nummer 7

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 9 fort.

Zu Nummer 8

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 20 der NIS-2-Richtlinie.

Zu Nummer 9

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 22 der NIS-2-Richtlinie.

Zu Nummer 10

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 11 der NIS-2-Richtlinie.

Zu Nummer 11

Die Begriffsbestimmung dient der Umsetzung von Artikel 23 Absatz 3 und Absatz 11 Unterabsatz 2 der NIS-2-Richtlinie. Bei den hier genannten finanziellen Verlusten sind Bagatellschäden regelmäßig ausgeschlossen.

Zu Nummer 12

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 41 der NIS-2-Richtlinie. Ein primäres Ziel im Sinne der Vorschrift dürfte ab einem Überschreiten von 50 Prozent der Gesamttätigkeit gegeben sein.

Zu Nummer 13

Die Begriffsbestimmung dient der Umsetzung von Artikel 20 der NIS-2-Richtlinie. Da die Pflichten und Befugnisse der Leitungen von Einrichtungen des Bundes nach § 29 abweichend in § 43 geregelt sind, werden diese hier explizit von der Definition ausgenommen.

Zu Nummer 14

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 13 der NIS-2-Richtlinie. Mit „IKT-Dienst“ ist in der Verordnung (EU) 2019/881 ein Dienst gemeint, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels informationstechnischer Systeme, Komponenten und Prozessen besteht.

Zu Nummer 15

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 12 der NIS-2-Richtlinie. Mit „IKT-Produkt“ ist in der Verordnung (EU) 2019/881 ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems gemeint. Der Begriff wird zur europaweiten Vereinheitlichung der Terminologie im Rahmen der Umsetzung der NIS-2-Richtlinie eingeführt und ersetzt den alten Begriff des IT-Produkts in § 2 Absatz 9a BSI-Gesetz a. F. Inhaltlich ergeben sich zwischen beiden Begriffen keine Unterschiede. Die hier referenzierte Definition beinhaltet sowohl Hardwareprodukte als auch Softwareprodukte.

Zu Nummer 16

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 14 der NIS-2-Richtlinie. Mit dem Begriff „IKT-Prozess“ meint die Verordnung (EU) 2019/881 jegliche Tätigkeiten, mit denen ein ITK-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll.

Zu Nummer 17

Der Begriff Informationssicherheit wurde auch bisher bereits im BSI-Gesetz verwendet, jedoch nicht gesetzlich definiert. Aus Klarstellungsgründen erfolgt daher nunmehr eine entsprechende Legaldefinition, die sich an den bereits etablierten Definitionen des BSI IT-Grundschutzes orientiert.

Zu Nummer 18

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 1 fort.

Zu Nummer 19

Die Begriffsbestimmung führt die Legaldefinition im bisherigen § 14a Satz 1 fort, der Begriff wird nunmehr in den §§ 29 und 64 verwendet. Zur Vervollständigung der bisherigen Legaldefinition wurde die Deutsche Gesetzliche Unfallversicherung e. V. ergänzt.

Zu Nummer 20

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 18 der NIS-2-Richtlinie.

Zu Nummer 21

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 3 fort. Es wurde eine Begriffskonsolidierung vorgenommen – statt „Bundesbehörden“ nun „Einrichtungen der Bundesverwaltung“. Der Begriff wird über den Anwendungsbereich von § 29 definiert. Die Erweiterung der Definition ist vor dem Hintergrund der Zeitenwende geboten und ist mit Rücksicht darauf erforderlich, dass angesichts der komplexen digitalen Infrastruktur auch Informationstechnik schutzbedürftig sein kann, die nicht unmittelbar von Bundesbehörden betrieben oder verwendet wird. Eine Kompromittierung der Systeme einer Einrichtung der Bundesverwaltung ist geeignet, ein Risiko für alle damit vernetzten Einrichtungen darzustellen, auch wenn die konkret betroffene IT nur mittelbar z. B. durch Handeln Einzelner gefährdet ist.

Zu Nummer 22

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 10 BSI-Gesetz mit Änderungen aufgrund der neuen Regelungssystematik fort. Die Ergebnisse der Evaluierung dieser Norm gemäß Artikel 6 Absatz 1 Nummer 1 des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme wurden berücksichtigt. Die Vorschrift wird in absehbarer Zeit geändert, vgl. Artikel 2.

Zu Nummer 23

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 13 fort.

Zu Nummer 24

Die Begriffsbestimmung wurde aus § 1 Absatz 1 Nummer 3 BSI-KritisV übernommen.

Zu Nummer 25

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 40 der NIS-2-Richtlinie.

Zu Nummer 26

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 39 der NIS-2-Richtlinie.

Zu Nummer 27

Die Begriffsbestimmung dient der Vereinfachung der zahlreichen Zitate der NIS-2-Richtlinie im BSI-Gesetz.

Zu Nummer 28

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 28 der NIS-2-Richtlinie.

Zu Nummer 29

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 29 der NIS-2-Richtlinie.

Zu Nummer 30

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 33 der NIS-2-Richtlinie.

Zu Nummer 31

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 8 fort.

Zu Nummer 32

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 8a fort.

Zu Nummer 33

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 26 der NIS-2-Richtlinie.

Zu Nummer 34

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 27 der NIS-2-Richtlinie.

Zu Nummer 35

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 31 der NIS-2-Richtlinie. Die Datenverarbeitung umfasst dabei insbesondere auch Transport und Speicherung.

Zu Nummer 36

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 5 fort.

Zu Nummer 37

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 4 fort. Es wird eine Begriffskonsolidierung/Folgeänderung vorgenommen – statt Bundesbehörden nun Einrichtungen der Bundesverwaltung. Durch die Anpassung erweitert sich die Reichweite des Begriffs – mit Blick auf den Schutzzweck der Informationssicherheit der Netze des Bundes bzw. möglicher weiterer Regierungsnetze bedeutet die Erweiterung die Klarstellung, dass nicht allein Bundesbehörden an diese Netze angeschlossen sein können.

Zu Nummer 38

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 6 fort und dient gleichzeitig der Umsetzung von Artikel 6 Nummer 15 der NIS-2-Richtlinie.

Zu Nummer 39

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 2 Satz 2 fort.

Zu Nummer 40

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 6 der NIS-2-Richtlinie.

Zu Nummer 41

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 9b fort.

Zu Nummer 42

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 21 der NIS-2-Richtlinie.

Zu Nummer 43

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 24 der NIS-2-Richtlinie.

Zu Nummer 44

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 25 der NIS-2-Richtlinie.

Zu Nummer 45

Auf die Begründung zu Nummer 3 wird verwiesen.

Zu Nummer 46

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 7 fort.

Zu Teil 2 (Das Bundesamt)

Zu Kapitel 1 (Aufgaben und Befugnisse)

Zu § 3 (Aufgaben des Bundesamtes)

Mit der Umsetzung der NIS-2-Richtlinie wird der Katalog der Aufgaben des Bundesamtes erweitert. Wie es die Erfüllung der Aufgaben priorisiert, hat das Bundesamt im Hinblick auf Artikel 31 Absatz 2 Satz 1 der NIS-2-Richtlinie nachpflichtgemäßem Ermessen zu entscheiden.

Zu Absatz 1

Absatz 1 führt den bisherigen § 3 Absatz 1 fort und wurde durch eine Streichung in Satz 1 bereinigt. Da es sich bei „Sicherheit in der Informationstechnik“ um einen in § 2 Nummer 39 definierten Begriff handelt, welche die bereinigten Worte bereits beinhaltet, handelte es sich hier um einen Zirkelschluss.

Zu Nummer 1

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 1 fort.

Zu Nummer 2

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 2 fort.

Zu Nummer 3

Die Aufgabe dient der Umsetzung von Artikel 14 und 15 der NIS-2-Richtlinie in Form einer Aufgabe des Bundesamtes.

Zu Nummer 4

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 3 fort.

Zu Nummer 5

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 4 fort.

Zu Nummer 6

Die Aufgabe dient der Umsetzung von Artikel 19 der NIS-2-Richtlinie in Form einer Aufgabe des Bundesamtes.

Zu Nummer 7

Hier erfolgt eine gesetzliche Verankerung von Aufgaben, die nach dem Umsetzungsplan Bund und der Netzstrategie 2030 bereits dem Bundesamt zugewiesen sind. Die Begrifflichkeit knüpft an § 2 Absatz 3 BDBOSG an und präzisiert die Rolle des Bundesamtes bei der dort geregelten Aufgabe der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS): Das Bundesamt ist federführend bei der Gestaltung der Informationssicherheit in den ressortübergreifenden Kommunikationsinfrastrukturen. Im Benehmen mit den jeweiligen Betreibern legt es hierzu Informationssicherheitsanforderungen fest, prüft Planungen und Implementierungen aus sicherheitstechnischer Sicht, auch bei Dienstleistern und angeschlossenen Organisationen, berät zu Lösungsalternativen und Realisierungsmaßnahmen, begleitet Abnahmen sicherheitstechnisch und steuert das Sicherheitsmanagement insbesondere der Betriebsphase. Festgestellte Mängel, Risiken oder Sicherheitsvorfälle werden an die zuständigen Stellen berichtet.

Zu Nummer 8

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 5 fort.

Zu Nummer 9

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 5a fort.

Zu Nummer 10

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 6 fort.

Zu Nummer 11

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 7 fort.

Zu Nummer 12

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 8 fort.

Zu Nummer 13

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 9 fort.

Zu Nummer 14

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 10 fort.

Zu Nummer 15

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 11 fort. Es erfolgt eine Begriffskonsolidierung/Erweiterung des Anwendungsbereichs auf Einrichtungen der Bundesverwaltung. Die Erweiterung erfolgt zum Zwecke eines einheitlich hohen Sicherheitsniveaus für alle Einrichtungen, die Informationstechnik des Bundes betreiben. Zudem wird die Bereitstellung von IT-Sicherheitsprodukten durch die Bereitstellung von IT-Sicherheitsdienstleistungen ergänzt. Der Bedarf an IT-Sicherheitsprodukten und -dienstleistungen, einschließlich der Notwendigkeit einer VS-Zulassung, wird durch das Bundesamt ermittelt.

Zu Nummer 16

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 12 fort. Hier wird „Stellen des Bundes“ beibehalten, da eine Erweiterung auf alle Einrichtungen der Bundesverwaltung zu erheblich größerem Erfüllungsaufwand führen würde, der nicht im Verhältnis zum Nutzen stünde.

Zu Nummer 17

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 12a fort. Hier erfolgt eine Begriffskonsolidierung zu „Einrichtungen der Bundesverwaltung“. Komplementär zur Verpflichtung weiterer Einrichtungen auf Vorgaben des Bundesamtes ist auch die Beratungs- und Unterstützungsaufgabe des Bundesamtes auf diese Einrichtungen zu erweitern. Ergänzt wird diese Aufgabe durch die Bereitstellung von praxisnahen Hilfsmitteln, um deutlich zu machen, dass eine Unterstützung des Bundesamtes sich nicht nur auf die Betreuung einzelner Einrichtungen beschränkt, sondern auch die Bereitstellung einrichtungsübergreifender Hilfsmittel umfasst, die der Unterstützung aller oder mehrerer Einrichtungen dienen. Bei der (Fort-)entwicklung dieser Hilfsmittel berücksichtigt das Bundesamt die Erfahrungen aus der Praxis.

Zu Nummer 18

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 13 fort. 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 19

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 13a fort.

Zu Nummer 20

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 14 fort. Es erfolgt eine Begriffskonsolidierung zu Einrichtungen der Bundesverwaltung, damit Umkehrschluss vermieden wird, dass die über Stellen des Bundes hinausgehenden Einrichtungen nicht erfasst seien. 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 Nummer 21

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 14a fort.

Zu Nummer 22

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 15 fort.

Zu Nummer 23

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 16 fort.

Zu Nummer 24

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 17 fort. Es wird eine Folgeänderung aufgrund Anpassung der Systematik vorgenommen: „Betreiber Kritischer Infrastrukturen“ nunmehr einheitlich „Betreiber kritischer Anlagen“, ferner gehen „Anbieter digitaler Dienste“ und „Unternehmen im besonderen öffentlichen Interesse“ in „besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“ auf.

Zu Nummer 25

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 18 fort. Im Übrigen erfolgt eine Anpassung des fehlerhaften Verweises auf den bisherigen § 5a anstatt den bisherigen § 5b , letzterer wird durch § 11 fortgeführt.

Zu Nummer 26

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 19 fort.

Zu Nummer 27

Die Aufgabe führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 20 fort.

Zu Nummer 28

Diese neue Aufgabe des Bundesamtes dient der Umsetzung von Artikel 10 Absatz 8 der NIS-2-Richtlinie. Bei dieser Aufgabe handelt es sich um eine konkrete gesetzliche Ausgestaltung zwischeneuropäischer Amtshilfe, die das Bundesamt im Rahmen seiner bestehenden Befugnisse ausüben kann.

Zu Nummer 29

Diese neue Aufgabe des Bundesamtes dient der Sicherstellung der notwendigen Abstimmung mit der BaFin. Diese wird vor dem Hintergrund der sektorspezifischen Verordnung (EU) 2022/2554 notwendig.

Zu Absatz 2

Absatz 2 führt den bisherigen § 3 Absatz 2 fort.

Zu Absatz 3

Absatz 3 führt den bisherigen § 3 Absatz 3 fort. Er enthält eine Folgeänderung aufgrund der neuen Bezeichnung „kritische Anlagen“.

Zu § 4 (Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes)

Zu Absatz 1

Absatz 1 führt den bisherigen § 4 Absatz 1 fort. Er enthält eine Begriffskonsolidierung zu „Einrichtungen der Bundesverwaltung“.

Zu Absatz 2

Absatz 2 führt den bisherigen § 4 Absatz 2 fort. In Nummer 1 wird der neue Begriff der „Schwachstelle“ verwendet. Ferner erfolgt eine Begriffskonsolidierung zu „Einrichtungen der Bundesverwaltung“ in Nummer 2. Zudem wird in Nummer 3 ergänzt, dass das Bundesamt den Einrichtungen der Bundesverwaltung zusätzlich Empfehlungen bereitstellen muss, welche sich konkret auf den Umgang mit den vom Bundesamt identifizierten Gefahren beziehen.

Zu Absatz 3

Absatz 3 führt den bisherigen § 4 Absatz 4 fort.

Zu § 5 (Allgemeine Meldestelle für die Sicherheit in der Informationstechnik)

Zu Absatz 1

§ 5 Absatz 1 führt den bisherigen § 4b Absatz 1 fort. Anpassungen erfolgen zur Umsetzung von Artikel 12 Absatz 1 Satz 1 der NIS-2-Richtlinie (entsprechend zu § 9a BSI-Gesetz aF.).

Zu Absatz 2

§ 5 Absatz 2 führt den bisherigen § 4b Absatz 2 fort. Ergänzung in Satz 1 erfolgt zur Umsetzung Artikel 30 Absatz 1 der NIS-2-Richtlinie.

Zu Absatz 3

§ 5 Absatz 3 führt den bisherigen § 4b Absatz 3 fort. Die neue Nummer 5 dient der Umsetzung von Artikel 30 Absatz 2 der NIS-2-Richtlinie.

Zu Absatz 4

§ 5 Absatz 4 führt den bisherigen § 4b Absatz 4 fort.

Zu Absatz 5

§ 5 Absatz 5 führt den bisherigen § 4b Absatz 5 fort.

Zu § 6 (Informationsaustausch)

Die neue Vorschrift dient der Umsetzung von Artikel 29 der NIS-2-Richtlinie. Das Bundesamt ermöglicht den Informationsaustausch zu Cyberbedrohungen (§ 2 Nummer 6), Beinahevorfällen (§ 2 Nummer 1), Schwachstellen (§ 2 Nummer 38), Techniken und Verfahren (techniques and procedures), Kompromittierungsindikatoren (indicators of compromise), gegnerische Taktiken (adversarial tactics), bedrohungsspezifische Informationen (threat-actor-specific information), Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten sowie zur Aufdeckung von Cyberangriffen. Dieser Informationsaustausch ermöglicht den teilnehmenden Einrichtungen einen verbesserten Zugang zu Lageinformationen sowie den bidirektionalen Austausch von Informationen und ermöglicht den Teilnehmern auch untereinander frühzeitig zu beobachteten Bedrohungen in Austausch zu treten und fördert damit die Cybersicherheit und Resilienz der Einrichtungen.

Durch die Erstellung von Teilnahmebedingungen kann das Bundesamt die organisatorischen Rahmenbedingungen des Informationsaustausches regeln um den geordneten und sicheren Betrieb des Informationsaustauschs bzw. des dafür vorgesehenen Online-Portals sicherzustellen.

In diesem Zusammenhang kann etwa der Umgang mit vertraulichen Informationen (z. B. durch Einhaltung des sog. „Traffic Light Protocols“ oder den Einsatz verschlüsselter E-Mail-Kommunikation) geregelt werden.

Zu § 7 (Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte)

Zu den Absätzen 1 bis 7

Die Vorschrift führt den bisherigen § 4a fort. In Absatz 4 erfolgt eine Anpassung im Rahmen der mit diesem Gesetz vorgesehenen Begriffskonsolidierung zu „Einrichtungen der Bundesverwaltung“ sowie die mit diesem Gesetz geschaffenen verantwortlichen Stellen für das Informationssicherheitsmanagements des Bundes, für deren effektive Aufgabenerfüllung auch eine entsprechende Ausweitung der Mitteilungspflichten des Bundesamtes erforderlich ist. Mit dem Betreiber ist die betroffene Einrichtung gemeint, welche die überprüfte Kommunikationstechnik des Bundes betreibt. Die Ergebnisse der Kontrollen werden der jeweiligen Einrichtungsleitung übermittelt. Zudem wird eine Sachverhaltsklärung ergänzt, um Missverständnissen und Fehlern vorzubeugen. Darüber hinaus steht es jeder geprüften Einrichtung frei, zum Prüfbericht des Bundesamtes eine eigene Stellungnahme gegenüber denjenigen Stellen abzugeben, die den Prüfbericht des Bundesamtes erhalten haben, also insbesondere gegenüber dem eigenen Informationssicherheitsbeauftragten des Ressorts und der eigenen Fach- und Rechtsaufsicht. In Absatz 5 wird die Befugnis des Bundesamtes zur Anweisung der Umsetzung der Verbesserungsvorschläge innerhalb einer angemessenen Frist ergänzt. Diese dient der Umsetzung von Artikel 32 Absatz 4 Buchstabe d und f der NIS-2-Richtlinie. Die Befugnis bildet ein wirksames Element für effektive Nachsteuerung, wenn Anlass dafür gegeben ist. Anlässe können etwa sein, wenn im Rahmen einer Kontrolle beispielsweise eine wiederholte erhebliche Unterschreitung der Anforderungen an das Informationssicherheitsmanagement deutlich wird.

Zur Beseitigung der identifizierten Mängel stellt das Bundesamt Beratungs- und Unterstützungsleistungen des Bundesamtes gemäß § 3 Absatz 1 Nummer 17 bereit. Im Übrigen erfolgen redaktionelle Änderungen.

Zu Absatz 8

Absatz 8 dient der Umsetzung von Artikel 35 der NIS-2-Richtlinie. Auf die Begründung zu § 61 Absatz 11 wird verwiesen.

Zu Absatz 9

Die neue Vorschrift dient dem Ziel, mehr Umsetzungsverantwortung zu schaffen. Bislang sind die Prüfungen nach dem bisherigen § 4a BSI-Gesetz ohne greifbare Konsequenz für die überprüften Stellen. Der Bericht erfolgt an den Haushaltsauschuss des Deutschen Bundestages, weil dadurch an diejenige Stelle berichtet wird, die über Mittel verfügt, eine Beseitigung von Missständen zu ermöglichen. Sie soll die Berichtspflicht des Bundesministerium des Innern und für Heimat an den Haushaltsausschuss des Deutschen Bundestages über die Ergebnisse der Analyse der IT-Sicherheit der Rechenzentren der Bundesverwaltung mittels Hochverfügbarkeits-Benchmark ersetzen (Beschluss des Haushaltsausschusses des Deutschen Bundestages vom 17. Juni 2015, Ausschussdrucksache 18(8)2134). Eine allgemeine Berichtspflicht gegenüber dem Ausschuss für Inneres und Heimat des Deutschen Bundestages besteht gemäß § 58 Absatz 3 ohnehin, sie schließt Berichterstattung über die Anwendung dieser Vorschrift ein.

Zu § 8 (Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes)

§ 8 führt den bisherigen § 5 fort.

Zu Absatz 1

Absatz 1 führt den bisherigen § 5 Absatz 1 fort. In Satz 3 erfolgt eine Begriffskonsolidierung zu „Einrichtungen der Bundesverwaltung“, diese Erweiterung des Anwendungsbereichs erfolgt zum Zweck des Schutzes der gesamten Kommunikationstechnik des Bundes.

Zu Absatz 2

Absatz 2 führt den bisherigen § 5 Absatz 2 fort.

Zu Absatz 3

Absatz 3 führt den bisherigen § 5 Absatz 2a fort.

Zu Absatz 4

Absatz 4 führt den bisherigen § 5 Absatz 3 fort.

Zu Absatz 5

Absatz 5 führt den bisherigen § 5 Absatz 4 fort.

Zu Absatz 6

Absatz 6 führt den bisherigen § 5 Absatz 5 fort. Sowohl Absatz 6 als auch Absatz 7 beziehen sich auf Daten im Sinne des Absatz 1, die dem Schutz des Fernmeldegeheimnisses und dem Schutz personenbezogener Daten unterfallen und bei denen eine Weiterverwendung nach Absatz 4 erforderlich ist. Da in Absatz 4 die Verwendung der Daten nur durch einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet werden darf, wird dies entsprechend auch in Absatz 6 ergänzt.

Zu Absatz 7

Absatz 7 führt den bisherigen § 5 Absatz 6 fort. Ergänzt wird die Möglichkeit, dass Bundesamt die nach Absatz 4 verwendeten personenbezogenen Daten an die Einrichtungen der Bundesverwaltung, für deren Schutz die Daten technisch erhoben wurden, übermitteln kann, soweit dies für die Verwendung nach Absatz 4 oder die Abwehr von sonstigen erheblichen Gefahren für die Informationssicherheit erforderlich ist. So wird gewährleistet, dass die Einrichtungen des Bundes alle relevanten Informationen zur Gewährleistung des Schutzes der Kommunikationstechnik des Bundes erhalten.

Zu Absatz 8

Absatz 8 führt den bisherigen § 5 Absatz 7 fort.

Zu Absatz 9

Absatz 9 führt den bisherigen § 5 Absatz 8 fort. Die Nennung des „Rat der IT-Beauftragten der Bundesregierung“ wird durch „Ressorts“ ersetzt, um die Gremienstruktur untergesetzlich regeln zu können.

Zu Absatz 10

Absatz 10 führt den bisherigen § 5 Absatz 9 fort.

Zu Absatz 11

Absatz 11 führt den bisherigen § 5 Absatz 10 fort.

Zu § 9 (Verarbeitung von Protokollierungsdaten der Kommunikationstechnik des Bundes)

§ 9 führt den bisherigen § 5a fort. Die geänderte Überschrift spiegelt die Begriffskonsolidierung und den inhaltlichen Bezug zu § 8 wider. Es wird eine Begriffskonsolidierung vorgenommen zu „Einrichtungen der Bundesverwaltung“. Die Erweiterung des Anwendungsbereichs erfolgt zum Zweck des Schutzes der gesamten Kommunikationstechnik des Bundes.

Zu § 10 (Anordnungen von Maßnahmen zur Abwendung oder Behebung von Sicherheitsvorfällen)

Die neue Vorschrift dient der Umsetzung von Artikel 32 Absatz 4 Buchstabe b sowie Absatz 5 der NIS-2-Richtlinie gegenüber Einrichtungen der Zentralregierung bei der Reaktion auf akute Sicherheitsvorfälle; im Interesse eines kohärenten Regelungsregimes und effektiven operativen Vorfallsmanagements werden die Befugnisse wie in § 29 angelegt auch auf die übrigen Einrichtungen der Bundesverwaltung erstreckt. Wenn das Bundesamt die Gefahr oder das Vorliegen eines Sicherheitsvorfalles feststellt, weist es die Einrichtungen der Bundesverwaltung auf die aus seiner Sicht notwendigen Maßnahmen zur Abwendung oder Behebung hin. Wenn die Einrichtungen diese Maßnahmen nicht innerhalb eines angemessenen Zeitraums umsetzen, obwohl diese nach Ansicht des Bundesamtes erforderlich sind, kann es die Einrichtungen zur Umsetzung anweisen. Dabei wird es die Einrichtungen in der Regel vorher anhören. Bei Gefahr im Verzug kann es die Anordnung auch erlassen, ohne den Einrichtungen zuvor Gelegenheit zur Stellungnahme zu geben. Bei der Erteilung von Anweisungen berücksichtigt das Bundesamt potentielle Auswirkungen auf Dritte, wie Kunden oder Dienstleister. Die Anweisung des Bundesamtes gegenüber Einrichtungen der Bundesverwaltung werden an die jeweilige Einrichtungsleitung adressiert. Mögliche Beispiele für Anweisungen des Bundesamtes können lageabhängig nach sachlicher und rechtlicher Einzelfallprüfung sein: Übergabe von Systemen oder Daten zur Analyse an das Bundesamt; erhöhte Protokollierung zur Anomaliedetektion; Verlängerung von Speicherfristen; Verhindern von Datenlöschung; Installation eines Netzwerksensors des Bundesamtes zur Detektion; Verpflichtung, Mitarbeiter, Dienstleister, Kunden und Partner über bestimmte Tatsachen zu informieren oder nicht zu informieren; Nichtnetztrennung zur Sicherstellung der Analyse von Angreiferverhalten; im Extremfall Netztrennung. Entsprechend der unterschiedlichen Rollen im Aufsichtsgefüge ist eine Berichterstattung gleichermaßen vorgesehen an Bundesamt als operativer Aufsichtsbehörde sowie des Informationssicherheitsbeauftragten des Ressorts als zuständiger Fachaufsicht.

Zu § 11 (Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen)

§ 11 führt den bisherigen § 5b fort.

Zu Absatz 1

Absatz 1 führt den bisherigen § 5b Absatz 1 fort. Es erfolgt eine Folgeänderungen aufgrund neuer Einrichtungskategorien sowie einer Anpassung in Umsetzung von Artikel 11 Absatz 1 Buchstabe d der NIS-2-Richtlinie. Ferner wird eine Begriffskonsolidierung vorgenommen zu „Einrichtungen der Bundesverwaltung“.

Zu Absatz 2

Absatz 2 führt den bisherigen § 5b Absatz 2 fort.

Zu Absatz 3

Absatz 3 führt den bisherigen § 5b Absatz 3 fort. Es erfolgte eine redaktionelle Änderung, da nach Artikel 4 Nummer 2 Datenschutz-Grundverordnung der Verarbeitungsbegriff das Erheben bereits miteinschließt.

Zu Absatz 4

Absatz 4 führt den bisherigen § 5b Absatz 4 fort. Der Begriff „Informationen“ umfasst jegliches auf die betroffene Einrichtung bezogenes Wissen, von dem das Bundesamt im Rahmen seiner Leistungen nach § 11 Kenntnis erlangt.

Zu Absatz 5

Absatz 5 führt den bisherigen § 5b Absatz 5 fort.

Zu Absatz 6

Absatz 6 führt den bisherigen § 5b Absatz 6 fort.

Zu Absatz 7

Absatz 7 führt den bisherigen § 5b Absatz 7 fort.

Zu Absatz 8

Absatz 8 führt den bisherigen § 5b Absatz 8 fort.

Zu § 12 (Bestandsdatenauskunft)

§ 12 führt den bisherigen § 5c fort. Die Begriffe werden an die neuen Kategoriebezeichnungen angepasst.

Zu § 13 (Warnungen)

§ 13 führt den bisherigen § 7 fort.

Zu Absatz 1

Absatz 1 führt den bisherigen § 7 Absatz 1 fort. Der neue Nummer 1 Buchstabe e dient der Umsetzung Artikel 32 Absatz 4 Buchstabe a und Artikel 33 Absatz 4 NIS-2-Richtlinie.

Zu Absatz 2

Absatz 2 führt den bisherigen § 7 Absatz 1a fort.

Zu Absatz 3

Absatz 3 führt den bisherigen § 7 Absatz 2 fort. Die Vorschrift wird um eine Regelung zur Archivierung von Warnungen ergänzt. Hintergrund ist der Beschluss des BverfG vom 21. März 2018 (– 1 BvF 1/13 –) zu § 40 LFGB. Eine gesetzliche Regelung zur zeitlichen Begrenzung der Informationsverbreitung fehlte im LFGB. Dies ist mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar, da mit Zeitablauf nach der Veröffentlichung der Grundrechtseingriff zulasten des Herstellers einerseits und der mit Warnung verfolgte Zweck andererseits außer Verhältnis geraten.

Art und Umfang etwaiger Ersatzansprüche richten sich nach den allgemeinen staatshaftungsrechtlichen Grundsätzen.

Zu § 14 (Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen)

§ 14 führt den bisherigen § 7a fort.

Zu Absatz 1

Absatz 1 führt den bisherigen § 7a Absatz 1 fort.

Zu Absatz 2

Absatz 2 führt den bisherigen § 7a Absatz 2 fort.

Zu Absatz 3

Absatz 3 führt den bisherigen § 7a Absatz 3 fort.

Zu Absatz 4

Absatz 4 führt den bisherigen § 7a Absatz 4 fort. Die vorgenommene Ergänzung ist erforderlich, um einen Austausch zu Dritten (wie z. B. auch zu anderen Aufsichtsbehörden) zu ermöglichen und zu vereinfachen, wenn es z. B. nur um Kategorien von Produkttypen und gefundenen Schwachstellen geht, die auch ohne konkreten Hersteller-/Produktbezug weitergegeben werden sollen. Da in diesem Fall die Eingriffsintensität gegenüber den Herstellern der untersuchten Produkte und Systeme mangels Bezugnahme als sehr gering anzusehen ist, würde eine vorab einzuholende Stellungnahme die Weitergabe kritischer Schwachstellen an Dritte (wie z. B. andere Aufsichtsbehörden) unnötig erschweren.

Zu Absatz 5

Absatz 5 führt den bisherigen § 7a Absatz 5 fort.

Zu § 15 (Detektion von Angriffsmethoden und von Sicherheitsrisiken für die Netz- und IT-Sicherheit)

§ 15 führt den bisherigen § 7b fort und dient zugleich der Umsetzung der NIS-2-Richtlinie. Bei den sog. Schwachstellenscans handelt es sich um eine Aufsichtsmaßnahme des BSI, mit der sichergestellt werden soll, dass die adressierten Einrichtungen der Bundesverwaltung sowie die besonders wichtigen und die wichtigen Einrichtungen keine informationstechnischen Systeme betreiben, denen eine bekannte Schwachstelle oder ein anderes bekanntes Sicherheitsrisiko anhaftet. Mit der Abfragebefugnis nach Absatz 1 korrespondiert deswegen als einziger Zweck der Datenverarbeitung eine Informationspflicht nach Absatz 2. § 15 ermächtigt indes nicht zur Entdeckung von besonders sensiblen, unbekannten Schwachstellen (auch: Zero-Day-Schwachstellen).

Zu Absatz 1

Absatz 1 führt den bisherigen § 7b Absatz 1 entsprechend der Begründung zum IT-SIG 2.0 fort. Die Änderungen dienen zuvörderst der Umsetzung von Artikel 11 Absatz 3 Buchstabe e, Artikel 32 Absatz 2 Buchstabe d und Artikel 33 Absatz 2 Buchstabe c der NIS-2-Richtlinie, die die Durchführung von Schwachstellenscans bei wichtigen und wesentlichen Einrichtungen als zwingende Aufgabe der CSIRTs und Aufsichtsmaßnahme ansehen. Als andere bereits bekannte Sicherheitsrisiken im Sinne des Satz 1 kommen beispielsweise fehlerhafte Konfigurationen in Betracht Die Detektion von Schwachstellen ist neben Portscans auch über weitere webseiten-/ domainbasierte Methoden möglich. Da sich die Art von Schwachstellenscans durch den technischen Fortschritt verändern kann, war eine entwicklungsoffene Formulierung zu wählen. Die Regelung ermöglicht richtliniengemäß auch Scans z. B. bei den von den IT-Dienstleistern für die Einrichtung betriebenen Systemen. Der gewählte Begriff der Abfrage bezeichnet eine entwicklungsoffene, nicht-intrusive Art einer informationstechnischen Abfrage an die öffentlich erreichbaren Schnittstellen, die im Rahmen der technischen Spezifikation der Schnittstelle grundsätzlich vorgesehen ist. Sie dient ausschließlich der Detektion von Systemeigenschaften und schließt eine Einflussnahme auf das System aus. Wenn Schwachstellen in der Spezifikation oder der Implementation einer Schnittstelle bekannt werden, dürfen die Abfragen an die öffentlich erreichbaren Schnittstellen in einer Weise erfolgen, mit der überprüft werden kann, ob die abgefragten Systeme diese Art von Schwachstellen aufweisen. Zudem war die Regelung an die neuen Einrichtungskategorien aus der NIS-2-Richtlinie anzupassen. Statt des Begriffs der Sicherheitslücke wird zur europaweiten Vereinheitlichung der Terminologie der der Schwachstelle im Sinne von Artikel 6 Nummer 15 der NIS-2-Richtlinie verwendet, ohne dass damit eine inhaltliche Änderung verbunden ist. Die Streichung von § 7b Absatz 2 ist eine Folgeänderung zur Anpassung der Tatbestandsvoraussetzungen nach Absatz 1, die im Gegenzug für die Absenkung der Eingriffsschwelle eine Begrenzung der Verwendungsmöglichkeiten detektierter, bekannter Schwachstellen vorsieht. Das Bundesamt kann so die informationstechnischen Systeme der genannten Einrichtungen auf das Vorhandensein solcher Schwachstellen untersuchen, die bisher nicht notwendig öffentlich, aber jedenfalls informierten Fachkreisen bekannt sind. Es darf damit einerseits die Norm nicht zur Ausforschung und Nutzung unbekannter neuer Schwachstellen (Zero-Day-Exploits) nutzen, andererseits darf es zur Information der Betroffenen mit dem Abgleich und der Untersuchung bekannter Schwachstellen bereits beginnen, ohne dass die Schwachstellen zuvor einer breiten Öffentlichkeit bekannt gemacht worden sein müssen.

Zu Absatz 2

Absatz 2 führt den bisherigen § 7b Absatz 3 fort. Eine Weitergabe der konkreten Informationen über die nach Absatz 1 detektierten Schwachstellen ist weder über § 8 Absatz 7 noch nach § 3 Absatz 1 Nummer 2 erlaubt. Absatz 2 gilt diesbezüglich als abschließende Regelung. Damit detektierte Schwachstellen schnellstmöglich geschlossen werden, ist die Informationspflicht des Bundesamtes bei betroffenen Einrichtungen der Bundesverwaltung auf die Informationssicherheitsbeauftragten der Einrichtung und des Ressorts zu erstrecken (Fachaufsicht).

Für das Lagebild darf das Bundesamt abstrahierte Informationen aus den Schwachstellenscans aufbereiten, in dieser Form weitergeben und veröffentlichen (z. B. zur Zahl und Art der betroffenen Einrichtungen oder der Art der Schwachstellen).

Zu Absatz 3

Absatz 3 führt den bisherigen § 7 b Absatz 3 Satz 4 fort.

Zu Absatz 4

Absatz 4 setzt den bisherigen § 7b Absatz 1 Satz 2 und 3 fort, entbindet das Bundesamt aber von der aufwendigen Pflege der sog. „Weißen Liste“, die auch IP-Adressen von informationstechnischen Systemen erfasste, die nicht gescannt wurden. Der damit verbundene Entfall einer Vorabkontrolle wird dadurch kompensiert, dass der BfDI durch die eingeführte Aufforderungsmöglichkeit nun auf Anforderungkontrollieren kann, dass die vom Bundesamt tatsächlich gescannten IT-Systeme auch einer Einrichtung der Bundesverwaltung, einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung zugeordnet sind.

Gegenüber § 7b Absatz 1 entfällt zudem die bisherige Beschränkung auf Internet-Protokolladressen. Stattdessen werden auch andere Systeme einbezogen, bei denen es sich neben Internet-Protokolladressen beispielsweise auch um zu scannende Domains handeln kann. Da es bei den Schwachstellenscans in Abhängigkeit von der etwaigen Schwachstelle zu nicht intendierten Eingriffen in das Grundrecht auf informationelle Selbstbestimmung aus Artikel 2 Absbsatz 1 in Verbindung mit Artikel 1 Absatz 1 GG sowie in das Telekommunikationsgeheimnis aus Artikel 10 Absatz 1 GG kommen kann, übt die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit im Rahmen ihrer oder seiner Unabhängigkeit eine Kontrollmöglichkeit für die Betroffenen aus.

Zu Absatz 5

Absatz 5 führt den bisherigen § 7b Absatz 4 fort.

Zu § 16 (Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von Telekommunikationsdiensten)

§ 16 führt den bisherigen § 7c fort.

Zu Absatz 1

Absatz 1 führt den bisherigen § 7c Absatz 1 fort. Da der Begriff „Diensteanbieter“ aufgrund der Umsetzung der NIS-2-Richtlinie nun im Gesetz auch mit anderer Bedeutung genutzt wird, war eine Anpassung der Legaldefinition erforderlich, die nur für die Zwecke dieser Vorschrift erfolgte. Das in der bisherigen Vorschrift enthaltene Wort „konkreter“ ist im Wege einer redaktionellen Klarstellung entfallen.

Zu Absatz 2

Absatz 2 führt den bisherigen § 7c Absatz 2 fort. In Nummer 1 erfolgt eine Folgeänderung aufgrund der neuen Kategoriebezeichnungen.

Zu Absatz 3

Absatz 3 führt den bisherigen § 7c Absatz 3 fort.

Zu Absatz 4

Absatz 4 führt den bisherigen § 7c Absatz 4 fort.

Zu § 17 (Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von digitalen Diensten)

§ 17 führt den bisherigen § 7d fort. Die in der bisherigen Vorschrift in Satz 1 enthaltenen Wörter „begründeten“ und „konkreter“ sind im Wege einer redaktionellen Klarstellung entfallen.

Zu § 18 (Anordnungen von Maßnahmen des Bundesamtes gegenüber Herstellern von IKT-Produkten)

§ 18 führt den bisherigen § 8b Absatz 6 fort. Einrichtungen des Bundes – insbesondere solche, die IT-Dienstleister des Bundes sind – können ebenfalls Hersteller sein, sofern sie IKT-Produkte erstellen.

Zu § 19 (Bereitstellung von IT-Sicherheitsprodukten)

§ 19 führt den § 8 Absatz 3 Satz 1-3 fort. Es erfolgt eine Begriffskonsolidierung zu „Einrichtungen der Bundesverwaltung“, um den Anwendungsbereich zum Schutz der gesamten Kommunikationstechnik des Bundes zu erweitern, wobei eine Konkretisierung der Rolle des Bundesamtes im Hinblick auf § 3 Absatz 1 Nummer 15 erfolgt. Zudem wird auf die Einhaltung der Bundeshaushaltsordnung hingewiesen.

Zu Kapitel 2 (Datenverarbeitung)

Zu § 20 (Verarbeitung personenbezogener Daten)

§ 20 führt den bisherigen § 3a fort.

Zu § 21 (Beschränkungen der Rechte der betroffenen Person)

§ 21 führt den bisherigen § 6 fort.

Zu § 22 (Informationspflicht bei Erhebung von personenbezogenen Daten)

§ 22 führt den bisherigen § 6a fort.

Zu § 23 (Auskunftsrecht der betroffenen Person)

§ 23 führt den bisherigen § 6b fort.

Zu § 24 (Recht auf Berichtigung)

§ 24 führt den bisherigen § 6c fort.

Zu § 25 (Recht auf Löschung)

§ 25 führt den bisherigen § 6d fort.

Zu § 26 (Recht auf Einschränkung der Verarbeitung)

§ 26 führt den bisherigen § 6e fort.

Zu § 27 (Widerspruchsrecht)

§ 27 führt den bisherigen § 6f fort.

Zu Teil 3 (Sicherheit in der Informationstechnik von Einrichtungen)

Zu Kapitel 1 (Anwendungsbereich)

Zu § 28 (Besonders wichtige Einrichtungen und wichtige Einrichtungen)

Der § 28 dient der Umsetzung von Artikel 3 NIS-2-Richtlinie.

Zu Absatz 1

Absatz 1 dient der Definition besonders wichtiger Einrichtungen. Durch die Einbeziehung von rechtlich unselbstständigen Organisationseinheiten einer Gebietskörperschaft wird sichergestellt, dass Eigenbetriebe und Landesbetriebe, die entsprechende Dienste gemäß der Einrichtungsdefinitionen erbringen, adäquat adressiert werden können, auch wenn diese keine juristische oder natürliche Person sind. Die in der Kommissionsempfehlung 2003/361 EG genannten Größenschwellen für Mitarbeiteranzahl und Jahresumsatz werden zur Verbesserung der Lesbarkeit in diesem Gesetz grundsätzlich ausdefiniert.

Soweit in diesem Absatz Einrichtungskategorien ohne eine explizite Angabe der Mitarbeiteranzahl, des Jahresumsatzes oder der Jahresbilanzsumme angegeben sind, gelten diese Definitionen jeweils unabhängig von der Unternehmensgröße.

Zu Nummer 1

Nummer 1 dient der Umsetzung von Artikel 3 Absatz 1 Buchstabe f der NIS-2-Richtlinie, wonach gemäß der CER-Richtlinie als kritische Einrichtung bzw. Betreiber kritischer Anlagen auch als besonderes wichtige Einrichtung im Sinne dieses Gesetzes gelten.

Zu Nummer 2

Nummer 2 dient der Umsetzung von Artikel 3 Absatz 1 Buchstabe b der NIS-2-Richtlinie.

Zu Nummer 3

Nummer 3 dient der Umsetzung von Artikel 3 Absatz 1 Buchstabe c der NIS-2-Richtlinie.

Zu Nummer 4

Nummer 4 dient der Umsetzung von Artikel 3 Absatz 1 Buchstabe a der NIS-2-Richtlinie.

Zu Absatz 2

Absatz 2 dient der Definition wichtiger Einrichtungen und der Umsetzung Artikel 3 Absatz 2 der NIS-2-Richtlinie. Die obenstehenden Hinweise in der Begründung zu Absatz 1 gelten entsprechend.

Zu Absatz 3

Bei der Bestimmung der maßgeblichen Mitarbeiterzahlen und des Umsatzes sind nur diejenigen Teile der Einrichtung einzubeziehen, die tatsächlich im Bereich der in den Anlagen 1 und 2 genannten Definitionen der Einrichtungskategorien tätig sind, Querschnittsaufgaben wie beispielsweise Personal, Buchhaltung etc. sind hierbei anteilig zu berücksichtigen. Hierdurch wird sichergestellt, dass Einrichtungen, die insgesamt die Größenschwelle für Mitarbeiteranzahl, Jahresumsatz oder Jahresbilanzsumme überschreiten, deren hauptsächliche Geschäftstätigkeit jedoch nicht einer Einrichtungskategorie gemäß Anlage 1 oder 2 dieses Gesetzes zuzuordnen ist, nicht in unverhältnismäßiger Weise erfasst werden.

Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme ist im Übrigen für Einrichtungen, die keine rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft sind, die Empfehlung 2003/361/EG mit Ausnahme von Artikel 3 Absatz 4 der Empfehlung anzuwenden. Danach beziehen sich die Daten grundsätzlich auf den letzten Rechnungsabschluss der Einrichtung und werden auf Jahresbasis berechnet, vgl. Artikel 4 Absatz 1 des Anhangs zur Empfehlung 2003/361/EG. Dies bedeutet, dass insbesondere saisonale Überschreitungen des Schwellenwerts bei der Mitarbeiteranzahl innerhalb eines Jahres nicht ausschlaggebend sind. Des Weiteren verliert eine Einrichtung den Status eines mittleren Unternehmens, eines kleinen Unternehmens oder eines Kleinstunternehmens erst dann, wenn es in zwei aufeinanderfolgenden Geschäftsjahren zu einer Über- oder Unterschreitung der Größenschwelle kommt, vgl. Artikel 4 Absatz 2 des Anhangs zur Empfehlung 2003/361/EG. Damit führen gegebenenfalls einzelne wirtschaftlich besonders erfolgreiche oder nichterfolgreiche Geschäftsjahre nicht für sich allein zu einer Erfassung als besonders wichtige oder wichtige Einrichtung.

Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung 2003/361/EG sind nicht hinzuzurechnen, wenn das betreffende Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse ausübt, die das Unternehmen für die Erbringung seiner Dienste nutzt. Ein bestimmender Einfluss auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse liegt insbesondere vor, wenn grundsätzliche Entscheidungen zur Beschaffung, zum Betrieb und zur Konfiguration der informationstechnischen Systeme, Komponenten und Prozesse durch die Einrichtung eigenverantwortlich getroffen werden können. Dies ist beispielsweise regelmäßig zu verneinen, wenn die informationstechnischen Systeme, Komponenten und Prozesse vollständig durch eine Konzernmutter betrieben werden, und die Einrichtung selbst demnach tatsächlich keinerlei Einfluss auf die vorgenannten Eigenschaften nehmen kann. Ein bestimmender Einfluss liegt jedoch regelmäßig vor, wenn die informationstechnischen Systeme, Komponenten und Prozesse im Auftrag durch einen Dienstleister betrieben werden, da hier durch vertragliche Regelungen bestimmender Einfluss auf die vorgenannten Eigenschaften ausgeübt werden kann. Hierdurch

wird sichergestellt, dass Partnerunternehmen oder Tochterunternehmen, die für sich alleine gesehen die vorgesehenen Schwellen für Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nicht erreichen oder überschreiten, nur in denjenigen Fällen als besonders wichtige Einrichtung gelten können, wenn sie keinen bestimmenden Einfluss auf ihre eigenen informationstechnischen Systeme, Komponenten und Prozesse ausüben, weil diese beispielsweise von einem Partnerunternehmen betrieben werden.

Zu Absatz 4

Absatz 4 regelt Ausnahmen für bestimmte Einrichtungskategorien, die spezialgesetzlich reguliert werden. Absatz 4 führt den bisherigen § 8d Absatz 2 fort. Die Ergebnisse der Evaluierung dieser Norm gemäß Artikel 6 Absatz 1 Nummer 1 des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme wurden berücksichtigt. Für Betreiber von öffentlichen Telekommunikationsnetzen, Energieversorgungsnetzen und Energieanlagen werden die derzeit bestehenden spezialgesetzlichen Regelungen mit einer entsprechenden Zuständigkeit der Bundesnetzagentur und hierfür durch die Bundesnetzagentur erstellter IT-Sicherheitskataloge fortgeführt.

Absatz 4 Satz 1 nimmt dazu zunächst all jene Einrichtungen von den aufgeführten Regelungen des BSIG aus, die eine von TKG bzw. EnWG erfasste Anlage betreiben. Ziel ist insoweit die Vermeidung einer Doppelregulierung durch BnetzA und BSI: die NIS-2-Richtlinie wird in diesem Fall vollständig durch die Regelungen des TKG beziehungsweise des EnWG umgesetzt.

Gleichzeitig soll die Anwendbarkeit des BSIG, und damit die Zuständigkeit des BSI, für weitere Sektoren durch diese Ausnahmeregelung nicht eingeschränkt werden. Denkbar wäre etwa der beispielhafte Fall, in dem eine Einrichtung gleichzeitig ein Wasserwerk nach Anlage 1 Nummer 5.1.1 wie auch ein Stromkraftwerk nach Anlage 1 Nummer 1.1.4 umfasst, deren IT-Systeme zwar grundsätzlich getrennt voneinander betrieben werden, die jedoch beide Schnittstellen zu einem gemeinsamen Monitoringssystem aufweisen.

In diesem Fall regelt Absatz 4 Sätze 2 und 3 eine entsprechende Rückausnahme, die sich auf die IT des Wasserwerks einschließlich dessen Schnittstelle zum Monitoringsystem erstrecken würde. Von der Rückausnahme erfasst ist also sämtliche IT, die für die Tätigkeiten in diesen Sektoren – bzw. den Betrieb der entsprechenden kritischen Anlage – erheblich ist. Diese unterliegt also wieder den Anforderungen des BSIG, womit insbesondere auch entsprechende Branchenspezifische Sicherheitsstandards nach § 30 Absatz 8 und 9 zur Anwendung kommen können.

Von der Rückausnahme nicht erfasst wird demgegenüber Unternehmens-IT, die für die Tätigkeit in diesen weiteren Sektoren nicht erheblich ist (z. B. „Office-IT“ ohne Schnittstellen zu kritischen Anlagen).

Theoretisch kann demzufolge auch der Fall eintreten, dass Teile der IT sowohl der Aufsicht der BnetzA als auch des BSI unterfallen, nämlich dann, wenn diese für die Tätigkeit in verschiedenen Sektoren erheblich ist.

Im Ergebnis unterliegen damit alle IT-Systeme einer Einrichtung einer Regulierung (so auch die Vorgabe aus Artikel 21 Absatz 1 der NIS-2-Richtlinie).

Zu Absatz 5

Zu Nummer 1

In Umsetzung von Erwägungsgrund 28 der NIS-2-Richtlinie gilt die Verordnung (EU) 2022/2554 (DORA-VO) für Finanzunternehmen als lex specialis. Somit sind diese Unternehmen von den hier genannten Verpflichtungen ausgenommen.

Zu Nummer 2

Nummer 2 führt den bisherigen § 8d Absatz 2 Nummer 3 sowie Absatz 3 Nummer 3 fort.

Zu Absatz 6

Absatz 6 regelt, dass für Betreiber kritischer Anlagen, deren Dienstleistungsempfänger bereits der Verordnung (EU) 2022/2554 (DORA) unterliegen und nach dieser meldepflichtig sind, eine weitere Meldepflicht nach § 32 dieses Gesetzes entfällt. Freiwillige Meldungen nach § 5 sind weiterhin möglich.

Zu Absatz 7

Absatz 7 dient der Definition von Betreibern kritischer Anlagen.

Zu Absatz 8

Mit dieser Öffnungsklausel können durch die Länder in eigener Verantwortung solche Einrichtungen aus dem Anwendungsbereich dieses Gesetzes ausgenommen werden, die zu 100 Prozent im Eigentum von Ländern und Kommunen stehen und zu dem Zweck errichtet wurden, im öffentlichen Auftrag Leistungen für Verwaltungen zu erbringen. Schließlich ist notwendig, dass das die Einrichtung Gegenstand einer mit den Regelungen dieses Gesetzes vergleichbaren NIS-2-Umsetzung durch das betreffende Land ist und das Land mit der Bezugnahme auf die Öffnungsklausel auch – bewusst – Gebrauch von dieser Öffnungsklausel macht. Letzteres soll gewährleisten, dass keine Einrichtungen regulierungsfrei gestellt werden, die durch die Bundesrepublik Deutschland in Umsetzung der NIS-2-Richtlinie zu regulieren sind.

Der Anwendungsbereich des § 28 erfasst lediglich wirtschaftlich tätige Einrichtungen. Insoweit können auch nur solche rechtlich unselbstständige Organisationseinheiten von Gebietskörperschaften und juristische Personen mittels dieser Öffnungsklausel ausgenommen werden, die wirtschaftlich tätig sind.

Zu § 29 (Einrichtungen der Bundesverwaltung)

§ 29 bezieht Einrichtungen der Bundesverwaltung als Kategorie in das Regelungsregime ein, das mit Umsetzung der NIS-2-Richtlinie etabliert wird. In vielen Einrichtungen der Bundesverwaltung besteht ein Defizit bei der Umsetzung von Maßnahmen zum Eigenschutz im Bereich der Informationssicherheit. Die bisherigen Steuerungsinstrumente auf überwiegend untergesetzlicher Basis (etwa Umsetzungsplan Bund) haben sich als nicht ausreichend effektiv erwiesen, um eine flächendeckende wirksame Steigerung des Sicherheitsniveaus zu erreichen. Vor dem Hintergrund der durch aktuelle geopolitische Entwicklungen („Zeitenwende“) abermals verschärften Bedrohungslage hat sich das Risiko für staatliche Einrichtungen zudem weiter erhöht, durch Gefährdungen aus dem Cyberraum in ihrer Handlungsfähigkeit eingeschränkt zu werden. Die Umsetzung der NIS-2-Richtlinie wird deshalb durch diese und weitere Bestimmungen begleitet mit weiteren Regelungen für die Bundesverwaltung, die über die reine Umsetzung der NIS-2-Richtlinie hinausgehen. Um auf Bundesebene auch vor dem Hintergrund von Verflechtung und Konsolidierung der IT insgesamt ein gemeinsames, kohärentes und handhabbares Regime zu erreichen, werden in nationaler Verantwortung Anforderungen formuliert, die inhaltlich an denjenigen für besonders wichtige Einrichtungen orientiert sind.

Zu Absatz 1

Absatz 1 bestimmt die Kategorie der Einrichtungen der Bundesverwaltung im Sinne dieses Gesetzes. Vor dem Hintergrund des Schutzzwecks der Informationssicherheit des Bundes und zum Zwecke der Begriffskonsolidierung ist die Definition grundsätzlich orientiert am Anwendungsbereich des bisherigen § 8 Absatz 1 sowie dem Geltungsbereich des Umsetzungsplans Bund, mit dem der Begriff der Einrichtungen der Bundesverwaltung bereits etabliert worden ist. Die Verwaltung des Bundestags sowie das Sekretariat des Bundesrats sind als Bundesbehörden von Nummer 1 mit umfasst. Nicht umfasst sind die Versorgungsanstalt der deutschen Bühnen, die Versorgungsanstalt der deutschen Kulturorchester und die Versorgungsanstalt der bevollmächtigten Bezirksschornsteinfeger, die von einer Landesbehörde verwaltet werden. Mit Nummer 3 wird das bisherige Anordnungserfordernis („Opt-In“) beibehalten. Grundsätzlich sollte eine Anordnung weiterer unmittelbarer Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihrer Vereinigung erfolgen, wenn die betroffene Einrichtung öffentlich-rechtliche Verwaltungsaufgaben wahrnimmt und sich durch eine Nicht-Anordnung der Einrichtung erkennbare nachteilige Auswirkungen für die Informationssicherheit des Bundes ergeben könnten. Erkennbare nachteilige Auswirkungen für die Informationssicherheit des Bundes können insbesondere dann entstehen, wenn die Einrichtung ein potentielles Verbundrisiko für andere Einrichtungen des Bundes darstellt; bspw. Falls die Einrichtung an die Netze des Bundes angebunden ist oder Leistungen der IT-Konsolidierung des Bundes nutzt. Um die potentiellen nachteiligen Auswirkungen angemessen einschätzen zu können, erfolgt die Anordnung durch das Bundesamt im Einvernehmen mit dem jeweils zuständigen Ressort. Zusätzlich werden die öffentlich-rechtlich organisierten IT-Dienstleister der Bundesverwaltung explizit in den Anwendungsbereich mit einbezogen, d.h. der Verbund der IT-Dienstleister des Bundes (VITD) mit Ausnahme der privatrechtlich organisierten BWI GmbH und der als KRITIS regulierten Bundesagentur für Arbeit und Deutsche Rentenversicherung als Institutionen der Sozialen Sicherung.

Zu Absatz 2

Absatz 2 dient als Generalklausel zur grundsätzlichen Erweiterung des Anwendungsbereichs 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 2 erfüllt wird und nur für das Bundeskanzleramt und die Bundesministerien, ohne den jeweiligen nachgeordneten Geschäftsbereich gilt. Für alle übrigen Einrichtungen der Bundesverwaltung gilt § 44 Absatz 1, welcher den bisherigen § 8 Absatz 1 fortführt. Folgende Regelungen für besonders wichtige oder wichtige Einrichtungen finden keine Anwendung: §§ 38, 40 Absatz 3, § 61 und 6565, da stattdessen folgende abweichende Regelungen Anwendung finden: §§ 4, 7, 10, 43 Absatz 1, 2, 4 und 5.

Zu Absatz 3

Absatz 3 dient der Festlegung der in der NIS-2-Richtlinie angelegten Ausnahme für den Bereich der Verteidigung und den Bereich der nationalen Sicherheit. Die NIS-2-Richtlinie gilt zudem laut ihrem Erwägungsgrund 8 nicht für diplomatische und konsularische Vertretungen der Mitgliedstaaten in Drittländern. Um den Besonderheiten des Auswärtigen Dienstes Rechnung zu tragen, wird das Auswärtige Amt deshalb in seinem Geschäftsbereich eigene Maßnahmen ergreifen, um die Ziele der Richtlinie umzusetzen.

Zu Kapitel 2 (Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten)

Zu § 30 (Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen)

§ 30 dient der Umsetzung von Artikel 21 der NIS-2-Richtlinie. Für Einrichtungen der Bundesverwaltung wird § 30 durch § 44 umgesetzt.

Zu Absatz 1

Absatz 1 dient der Umsetzung von Artikel 21 Absatz 1 und 4 NIS-2-Richtlinie. Während das BSIG im Bereich von Cybersicherheitsmaßnahmen bislang für Betreiber Kritischer Infrastrukturen auf diejenigen informationstechnischen Systeme, Komponenten und Prozesse abstellte, die für die Funktionsfähigkeit der Kritischen Infrastruktur maßgeblich sind, sind in Folge der Umsetzung der NIS-2-Richtlinie zukünftig sämtliche informationstechnischen Systeme, Komponenten und Prozesse zu berücksichtigen, die von der jeweiligen Einrichtung für die Erbringung ihrer Dienste genutzt werden. Der Begriff „Erbringung ihrer Dienste“ ist hierbei weit gefasst und insbesondere nicht mit der Erbringung (kritischer) Versorgungsdienstleistungen zu verwechseln. Vielmehr sind die hier gemeinten Dienste sämtliche Aktivitäten der Einrichtung, für die IT-Systeme eingesetzt werden, dies beinhaltet beispielsweise auch Büro-IT oder andere IT-Systeme, die durch die Einrichtung betrieben werden.

Risiken sind das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird. Absatz 1 stellt klar, dass hierbei durch die Einrichtung nur geeignete, verhältnismäßige und wirksame Maßnahmen zu ergreifen sind. Im Bezug auf die Verhältnismäßigkeit sind insbesondere die Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Dies dient der Umsetzung von Artikel 21 Absatz 1 Unterabsatz 2 NIS-2-Richtlinie. Damit keine unverhältnismäßige finanzielle und administrative Belastung für besonders wichtige und wichtige Einrichtungen entstehen, sollen die genannten Risikomanagementmaßnahmen in einem angemessenen Verhältnis zu den Risiken stehen, denen das betroffene Netz- und Informationssystem ausgesetzt wird. Hierbei werden u. a. auch den Kosten der Umsetzung sowie der Größe der Einrichtung Rechnung getragen. In die Bewertung der Angemessenheit und Verhältnismäßigkeit kann ebenfalls einfließen, ob es sich um eine wichtige Einrichtungen, eine besonders wichtige im Vergleich zu wesentlichen Einrichtung oder einen Betreiber einer kri-

tischen Anlage handelt, da in diesen Einrichtungskategorien von einem unterschiedlichen Grad der Risikoexposition ausgegangen werden kann grundsätzlich einer unterschiedlichen Risikoexposition ausgesetzt sind. „Risiko“ wird als Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird. Bei der Bewertung der Angemessenheit und Verhältnismäßigkeit der jeweiligen Maßnahmen kann überdies berücksichtigt werden, ob hierdurch Dienste geschützt werden, die in einem zwingenden betrieblichen Zusammenhang zu den Waren oder Dienstleistungen stehen, die zu einer Zuordnung zu einer der in Anlage 1 oder 2 bestimmten Einrichtungsarten geführt haben.

Vergleichbar zur Rechenschaftspflicht nach Artikel 5 Absatz 2 der Verordnung (EU) 2016/679 (Datenschutzgrundverordnung) sind Einrichtungen verpflichtet, die Umsetzung und Einhaltung von Maßnahmen angemessen zu dokumentieren. Durch diese Pflicht wird sichergestellt, dass Einrichtungen nach Anforderungen von Nachweisen des Bundesamtes gemäß § 61 Absatz 3 dem Bundesamt entsprechende Nachweisdokumente vorlegen können. Entsprechende Dokumentationen können beispielsweise sein: interne Richtlinien, Handlungsanweisungen, Checklisten, Mitarbeiterschulungen, Vereinbarungen, Merkblätter o. Ä., aber auch Auditberichte, Zertifizierungen oder Prüfungen.

Zu Absatz 2

Absatz 2 dient der Umsetzung von Artikel 21 Absatz 2 der NIS-2-Richtlinie. Die hier genannten Vorgaben insbesondere im Bereich der Sicherheit der Lieferkette können auch die Durchführung von External Attack Surface (EAS) Scans beinhalten. Mit der Vorgabe in Nummer 2 ist der Fachbegriff „incident response“ gemeint.

Unter dem Begriff „Cyberhygiene“ im Sinne der NIS-2-Richtlinie werden verschiedene grundlegenden Verfahren und Herangehensweisen umschrieben, welche allgemein zu einer Verbesserung des Cybersicherheitsniveaus einer Einrichtung führen können. Dies beinhaltet beispielsweise ein Patchmanagement, Regelungen für sichere Passwörter, die Einschränkung von Zugriffskonten auf Administratorenebene, Netzwerksegmentierungen, sowie Backup- und Sicherungskonzepte für Daten. Ebenfalls gehören hierzu allgemeine Informations- und Schulungsmaßnahmen, um das allgemeine Bewusstsein der Mitarbeiter für die Risiken im Zusammenhang mit IKT-Produkten zu schärfen.

Unter Maßnahmen zur Sicherheit der Lieferkette sind beispielsweise vertragliche Vereinbarungen mit Zulieferern und Dienstleistern zu Risikomanagementmaßnahmen, Bewältigung von Cybersicherheitsvorfällen, Patchmanagement, sowie der Berücksichtigung von Empfehlungen des Bundesamt in Bezug auf deren Produkten und Dienstleistungen zu nennen. Ebenfalls kann dies beinhalten, Zulieferer und Dienstleister zur Beachtung von grundsätzlichen Prinzipien wie Security by Design oder Security by Default anzuhalten. Hierbei Bei der Erwägung geeigneter Maßnahmen nach Absatz 4 Nummer 4 sind durch die Einrichtung die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse zu berücksichtigen. Einrichtungen müssen bei der Erwägung geeigneter Maßnahmen nach Satz 1 die Ergebnisse der gemäß Artikel 22 Absatz 1 der NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen kritischer Lieferketten berücksichtigen.

Zu Absatz 3

Absatz 3 dient der Umsetzung von Artikel 21 Absatz 5 Unterabsatz 1 der NIS-2-Richtlinie.

Zu Absatz 4

Absatz 4 dient der Umsetzung von Artikel 21 Absatz 5 Unterabsatz 2 der NIS-2-Richtlinie. Soweit die Europäische Kommission einen Durchführungsrechtsakt gemäß Artikel 24 Absatz 2 der NIS-2-Richtlinie erlässt, gehen die darin enthaltenen Vorgaben an den Einsatz zertifizierter IKT-Produkte, IKT-Dienste und IKT-Prozesse denen des Satzes 1 vor.

Zu Absatz 5

Zur angemessenen Berücksichtigung der Bedrohungslage muss das Bundesamt die Möglichkeit haben, über die ggf. von der Europäischen Kommission erlassenen Maßnahmen hinaus, die Umsetzung angemessener Maßnahmen zu fordern.

Zu Absatz 6

Absatz 6 dient der Umsetzung von Artikel 24 der NIS-2-Richtlinie. Gemäß Artikel 24 Absatz 2 der NIS-2-Richtlinie ist die EU Kommission ebenfalls befugt, delegierte Rechtsakte nach Artikel 290 AEUV zu erlassen, die ebenfalls den verpflichtenden Einsatz nach europäischen Schemata zertifizierter Produkte, Dienste oder Prozesse vorschreiben kann. Diese delegierten Rechtsakte haben entsprechend Vorrang gegenüber einer nach Absatz 6 dieser Regelung erlassen Rechtsverordnung des Bundesministeriums des Innern und für Heimat.

Vor Erlass einer solchen Rechtsverordnung ist durch das Bundesministerium des Innern und für Heimat und die weiteren beteiligten Ressorts sicherzustellen, dass entsprechende Zertifizierungsschemata vorhanden sind und nach diesen zertifizierten Produkten, Dienste oder Prozesse ausreichend am Markt verfügbar sind, um nachgelagerte Probleme durch Lieferengpässe oder -schwierigkeiten zu vermeiden.

Zu Absatz 7

Absatz 7 geht über die reine 1:1-Umsetzung der NIS-2-Richtlinie hinaus. Da die Umsetzung des Artikel 29 der NIS-2-Richtlinie über die zentrale Austauschplattform des Bundeamtes (BISP) umgesetzt wird, soll durch diesen Absatz 7 der bidirektionale Austausch sichergestellt werden.

Zu Absatz 8

Die Möglichkeit für KRITIS-Betreiber, für die Erfüllung der gesetzlichen Anforderungen branchenspezifische Sicherheitsstandards (B3S) vorzuschlagen, die anschließend vom Bundesamt im Einvernehmen Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie der zuständigen Aufsichtsbehörde des Bundes auf ihre Eignung geprüft werden, hat sich in der Umsetzung der NIS-1 Richtlinie aus Sicht der Bundesregierung grundsätzlich sehr bewährt. Da auch aus der Wirtschaft im Zuge der Evaluierung der KRITIS-bezogenen Bestandteile des IT-Sicherheitsgesetzes 2.0 einstimmig eine Einführung eines vergleichbaren Verfahrens angeregt wurde, wird in Absatz 9 eine vergleichbare Regelung für besonders wichtige Einrichtungen eingeführt. Bei der Erarbeitung von branchenspezifischen Sicherheitsstandards durch Betreiber kritischer Anlagen und ihre Branchenverbände zur Erfüllung der Nachweispflichten nach § 39 Absatz 1 kann es sinnvoll sein, die Maßnahmen auf diejenigen informationstechnischen Systeme, Komponenten und Prozesse zu beschränken, die für die Funktionsfähigkeit der kritischen Anlagen maßgeblich sind. Ein solcher branchenspezifischer Sicherheitsstandard ist dann jedoch nur für den Nachweis der Anforderungen nach § 39 Absatz 1 durch Betreiber kritischer Anlagen geeignet. Sofern das Bundesamt gemäß § 61 Absatz 3 Nachweise von besonders wichtigen Einrichtungen verlangt, die gleichzeitig Betreiber kritischer Anlagen sind, sind durch die Einrichtung entsprechend für diejenigen informationstechnischen Systeme, Komponenten und Prozesse, welche die Einrichtung für die Erbringung ihrer Dienste nutzt, die jedoch nicht vom branchenspezifischen Sicherheitsstandard abgedeckt sind, weitere Nachweisunterlagen zu erbringen.

In den Fällen, in denen im Sektor Gesundheitswesen keine zuständige Aufsichtsbehörde des Bundes besteht, ist bei der Feststellung der branchenspezifischen Sicherheitsstandards das Benehmen mit dem Bundesministerium für Gesundheit herzustellen. Dadurch soll eine rechtliche Harmonisierung mit den Anforderungen des Fünften Buches Sozialgesetzbuch sichergestellt werden.

Zu Absatz 9

Absatz 9 führt den bisherigen § 8a Absatz 2 fort.

Zu § 31 (Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen)

§ 31 definiert zusätzliche Anforderungen für Betreiber kritischer Anlagen.

Zu Absatz 1

Absatz 1 sieht vor, dass bei den nach § 30 umzusetzenden Maßnahmen durch Betreiber kritischer Anlagen in Bezug auf versorgungsrelevante informationstechnische Systeme, Komponenten und Prozesse erhöhte Anforderungen bestehen im Vergleich zu den Anforderungen an besonders wichtige Einrichtungen für sonstige, nicht versorgungsrelevante Bereiche. Betreiber kritischer Anlagen haben innerhalb ihrer Einrichtung für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, gegenüber wichtigen und besonders wichtigen Einrichtungen ein nochmals

erhöhtes Sicherheitsniveau zu gewährleisten. Hinsichtlich der besonders schweren gesellschaftlichen und wirtschaftlichen Auswirkungen einer Beeinträchtigung ist die Versorgungserheblichkeit der kritischen Anlagen für die Bevölkerung besonderes Indiz für die wirtschaftliche Angemessenheit der Vornahme von Sicherungsmaßnahmen. Daher gelten Maßnahmen, welche die Resilienz der Anlage erhöhen, um auch in Bezug auf gängige realistische Bedrohungsszenarien entsprechend der aktuellen Lageberichte und Bewertungen des Bundesamtes die Versorgungssicherheit der Bevölkerung auf einem möglichst hohen Niveau sicherzustellen, grundsätzlich gegenüber dem erforderlichen Aufwand als angemessen.

Der Absatz trifft mit dem Bezug auf Absatz 2 keine Aussage zur technischen Angemessenheit im Sinne der Eignung einer Maßnahme für die Minimierung eines Risikos, sondern konkretisiert, dass bei kritischen Anlagen eine grundsätzliche Abwägung zugunsten der Vornahme einer Maßnahme gegenüber dagegenstehenden Wirtschaftlichkeitserwägungen zu treffen ist. Dabei fällt in Abgrenzung zu wichtigen und besonders wichtigen Einrichtungen die Abwägung noch stärker zugunsten der Sicherheit der Funktionsfähigkeit der Anlage aus. Die Abwägung bezieht sich auf Maßnahmen für die zur Funktionsfähigkeit erforderlichen informationstechnischen Systeme, Komponenten und Prozesse in der Anlage und somit nicht auf die gesamte Einrichtung.

Zu Absatz 2

Absatz 2 verpflichtet Betreiber kritischer Anlagen, Systeme zur Angriffserkennung einzusetzen.

Zu § 32 (Meldepflichten)

Zu Absatz 1

Absatz 1 dient der Umsetzung von Artikel 23 Absatz 4 Satz 1 der NIS-2-Richtlinie. Mit „Kenntniserlangung“ ist gemeint, dass eine Mitarbeiterin oder ein Mitarbeiter der Einrichtung innerhalb seiner Arbeitszeit Kenntnis über einen erheblichen Sicherheitsvorfall erlangt. Das Bundesamt ermöglicht im Rahmen seiner Möglichkeiten eine Kommunikation auf Englisch.

Betrifft ein meldepflichtiger Sicherheitsvorfall mehrere Einrichtungen innerhalb einer Konzerngruppe, und sind für diese Einrichtungen innerhalb der Konzerngruppe eine oder mehrere einheitliche, ggf. auch branchenübergreifende Kontaktstellen benannt, so kann bei Abgabe einer Vorfallsmeldung nach Absatz 1 auch unmittelbar im Meldeformular angegeben werden, welche weiteren Einrichtungen innerhalb der Konzerngruppe vom Vorfall betroffen sind. Hierdurch können Mehrfachmeldungen innerhalb einer Konzerngruppe zu ein- und demselben Vorfall mit dem Ziel der Bürokratieminimierung vermieden werden. Innerhalb der Konzerngruppe ist jedoch in diesem Fall sicherzustellen, dass die innerhalb der Konzerngruppe benannten Kontaktstellen auch zu anlagen- oder einrichtungsspezifischen Rückfragen des Bundesamtes beispielsweise zu Auswirkungen des Sicherheitsvorfalls, Auskunft erteilen oder einen Ansprechpartner benennen können.

Die auf Grund dieser Vorschrift einzurichtende Meldestelle kann perspektivisch erweitert werden, um auch weitere Meldepflichten, etwa nach der Verordnung EU 2022/2554, abzubilden.

Zu Absatz 2

Absatz 2 dient der Umsetzung von Artikel 23 Absatz 4 Satz 1 Buchstabe e der NIS-2-Richtlinie.

Zu Absatz 3

Absatz 3 regelt, dass KRITIS-Betreiber bei der Erfüllung der Meldepflicht für Sicherheitsvorfälle auch weiterhin weitergehende Angaben in Bezug auf die betroffenen Anlagen, die betroffene kritische Dienstleistung sowie den Auswirkungen des Sicherheitsvorfalls auf diese Dienstleistung zu übermitteln haben.

Zu Absatz 4

Um ein effizientes und bürokratiearmes Meldeverfahren sicherzustellen, legt das Bundesamt Einzelheiten des Meldeverfahrens nach Anhörung der betroffenen Betreiber und Wirtschaftsverbände fest. Soweit die Europäische Kommission einen Durchführungsrechtsakt gemäß Artikel 23 Absatz 11 Unterabsatz 1 der NIS-2-Richtlinie erlässt, in dem die Art der Angaben, das Format oder das Verfahren der Meldungen festgelegt ist, sind diese Vorgaben einzuhalten.

Zu Absatz 6

Absatz 6 enthält einen Verweis auf die Rückmeldungen des Bundesamtes gegenüber meldenden Einrichtungen nach § 36 Absatz 1. Ein Rechtsanspruch der meldenden Einrichtung auf eine Unterstützungsleistung des Bundesamtes ist damit nicht verbunden. Das Bundesamt entwickelt seine Unterstützungs- und Informationsangebote für die meldenden Einrichtungen und die Gesamtwirtschaft im Rahmen seiner Möglichkeiten und in Erfüllung seiner bestehenden gesetzlichen Aufgaben fortlaufend adressatengerecht weiter.

Zu § 33 (Registrierungspflicht)

§ 33 dient der Umsetzung von Artikel 3 Absatz 3 der NIS-2-Richtlinie. In § 43 Absatz 4 wird ergänzend geregelt, dass die Registrierung bei Einrichtungen der Bundesverwaltung der Einrichtungsleitung obliegt.

Die Benennung der für die Tätigkeit, aufgrund derer die Registrierung erfolgt, zuständigen Aufsichtsbehörden des Bundes ist erforderlich, damit das Bundesamt den Beteiligungs- und Informationserfordernissen im Bezug auf diese Behörden nachkommen kann.

Zu Absatz 1

Absatz 1 dient der Umsetzung von Artikel 3 Absatz 4 Unterabsatz 2 Satz 1 der NIS-2-Richtlinie. Gemäß § 29 trifft die Registrierungspflicht entsprechend auch Einrichtungen der Bundesverwaltung im gleichen Umfang. Dies wird in § 43 Absatz 4 Satz 1 klargestellt.

Für Konzernstrukturen kann unter Effizienzgesichtspunkten die Benennung einer oder mehrere einheitlicher Kontaktstellen innerhalb des Konzerns für mehrere Unternehmensteile sinnvoll sein. Dies ist grundsätzlich möglich, sofern sichergestellt ist, dass für alle registrierungspflichten Einrichtungen bzw. Anlagen die in Absatz 1 genannten Informationen vorliegen, und die benannte übergeordnete Kontaktstelle innerhalb des Konzerns auch auf anlagen- oder einrichtungsspezifische Rückfragen des Bundesamt Auskunft geben kann.

Zu Nummer 1

Nummer 1 dient der Umsetzung von Artikel 3 Absatz 4 Unterabsatz 1 Buchstabe a der NIS-2-Richtlinie. Die Vorgabe wird um die Handelsregisternummer erweitert, da die Firma allein nicht eindeutig ist.

Zu Nummer 2

Nummer 2 dient der Umsetzung von Artikel 3 Absatz 4 Unterabsatz 1 Buchstabe b der NIS-2-Richtlinie.

Zu Nummer 3

Nummer 3 dient der Umsetzung von Artikel 3 Absatz 4 Unterabsatz 1 Buchstabe c der NIS-2-Richtlinie.

Zu Nummer 4

Nummer 4 dient der Umsetzung von Artikel 3 Absatz 4 Unterabsatz 1 Buchstabe d der NIS-2-Richtlinie.

Zu Nummer 5

Die Vorschrift dient der Erleichterung der Zusammenarbeit mit den im Einzelfall zuständigen Aufsichtsbehörden.

Zu Absatz 2

Absatz 3 regelt für Betreiber kritischer Anlagen zusätzlich zu übermittelnden Angaben bei der Registrierung. Absatz 3 führt den bisherigen § 8b Absatz 3 Satz 1 und 3 fort. Es wird ergänzt, dass Betreiber kritischer Anlagen auch die Versorgungskennzahlen ihrer kritischen Anlage übermitteln müssen.

Zu Absatz 3

Absatz 3 regelt, dass eine Registrierung von Einrichtungen und Diensteanbietern auch durch das Bundesamt selbst vorgenommen werden kann, wenn eine Einrichtung oder ein Anbieter ihre oder seine Pflicht zur Registrierung nicht erfüllt. Absatz 3 führt den bisherigen § 8b Absatz 3 Satz 2 fort und erweitert diesen auf die hier genannten Einrichtungsarten.

Zu Absatz 4

Absatz 4 führt den bisherigen § 8b Absatz 3a fort. Die hier genannten Geheimschutzinteressen oder überwiegenden Sicherheitsinteressen beziehen sich auf entsprechende Interessen der Bundesrepublik Deutschland. Betriebs- und Geschäftsgeheimnisse beteiligter Unternehmen allein begründen hiernach keine rechtmäßige Ablehnung einer Vorlage der Informationen.

Zu Absatz 5

Absatz 5 dient der Umsetzung von Artikel 3 Absatz 4 Unterabsatz 2 Satz 2 der NIS-2-Richtlinie.

Zu Absatz 6

Um einheitliche Registrierungsprozesse zu ermöglichen und somit den Verwaltungsaufwand für das Bundesamt sowie den Erfüllungsaufwand für die Wirtschaft effizient zu gestalten, ist vorgesehen, dass das Bundesamt einheitliche Vorgaben zum Registrierungsverfahren festlegt.

Zu § 34 (Besondere Registrierungspflicht für bestimmte Einrichtungsarten)

§ 34 dient der Umsetzung von Artikel 27 Absatz 2 bis 5 der NIS-2-Richtlinie.

Zu Absatz 4

Absatz 4 sieht vor, dass das Bundesamt für die Registrierung etwa die Verwendung eines Online-Formulars oder Vordrucks vorsehen kann, um die einheitliche Datenerfassung zu erleichtern.

Zu § 35 (Unterrichtungspflichten)

Zu Absatz 1

Absatz 1 dient der Umsetzung von Artikel 23 Absatz 1 Satz 2 der NIS-2-Richtlinie.

Wenn die Erbringung von Diensten durch besonders wichtige und wichtige Einrichtungen in Folge von aufgetretenen erheblichen Sicherheitsvorfällen beeinträchtigt wird, kann dies regelmäßig auch zu weiteren Einschränkungen, darunter auch mittelbare Einschränkungen, bei den Empfängern dieser Dienste führen. Dies kann beispielsweise der Fall sein, wenn diese Dienste bei den Empfängern zur Erbringung weiterer oder anderer Dienste für Dritte genutzt werden. Solche Supply-Chain-Angriffe sind regelmäßig schwer abzuwehren, da die Schadensauswirkungen mit zeitlicher Verzögerung, an anderen Orten sowie bei vom ursprünglichen Sicherheitsvorfall nicht unmittelbar betroffenen Unternehmen auftreten können. Beispiele für solche Supply-Chain-Angriffe, die bei unbeteiligten dritten Unternehmen zu weiteren Schadensauswirkungen führten, sind beispielsweise die presseöffentlich bekannten Vorfälle bei Solarwinds (2020), Kaseya (2021) oder ViaSat (2022). Um in Bezug auf solche Angriffe die Resilienz in der Wirtschaft insgesamt zu erhöhen, kann es im Einzelfall erforderlich sein, dass das Bundesamt entsprechende von einem Sicherheitsvorfall betroffene Einrichtungen anweist, die Empfänger ihrer Dienste über den Sicherheitsvorfall zu unterrichten, damit diese wiederum die erforderlichen Maßnahmen umsetzen können, um weitere Schadensauswirkungen auf ihre eigenen Dienste möglichst zu vermeiden. Das Bundesamt setzt die zuständige Aufsichtsbehörde des Bundes über eine Anordnung nach dieser Vorschrift in Kenntnis.

Zu Absatz 2

Absatz 2 dient der Umsetzung von Artikel 23 Absatz 2 der NIS-2-Richtlinie. Nicht in allen Sektoren können die Empfänger von Diensten selbst Maßnahmen gegen Cyberbedrohungen ergreifen. Gerade bei der Versorgung mit Elektrizität oder Waren sind die Empfänger nicht selbst der Cyberbedrohung ausgesetzt, sondern erst deren Folgen. In den Sektoren, in denen die Dienste selbst mit Informationssystemen der Empfänger der Dienste interagieren, ist eine Information der Empfänger oftmals sinnvoll. Die Einrichtungen haben sie daher über die Bedrohung selbst und über mögliche Maßnahmen zu unterrichten, die die Empfänger selbst zu ihrem Schutz ergreifen können.

Zu § 36 (Rückmeldungen des Bundesamtes gegenüber meldenden Einrichtungen)

Zu Absatz 1

Absatz 1 dient der Umsetzung von Artikel 23 Absatz 5 der NIS-2-Richtlinie. Wird bei dem erheblichen Sicherheitsvorfall ein strafbarer Hintergrund vermutet, gibt das Bundesamt ferner Orientierungshilfen für die Meldung

des Sicherheitsvorfalls an die Strafverfolgungsbehörden. Das Bundesamt wird als Orientierungshilfen für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden auf seiner Internetseite bereitstellen und auf diese gegebenenfalls verweisen.

Zu Absatz 2

Absatz 2 dient der Umsetzung von Artikel 23 Absatz 7 der NIS-2-Richtlinie. Nur das Bundesamt verfügt als zentrale Stelle nach der NIS-2-Richtlinie über die Informationen und das Lagebild, um entsprechende bundesweite Informationen auszugeben.

Zu § 37 (Ausnahmebescheid)

§ 37 dient der Umsetzung von Artikel 2 Absatz 8 der NIS-2-Richtlinie. Damit wird von der Möglichkeit der Schaffung einer Ausnahme Gebrauch gemacht. Der Grund einer teilweisen oder vollständigen Ausnahme von den in Artikel 21, 23 und 27 der NIS-2-Richtlinie – umgesetzt in den §§ 30 ff. – genannten Pflichten ist die Wahrung des nationalen Sicherheitsinteresses. So ist es in den Erwägungsgründen 9 und 10 der NIS-2-Richtlinie angelegt, dass es zur Wahrung wesentlicher Interessen der nationalen Sicherheit, dem Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit der Mitgliedstaaten erforderlich sein muss, Einrichtungen von obigen Pflichten auszunehmen, wenn derartige Auskünfte bzw. eine Preisgabe dem nationalen Sicherheitsinteresse zuwiderliefe. Als relevante Bereiche führt Artikel 2 Absatz 8 der NIS-2-Richtlinie die Bereiche der nationalen Sicherheit, öffentlichen Sicherheit, der Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten an. Um dem Sinne einer Ausnahmeregelung, die nicht zu weit greift, gerecht zu werden, ist ein Ausgleich zwischen einem „hohen gemeinsamen Cybersicherheitsniveau“ (siehe Erwägungsgrund 138, 142 der NIS-2-Richtlinie; ausdrückliches Ziel der NIS-2-Richtlinie) und dem Mitgliedstaatsinteresse der Wahrung nationaler Sicherheitsinteressen zu erbringen.

Bei dem hiesigen Ausnahmebescheid ist von einem nichtbegünstigenden Verwaltungsakt auszugehen. Gemäß § 48 Absatz 1 Satz 2 VwVfG bestimmt die Legaldefinition die Begünstigung wie folgt: Ein Verwaltungsakt ist begünstigend, wenn er ein Recht oder einen rechtlich erheblichen Vorteil begründet oder bestätigt. Ein Recht könnte in der Art begründet sein, als dass die der Befreiung unterliegende Einrichtung entweder ganz oder teilweise den Pflichten der §§ 30 ff. nicht nachkommen muss. Andererseits entfallen diese Pflichten nicht einfach. Eine Begünstigung ist nach dem objektiven Regelungsgehalt des Verwaltungsakts unter Berücksichtigung des Zwecks der ihm zugrunde liegenden Norm zu beurteilen, nämlich derart, dass eine Befreiung von obigen Pflichten nicht der Einrichtung, die den Ausnahmebescheid erhält, sondern dem nationalen Sicherheitsinteresse zugutekommen. Der Ausnahmebescheid soll gerade kein Recht verleihen, sondern nur die Pflichten des Adressaten des Ausnahmebescheids anderweitig ausgestalten, zumal gleichwertige Maßnahmen, die denen der Befreiung gleichkommen, (siehe §§ 30 ff.) getroffen werden müssen.

Für Einrichtungen der Bundesverwaltung ist eine zusätzliche Möglichkeit zur Schaffung von Ausnahmen von den Regelungen nach Teil 3 ergänzend in § 46 Absatz 5 geregelt.

Zu Absatz 1

Zunächst wird obig genanntem Ziel durch ein begrenztes Vorschlagsrecht, durch Bundeskanzleramt, Bundesministerium für Verteidigung, Bundesministerium des Innern und für Heimat, Bundesministerium der Justiz und der Ministerien für Inneres und Justiz der Länder entsprochen. Dabei ist ein Antragsrecht der betreffenden Einrichtung bewusst nicht vorgesehen. Weiterhin einschränkend wirken die umfassten Bereiche der Einrichtungen. Hierbei wird insbesondere auf die auch in der NIS-2-Richtlinie explizit genannten, rechtlich anerkannten Kategorien, der öffentlichen Sicherheit und Ordnung verwiesen. Als Begrenzung der Ausnahmeregelung einzubeziehender Erwägungsgrund sollte auf die Wesentlichkeit der Interessen der nationalen Sicherheit abzustellen sein.

Nicht zuletzt muss andererseits jedoch bei Ausnehmen von den genannten Pflichten das hohe gemeinsame Cybersicherheitsniveau durch Umsetzung gleichwertiger Maßnahmen (siehe Erwägungsgründe 13 und 137 der NIS-2-Richtlinie) gewährleistet werden. Hierbei wird auf den Erwägungsgrund 137 der NIS-2-Richtlinie verwiesen, die vorsieht, dass ein hohes Maß an Verantwortung für die Risikomanagementmaßnahmen und die Berichtspflichten im Bereich der Cybersicherheit sicherzustellen ist. Dem soll dadurch Rechnung getragen werden, dass Absatz 1 bestimmt, dass bei einer Ausnahme die Einrichtung gleichwertige Vorgaben zu erfüllen hat. Die Kontrolle über die Einhaltung obläge dem vorschlagenden Ressort.

Zu Absatz 2

Absatz 2 dient der Umsetzung von Artikel 2 Absatz 8 Satz 1 und 2 der NIS-2-Richtlinie. Absatz 2 Satz 1 setzt die Möglichkeit der Schaffung einer Ausnahme, wie von der Richtlinie vorgesehen, um. Dabei bestimmt Absatz 2 einen einfachen Ausnahmebescheid, die Befreiung von Risikomanagementmaßnahmen und Meldepflichten. Satz 2 verweist hierbei, wie obig bereits angemerkt, auf die Schaffung gleichwertiger Standards zur Wahrung der Informationssicherheit.

Zu Absatz 3

Absatz 3 dient der Umsetzung von Artikel 2 Absatz 8 Satz 3 der NIS-2-Richtlinie.

Mit Absatz 3 wurde die Möglichkeit einer vollständigen Befreiung von sowohl Risikomanagementmaßnahme und Meldepflichten als auch Registrierungspflichten im Rahmen eines sogenannten erweiterten Ausnahmebescheids geschaffen. Betroffene Einrichtungen müssen hierfür ausschließlich in den obig genannten Bereichen tätig sein oder Dienste erbringen. Satz 2 stellt die Wahrung von gleichwertigen Maßnahmen sicher.

Zu Absatz 4

Absatz 4 dient der Umsetzung von Artikel 2 Absatz 9 der NIS-2-Richtlinie.

Zu Absatz 5

Absatz 5 sieht eine Regelung des Widerrufs einer rechtmäßigen Befreiung vor. Für den Widerruf einer rechtmäßigen Befreiung sollte von § 49 VwVfG abgewichen werden, um der spezifischen Interessenlage der Vorschrift Genüge zu tun. Absatz 5 Satz 1 regelt den Fall des späteren Wegfalls der Voraussetzungen zur Erteilung eines Ausnahmebescheids. Satz 2 sieht hiervon eine Rückausnahme vor, wenn die Voraussetzungen nur vorübergehend entfallen.

Zu § 38 (Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen)

§ 38 dient der Umsetzung von Artikel 20 der NIS-2-Richtlinie.

Zu Absatz 1

Absatz 1 dient der Umsetzung von Artikel 20 Absatz 1 der NIS-2-Richtlinie und der dort vorgesehenen Pflichten der organschaftlichen Geschäftsleitungen. Nach dieser Verpflichtung haben die Geschäftsleitungen die konkret zu ergreifenden Maßnahmen zunächst als für geeignet zu billigen und deren Umsetzung kontinuierlich zu überwachen. Auch bei Einschaltung von Hilfspersonen bleibt das Leitungsorgan letztverantwortlich. Für Einrichtungen der Bundesverwaltung ist die Verantwortlichkeit der Leitungen in § 43 Absatz 1 geregelt.

Zu Absatz 2

Absatz 2 dient der Umsetzung von Artikel 20 Absatz 1 am Ende der NIS-2-Richtlinie. Die Binnenhaftung des Geschäftsleitungsorgans bei Verletzung von Pflichten nach dem BSI-Gesetz ergibt sich grundsätzlich aus den allgemeinen Grundsätzen (bspw. § 93 AktG). Für solche Rechtsformen, für die nach den anwendbaren gesellschaftsrechtlichen Bestimmungen keine solche Binnenhaftung besteht, sieht die Vorschrift einen Auffangtatbestand vor. Bei Amtsträgern gehen beamtenrechtliche Vorschriften vor, eine Ausweitung der bestehenden Haftung von Amtsträgern erfolgt mithin vor dem Hintergrund von Artikel 20 Absatz 1 Unterabsatz 2 der NIS-2-Richtlinie auch insoweit nicht. Für Einrichtungen der Bundesverwaltung ist die Verantwortlichkeit der Leitungen in § 43 Absatz 1 geregelt.

Zu Absatz 3

Absatz 3 dient der Umsetzung von Artikel 20 Absatz 2 der NIS-2-Richtlinie im Hinblick auf Geschäftsleitungen. Wichtige und besonders wichtige Einrichtungen werden aufgefordert, derartige Schulungen für alle Beschäftigten anzubieten. Als „regelmäßig“ im Sinne dieser Vorschrift gelten Schulungen, die mindestens alle drei Jahre angeboten werden. Für Einrichtungen der Bundesverwaltung gilt abweichend § 43 Absatz 2.

Zu § 39 (Nachweispflichten für Betreiber kritischer Anlagen)

§ 39 führt den bisherigen § 8a fort. Die Ergebnisse der Evaluierung dieser Norm gemäß Artikel 6 Absatz 1 Nummer 1 des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme wurden berücksichtigt.

Bei der Bestimmung des Zeitpunkts für die erstmalige Nachweiserbringung nach diesem Gesetz berücksichtigt das Bundesamt eine letztmalige Nachweiserbringung nach der alten Rechtslage insoweit, dass die Nachweiserbringung kontinuierlich etwa alle drei Jahre erfolgt.

Zu Absatz 1

Absatz 1 führt den bisherigen § 8a Absatz 3 fort.

Für Betreiber im Luftverkehrssektor bestehen mit der Verordnung (EG) 300/2008 in Verbindung mit dem Anhang der DVO (EU) 2015/1998 sowie der Verordnung (EU) 2018/1139 umfangreiche Sicherheitsvorgaben. Entsprechende Nachweise nach den vorgenannten Verordnungen können durch das Bundesamt für die Erfüllung von Nachweispflichten nach dieser Vorschrift berücksichtigt werden.

Zu Absatz 2

Absatz 2 führt den bisherigen § 8a Absatz 5 fort.

Zu Absatz 3

Um die Prüfung der durch die Betreiber kritischer Anlagen vorgelegten Nachweise durch das Bundesamt zeitlich zu entzerren, wird hier festgelegt, dass nicht sämtliche Nachweise am selben Datum beim Bundesamt vorgelegt werden müssen, sondern dass das Bundesamt jedem Betreiber einen eigenen Nachweistermin nennt. Hierbei ist durch das Bundesamt sicherzustellen, dass alle Betreiber mindestens drei Jahre zur Erbringung eines jeden Nachweises Zeit haben. Für Betreiber kritischer Anlagen, die vor Inkrafttreten dieses Gesetzes als Betreiber Kritischer Infrastrukturen nach § 8a BSIG in den Fassungen des ersten IT-Sicherheitsgesetzes und des IT-Sicherheitsgesetzes 2.0 zum Nachweis verpflichtet waren, ist hierbei der Zeitpunkt des letzten Nachweises nach der ehemaligen Rechtslage als Ausgangspunkt zu wählen.

Zu § 40 (Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen)

§ 40 führt den bisherigen § 8b fort. Die Ergebnisse der Evaluierung dieser Norm gemäß Artikel 6 Absatz 1 Nummer 1 des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme wurden berücksichtigt.

Die geänderte Vorschrift dient der Umsetzung des Artikels 8 Absatz 3 bis 5 der NIS-2-Richtlinie. Um die Resilienz der Wirtschaft europaweit zu steigern, sieht die NIS-2-Richtlinie u. a. einen koordinierten Austausch von Informationen zwischen den Mitgliedstaaten untereinander und mit Stellen der Union vor. Dieser erfolgt für Deutschland zentral über das Bundesamt in seiner Eigenschaft als zentrale Stelle nach der NIS-2-Richtlinie.

Zu Absatz 1

Absatz 1 führt den bisherigen § 8b Absatz 1 fort. Die geänderte Vorschrift dient der Umsetzung des Artikels 8 Absatz 3 bis 5 der NIS-2-Richtlinie.

Zu Absatz 2

Absatz 2 dient der Umsetzung des Artikels 8 Absatz 4 und 5 der NIS-2-Richtlinie.

Zu Absatz 3

Absatz 3 führt den bisherigen § 8b Absatz 2 fort.

Zu Nummer 1

Nummer 1 führt den bisherigen § 8b Absatz 2 Nummer 1 fort.

Zu Nummer 2

Nummer 2 führt den bisherigen § 8b Absatz 2 Nummer 2 fort.

Zu Nummer 3

Nummer 3 führt den bisherigen § 8b Absatz 2 Nummer 3 fort.

Zu Nummer 4

Zu Buchstabe a

Buchstabe a führt den bisherigen § 8b Absatz 2 Nummer 4 Buchstabe a fort. Die Vorschrift wird an die neuen Kategorien angepasst.

Zu Buchstabe b

Buchstabe b führt den bisherigen § 8b Absatz 2 Nummer 4 Buchstabe d fort.

Zu Buchstabe c

Für die Erfüllung seiner Aufgaben ist das Auswärtige Amt auf Informationen zu Sicherheitsvorfällen, die von wichtigen und besonders wichtigen Einrichtungen sowie Einrichtungen der Bundesverwaltung gemeldet wurden, und die von außenpolitischer Bedeutung sind, angewiesen. Das Bundesamt ist verpflichtet, das Auswärtige Amt über Sicherheitsvorfälle mit internationalem Bezug unverzüglich zu unterrichten.

Zu Buchstabe d

Buchstabe d führt den bisherigen § 8b Absatz 2 Nummer 4, Buchstaben b und c fort. Der Anwendungsbereich erstreckt sich dabei auf wichtige und besonders wichtige Einrichtungen. Für die Übermittlung von Registrierungsdaten und Vorfallsmeldungen („Rot-Meldungen“) können dabei die bereits im Kontext der bisherigen Regelungen zwischen Bund und Ländern abgestimmten Übermittlungskonzepte weiter Anwendung finden.

Zu Absatz 4

Zu Nummer 1

Nummer 1 dient der Umsetzung von Artikel 8 Absatz 3-5 der NIS-2-Richtlinie.

Zu Nummer 2

Nummer 2 dient der Umsetzung von Artikel 23 Absatz 8 der NIS-2-Richtlinie.

Zu Nummer 3

Nummer 3 dient der Umsetzung von Artikel 23 Absatz 6 der NIS-2-Richtlinie.

Zu Absatz 5

Absatz 5 führt den bisherigen § 8b Absatz 4a fort.

Zu Absatz 6

Absatz 6 führt den bisherigen § 8b Absatz 7 fort.

Zu § 41 (Untersagung des Einsatzes kritischer Komponenten)

Zu Absatz 1

Absatz 1 führt den bisherigen § 9b Absatz 1 fort.

Zu Absatz 2

Absatz 2 führt den bisherigen § 9b Absatz 2 fort.

Zu Absatz 3

Absatz 3 führt den bisherigen § 9b Absatz 3 fort.

Zu Absatz 4

Absatz 4 führt den bisherigen § 9b Absatz 4 fort.

Zu Absatz 5

Absatz 5 führt den bisherigen § 9b Absatz 5 fort.

Zu Absatz 6

Absatz 6 führt den bisherigen § 9b Absatz 6 fort.

Zu Absatz 7

Absatz 7 führt den bisherigen § 9b Absatz 7 fort.

Zu § 42 (Auskunftsverlangen)

§ 42 ersetzt den bisherigen § 8e. Die Ergebnisse der Evaluierung dieser Norm gemäß Artikel 6 Absatz 1 Nummer 1 des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme wurden berücksichtigt.

Aufgrund der Tätigkeiten als zuständige Behörde, CSIRT und zentrale Anlaufstelle erhält das Bundesamt nach der NIS-2-Richtlinie eine Vielzahl neuer Informationen über Wesentliche und Wichtige Einrichtungen und deren IT-Sicherheitsgefährdungen. Diese können sowohl einzeln als auch in Summe sensibel sein. Das Informationsfreiheitsgesetz sieht eine Versagung nur dann vor, wenn die herausgegebene Information für sich genommen sensibel ist und lässt daher eine Ausforschung durch Informationszugangsanträge zu, die für sich genommen auf unsensible Informationen gerichtet sind, aber in Summe die Zusammenfügung zu einem sensiblen Bild der Informationssicherheit besonders wichtiger und wichtiger Einrichtungen ermöglichen. Im Hinblick auf die geopolitische Lage und die zunehmende Gefahr von Cyberangriffen auch durch feindlich gesonnene Staaten, müssen diese Informationen daher besonders geschützt werden. Auch Artikel 11 Absatz 1 Buchstabe d NIS-2-Richtlinie schreibt daher die Sicherstellung der Vertraulichkeit für die Cybersicherheitseinrichtungen vor. Die Aktenzugangsrechte von Verfahrensbeteiligten im Rahmen von Widerspruchs- und Gerichtsverfahren gegen Anordnungen o. Ä. des Bundesamtes bleiben von dieser Regelung unberührt.

Zu Kapitel 3 (Informationssicherheit der Einrichtungen der Bundesverwaltung)

Zu § 43 (Informationssicherheitsmanagement)

§ 43 schafft eine neue zentrale Vorschrift zur gesetzlichen Verankerung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung.

Zu Absatz 1

Absatz 1 dient der grundsätzlichen Verantwortungszuweisung für die Informationssicherheit und macht Vorgaben zu den Pflichten, die damit verbunden sind und die in diesem Kapitel weiter konkretisiert werden. 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. Dazu zählen gemäß § 44 Absatz 2 die BSI-Mindeststandards sowie für Bundesministerien und das Bundeskanzleramtes nach § 44 Absatz 2 zusätzlich der vom Bundesamt vorgegebene IT-Grundschutz, der inhaltlich kompatibel ist mit ISO/IEC 27001, der zur von Erwägungsgrund 79 der NIS-2-Richtlinie referenzierten Reihe ISO/IEC 27000 gehört. Die bestehenden untergesetzlichen Regelungen des Kabinettbeschluss UP Bund bleiben hiervon unberührt. Zudem verantwortet die Einrichtungsleitung interne Regelungen, die Übernahme von Restrisiken und das Bereitstellen von Ressourcen für die Informationssicherheit. Die Einrichtungsleitung ist zuständig für übergreifende Entscheidungen hinsichtlich der Informationssicherheitsziele und der Informationssicherheitsstrategie. Dabei hat sie auch im Einzelfall ein ausgewogenes Verhältnis zwischen IT-Betrieb und Informationssicherheit herzustellen und zu diesem Zweck die Zusammenarbeit zwischen Verantwortlichen für den IT-Betrieb und Informationssicherheitsbeauftragten aktiv zu fördern. Hierzu zählt unter anderem ein bedarfsgerechter Mitteleinsatz zugunsten der Informationssicherheit.

Zu Absatz 2

Absatz 2 dient der Umsetzung Artikel 20 Absatz 2 der NIS-2-Richtlinie. Ein weiterer Bestandteil dieses Absatzes der NIS-2-Richtlinie sieht die stetige Sensibilisierung aller Beschäftigten einer Einrichtung vor. Diese Anforderung, insbesondere bezogen auf Phishing und Social Engineering gemäß Erwägungsgrund 89 der NIS-2-Richtlinie, wird bereits durch § 44 Absatz 2 mit Bezug zum IT-Grundschutz berücksichtigt. Angebote des zentralen Fortbildungsdienstleisters der Bundesverwaltung, der Bundesakademie für öffentliche Verwaltung im Bundesmi-

nisterium des Innern und für Heimat, werden durch das Bundesamt für alle Einrichtungen der Bundesverwaltung qualitätsgesichert. Damit werden Teile der Anforderungen des Umsetzungsplans Bund 2017 verpflichtend umgesetzt.

Zu Absatz 3

Absatz 3 ist eine Generalklausel zum Zweck der Verantwortungszuweisung an Einrichtungsleitungen im Falle der Beauftragung öffentlicher Dienstleister – beispielsweise auf Landesebene – oder privater Dienstleister, wie sie bisher bereits nach Kapitel 7 des Umsetzungsplans Bund gilt. Er regelt die Notwendigkeit, dass öffentlich-rechtlich oder privatrechtlich organisierte Stellen, die mit Leistungen (z. B. Dienst- oder Betriebsleistung) für die Informationstechnik des Bundes beauftragt werden, auf die Einhaltung der Voraussetzungen zur Gewährleistung der Informationssicherheit verpflichtet werden müssen. Verantwortlich ist die Leitung der beauftragenden Einrichtung der Bundesverwaltung (Auftraggeber). Die Verpflichtung hat im notwendigen und angemessenen Umfang abhängig vom konkreten Auftragsgegenstand bzw. der beauftragten Leistung zu erfolgen. Die Verpflichtung umfasst in der Regel die Umsetzung des IT-Grundschutzes und relevanter Mindeststandards. Es sind außerdem notwendige Einsichts-/Kontrollrechte und die Zusammenarbeit mit dem Auftraggeber oder dem Bundesamt zur Meldung und Behebung von Störungen oder Sicherheitsvorfällen (z. B. Informations- und Mitwirkungspflichten) zu regeln (bei Bedarf verknüpft mit angemessenen Vertragsstrafen). Bei der Beauftragung sind auch die Prüf- und Anordnungsbefugnisse des Bundesamtes, die die beauftragende Einrichtung treffen, vertraglich entsprechend auf die Dienstleister zu erstrecken.

Zu Absatz 4

Satz 1 stellt klar, dass die Registrierungspflicht aus § 33 gemäß § 29 auch Einrichtungen der Bundesverwaltung trifft. Die nach Satz 2 zu erbringenden Nachweise dienen u. a. der Herstellung von Transparenz über die Informationssicherheitslage in der Bundesverwaltung. So wird sichergestellt, dass fünf Jahre nach Inkrafttreten des Gesetzes und danach regelmäßig ein Überblick über den Umsetzungsstand in der Bundesverwaltung geschaffen werden kann. Der Nachweis über die Erfüllung der Anforderungen kann schrittweise gemäß einer durch das Bundesamt vorgegebenen Priorisierung nach Dringlichkeit erfolgen. Die Regelung dient der Umsetzung des Artikels 32 Absatz 2 Buchstabe g der NIS-2-Richtlinie und sieht vor, dass Nachweise nicht nur „auf geeignete Weise“ zu erbringen sind, sondern Einrichtungen der Bundesverwaltung hierzu „nach Vorgaben des Bundesamtes“ handeln müssen. Zunächst ist dafür die Form einer standardisierten Selbsterklärung vorgesehen, in der die Einrichtungen die Umsetzung des IT-Grundschutzes und der Mindeststandards nachweisen, soweit dem Bundesamt nicht bereits hinreichend aktuelle Ergebnisse eigener Prüfungen nach § 7 für die jeweilige Einrichtung vorliegen. Damit kann innerhalb der Einrichtungen der Bundesverwaltung die erforderliche Nachweisdichte risikobasiert weiter differenziert und der Prüfaufwand im Rahmen von § 7 für überprüfte Einrichtungen und Bundesamt gleichermaßen reduziert werden, wo die Gefährdungslage dies erlaubt.

Zu Absatz 5

Satz 1 führt den bisherigen § 4 Absatz 3 fort. Satz 2 führt den bisherigen § 4 Absatz 4 fort. Satz 3 wird neu eingefügt, um mit den betreffenden Informationen („Nullmeldungen“) eine erheblich bessere Gesamtbewertung der Gefährdungslage zu ermöglichen. Zur Vermeidung von Rückschlüssen sind der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz von den Nullmeldungen ausgenommen. Die Begrifflichkeiten der Regelungen werden von Bundesbehörden zu Einrichtungen der Bundesverwaltung konsolidiert und von „IT anderer Behörden“ zu „Kommunikationstechnik des Bundes“, womit das Schutzgut in den Vordergrund der Regelung gerückt wird. Mit Blick auf das Schutzgut und vor dem Hintergrund der sich entwickelnden Bedrohungslage ist die Erweiterung des Anwendungsbereichs durch die Erweiterung auf Einrichtungen der Bundesverwaltung sachgerecht.

Zu Absatz 6

Absatz 6 führt den bisherigen § 4 Absatz 6 fort. Der bisherige Verweis auf den Rat der IT-Beauftragten der Bundesregierung wird durch „die Ressorts“ abgelöst, um die Durchführung des Gesetzes unabhängig von über die Legislaturperioden hinweg unterschiedlichen politischen Entwicklungen bei der Ausgestaltung der Gremienlandschaft der IT-Steuerung zu halten. Die Zustimmung der Ressorts kann durch Mehrheitsentscheidung in einem geeigneten Gremium erfolgen. Wie im Umsetzungsplan Bund wird der Begriff „Ressort“ im Zusammenhang mit Regelungen verwendet, die das Bundeskanzleramt oder ein Bundesministerium jeweils einschließlich des Geschäftsbereichs betreffen.

Zu § 44 (Vorgaben des Bundesamtes)

Zu Absatz 1

Die Vorschrift führt den bisherigen § 8 Absatz 1 fort. Es wurden rechtsförmliche Anpassungen vorgenommen, um die Vorschrift nicht als Ermächtigungs- sondern als Verweisungsnorm zu formulieren. Maßgebend für die einzuhaltenden Mindestanforderungen ist die jeweils geltenden Fassungen der Mindeststandards, die auf der BSI-Internetseite (aktuelle URL: www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mindeststandards_node.html) veröffentlicht werden und dauerhaft zugänglich sind.

Zu Absatz 2

Die Vorschrift knüpft an den bisherigen § 8 Absatz 1 an und verankert neben den dort bereits geregelten Mindeststandards gleichrangig für das Bundeskanzleramt und die Bundesministerien 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 ist die jeweils geltenden Fassungen der Bestandteile des IT-Grundschutzes, die auf der BSI-Internetseite (aktuelle URL: www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_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. Der IT-Grundschutz erhält hiermit – neben den Mindeststandards – für die Bundesministerien und das Bundeskanzleramt mittelbar Gesetzesrang. Für die restlichen Einrichtungen der Bundesverwaltung ergibt sich die Umsetzung des IT-Grundschutz unverändert aus dem bestehenden untergesetzlichen Kabinettbeschluss UP Bund. Um die Nachweisfrist von fünf Jahren ab Inkrafttreten (§ 43 Absatz 4 Satz 2) bei weiterhin knappen finanziellen und personellen Ressourcen umsetzen 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.

Zu Absatz 3

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 4

Die Beratung des Bundesamtes 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 5

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

Zu Absatz 6

Die Vorschrift führt Teile des bisherigen § 8 Absatz 3 fort. Hier enthalten ist die Befugnis, Nutzungsvorgaben für die Einrichtungen der Bundesverwaltung zu machen. Die allgemeine Befugnis des Bundesamtes 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 und für Heimat 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 § 45 (Informationssicherheitsbeauftragte der Einrichtungen der Bundesverwaltung)

Die neue Vorschrift führt auf gesetzlicher Ebene Informationssicherheitsbeauftragte (ISBs) in Einrichtungen der Bundesverwaltung als notwendige Funktion ein, wie sie bisher bereits im Umsetzungsplan Bund vorgesehen sind. Damit wird die herausgehobene Bedeutung der Informationssicherheit in allen Bereichen moderner Verwaltungstätigkeit unterstrichen. Eine klare gesetzliche Definition ihrer Aufgaben und Befugnisse erleichtert auch eine verbesserte Zusammenarbeit mit der jeweiligen Leitung sowie mit anderen Verantwortungsbereichen und deren Beauftragten, etwa Datenschutz und Geheimschutz. Im Umsetzungsplan Bund wurde bisher die inzwischen überholte Bezeichnung IT-Sicherheitsbeauftragter (IT-SiBe) verwendet, diese wird hiermit zugunsten des ISB überwunden.

Zu Absatz 1

Absatz 1 verankert die Bedeutung der Funktion der Informationssicherheitsbeauftragten in den Einrichtungen der Bundesverwaltung und stellt sicher, dass die Funktion auch im Fall der Verhinderung der primär damit betrauten Person wahrgenommen werden kann, damit etwa bei Digitalisierungsvorhaben abwesenheitsbedingte Verzögerungen vermieden werden können.

Zu Absatz 2

Absatz 2 regelt die Voraussetzungen, unter denen Einrichtungs-ISBs ihre Funktion ausüben. Zur Befähigung der ISBs dienen unter anderem ein bedarfsgerechter Mitteleinsatz, auch unter Berücksichtigung des Schadenspotenzials von Sicherheitsvorfällen oder Störungen, sowie die erforderliche Fachkunde. Fachkunde ist zwar nicht Voraussetzung für die Übertragung der Tätigkeit, muss jedoch wenigstens tätigkeitsbegleitend erworben werden. Dadurch wird einerseits die Besetzung entsprechender Funktionen vor dem Hintergrund des herrschenden Fachkräftemangels erleichtert. Andererseits müssen auch etablierte Funktionsträger ihre Fachkunde so kontinuierlich an die sich wandelnden Erfordernisse anpassen. Zum Nachweis der Fachkunde innerhalb der Bundesverwaltung kann eine Zertifizierung bei der Bundesakademie für öffentliche Verwaltung (BAköV) zur bzw. zum Informationssicherheitsbeauftragten dienen. Die Fachaufsicht wird zum Zwecke der notwendigen operativen Unabhängigkeit für die effektive Vertretung von Sicherheitsbelangen durch die fachkundigen Ressort-ISBs ausgeübt. In obersten Bundesbehörden ohne Geschäftsbereich bzw. nachgeordnete Behörden werden die Rollen des Einrichtungs-ISB und des Ressort-ISB in Personalunion wahrgenommen.

Zu Absatz 3

Absatz 3 regelt die Aufgaben der Einrichtungs-ISBs, die im Auftrag ihrer Einrichtungsleitung für die operative Umsetzung und Kontrolle von Maßnahmen im Rahmen des Informationssicherheitsmanagements zuständig sind. Indem sie die Anforderungen des Bundesamtes nach § 44 Absatz 1 erfüllen, also die Vorgaben des IT-Grundschutzes und der Mindeststandards, erfüllen sie die Pflicht zur Erstellung und Umsetzung des Informationssicherheitskonzepts vollumfänglich. Darüberhinausgehende Sicherheitsmaßnahmen, die ISBs im Einzelfall für erforderlich halten, können sie ergänzend im Informationssicherheitskonzept aufnehmen, ohne dass ein Weglassen solcher Maßnahmen eine Pflichtverletzung im Rahmen ihrer individuellen Verantwortung darstellen würde. Die Verantwortung der Einrichtungsleitung wird hierdurch nicht berührt. Es handelt sich bei der Konzepterstellung nicht um eine höchstpersönliche Aufgabe. Insbesondere kann das Gesamt-Informationssicherheitskonzept für die Einrichtung auch eine Auslagerung bzw. eine Beauftragung Dritter mit der Erstellung von Informationssicher-

heitskonzepten vorsehen. Die Berichtspflicht soll Compliance erwirken, für deren kontinuierliche Aufrechterhaltung eine mindestens quartalsweise Berichterstattung förderlich ist. Welche Häufigkeit für Regelmäßigkeit konkret angemessen ist, hängt darüber hinaus von den Umständen des jeweiligen Einzelfalls unter Abwägung des Schadenspotenzials ab. Aus den Aufgaben ergeben sich zugleich einrichtungsintern entsprechende Befugnisse, wie beispielsweise die Befugnis zur Überprüfung des Umsetzungsstands von Maßnahmen aus dem Sicherheitskonzept durch andere Organisationseinheiten der Einrichtung sowie die Befugnis, deren Umsetzung einzufordern. Um Interessens- und Rollenkonflikte, bspw. Zwischen der Informationssicherheit und dem IT-Management, zu vermeiden, müssen die Einrichtungs-ISBs ihre Berichts- und Beratungsaufgaben unabhängig und weisungsfrei erfüllen können.

Zu Absatz 4

Absatz 4 räumt den Einrichtungs-ISBs Beteiligungs- und Vortragsrechte ein und stellt sicher, dass sie wegen der Erfüllung ihrer Aufgaben nicht abberufen oder benachteiligt werden dürfen. Zur Vermeidung von Parallel-/Doppelzuständigkeiten gilt die Beteiligungspflicht nicht für Maßnahmen, die primär verwandten Bereichen der Informationssicherheit zuzuordnen sind, für die gesonderte Regelungs-Regimes und Zuständigkeiten bestehen (z. B. Datenschutz, Geheimschutz, Notfall-/Krisenmanagement, Arbeitsschutz, Brandschutz). Die Vortragsrechte gegenüber der Einrichtungsleitung und dem jeweiligen Ressort-ISB dienen dazu, die Position der ISBs fachlich so unabhängig von der Organisation der Einrichtung zu gestalten, wie es für die Aufgabe zur Vermeidung von Interessenskonflikten erforderlich ist.

Zu § 46 (Informationssicherheitsbeauftragte der Ressorts)

Die neue Vorschrift gibt ISBs auf Ressortebene (Ressort-ISBs), wie sie schon bisher im Rahmen des Umsetzungsplans Bund angelegt sind, eine gesetzliche Grundlage. Zur Umsetzung von Artikel 31 Absatz 4 der NIS-2-Richtlinie ist operative Unabhängigkeit für die Aufsicht über Einrichtungen öffentlicher Verwaltung sicherzustellen. Diese operative Unabhängigkeit wird hier dadurch erreicht, dass Ressort-ISBs (a) ihre Berichts- und Beratungsaufgaben unabhängig und weisungsfrei erfüllen können müssen, (b) Fachkunde erwerben müssen, es sich also nicht um politische Funktionen handelt, sondern der Fokus bei der Aufgabenausübung auf der fachlichen Expertise liegt, (c) ein eigenes Budgetrecht besitzen, um handlungsfähig zu sein, und (d) wird die Unabhängigkeit im Hinblick auf Fragen der Informationssicherheit dadurch sichergestellt, dass Ressort-ISBs unmittelbar vor dem CISO Bund vortragen dürfen, der seinerseits Vortragsrechte unmittelbar gegenüber Organen der Legislative besitzt. Da es auch oberste Bundesbehörden gibt, die keinem Ressort angehören, ist auch für „ressort-unabhängige“ oberste Bundesbehörden die Rolle eines Ressort-ISB einzurichten. Weitere Regelungen in diesem Paragraphen, die für das jeweilige Ressort des oder der Informationssicherheitsbeauftragten getroffen werden, sind entsprechend auf die „ressort-unabhängige“ oberste Bundesbehörde und ihren Geschäftsbereich anzuwenden.

Zu Absatz 1

Absatz 1 regelt Bestellung und Zuständigkeit von Ressort-ISBs. Sie sind zuständig für ein funktionierendes und effektives Informationssicherheitsmanagement in ihrem Ressort, das die jeweilige oberste Bundesbehörde mitsamt ihrem jeweiligen Geschäftsbereich umfasst. Im Fall oberster Bundesbehörden sind die Funktionen von Ressort-ISB und Einrichtungs-ISB zu unterscheiden, können jedoch derselben Person übertragen werden. Die Angemessenheit der Informationssicherheit ist in Bezug auf Wechselwirkungen mit den Belangen des IT-Betriebs zu bewerten.

Zu Absatz 2

Absatz 2 regelt die Voraussetzungen, unter denen Ressort-ISBs ihre Funktion ausüben. Zur Befähigung der ISBs dienen unter anderem ein bedarfsgerechter Mitteleinsatz sowie die erforderliche Fachkunde. Fachkunde ist zwar nicht Voraussetzung für die Übertragung der Tätigkeit, muss jedoch wenigstens tätigkeitsbegleitend erworben werden, da die Ressort-ISBs die Fachaufsicht über die ISBs der Einrichtungen in ihrem Zuständigkeitsbereich führen können müssen. So wird einerseits die Besetzung entsprechender Funktionen vor dem Hintergrund des herrschenden Fachkräftemangels erleichtert. Andererseits müssen auch etablierte Funktionsträger ihre Fachkunde so kontinuierlich an die sich wandelnden Erfordernisse anpassen.

Zu Absatz 3

Absatz 3 normiert die Aufgaben der Ressort-ISBs, aus denen sich zugleich ressortintern die Befugnis zu Kontrolle und Umsetzungsmaßnahmen ergibt. Da die Einrichtungs-ISBs der fachlichen Aufsicht der Ressort-ISBs unterste-

hen, sind die Ressort-ISBs insoweit gegenüber dem Geschäftsbereich weisungsbefugt. Um Interessens und Rollenkonflikte, bspw. Zwischen der Informationssicherheit und dem IT-Management, zu vermeiden, müssen die Ressort-ISBs ihre Berichts- und Beratungsaufgaben unabhängig und weisungsfrei erfüllen können. Die Berichtspflicht dient als Mittel der Compliance-Förderung.

Zu Absatz 4

Das Veto-Recht zum Einsatz bestimmter IT-Produkte dient dem Zweck, bei Bedarf Informationssicherheitsbelange durchsetzen zu können. Mit der Begründungspflicht wird vermieden, dass mit dieser Möglichkeit andere Vorgaben etwa im Rahmen der IT-Konsolidierung umgangen werden. Die Möglichkeit, eine Nutzung nur teilweise zu untersagen, gestattet zwischen unterschiedlichen Anwendungszwecken zu unterscheiden, soweit etwa Produkte zum Zweck der Überprüfung verwendet werden müssen oder ein Einsatz in bestimmten IT-Umgebungen möglich ist, aus Sicherheitsgründen jedoch keine Nutzung im allgemeinen Geschäftsbetrieb erfolgen soll.

Zu Absatz 5

Absatz 5 regelt die Möglichkeit für Ressort-ISBs, Ausnahmebescheide für Einrichtungen innerhalb ihres Zuständigkeitsbereichs zu erlassen. Einrichtungen, die die Voraussetzungen des § 28 Absatz 1 Satz 1 oder § 28 Absatz 2 Satz 1 erfüllen können hiervon nicht umfasst werden, für diese wären Ausnahmebescheide nach § 37 zu erlassen. Dadurch wird sichergestellt, dass Einrichtungen der Bundesverwaltung, die vom Anwendungsbereich der Umsetzung der NIS-2-Richtlinie zu erfassen sind, nicht von den Verpflichtungen der NIS-2-Richtlinie ausgenommen werden können. Mit einem Ausnahmebescheid kann ein Ressort-ISB Einrichtungen seines Ressorts von den Verpflichtungen nach §§ 28 bis 50 befreien, solange sachliche Gründe für die Erteilung der Ausnahme vorliegen und durch die Befreiung keine erkennbaren nachteiligen Auswirkungen für die Informationssicherheit des Bundes zu befürchten sind. Sachliche Gründe können bspw. Vorliegen, wenn eine Einrichtung der mittelbaren Bundesverwaltung eine sehr geringe Anzahl an Mitarbeitern und Standorten aufweist und/oder ihren IT-Betrieb ausgelagert hat. Erkennbare nachteilige Auswirkungen für die Informationssicherheit des Bundes können insbesondere dann entstehen, wenn die Einrichtung ein potentielles Verbundrisiko für andere Einrichtungen des Bundes darstellt; bspw. Falls die Einrichtung an die Netze des Bundes angebunden ist oder Leistungen der IT-Konsolidierung des Bundes nutzt.

Zu Absatz 6

Absatz 6 räumt den Ressort-ISBs Beteiligungs- und Vortragsrechte ein und stellt sicher, dass sie wegen der Erfüllung ihrer Aufgaben nicht abberufen oder benachteiligt werden dürfen. Zur Vermeidung von Parallel-/Doppelzuständigkeiten gilt die Beteiligungspflicht nicht für Vorhaben, die primär verwandten Bereichen der Informationssicherheit zuzuordnen sind, für die gesonderte Regelungs-Regimes und Zuständigkeiten bestehen (z. B. Datenschutz, Geheimschutz, Notfall-/Krisenmanagement, Arbeitsschutz, Brandschutz).

Zu § 47 (Wesentliche Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes)

Zu Absatz 1

Absatz 1 sieht die Bestellung eigener ISBs für wesentliche Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes vor. Wegen der zunehmenden Bedeutung, Größe und Komplexität von IT-Vorhaben und -Strukturen können Einrichtungen der Bundesverwaltung diese nach Absatz 2 als wesentliche Digitalisierungsvorhaben einstufen, woraus sich die fachliche Notwendigkeit der Bestellung eigener ISBs für das Vorhaben ergibt.

Zu Absatz 2

Bei ressortübergreifenden Digitalisierungs¬vorhaben, wie beispielsweise der IT-Konsolidierung des Bundes, ist grundsätzlich von einer wesentlichen Bedeutung für allgemeine Sicherheitsbelange auszugehen, und die ressortübergreifenden Kommunikations-infrastrukturen, wie beispielsweise die Netze des Bundes haben für die Regierungskommunikation insgesamt eine herausgehobene Bedeutung.

Zu Absatz 3

Absatz 3 regelt die Verantwortung zur Bestellung des ISB. Die Entscheidungskompetenz des Bundesministeriums des Innern und für Heimat in Zweifelsfällen, wenn eine Einigung bezüglich der Verantwortung zur Bestellung eines ISB etwa nicht in einem geeigneten Gremium herbeigeführt werden kann, dient der Auflösung möglicher

Konflikte und der Sicherstellung, dass die Wahrnehmung der Funktion nicht von Zuständigkeitsfragen verzögert oder behindert wird.

Zu Absatz 4

Die Entscheidung, ob der ISB der Leitung der Einrichtung oder dem jeweiligen Ressort-ISB untersteht, obliegt dem jeweils zuständigen Ressort.

Zu Absatz 5

Absatz 5 führt den bisherigen § 8 Absatz 4 fort. Voraussetzung für die Gewährleistung der Informationssicherheit bei der Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben sind der Einsatz bedarfsgerechter Mittel für die Informationssicherheit sowie Fachkunde des jeweils zuständigen Informationssicherheitsbeauftragten.

Zu § 48 (Amt des Koordinators für Informationssicherheit)

Die neue Vorschrift regelt die Bestellung eines Koordinators oder einer Koordinatorin der Bundesregierung für Informationssicherheit (CISO Bund). Die konkrete organisatorische Anbindung sowie die Einbindung in relevante Gremien bleiben dem umsetzenden Kabinettbeschlusses vorbehalten. Um Interessenskonflikte zu vermeiden, sollte die Funktion möglichst unabhängig organisiert werden.

Zu Teil 4 (Datenbanken der Domain-Name-Registrierungsdaten)

Teil 4 dient der Umsetzung von Artikel 28 der NIS-2-Richtlinie.

Zu § 49 (Pflicht zum Führen einer Datenbank)

Zu Absatz 1

Absatz 1 dient der Umsetzung von Artikel 28 Absatz 1 der NIS-2-Richtlinie.

Zu Absatz 2

Zu Nummer 1

Nummer 1 dient der Umsetzung von Artikel 28 Absatz 2 Buchstabe a der NIS-2-Richtlinie.

Zu Nummer 2

Nummer 2 dient der Umsetzung von Artikel 28 Absatz 2 Buchstabe b der NIS-2-Richtlinie.

Zu Nummer 3

Nummer 3 dient der Umsetzung von Artikel 28 Absatz 2 Buchstabe c der NIS-2-Richtlinie.

Zu Nummer 4

Nummer 4 dient der Umsetzung von Artikel 28 Absatz 2 Buchstabe d der NIS-2-Richtlinie.

Zu Absatz 3

Absatz 3 dient der Umsetzung von Artikel 28 Absatz 3 der NIS-2-Richtlinie.

Zu Absatz 4

Absatz 4 dient der Umsetzung von Artikel 28 Absatz 4 der NIS-2-Richtlinie.

Zu Absatz 5

Absatz 5 räumt dem Bundesamt eine Prüfungskompetenz ein.

Zu § 50 (Verpflichtung zur Zugangsgewährung)

§ 50 dient der Umsetzung von Artikel 28 Absatz 5 der NIS-2-Richtlinie. Ein Antrag eines berechtigten Zugangsnachfragers ist als begründet zu werten, wenn der Antragsteller ein berechtigtes Interesse darlegt. Dies ist regelmäßig der Fall, wenn der Antrag mit dem Verweis auf einen Verwaltungsvorgang versehen wird und die angeforderte Auskunft zur Aufgabenerfüllung des Antragstellers geeignet, erforderlich und angemessen ist. Bei der Überprüfung der Vorgaben kann das Bundesamt hinsichtlich des Verfahrens zur Zugangsgewährung und hin-

sichtlich des dafür erforderlichen ordnungsgemäßen Vorhaltens der Datenbank verlangen, dass die Verpflichteten die dafür aus Sicht des Bundesamtes erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorlegen und Auskunft erteilen.

Zu § 51 (Kooperationspflicht)

§ 51 dient der Umsetzung von Artikel 28 Absatz 6 der NIS-2-Richtlinie. Die Kooperationspflicht ist nicht ausschließlich auf die Vermeidung der doppelten Erhebung von Domain-Namen-Registrierungsdaten ausgerichtet. Sie bezieht sich grundsätzlich auf alle in § 49 und § 50 festgelegten Verpflichtungen, auch z. B. die Anfragebeantwortung und den Prozess der Herausgabe von Registrierungsdaten. Sinn und Zweck der doppelten Adressierung von Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister in den §§ 49 und 50 ist es nicht, dass diese sämtliche Pflichten doppelt erfüllen, sondern im Rahmen einer vereinbarten Arbeitsteilung verpflichtend kooperieren, wie es weitgehend bereits der Fall ist. Registrierungsdaten dürfen nicht doppelt erhoben, verifiziert und gespeichert werden. Die Kooperationspflicht sichert die Erfüllung der Verpflichtungen, ohne dass doppelte Datenbanken geführt werden. Eine Verpflichtung zum Führen doppelter Datenbanken würde zu einem signifikanten Abfluss von Registrierungsdaten ins Nicht-EU-Ausland führen, da eine große Anzahl von Registries und Registraren dort ihren Sitz haben.

Zu Teil 5 (Zertifizierung, Konformitätserklärung und Kennzeichen)

Zu § 52 (Zertifizierung)

Zu Absatz 1

Absatz 1 führt den bisherigen § 9 Absatz 1 fort.

Zu Absatz 2

Absatz 2 führt den bisherigen § 9 Absatz 2 fort.

Zu Absatz 3

Absatz 3 führt den bisherigen § 9 Absatz 3 fort. Die Angebote der Bundesakademie für öffentliche Verwaltung zur Fortbildung und Zertifizierung der Informationssicherheitsbeauftragten der Bundesverwaltung werden wie im Umsetzungsplan 2017 Bund dargestellt fortgeführt.

Zu Absatz 4

Zu Nummer 1

Nummer 1 führt den bisherigen § 9 Absatz 4 Nummer 1 fort.

Zu Nummer 2

Nummer 2 führt den bisherigen § 9 Absatz 4 Nummer 2 fort.

Zu Absatz 5

Absatz 5 führt den bisherigen § 9 Absatz 4a fort.

Zu Absatz 6

Absatz 6 führt den bisherigen § 9 Absatz 5 fort.

Zu Absatz 7

Zu Nummer 1

Nummer 1 führt den bisherigen § 9 Absatz 6 Nummer 1 fort.

Zu Nummer 2

Nummer 2 führt den bisherigen § 9 Absatz 6 Nummer 2 fort.

Zu Absatz 8

Absatz 8 führt den bisherigen § 9 Absatz 7 fort.

Zu § 53 (Konformitätsbewertung und Konformitätserklärung)

Die Vorschrift dient der Angleichung der Konformitätsbewertungsverfahren im Bereich IT-Sicherheit an internationale Vorgaben und insbesondere die Verordnung (EU) 2019/881 (sog. Cybersecurity Act – CSA), die auch in der NIS-2-Richtlinie zur Anwendung kommt. Im CSA ist im Rahmen eines Zertifizierungsschemas auch eine Selbstbewertung der Konformität als Alternative zu einer klassischen Zertifizierung durch einen Dritten vorgesehen, in der ein Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen selbst alle Überprüfungen vornimmt, um sicherzustellen, dass die IKT-Produkte, -Dienste oder -Prozesse mit dem europäischen Schema für die Cybersicherheitszertifizierung konform sind. Mit der Selbstbewertung verbunden ist die Unterzeichnung einer Erklärung durch den Hersteller, Anbieter oder IT-Sicherheitsdienstleister, worin dieser bestätigt, dass die Anforderungen der Technischen Richtlinie eingehalten werden (Konformitätserklärung). Hierdurch übernimmt der Unterzeichner (Aussteller) die Verantwortung für die Einhaltung der Anforderungen. Vorteile der Selbstbewertung sind die niedrigeren Kosten und der geringere Aufwand für den Hersteller, Anbieter oder IT-Sicherheitsdienstleister. Darüber hinaus wird dem Bundesamt hierdurch ermöglicht, Vorgaben an die IT-Sicherheit niedrigschwellig auf dem Markt zu etablieren und zugleich die Kontrolle der Anforderungen auf einem dem Schutzniveau entsprechenden Niveau sicherzustellen, ohne den Markt mit den strengeren Vorgaben einer Zertifizierung zu belasten. Bei der Konformitätserklärung handelt es sich um eine rein nationale Regelung. Im Einklang mit der Verordnung (EU) 2019/881 wird das Bundesamt kein Schema betreiben, welches im Widerspruch zu einem europäisch harmonisierten Zertifizierungsschema steht. Zugleich kann das Bundesamt jedoch das Ziel verfolgen, ein bewährtes nationales Schema einer europäischen Harmonisierung im Wege der Verordnung (EU) 2019/881 zuzuführen.

Zu den Absätzen 1 und 2

Absatz 1 legt den Rahmen für eine Konformitätserklärung fest. In Abgrenzung zum IT-Sicherheitskennzeichen werden keine Verbraucherprodukte von der Konformitätserklärung nach dieser Regelung erfasst. Ein möglicher Anwendungsbereich ist insbesondere der bereits im Bundesamt etablierte IT-Grundschutz und entsprechende Selbstbewertungen von Personen (z. B. IT-Grundschutz-Praktiker) oder Institutionen.

Die Absätze 1 und 2 stellen zudem klar, dass die entsprechenden Technischen Richtlinien vom Bundesamt erstellt werden und festlegen, welche konkreten Vorgaben (insbesondere bezüglich der Durchführung und dem Nachweis der Konformitätsbewertung) mit der Selbstbewertung verbunden sind. Sowohl die Anforderungen, als auch die Vorgaben für Durchführung der Konformitätsbewertung können somit von Technischer Richtlinie zu Technischer Richtlinie variieren. Bei den Vorgaben an die Konformitätsbewertung kann dabei auf etablierte Akteure (Beispielsweise im Bereich Grundschutz) zurückgegriffen werden, die bereits heute eine Konformitätsbewertung anbieten. Wie Absatz 3 klarstellt, kann dabei auch auf akkreditierte Konformitätsbewertungsstellen zurückgegriffen werden.

Dieses Vorgehen entspricht in weiten Teilen dem Regelungsgehalt von Schemata im Anwendungsbereich der Verordnung (EU) 2019/881. Durch die so gewonnene Flexibilität kann das Bundesamt in der Technischen Richtlinie auf die jeweiligen Ziele und den konkreten Gegenstand der Selbstbewertung reagieren. Aufgrund der guten Erfahrungen mit dem IT-Sicherheitskennzeichen, soll es dem Bundesamt darüber hinaus ermöglicht werden, in der Technischen Richtlinie die Bereitstellung von aktuellen Informationen auf der Internetseite des Bundesamtes vorzusehen und dies gegebenenfalls durch einen dynamischen Bestandteil mit dem Kennzeichen des Schemas zu verknüpfen.

Zu Absatz 3

Um zusätzlich ein einheitliches Niveau in der Konformitätsbewertung sicherzustellen, kann das Bundesamt in seiner Technischen Richtlinie auf das System der Akkreditierung entsprechend dem Gesetz über die Akkreditierungsstelle (Akkreditierungsstellengesetz – AkkStelleG) zurückgreifen. Aussteller einer Konformitätserklärung müssen sich dann einer Konformitätsbewertung durch eine von der Deutschen Akkreditierungsstelle (DakkS) akkreditierten Konformitätsbewertungsstelle unterziehen, der das Bundesamt die Befugnis erteilt hat, als solche im Anwendungsbereich des § 53 tätig zu werden. Die Erteilung der Befugnis liegt im Ermessen des Bundesamtes und kann an Anforderungen geknüpft werden, die über diejenigen der Akkreditierung hinausgehen. Die Entscheidung kann mit Nebenbestimmungen verbunden werden. Mit der Stellung als die für die Erteilung der Befugnis zuständigen Behörde gehen die Rechte des Bundesamtes entsprechend dem AkkStelleG einher.

Zu Absatz 4

Absatz 3 Satz 1 stellt sicher, dass dem Bundesamt bei Bedarf die für die Aufsicht notwendigen Informationen und Dokumente vorliegen. Die nach Satz 2 vorzulegende Konformitätserklärung kann vom Bundesamt, soweit es das Schema vorsieht, gemeinsam mit weiteren Informationen und Dokumenten auf der Internetseite des Bundesamtes nach Absatz 2 Nummer 6 veröffentlicht werden.

Zu den Absätzen 5 und 6

Der Konformitätserklärung liegt –anders als es bei der Zertifizierung der Fall ist- keine Entscheidung des Bundesamtes in Gestalt eines Verwaltungsaktes zugrunde. Daher bedarf es zur Durchsetzung von Maßnahmen der Aufsicht einer eigenständigen Ermächtigungsgrundlage. Kontrolliert wird die Einhaltung der Vorgaben ex-post durch die bereits etablierte Marktaufsicht des Bundesamtes. Diese kann anlasslos oder anlassbezogen erfolgen. Werden Maßnahmen aufgrund eines begründeten Verdachts getroffen, so kann das Bundesamt gegenüber dem Adressaten der Maßnahme Gebühren erheben. Ein begründeter Verdacht kann sowohl auf eigenen Erkenntnissen des Bundesamtes, als auch durch vertrauenswürdige öffentliche Quellen oder Hinweisgeber beruhen. Flankiert wird die Aufsicht durch die Sanktionsvorschriften in § 65. Danach ist es strafbewehrt, wenn eine vom Bundesamt für ungültig erklärte Konformitätserklärung verwendet oder nur wahrheitswidrig behauptet wird, dass eine solche abgegeben wurde.

Zu § 54 (Nationale Behörde für die Cybersicherheitszertifizierung)

Zu Absatz 1

Absatz 1 führt den bisherigen § 9a Absatz 1 fort.

Zu Absatz 2

Absatz 2 führt den bisherigen § 9a Absatz 2 fort.

Zu Absatz 3

Absatz 3 führt den bisherigen § 9a Absatz 3 fort.

Zu Absatz 4

Absatz 4 führt den bisherigen § 9a Absatz 4 fort.

Zu Absatz 5

Absatz 5 führt den bisherigen § 9a Absatz 5 fort.

Zu Absatz 6

Zu Nummer 1

Nummer 1 führt den bisherigen § 9a Absatz 6 Nummer 1 fort.

Zu Nummer 2

Nummer 2 führt den bisherigen § 9a Absatz 6 Nummer 2 fort.

Zu Absatz 7

Zu Nummer 1

Nummer 1 führt den bisherigen § 9a Absatz 7 Nummer 1 fort.

Zu Nummer 2

Nummer 2 führt den bisherigen § 9a Absatz 7 Nummer 2 fort.

Zu § 55 (Freiwilliges IT-Sicherheitskennzeichen)

Zu Absatz 1

Absatz 1 führt den bisherigen § 9c Absatz 1 fort.

Zu Absatz 2

Zu Nummer 1

Nummer 1 führt den bisherigen § 9c Absatz 2 Nummer 1 fort.

Zu Nummer 2

Nummer 2 führt den bisherigen § 9c Absatz 2 Nummer 2 fort.

Zu Absatz 3

Absatz 3 führt den bisherigen § 9c Absatz 3 fort.

Zu Absatz 4

Absatz 4 führt den bisherigen § 9c Absatz 4 fort.

Zu Absatz 5

Zu Nummer 1

Nummer 1 führt den bisherigen § 9c Absatz 5 Nummer 1 fort.

Zu Nummer 2

Nummer 2 führt den bisherigen § 9c Absatz 5 Nummer 2 fort.

Zu Nummer 3

Nummer 3 führt den bisherigen § 9c Absatz 5 Nummer 3 fort.

Zu Absatz 6

Absatz 6 führt den bisherigen § 9c Absatz 6 fort.

Zu Absatz 7

Absatz 7 führt den bisherigen § 9c Absatz 7 fort. Der bisherige Verweis auf Absatz 3 war irreführend bzw. falsch. Daher wurde die Regelung für die Dauer hier explizit ausgegeben. Die Dauer, für die der Hersteller oder Diensteanbieter die Erfüllung der IT-Sicherheitsanforderungen zusichert, wird wie bisher durch Verordnung nach § 56 Absatz 2 und die hierin aufgeführten Verfahren bestimmt.

Zu Absatz 8

Zu Nummer 1

Nummer 1 führt den bisherigen § 9c Absatz 8 Nummer 1 fort.

Zu Nummer 2

Nummer 2 führt den bisherigen § 9c Absatz 8 Nummer 2 fort.

Zu Absatz 9

Absatz 9 führt den bisherigen § 9c Absatz 9 fort.

Zu Teil 6 (Verordnungsermächtigungen, Grundrechtseinschränkungen und Berichtspflichten)

Zu § 56 (Ermächtigung zum Erlass von Rechtsverordnungen)

Die Vorschrift führt zum Teil den bisherigen § 10 BSI-Gesetz fort. Aufgrund der ohnehin bestehenden Vorgabe nach § 62 Absatz 2 Satz 1 in Verbindung mit § 47 Absatz 1 der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) bei dem Erlass von Rechtsverordnungen u. a. Fachkreise und Verbände zu beteiligen, wird der mithin überflüssige gesetzliche Beteiligungsbefehl in den bisherigen Ermächtigungen zum Erlass von Rechtsverordnungen in § 10 des BSI-Gesetzes hier nicht fortgeführt.

Zu Absatz 1

Absatz 1 führt den bisherigen § 10 Absatz 2 fort. In der auf Basis dieses Absatzes erlassenen Rechtsverordnung können insbesondere jeweils für die Zertifizierung von Produkten oder Komponenten, informationstechnischen Systemen, Schutzprofilen sowie Personen und Anerkennung von sachverständigen Stellen die Modalitäten des Zertifizierungsverfahrens, wie etwa Antragsstellung und eventuelle Mitwirkungspflichten, sowie mögliche Nebenbestimmungen (wie zum Beispiel Befristungen) von Zertifikaten und Anerkennungen geregelt werden.

Zu Absatz 2

Absatz 2 führt den bisherigen § 10 Absatz 3 fort. Gemäß der Begründung zum IT-Sicherheitsgesetz 2.0 können in der Verordnung etwa die Details der Ausgestaltung (grafische Darstellung usw.) festgelegt werden. Auch die Verfahren zu Feststellung der Eignung branchenabgestimmter IT-Sicherheitsvorgaben sowie zu Antragsstellung auf Freigabe durch einen Hersteller können darin näher geregelt werden. Insbesondere ist dort das genaue Verfahren und die Gestaltung des Verweises auf Sicherheitsinformationen (zum Beispiel zu verfügbaren Sicherheitsupdates oder bekanntgewordenen Schwachstellen), der Teil des Etiketts des IT-Sicherheitskennzeichens sein soll, zu regeln.

Zu Absatz 3

Absatz 3 dient der Umsetzung von Artikel 24 der NIS-2-Richtlinie. Wenn informationstechnische Produkte, Dienste oder Prozesse für die Erbringung von Diensten der Einrichtung maßgeblich sind, können verpflichtende Zertifizierungen von diesen Produkten, Diensten oder Prozessen dazu beitragen, das Risiko für Sicherheitsvorfälle in diesen Bereichen zu verringern. Sofern Art und Ausmaß der Risikoexposition der Einrichtung diesen Eingriff rechtfertigen, ist daher vorgesehen, dass das BMI in Umsetzung des Artikel 24 Absatz 4 der NIS-2-Richtlinie eine Zertifizierung in diesen Bereichen verpflichtend vorschreiben kann. Diese Vorschrift greift nur, insoweit auch entsprechende Zertifizierungsschemata vorhanden sind. Vor Erlass der Rechtsverordnung ist durch das BMI und unter Beteiligung der potenziell betroffenen Einrichtungen zu prüfen, dass für die einzubeziehenden Produkte, Dienste oder Prozesse eine ausreichende Verfügbarkeit am Markt sichergestellt ist.

Zu Absatz 4

Absatz 4 führt den bisherigen § 10 Absatz 1 fort. Die Ergebnisse der Evaluierung dieser Norm gemäß Artikel 6 Absatz 1 Nummer 1 des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme wurden berücksichtigt. Die bisherige Praxis wird beibehalten, eine Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und Wirtschaftsverbände durchzuführen (vgl. § 62 Absatz 2 i. V. m. § 47 Absatz 3 GGO).

Der vorliegende Gesetzentwurf sieht vor, dass zusätzlich zu den gemäß der Vorgaben der NIS-2-Richtlinie verbindlichen Einrichtungskategorien innerhalb der Kategorie der besonders wichtigen Einrichtungen weiterhin KRITIS-Betreiber anhand von Schwellenwerten mit einem Bezug zur Versorgungsrelevanz definiert werden. Dies ist zum einen erforderlich, um einen Gleichklang mit dem KRITIS-Dachgesetz und dem dort in Umsetzung der CER-Richtlinie vorgesehenen Verfahren zur KRITIS Bestimmung zu erreichen. Gleichzeitig hat die Evaluierung der KRITIS bezogenen Bestandteile des IT-Sicherheitsgesetzes 2.0 ergeben, dass aufgrund der starken Ausweitung des Anwendungsbereichs des BSI-Gesetzes im Zuge der NIS-2-Umsetzung auch weiterhin eine Bestimmung von kritischen Infrastrukturen mit einem Fokus auf die Versorgungsrelevanz erfolgen sollte. Gemäß dieser Verordnung als KRITIS-Betreiber bestimmte Unternehmen gelten gleichzeitig als besonders wichtige Einrichtungen.

KRITIS-Betreiber werden in Zukunft weiterhin mit Schwellenwerten anhand ihrer Versorgungsrelevanz bestimmt.

Für den in der Rechtsverordnung festzusetzenden als bedeutend anzusehenden Versorgungsgrad anhand von branchenspezifischen Schwellenwerten soll das bereits in mehrjähriger Verwaltungspraxis etablierte Verfahren der Verordnung zu Bestimmung Kritischer Infrastrukturen (BSI-KritisV) weiter fortgeführt werden. Hierbei werden durch BMI gemeinsam mit den jeweils zuständigen Ressorts sowie unter Beteiligung der KRITIS-Betreiber und ihrer Branchenverbände geeignete Bemessungsgrößen für kritische Anlagen bestimmt, anhand derer der Versorgungsgrad im Sinne der durch die Anlage versorgten Personen näherungsweise bestimmt werden kann. Diese Bemessungsgrößen stellen typischerweise quantitative oder qualitative anlagenspezifische Eigenschaften wie Kapazitäten, Größen, Typ oder Art der Anlage dar, die entweder den Betreibern bereits bekannt sind oder zumindest

mit möglichst geringem Aufwand für die jeweiligen Anlagen ermittelt werden können. Anschließend werden für die so gefundenen Bemessungsgrößen Schwellenwerte bestimmt, bei deren Überschreitung der Versorgungsgrad der betreffenden Anlage als bedeutend im Sinne dieses Gesetzes gilt und damit die Anlage eine kritische Anlage darstellt.

Zu Absatz 5

Absatz 5 dient der Umsetzung von Artikel 23 Absatz 11 Unterabsatz 2 der NIS-2-Richtlinie. Das Bundesamt kann Vorgaben dazu machen, wann Sicherheitsvorfälle als erheblich gelten. Soweit die Europäische Kommission dahingehende Durchführungsrechtsakte erlässt, genießen diese Vorrang. Die Vorgaben des Bundesamtes haben dann nur noch konkretisierende Wirkung, soweit die Durchführungsrechtsakte Auslegungsspielräume lassen. Auch Rückmeldungen der Wirtschaft im Zuge der Erarbeitung des Referentenentwurfs lassen den Schluss zu, dass eine weitere Konkretisierung des Erheblichkeitskriteriums im Rahmen einer Rechtsverordnung sinnvoll ist. Da hierzu bis Oktober 2024 auch ein Durchführungsrechtsakt der Europäischen Kommission geplant ist, sollte jedoch von weitergehenden Konkretisierungen auf Gesetzesebene Abstand genommen werden. Dies würde sonst zu Unklarheiten bzw. Missverständnissen für die Rechtsanwender führen, wenn die Bestimmungen im BSI-Gesetz stünden, aber ggf. aufgrund anderweitiger Festlegungen im Durchführungsrechtsakt ungültig wären. Durch die Möglichkeit, mit einer nachgelagerten Rechtsverordnung hier auch ergänzend zum Durchführungsrechtsakt weitergehende Klarstellungen zu geben, ergibt sich dieses Problem nicht.

Zu Absatz 6

Absatz 6 sieht die Möglichkeit einer Verkürzung der in § 61 Absatz 3 Satz 5 geregelten Frist im Wege einer Rechtsverordnung vor. Sollte etwa der Gesundheitssektor vermehrt zum Ziel von Cyberkriminellen werden oder sollten durch neue Schwachstellen erfolgreiche Angriffe wahrscheinlicher werden, kann so auf die geänderte Cyberbedrohungslage reagiert werden.

Zu § 57 (Einschränkung von Grundrechten)

Die Vorschrift führt den bisherigen § 11 fort.

Zu § 58 (Berichtspflichten des Bundesamtes)

In der Überschrift erfolgt eine klarstellende Ergänzung, dass Berichtspflichten sich stets auf das Bundesamt beziehen. Im Gegensatz dazu beziehen sich Meldepflichten stets auf Einrichtungen.

Zu Absatz 1

Absatz 1 führt den bisherigen § 13 Absatz 1 fort.

Zu Absatz 2

Absatz 2 führt den bisherigen § 13 Absatz 2 fort.

Zu Absatz 3

Absatz 3 führt den bisherigen § 13 Absatz 3 fort.

Zu Absatz 4

Absatz 7 dient der Umsetzung von Artikel 23 Absatz 9 der NIS-2-Richtlinie. Für die zu übermittelnden Informationen gelten die Ausnahmen des Artikel 2 Absatz 11 (nationale, öffentliche Sicherheit oder Verteidigung) und Absatz 13 (Vertraulichkeit von Geschäftsgeheimnissen) der NIS-2-Richtlinie. Der Begriff der Anonymisierung ist im Sinne der Pseudonymisierung gemäß Artikel 4 Nummer 5 der Verordnung (EU) 2016/679 auszulegen. 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

Zu Nummer 1

Nummer 1 dient der Umsetzung von Artikel 3 Absatz 5 Buchstabe a NIS-2-Richtlinie.

Zu Nummer 2

Nummer 2 dient der Umsetzung von Artikel 3 Absatz 5 Buchstabe b NIS-2-Richtlinie.

Zu Teil 7 (Aufsicht)

Zu § 59 (Zuständigkeit des Bundesamtes)

Die Vorschrift dient der Umsetzung von Artikel 8 Absatz 1 bis 2, Artikel 26 Absatz 1 der NIS-2-Richtlinie. Die Zuständigkeit für wichtige und besonders wichtige Einrichtungen bestimmt sich nach dem Niederlassungsprinzip. Die Zuständigkeit für Betreiber kritischer Anlagen bestimmt sich nach Belegenheitsprinzip hinsichtlich der jeweiligen kritischen Anlagen.

Zu § 60 (Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten)

Zu Absatz 1

Absatz 1 dient der Umsetzung von Artikel 26 Absatz 1 Buchstabe b der NIS-2-Richtlinie.

Zu Absatz 2

Absatz 2 dient der Umsetzung von Artikel 26 Absatz 2 der NIS-2-Richtlinie.

Zu Absatz 3

Absatz 3 dient der Umsetzung von Artikel 26 Absatz 3 der NIS-2-Richtlinie. Vertreter kann eine in der Europäischen Union niedergelassene natürliche oder juristische Person sein, die ausdrücklich benannt wurde, um im Auftrag einer Einrichtung, die nicht in der Europäischen Union niedergelassen ist, zu handeln, und an die sich das Bundesamt in Fragen der der Pflichten der benennenden Einrichtung nach diesem Gesetz wenden kann.

Zu Absatz 4

Absatz 4 dient der Umsetzung von Artikel 26 Absatz 4 der NIS-2-Richtlinie.

Zu Absatz 5

Absatz 5 dient der Umsetzung von Artikel 26 Absatz 5 der NIS-2-Richtlinie.

Zu § 61 (Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen)

Zu Absatz 1

Die Vorschrift dient der Umsetzung von Artikel 32 sowie Artikel 31 Absatz 1 in Verbindung mit Artikel 20 Absatz 2 der NIS-2-Richtlinie. Da eine regelmäßige Nachweispflicht für die Umsetzung von Risikomanagementmaßnahmen ausschließlich für Betreiber kritischer Anlagen gilt, ist vorgesehen, dass das Bundesamt die hier vorgesehenen Aufsichtsmaßnahmen in Bezug auf einzelne Einrichtungen ausüben kann. Demnach ist das Bundesamt unter Anderem befugt, Einrichtungen zu verpflichten, Audits, Prüfungen oder Zertifizierungen von unabhängigen Stellen durchführen zu lassen. Auch ohne verpflichtend durchzuführende Audits, Prüfungen oder Zertifizierungen kann das Bundesamt von einzelnen Einrichtungen Nachweise über die Erfüllung einzelner oder aller Anforderungen nach den §§ 30, 31 und 32 verlangen. Sofern durch die Einrichtung keine Audits, Prüfungen oder Zertifizierungen durchgeführt wurden, kann das Bundesamt hiernach auch andere Nachweisunterlagen verlangen. Hierzu gehören beispielsweise unternehmenseigene Richtlinien und Dokumentationen, Berichte oder Selbsterklärungen. Das Bundesamt kann ferner die Erfüllung der Schulungspflicht (§ 38 Absatz 3) überprüfen.

Gemäß den Anforderungen der NIS-2-Richtlinie ist es bei der Ausübung dieser Aufsichtsmaßnahmen in Bezug auf besonders wichtige Einrichtungen nicht erforderlich, dass dem Bundesamt Hinweise oder Informationen vorliegen, welche die Annahme rechtfertigen, dass eine Einrichtung die Anforderungen der §§ 30, 31 und 32 nicht oder nicht richtig umgesetzt hat. Stattdessen hat das Bundesamt bei der Auswahl der Einrichtungen im Sinne einer Priorisierung die in Absatz 4 genannten Kriterien zu berücksichtigen. Der Ermessensspielraum des Bundesamtes bei der Auswahl von Einrichtungen ist im Sinne der NIS-2-Richtlinie entsprechend weit auszulegen. Die in Absatz 4 genannten Kriterien dienen insoweit der Priorisierung, in Bezug auf welche Einrichtungen die Aufsichtsmaßnahmen prioritär angewendet werden sollten. Die in Absatz 4 genannten Kriterien eignen sich dagegen nicht zum Ausschluss, beispielsweise um zu begründen, dass bestimmte Aufsichtsmaßnahmen nicht auf einzelne Einrichtungen anzuwenden sein sollten, da sie zum Beispiel besonders klein sind oder die Eintrittswahrscheinlichkeit

von Sicherheitsvorfällen als niedrig eingeschätzt wird. Denn nach den Anforderungen der NIS-2-Richtlinie muss das Bundesamt befugt sein, die hier genannten Aufsichtsmaßnahmen in Bezug auf alle besonders wichtige Einrichtungen ausüben zu können.

Die Zuständigkeit des Bundesamtes für Einrichtungen der Bundesverwaltung richtet sich nach den Befugnissen des Bundesamtes in Teil 2 Kapitel 1 sowie Teil 3.

Zu Absatz 6

Absatz 6 dient der Umsetzung von Artikel 32 Absatz 4 Buchstabe b der NIS-2-Richtlinie.

Zu Absatz 7

Absatz 7 dient der Umsetzung von Artikel 32 Absatz 4 Buchstabe c, d und f der NIS-2-Richtlinie. Die Nachweise können durch dokumentierte IT-Sicherheitskonzepte, Prozessbeschreibungen, Richtlinien, Daten, Dokumente und sonstige Informationen, die für die Bewertung der von der betreffenden Einrichtung ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit erforderlich sind.

Zu Absatz 8

Absatz 8 Satz 1 dient der Umsetzung von Artikel 32 Absatz 4 Buchstabe e der NIS-2-Richtlinie. Absatz 8 Satz 2 dient der Umsetzung von Artikel 32 Absatz 4 Buchstabe h der NIS-2-Richtlinie.

Zu Absatz 9

Absatz 9 dient der Umsetzung von Artikel 32 Absatz 5 Unterabsatz 1 der NIS-2-Richtlinie. Die nationale Umsetzung der Durchsetzungsmaßnahmen Aussetzung (Satz 2 Nummer 1) und Untersagung (Satz 2 Nummer 2) ist aufgrund der jeweiligen Schwere der Grundrechtseingriffe im Einklang mit Artikel 32 Absatz 5 Unterabsatz 2 der NIS-2-Richtlinie an zusätzliche Tatbestandsvoraussetzungen geknüpft. Die Anwendung dieser beiden Durchsetzungsmaßnahmen kommt aus Gründen der Verhältnismäßigkeit grundsätzlich nur als letztes Mittel in Betracht. Mithin sind mildere, gleich wirksame Mittel zur Durchsetzung einer Anordnung des Bundesamtes vorher erfolglos auszuschöpfen, insbesondere solche der Verwaltungsvollstreckung nach dem VwVG. Ist dem Bundesamt oder der zuständigen Aufsichtsbehörde die Unzuverlässigkeit der Geschäftsleitung bereits aus vorherigen Verwaltungsverfahren bekannt, so kann sich die erfolglose Ausschöpfung anderer Mittel vor einer Untersagung (Satz 2 Nummer 2) erübrigen. Dies dürfte insbesondere dann der Fall sein, wenn in vorherigen Verwaltungsverfahren nur die Untersagung (Satz 2 Nummer 2) zum Erfolg führte.

Die Tatbestandsvoraussetzung „wenn ein Zusammenhang mitzwischen Durchsetzungsmaßnahme und der Anordnung besteht“ soll sicherstellen, dass z. B. keine Genehmigung ausgesetzt wird, die nicht im Zusammenhang mit der durchzusetzenden informationssicherheitsrechtlichen Anordnung des Bundesamtes steht. Also etwa keine Genehmigung zur – allein physischen – Lagerungen von Gefahrstoffen ausgesetzt wird, weil die Einrichtung die Daten ihrer Kunden einer Tätigkeit im Anwendungsbereich des § 28 Absatz 1 oder 2 ohne IT-Sicherungen speichert.

Zu Absatz 10

Absatz 10 dient der Umsetzung von Artikel 32 Absatz 9 der NIS-2-Richtlinie.

Zu Absatz 11

Absatz 11 dient der Umsetzung von Artikel 35 der NIS-2-Richtlinie und trägt dem Umstand Rechnung, dass bei Verstößen gegen die dort adressierten Pflichten auch Verstöße gegen andere unionsrechtliche Vorgaben vorliegen können. Auch wenn das Bundesamt im Rahmen seiner Kompetenzen technische und keine datenschutzrechtlichen Kontrollen vornimmt, soll damit sichergestellt werden, dass aufgrund der engen Verbindung von Datensicherheit und Datenschutz bei zufällig im Rahmen der Prüfung aufgefundenen, augenscheinlichen Verstößen gegen datenschutzrechtliche Regelungen die zuständigen Behörden unverzüglich in Kenntnis gesetzt werden und eine Prüfung durchführen können. Die NIS-2-Richtlinie bezeichnet dabei den Bereich der Verstöße, die eine Verletzung personenbezogener Daten zur Folge haben können, sowohl bei nicht ausreichenden Risikomanagementmaßnahmen im Bereich der Cybersicherheit, als auch bei einem Zurückbleiben hinter den gesetzlich vorgegebenen Berichtspflichten. Die Unterrichtung ist unverzüglich nach der technischen Kontrolle gegenüber der nach Artikel 55 oder 56 der Verordnung (EU) 2016/679 zuständigen Aufsichtsbehörde für den Datenschutz vorzunehmen.

Zu Absatz 12

Absatz 12 regelt in Umsetzung von Artikel 37 der NIS-2-Richtlinie Einzelheiten zur Amtshilfe für zuständige Aufsichtsbehörden in anderen Mitgliedstaaten der Europäischen Union, wenn Einrichtungen Dienstleistungen in mehreren Mitgliedstaaten erbringen, und hierfür beispielsweise IT-Systeme, Komponenten oder Prozesse eingesetzt werden, die sich in Deutschland befinden.

Zu § 62 (Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen)

Die Vorschrift dient der Umsetzung von Artikel 33 der NIS-2-Richtlinie. Für wichtige Einrichtungen sind gemäß dieser Vorschrift grundsätzlich die gleichen Aufsichtsmaßnahmen des Bundesamtes vorgesehen, wie in § 61 für besonders wichtige Einrichtungen. Jedoch gilt für wichtige Einrichtungen als Voraussetzung zur Ausübung dieser Aufsichtsmaßnahmen, dass Tatsachen die Annahme rechtfertigen, dass eine wichtige Einrichtung die gesetzlichen Verpflichtungen nicht oder nicht richtig umgesetzt hat.

Zu § 63 (Verwaltungszwang)

Die Vorschrift dient der Umsetzung von Artikel 34 Absatz 6 der NIS-2-Richtlinie.

Zu § 64 (Zuwiderhandlungen durch Institutionen der sozialen Sicherung)

Die Vorschrift führt den bisherigen § 14a fort.

Zu Teil 8 (Bußgeldvorschriften)

Zu § 65 (Bußgeldvorschriften)

Die Vorschrift führt den bisherigen § 14 fort. Die Bußgeldtatbestände wurden insbesondere entsprechend der Vorgaben der NIS-2-Richtlinie ergänzt und der Bußgeldrahmen angepasst.

Zu Absatz 1

Absatz 1 führt den bisherigen § 14 Absatz 1 fort. Absatz 1 sanktioniert, wie bisher, Fälle, in denen die von den Betreibern Kritischer Anlagen zu erbringenden Nachweisen, Nachforderungen, Auskünfte und Kennzahlen vorsätzlich nicht richtig oder nicht vollständig erbracht werden.

Zu Absatz 2

Mit Absatz 2 Nummer 1 Buchstaben a, b, c und d werden Fälle von Zuwiderhandlungen gegen vollziehbare Anordnungen erfasst. Eine separate Aufzählung soll, aufgrund unterschiedlicher Schwere der Zuwiderhandlungen, eine entsprechende Bebußung in unterschiedlicher Höhe ermöglichen.

Zu Nummer 1

Zu Buchstabe a

Der genannte § 11 Absatz 6 führt den bisherigen § 5b Absatz 6, § 16 Absatz 1 Satz 1 den bisherigen § 7c Absatz 1 Satz 1, § 17 den bisherigen § 7d und § 39 Absatz 1 Satz 5 den bisherigen § 8a Absatz 3 Satz 5 fort.

Zu Buchstabe b

Dieser Bußgeldtatbestand führt den bisherigen aus § 7a Absatz 2 Satz 1 bebußten Tatbestand fort.

Zu Buchstabe c

§ 8c Absatz 4 Satz 1 entfällt, da die Kategorie „Anbieter digitaler Dienste“ in den neuen Einrichtungskategorien aufgeht.

Mit Variante 1 wurde ein neuer Bußgeldtatbestand geschaffen, der die Weigerung der Herausgabe notwendiger Informationen zur Bewältigung einer Störung bei Betreibern kritischer Anlagen ahnden soll.

Ebenfalls werden neue Bußgeldtatbestände entsprechend der Vorgaben nach Artikel 32 Absatz 4 Buchstabe i NIS-2-Richtlinie für besonders wichtige und nach Artikel 33 Absatz 4 Buchstabe h NIS-2-Richtlinie für wichtige Einrichtungen ergänzt:

Es wurde entsprechend der Vorgaben der NIS-2-Richtlinie nach Artikel 32 Absatz 4 Buchstabe d für besonders wichtige sowie nach Artikel 33 Absatz 4 Buchstabe d für wichtige Einrichtungen – umgesetzt in § 62 Absatz 3 Satz 1, in Verbindung mit § 63 – eine Bebußung aufgenommen: Dies gilt für Zuwiderhandlungen gegen Anweisungen innerhalb einer bestimmten Frist sicherzustellen, dass Risikomanagementmaßnahmen im Bereich der Cybersicherheit mit Artikel 21 im Einklang stehen, bzw. die in Artikel 23 festgelegten Berichtspflichten erfüllt werden.

§ 61 Absatz 6 Satz 1 oder 3, auch in Verbindung mit § 62 sieht eine Bebußung bei Verstößen besonders wichtiger und wichtiger Einrichtungen gegen Anordnungen nach § 62 Absatz 6 vor. Dieser bestimmt, dass das Bundesamt gegenüber besonders wichtigen und wichtigen Einrichtungen Anweisungen in Bezug auf Maßnahmen anordnen kann, die zur Verhütung oder Behebung eines Sicherheitsvorfalls oder eines Mangels erforderlich sind. Ferner kann das Bundesamt die Berichterstattung den nach Satz 1 angeordneten Maßnahmen verlangen. Es werden hiermit Vorgaben aus Artikel 32 Absatz 4 Buchstabe i und Artikel 33 Absatz 4 Buchstabe h NIS-2-Richtlinie umgesetzt. Demnach ist eine Bebußung bei Zuwiderhandlung nach Artikel 32 Absatz 4 Buchstabe b bzw. Artikel 33 Absatz 4 Buchstabe b vorzunehmen.

Es wird ein Zuwiderhandeln gegen eine verbindliche Anweisung nach § 61 Absatz 7 Satz 1 oder 3, jeweils in Verbindung mit § 62 geahndet. Mit der Schaffung dieses Bußgeldtatbestandes werden Artikel 32 Absatz 4 Buchstabe i in Verbindung mit Buchstabe c und f, und Artikel 33 Absatz 4 Buchstaben h in Verbindung mit Buchstabe c und f der NIS-2-Richtlinie umgesetzt, die eine respektive Bebußung von wichtigen und besonders wichtigen Einrichtungen vorsehen.

§ 62 Absatz 8 oder auch in Verbindung mit § 62 sehen respektive für besonders wichtige und wichtige Einrichtungen vor, dass das Bundesamt sie anweisen kann, die natürlichen oder juristischen Personen, für die sie Dienste erbringen oder Tätigkeiten ausüben und die potenziell von einer erheblichen Cyberbedrohung betroffen sind, über die Art der Bedrohung und mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten, die von diesen natürlichen oder juristischen Personen als Reaktion auf diese Bedrohung ergriffen werden können. Zudem kann es wichtige und besonders wichtige Einrichtungen anweisen, Informationen zu Verstößen gegen diese Richtlinie nach bestimmten Vorgaben öffentlich bekannt zu machen. Mit der Schaffung dieses Bußgeldtatbestandes wird den Anforderungen aus Artikel 32 Absatz 4 Buchstabe i in Verbindung mit Buchstaben e und g der NIS-2-Richtlinie sowie Artikel 33 Absatz 4 Buchstabe h in Verbindung mit Buchstaben e und g nachgekommen.

Zu Buchstabe d

Es wird mit Buchstabe d entsprechend der Vorgaben der NIS-2-Richtlinie ein neuer Bußgeldtatbestand aufgenommen.

§ 35 Absatz 1 Satz 1 sieht vor, dass das Bundesamt im Falle eines erheblichen Sicherheitsvorfalls besonders wichtige Einrichtungen und wichtige Einrichtungen anweisen kann, die Empfänger ihrer Dienste unverzüglich über diesen erheblichen Sicherheitsvorfall zu unterrichten, der die Erbringung des jeweiligen Dienstes beeinträchtigen könnte. Artikel 34 Absatz 4 der NIS-2-Richtlinie setzt eine Bebußung des Artikel 23 Absatz 1 NIS-2-Richtlinie fest.

Eine Bebußung von Zuwiderhandlungen gegen § 36 Absatz 2 Satz 1 sieht Artikel 34 Absatz 7 der NIS-2-Richtlinie vor.

Zu Nummer 2

In Nummer 2 wurden die Verweise angepasst. Der bisherige Bußgeldtatbestand schuf eine Sanktionsmöglichkeit dafür, dass entgegen § 8a Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig getroffen wird. Dieser sah vor, dass angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu getroffen werden, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.

Der Verweis wurde angepasst und bezieht sich nunmehr auf Verstöße gegen den neugeschaffenen § 30 (Risikomanagementmaßnahmen), der § 8a Absatz 1 Satz 1 ersetzt. Zudem wird hiermit den Anforderungen der NIS-2-

Richtlinie (Artikel 34 Absatz 4 in Verbindung mit Artikel 21 NIS-2-Richtlinie) nach einer Bebußung bei Verstößen gegen Risikomanagementmaßnahmen nachgekommen.

Zu Nummer 3

In Nummer 3 wurde ein neuer Bußgeldtatbestand geschaffen, der Verstöße gegen § 30 Absatz 1 Satz 3 (die Einhaltung der Dokumentationspflicht) ahndet. Es wird hiermit den Anforderungen der NIS-2-Richtlinie, Artikel 34 Absatz 4 in Verbindung mit Artikel 21 NIS-2-Richtlinie, hier Absatz 4, Rechnung getragen.

Zu Nummer 4

§ 32 Absatz 1 Satz 1 definiert die Meldepflichten für besonders wichtige und wichtige Einrichtungen (Umsetzung des Artikels 23 der NIS-2-Richtlinie). Es wird hiermit die Anforderung nach einer Bebußung aus Artikel 34 Absatz 4 in Verbindung mit Artikel 23 Absatz 4 NIS-2-Richtlinie umgesetzt.

§ 8c und 8f entfallen, da die Regelungsadressaten in den neuen Einrichtungskategorien aufgehen

Zu Nummer 5

Nummer 5 sieht eine Bebußung vor, wenn entgegen § 32 Absatz 2 Satz 2 eine Abschlussmeldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gemacht wird. Es wird hiermit Artikel 34 Absatz 4 in Verbindung mit Artikel 23 Absatz 4 Buchstabe e NIS-2-Richtlinie umgesetzt.

Zu Nummer 6

Nach Nummer 6 handelt ordnungswidrig, wer eine Angabe oder eine Änderung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt. § 8b Absatz 3 Satz 1 wird durch § 33 Absatz 1 und 2 ersetzt und auf die neugeschaffenen Einrichtungskategorien angepasst: Absatz 1 definiert die Registrierungspflichten für wichtige und besonders wichtige Einrichtungen, Absatz 2 die Anforderungen für Betreiber kritischer Anlagen.

§ 8f Absatz 5 Satz 1 entfällt, da dieser in den neuen Einrichtungskategorien aufgeht. Ein Ersatz erfolgt jedoch durch § 34 Absatz 1 und 2, der Registrierungspflichten für andere Einrichtungsarten vorsieht.

Zu Nummer 7

Nummer 7 sieht eine Bebußung für Betreiber kritischer Anlagen vor. Diese haben nach § 33 Absatz 2 Satz 2 sicherzustellen, dass sie über ihre in Absatz 1 genannten Kontaktdaten jederzeit erreichbar sind.

Zu Nummer 8

In Nummer 8 wurde ein neuer Bußgeldtatbestand geschaffen. § 34 Absatz 2 sieht vor, dass Änderungen der nach § 34 Absatz 1 zu übermittelnden Angaben unverzüglich, spätestens jedoch zwei Wochen ab dem Zeitpunkt der Änderung dem Bundesamt zu übermitteln sind.

Eine Sanktionierung ist erforderlich, um eine bessere Durchsetzbarkeit der Registrierungspflichten zu ermöglichen. Zweck dieser ist es, die unverzügliche Weiterleitung wichtiger Sicherheitsinformationen an betroffene Betreiber sicherzustellen. So kann bei Störungen und sonstigen IT-Sicherheitsinformationen, die für die Verfügbarkeit und Funktionsfähigkeit der Betreiber maßgeblich sind, ein verlässlicher, beständiger und schneller Informationsfluss gewährleistet werden. Nur durch eine Erweiterung der Pflicht zur zeitnahen Mitteilung von Änderungen kann diese effektiv gewährleistet werden.

Zu Nummer 9

Eine Bebußung von Zuwiderhandlungen gegen § 35 Absatz 2 Satz 1, auch in Verbindung mit Satz 2 sieht Artikel 34 Absatz 4 in Verbindung mit Artikel 23 Absatz 2 NIS-2 Richtlinie vor.

Zu Nummer 10

Hier wurde der Verweis zur Aktualisierung der Nachweispflichten (siehe bereits unter Absatz 1) angepasst: Hier bestimmt § 39 Absatz 1 Satz 1 die für kritische Einrichtungen.

Zu Nummer 11

Nummer 11 sanktioniert, sofern nach § 49 Absatz 3 Satz 1 dort genannte Vorgaben oder Verfahren nicht vorgehalten werden. Mit den Nummern 11, 12 und 13 wird die in Artikel 36 der NIS-2-Richtline vorgesehene Mög-

lichkeit, die Nichtbefolgung der Vorgaben für Maßnahmen auch für Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister zu sanktionieren, umgesetzt. Das schafft eine Durchsetzbarkeit der gesetzlich festgelegten Verpflichtung, eine Datenbank über die Domains und ihre Domain-Namen-Registrierungsdaten vorzuhalten und auf berechtigten Antrag diese Daten für Anfragende zugänglich machen zu können.

Zu Nummer 12

Nummer 12 bestimmt eine Bebußung, wenn entgegen § 49 Absatz 3 Satz 2 oder Absatz 4 dort genannte Vorgaben, Verfahren oder Daten nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig zugänglich gemacht werden.

Zu Nummer 13

Nummer 13 nimmt eine Bebußung vor, wenn entgegen § 50 Absatz 1 Satz 1 ein Zugang nicht oder nicht rechtzeitig gewährt wird.

Zu Nummer 14

Mit Nummer 14 wurde ein neuer Bußgeldtatbestand geschaffen: § 52 Absatz 2 Satz 4 bestimmt, dass ein Zertifikat nach Satz 1 nur dann für ein Produkt, eine Leistung, eine Person oder einen IT-Sicherheitsdienstleister verwendet werden darf, wenn das Bundesamt ein entsprechendes Zertifikat erteilt hat und dieses nicht aufgehoben wurde oder auf andere Weise ungültig geworden ist. Eine Ahndung im Rahmen eines Bußgeldes bei Verwendung entgegen angeführter Voraussetzungen ist aufgrund des Missbrauchspotentials sowie damit einhergehender unbefugter Nutzung erforderlich; auch da hier keine effektive Verwaltungszwangsmöglichkeit besteht. Ebenfalls wird eine Bebußung für Fälle vorgesehen, in denen entgegen § 53 Absatz 1 Satz 4 eine Erklärung nach § 53 Absatz 1 Satz 2 verwendet wird.

Bei § 54 Absatz 6 Satz 2 handelt es sich um einen neuen Bußgeldtatbestand, der das Verwenden widerrufener Cybersicherheitszertifikate oder für ungültig erklärte EU-Konformitätserklärungen bebußt. Eine Notwendigkeit für die Ahndung ergibt sich aus vergleichbarem Missbrauchspotential, Folgen einer unbefugten Nutzung und der fehlenden effektiven Verwaltungszwangsmöglichkeit.

§ 55 Absatz 4 Satz 1 führt den bisherigen § 9c Absatz 4 Satz 1 fort.

Zu Nummer 15

Mit § 53 wurde die Möglichkeit geschaffen, selbst eine Konformitätserklärung nach den Vorgaben des Bundesamtes und unter deren Aufsicht abzugeben. Obwohl der Aussteller dabei selbst die Verantwortung für seine Konformitätserklärung trägt, besteht ein Vertrauen des Marktes in die Möglichkeiten des Bundesamtes nach § 53, gegen erkannte Abweichungen von den zugrundeliegenden Anforderungen vorzugehen. Dieses Vertrauen setzt aber voraus, dass das Bundesamt auch gegen solche Akteure vorgehen kann, die über keine gültige Konformitätserklärung im Sinne des § 53 verfügen und nur bewusst oder fahrlässig (beispielsweise durch das Verwenden eines entsprechenden Kennzeichens) vorgeben, sich den Anforderungen des § 53 unterworfen zu haben. § 53 Absatz 3 Satz 2 sieht eine Bebußung vor, wenn ohne eine Befugniserteilung als Konformitätsbewertungsstelle gehandelt wird

§ 54 Absatz 2 Satz 2 führt den bisherigen § 9a Absatz 2 Satz 2 fort. Es wurde eine Ergänzung vorgenommen: Nach § 53 Absatz 3 Satz 2 bedarf es zur Konformitätsbewertung, soweit eine Akkreditierung der in der Technischen Richtlinie durch das Bundesamt vorgesehen wurde, einer Befugniserteilung. Führt eine Stelle Konformitätsbewertungstätigkeiten durch, ohne eine solche Befugnis zu haben, gefährdet dies die Vergleichbarkeit der Konformitätsbewertungs-verfahren und in der Folge das besondere Vertrauen in die Konformitätserklärung, das durch die Vorgabe erzeugt werden sollte.

Zu Nummer 16

Der bisherige § 14 Absatz 2 Nummer 8 mit einer Bußgeldahndung für Verstöße gegen § 8c Absatz 1 Satz 1 wurde gestrichen, da dieser in den neuen Einrichtungskategorien aufgeht.

Die Vorschrift sieht eine Bebußung bei besonders wichtigen Einrichtungen vor (§ 61 Absatz 5 Satz 3). Sofern das Betreten eines dort genannten Raums nicht gestattet, eine dort genannte Unterlage nicht oder nicht rechtzeitig vorlegt, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder Unterstützung nicht oder nicht rechtzeitig gewährt.

Zu Absatz 3

Absatz 3 führt den bisherigen § 14 Absatz 3 fort.

Zu Absatz 4

Zu Nummer 1

Nummer 1 führt den bisherigen § 14 Absatz 4 Nummer 1 fort.

Zu Nummer 2

Nummer 2 führt den bisherigen § 14 Absatz 4 Nummer 2 fort.

Zu Absatz 5

Absatz 5 regelt die Höhe der jeweiligen Bußgelder. Das bisherige Stufensystem wurde beibehalten, wobei die Stufen angepasst wurden. Die Stufen sind auf den Werten 10 bzw. 7 Millionen, (höchste Stufe), 2 Millionen Euro (zweite Stufe), 1 Millionen (dritte Stufe), 500.000 Euro (vierte Stufe) und 100.000 Euro (fünfte Stufe) angesetzt. Vorgaben aus Artikel 34 NIS-2-Richtlinie bedingen Modifizierungen im Rahmen von Umsatzregelungen.

Zu Nummer 1

Auf höchster Stufe sind Verstöße gegen Absatz 2 Nummer 1 Buchstabe d, Nummer 2 bis 5 sowie Nummer 9 einzuordnen. In diesen Nummern werden Verstöße gegen Risikomanagementmaßnahmen und Meldepflichten bebußt (höchste Bußgeldstufe).

Zu Buchstabe a

Für Verstöße gegen Absatz 2 Nummer 1 Buchstabe d, Nummern 2 bis 5 sowie Nummer 9 bei besonders wichtigen Einrichtungen traf Artikel 34 Absatz 4 NIS-2-Richtlinie dezidierte Vorgaben: 10 Millionen Euro oder mindestens 2 Prozent des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört.

Zu Buchstabe b

Für Verstöße gegen Absatz 2 Nummer 1 Buchstabe d, Nummer 2 bis 5 sowie 9 bei wichtigen Einrichtungen sieht Artikel 34 Absatz 5 der NIS-2-Richtlinie eine Höhe von 7 Millionen Euro oder mindestens 1,4 Prozent des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört, vor.

Zu Nummer 2

Auf zweiter Stufe (2 Millionen Euro) sind Verstöße gegen Absatz 2 Nummer 1 Buchstabe a angesiedelt. Es wurde keine Veränderung der Bußgeldhöhe vorgenommen; durch den übernommenen Verweis auf § 30 Absatz 2 Satz 3 OwiG in § 14 Absatz 5 alte Fassung ist eine Modifizierung in Form einer Verzehnfachung möglich.

Zu Nummer 3

Auf dritter Stufe (eine Millionen Euro) sind Verstöße gegen Absatz 1 und Absatz 2 Nummer 10 einzuordnen: Es tritt keine Veränderung der Bußgeldhöhe ein, der frühere Verweis auf § 30 Absatz 2 Satz 3 OwiG, wurde übernommen.

Zu Nummer 4

Für die vierte Stufe wurde ein Wert von 500.000 Euro angesetzt.

Für einen Verstoß gegen Absatz 2 Nummer 1 Buchstabe c (§ 18) ergab sich hierbei keine Veränderung. Verstöße gegen Aufsichts- und Durchsetzungsmaßnahmen nach § 63 Absatz 3 Satz 1, Absatz 6 Satz 1 und3 und Absatz 7 Satz 1 und 3 und Absatz 8, jeweils auch in Verbindung mit § 64, wurden aufgrund Ihrer Bedeutung ebenfalls auf dieser Stufe aufgenommen.

Auf dieser Stufe wurde ebenfalls ein Verstoß gegen Absatz 2 Nummer 6 und 8 aufgenommen. Bei diesem handelt es sich um einen Verstoß gegen die Registrierungspflichten.

Verstöße gegen Absatz 2 Nummer 11 bis 13 für Nichtbefolgung der Vorgaben für Maßnahmen auch für Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister fallen ebenfalls unter diese Einstufung.

Für einen Verstoß gegen Absatz 2 Nummer 14 Variante 4 ergab sich keine Veränderungen in der Bußgeldhöhe.

Auf der vierten Stufe wurden zudem Verstöße gegen den neueingeführten Absatz 2 Nummer 14 Variante 1, 2 und 3aufgenommen. Bei der Einstufung wurde sich an der Bußgeldhöhe von Nummer 14 Variante 4 und Nummer 15, die in der vormaligen und jetzigen Fassung ebenfalls in dieser Höhe angesiedelt sind und im Unrechtsgehalt eine Entsprechung finden, orientiert.

Für Absatz 4 ergaben sich keine Veränderungen.

Zu Nummer 5

Als niedrigste Stufe wurde die frühere 100.000-Euro-Stufe übernommen.

Hierbei ergaben sich für Verstöße gegen Absatz 2 Nummer 1 Buchstabe b, Nummer 7, 16 und Absatz 3 in der Bußgeldhöhe keine Veränderungen.

Zu Absatz 6

Absatz 6 schafft die von Artikel 34 Absatz 4 NIS-2-Richtlinie vorgesehene Grundlage, zur Verhängung eines Bußgeldes in Höhe von mindestens 2 Prozent des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört bei besonders wichtigen Einrichtungen, sofern ein Verstoß gegen Risikomanagementmaßnahmen oder Meldepflichten vorliegt.

Zu Absatz 7

Absatz 7 schafft die von Artikel 34 Absatz 5 der NIS-2-Richtlinie vorgesehene Grundlage, zur Verhängung eines Bußgeldes in Höhe von mindestens 1,4 Prozent des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört bei wichtigen Einrichtungen, sofern ein Verstoß gegen Risikomanagementmaßnahmen oder Meldepflichten vorliegt.

Zu Absatz 8

Absatz 8 konkretisiert die Bedeutung des in Absatz 6 und 7 verwendeten Begriffs des Jahresumsatzes.

Zu Absatz 9

Absatz 9 führt den bisherigen § 14 Absatz 6 fort.

Zu Absatz 10

Absatz 10 dient der Umsetzung von Artikel 35 Absatz 2 der NIS-2-Richtlinie.

Zu Anlage 1 (Sektoren besonders wichtiger und wichtiger Einrichtungen)

Die Anlage dient der Umsetzung von Anhang I der NIS-2-Richtlinie.

Zur Definition von Gesundheitsdienstleister unter Nummer 4.1.1: Die NIS-2-Richtlinie stellt für die einzubeziehenden Einrichtungskategorien in Anhang 1 Nummer 5 auf Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie (EU) 2011/24 des Europäischen Parlaments und des Rates (Patientenmobilitätsrichtlinie) ab. Gemäß Artikel 3 Absatz 3 Buchstabe a der genannten Richtlinie fallen Einrichtungen der Langzeitpflege, deren Ziel darin besteht, Personen zu unterstützen, die auf Hilfe bei routinemäßigen, alltäglichen Verrichtungen angewiesen sind, nicht in den Anwendungsbereich der EU-Patientenmobilitätsrichtlinie. Daher gelten Einrichtungen der Langzeitpflege nicht als Gesundheitsdienstleister im Sinne des vorliegenden Gesetzes.

Zu Anlage 2 (Sektoren wichtiger Einrichtungen)

Die Anlage dient der Umsetzung von Anhang II der NIS-2-Richtlinie. Die in den Nummern 3.1.1 und 5.2.1 bis 5.6.1 enthaltenen Verweise auf die NACE Rev. 2 („NACE-Nummern“) sind identisch mit denen der Klassifikation der Wirtschaftszweige, Ausgabe 2008 („WZ-Nummern“).

Zu Artikel 2 (Änderung des BND-Gesetzes)

Es handelt sich um eine Folgeänderung. Der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes wird angepasst.

Zu Artikel 3 (Änderung der Sicherheitsüberprüfungsfeststellungsverordnung)

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 4 (Änderung der Besonderen Gebührenverordnung des Bundesministeriums des Innern, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich)

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 5 (Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes)

Es handelt sich um eine Folgeänderung. Der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes wird angepasst.

Zu Artikel 6 (Änderung der Gleichstellungsbeauftragtenwahlverordnung)

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 7 (Änderung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme)

Die bis zum 1. Mai 2025 durchzuführende Evaluierung der übrigen Vorschriften des IT-SiG 2.0 erübrigt sich da diese in weiten Teilen im Zuge der NIS-2-Umsetzung geändert werden. Die unveränderten Vorschriften sind bereits durch dieses Gesetz bestätigt.

Zu Artikel 8 (Änderung der BSI-Zertifizierungs- und Anerkennungsverordnung)

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 9 (Änderung der BSI-IT-Sicherheitskennzeichenverordnung)

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 10 (Änderung des De-Mail-Gesetzes)

Es handelt sich um eine Folgeänderung. Der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes wird angepasst.

Zu Artikel 11 (Änderung des E-Government-Gesetz)

Löschung des Verweises auf das BSI-Gesetz wegen Wegfalls der Regelung zum IT-Rat im bisherigen § 12 BSI-Gesetz.

Zu Artikel 12 (Änderung der Passdatenerfassungs- und Übermittlungsverordnung)

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 13 (Änderung der Personalausweisverordnung)

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 14 (Änderung des Hinweisgeberschutzgesetzes)

Es handelt sich um Folgeänderungen. Die Kategorie der Anbieter digitaler Dienste des bisherigen § 2 Absatz 12 geht in den besonders wichtigen und wichtigen Einrichtungen auf Anhang 1 Nummer 6.1.4. (Cloud-Computing), Anhang 2 Nummer 6.1.1 (Online-Marktplätze) und Nummer 6.1.2 (Online-Suchmaschinen).

Zu Artikel 15 (Änderung der Kassensicherungsverordnung)

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 16 (Änderung des Atomgesetzes)

Es handelt sich um eine Folgeänderung. Der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes wird angepasst.

Zu Artikel 17 (Änderung des Energiewirtschaftsgesetzes)

Zu Nummer 1

Die Vorschrift wird ergänzt, da der durch die Bundesnetzagentur zu erstellende Sicherheitskatalog mindestens die in Umsetzung der NIS-2 Richtlinie in § 30 des BSI-Gesetzes genannten Risikomanagementmaßnahmen für besonders wichtige Einrichtungen enthalten muss.

Zu Nummer 2

Zu § 5c (IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz)

Die bisher in § 11 Absatz 1a – 1g EnWG verankerten Anforderungen an IT-Sicherheit der Anlagen und Netze werden in den neu eingeführten § 5c ausgegliedert und erweitert. Dies trägt dem Umstand Rechnung, dass Vorkehrungen zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme nicht nur durch Betreiber von Energieversorgungsnetzen, sondern auch durch Betreiber von Energieanlagen, die als Kritische Infrastruktur nach der BSI-KritisV bestimmt wurden, zu treffen sind. Darüber hinaus wird der Anwendungsbereich um die besonders wichtigen und wichtigen Einrichtungen, wie sie im BSI-Gesetz definiert wurden, erweitert, um damit die 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) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) im Energiebereich umzusetzen. Die Vereinheitlichung und Bündelung der cybersicherheitsrelevanten Anforderungen, die sich damit an alle im Energiebereich aktiven Akteure richten, wird eine homogene Einhaltung der IT-Sicherheitsstandards sicherstellen und dadurch die Resilienz gegen IT-Sicherheitsvorfälle der für die Energiewende benötigten Einrichtungen erhöhen.

Zu Absatz 1

Absatz 1 entspricht dem gestrichenen § 11 Absatz 1a. Entsprechend des Art. 21 Abs. 1 NIS-2-Richtlinie werden die Cybersicherheitsanforderungen auf alle Telekommunikations- und Datenverarbeitungssysteme, die die Betreiber zur Erbringung ihrer Dienste nutzen, erweitert. Die Anforderungen werden außerdem um eine Vorgabe zur Berücksichtigung erforderlicher Vorkehrungen bei der Beschaffung von Anlagengütern und Dienstleistungen erweitert. Diese sollen bei der Gewährleistung des Schutzes der Energieversorgungsnetze gegen Störungen und Bedrohungen der Telekommunikations- und elektronischen Datenverarbeitungssysteme berücksichtigt werden. Der Schutz der Einrichtungen gegen Angriffe setzt bereits auf Ebene der Auswahl und der Bestellung von Komponenten und Diensten ein, die insbesondere wegen der voranschreitenden Digitalisierung des Energiesystems Einfluss auf die Sicherheit der Systeme haben können. Zu den Vorkehrungen können insbesondere konkrete Anforderungen an die Zertifizierung von Anlagengütern und nachvollziehbare Herstellererklärungen gehören. Außerdem soll die Bundesnetzagentur für die Beteiligung der Öffentlichkeit sorgen, indem sie die betroffenen Betreiber und deren Verbände konsultiert, um dadurch die branchenspezifischen Anforderungen besser berücksichtigen zu können. Der IT-Sicherheitskatalog ist alle zwei Jahre auf dessen Aktualität zu prüfen. Weiterhin liegt der angemessene Schutz der Telekommunikations- und Datenverarbeitungssysteme nur dann vor, wenn die Anforderungen des IT-Sicherheitskataloges erfüllt sind.

Der Begriff „Regulierungsbehörde“ wird durch „Bundesnetzagentur“ ersetzt, um eine einheitliche Formulierung sicherzustellen.

Zu Absatz 2

Absatz 2 entspricht dem gestrichenen § 11 Absatz 1b. Der Anwendungsbereich wird jedoch entsprechend des Anwendungsbereichs der NIS-2-Richtlinie um die besonders wichtigen und wichtigen Einrichtungen, wie sie sich aus dem BSI-Gesetz ergeben, erweitert. Wie im Artikel 21 Absatz 1 NIS-2-Richtlinie vorgesehen, werden die Cybersicherheitsanforderungen auf alle Telekommunikations- und Datenverarbeitungssysteme, die die Betreiber zur Erbringung ihrer Dienste nutzen, erweitert. Die Anforderungen werden außerdem um eine Vorgabe zur Berücksichtigung erforderlicher Vorkehrungen bei der Beschaffung von Anlagengütern und Dienstleistungen erweitert. Diese sollen bei der Gewährleistung des Schutzes der Energieanlagen gegen Störungen und Bedrohungen der Telekommunikations- und elektronischen Datenverarbeitungssysteme berücksichtigt werden. Der Schutz der Einrichtungen gegen Angriffe setzt bereits auf Ebene der Auswahl und der Bestellung von Komponenten und Diensten ein, die insbesondere wegen der voranschreitenden Digitalisierung des Energiesystems Einfluss auf die Sicherheit der Systeme haben können. Zu den Vorkehrungen können insbesondere konkrete Anforderungen an die Zertifizierung von Anlagengütern und nachvollziehbare Herstellererklärungen gehören. Außerdem soll die Bundesnetzagentur für die Beteiligung der Öffentlichkeit sorgen, indem sie die betroffenen Betreiber und deren Verbände konsultiert, um dadurch die branchenspezifischen Anforderungen besser berücksichtigen zu können. Der IT-Sicherheitskatalog ist alle zwei Jahre auf dessen Aktualität zu prüfen. Weiterhin liegt der angemessene Schutz der Telekommunikations- und Datenverarbeitungssysteme nur dann vor, wenn die Anforderungen des IT-Sicherheitskataloges erfüllt sind.

Der Begriff „Regulierungsbehörde“ wird durch „Bundesnetzagentur“ ersetzt, um eine einheitliche Formulierung sicherzustellen.

Zu Absatz 3

Absatz 3 dient der Umsetzung des Art. 21 der NIS-2-Richtlinie und führt Vorgaben zur Ausgestaltung der IT-Sicherheitskataloge ein. Dabei sind auch in Anlehnung an die internationalen Normen in den IT-Sicherheitskatalogen Vorgaben zu Angriffserkennungssystemen zu machen. Dadurch wird die Zuständigkeit zur Überprüfung des Einsatzes von Angriffserkennungssystemen vom Bundesamt für Sicherheit in der Informationstechnik auf die Bundesnetzagentur übertragen.

In den Absätzen 1 und 2 werden die IT-Sicherheitskataloge entsprechend den Vorgaben der NIS-2-Richtlinie erweitert und werden alle Dienste, die die Betreiber erbringen, umfassen und nicht nur diejenige, die für den sicheren Netz- oder Anlagenbetrieb notwendig sind. Die Bundesnetzagentur ist befugt die Maßnahmen im Sinne der Verhältnismäßigkeit insbesondere mit Blick auf den sicheren Netz- oder Anlagenbetrieb abzustufen und kann dabei sowohl höhere als auch niedrigere Anforderungen an die IT-Sicherheitsmaßnahmen vorsehen. Die Bundesnetzagentur ist als die zuständige Behörde beauftragt die Einhaltung der Sicherheitsanforderungen zu überwachen und kann in den IT-Sicherheitskatalogen Bestimmungen zur Dokumentation der Einhaltung der Sicherheitsanforderungen treffen, dazu gehören beispielsweise Vorgaben zur Sicherheitsaudits, Prüfungen und Zertifizierungen. Die Bundesnetzagentur ist deshalb befugt im Sinne der Verhältnismäßigkeit abzustufen und strengere Nachweisvorgaben für den sicheren Netz- oder Anlagenbetrieb vorzusehen.

Da der Anwendungsbereich des Absatzes 2 von Betreiber kritischen Anlagen auf besonders wichtige und wichtige Einrichtungen erweitert wurde, wird die Bundesnetzagentur befugt in den IT-Sicherheitskatalogen Angaben zu deren Inkrafttreten zu machen. Dadurch wird für eine angemessene Übergangsfrist gesorgt.

Zu Absatz 4

Durch Absatz 4 wird die Überprüfung der Einhaltung der Sicherheitsstandards durch die Bundesnetzagentur neu strukturiert. Die Betreiber werden in Anlehnung an die Vorgaben des BSI-Gesetzes zur Vorlage der Dokumentation der Einhaltung der Sicherheitsanforderungen verpflichtet. Bei Bedarf kann die Bundesnetzagentur die Vorlage von Mängelbeseitigungspläne verlangen. Dadurch wird die Bundesnetzagentur über die während des Zertifizierungsverfahrens identifizierten Sicherheitsmängel informiert. Der Nachweis dient der Kontrolle und Überprüfung der von den Betreibern getroffenen Maßnahmen und damit der Einhaltung eines angemessenen Sicherheitsniveaus. Bei Sicherheitsmängeln kann die Bundesnetzagentur die Beseitigung der Sicherheitsmängel verlangen. Die Bundesnetzagentur ist darüber hinaus berechtigt, Vor-Ort-Untersuchungen durchzuführen und durch-

führen zu lassen und die Vorlage von Unterlagen zu verlangen. Diese sollen insbesondere bei Verdachtsfällen durchgeführt werden.

Zu Absatz 5

Absatz 5 dient der Umsetzung der Artikel 32 und 33 der NIS-2-Richtlinie.

Zu Absatz 6

Absatz 6 dient der Umsetzung des Artikels 23 der NIS-2-Richtlinie.

Zu Absatz 7

Absatz 7 dient der effizienten Gestaltung des Meldewesens nach Absatz 6. Das Bundesamt für Sicherheit in der Informationstechnik wird weiterhin die zentrale Stelle bleiben, um die Meldungen zu den Sicherheitsproblemen entgegenzunehmen. Die Rolle des Bundesamtes für Sicherheit in der Informationstechnik als „Kompetenzzentrum“ ist sinnvoll, um Wissen und Erfahrungen bestmöglich zu bündeln. Absatz 5 sieht vor, dass erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes, der betreffenden Energieanlage oder des digitalen Energiedienstes führen können oder bereits geführt haben, weiterhin unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik zu melden sind. Allerdings wird nach Absatz 7 die Rolle der Bundesnetzagentur in dem Prozess gestärkt, indem alle an das Bundesamt für Sicherheit in der Informationstechnik nach Absatz 6 und nach dem BSI-Gesetz eingegangenen Meldungen an die Bundesnetzagentur unverzüglich weiterzuleiten sind, wenn diese für die Energieversorgungssicherheit und Erfüllung der Ziele nach § 1 relevant sind. Daraufhin wird die Bundesnetzagentur eine energiewirtschaftliche Bewertung des Vorfalls vorbereiten, um die die BSI-Sicherheitswarnung erweitert wird. Ziel solchen Vorgangs ist einerseits Akteure der Energiewirtschaft über Sicherheitsvorfälle besser zu informieren und andererseits eine Einschätzung der Auswirkungen auf den Energiesektor und dadurch eine effiziente Krisenvorsorge und ggf. Einleitung von Gegenmaßnahmen zu ermöglichen. Eine energiesystemische und -wirtschaftliche Bewertung würde Zusammenhänge oder Wechselwirkungen im Energiesystem sichtbar machen. Darüber hinaus können so die Kompetenzen der Fachbehörden gezielt eingesetzt werden. Die Bundesnetzagentur kann bei Vorbereitung der Auswertung die Betreiber von Übertragungs-, Fernleitungs- und Verteilnetzen einbeziehen, was an deren Rolle und Systemverantwortung liegt (§ 13 und § 16 EnWG). Eine Einbeziehung der Betreiber von Übertragungs- und Fernleitungsnetzen in die Auswertung und der daraus resultierende Dialog mit der Branche könnten den Informationsfluss konzentrieren und zudem vertrauensbildend wirken. Diese Einbeziehung kann sich insbesondere durch Einberufung eines Expertengremiums realisieren lassen, das sich aus Vertretern des Bundesamtes für Sicherheit in der Informationstechnik, der Bundesnetzagentur und der Übertragungs- und Fernleitungsnetzbetreiber zusammensetzen würde. Der gesetzliche Auftrag zur Durchführung einer gemeinsamen Bewertung durch das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur wird darüber hinaus um eine Pflicht zur Durchführung einer abschließenden Bewertung des IT-Sicherheitsvorfalls nach deren Behebung ergänzt.

Zu Absatz 8

Absatz 8 entspricht dem gestrichenen § 11 Absatz 1d. Dabei dient Absatz 8 der Umsetzung des Artikels 3 der NIS-2-Richtlinie.

Zu Absatz 12

Absatz 9 entspricht dem gestrichenen § 11 Absatz 1g.

Zu Nummer 3

Es handelt sich um Folgeänderungen. Die Bezüge im Gesetz werden an die voranstehenden Änderungen angepasst.

Zu Nummer 4

Es handelt sich um Folgeänderungen. Die Bezüge im Gesetz werden an die voranstehenden Änderungen angepasst.

Zu Nummer 5

Es handelt sich um Folgeänderungen. Die Bezüge im Gesetz werden an die voranstehenden Änderungen angepasst.

Zu Nummer 6

Die Vorschrift zur Meldung von Sicherheitsvorfällen wird unter Berücksichtigung der neuen Mindestvorgaben aus Artikel 23 der NIS-2-Richtlinie neu gefasst.

Zu Artikel 18 (Änderung des Messstellenbetriebsgesetzes)

Es handelt sich um eine Folgeänderung. Der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes wird angepasst.

Zu Artikel 19 (Änderung des Energiesicherungsgesetzes)

Zu Nummer 1

Soweit die Bundesnetzagentur als zuständige Behörde das Gesetz ausführt, wird die bisherige Übermittlungsregelung dahingehend ergänzt, dass die nach § 1 der Gassicherungsverordnung (GasSV) und § 2a des Energiesicherungsgesetzes (EnSiG) von der Bundesnetzagentur erlangten Daten auf Ersuchen der Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) der Bafin zur Verfügung gestellt werden. Dabei erfolgt dies unter enger Zweckbindung der gesetzlichen Aufgaben der Bafin. Die Bafin soll dadurch in die Lage versetzt werden, unter anderem potenziell stabilitätsgefährdende Risiken, etwa für einzelne von der Bafin beaufsichtigte Unternehmen, sowie daraus resultierende Gefahren für die Gesamtwirtschaft frühzeitig identifizieren zu können. So könnten sich beispielsweise im Fall einer Gasmangellage Unternehmensrisiken auf investierte Banken und somit auf den gesamten Finanzmarkt übertragen. Durch Verweis auf § 1 GasSV und § 2a EnSiG wird der Umfang der hiervon betroffenen Daten präzisiert. Die Verwendung der erlangten Daten hat die Bafin nach Maßgabe der datenschutzrechtlichen Vorschriften vorzunehmen und auf das zur Erfüllung der Aufgaben erforderliche Maß zu beschränken.

Zu Nummer 2

Es handelt sich um Folgeänderungen. Die Begrifflichkeiten und der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 20 (Änderung des Wärmeplanungsgesetzes)

Es handelt sich um Folgeänderungen. Die Verweise auf Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 21 (Änderung des Fünften Buches Sozialgesetzbuch)

Es handelt sich um Folgeänderungen. Die Verweise auf Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 22 (Änderung der Digitale Gesundheitsanwendungen-Verordnung)

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 23 (Änderung des Sechsten Buches Sozialgesetzbuch)

Zu Nummer 1

Notwendige Anpassung der Inhaltsübersicht aufgrund der Änderung durch dieses Gesetz.

Zu Nummer 2

Die Deutsche Rentenversicherung Bund nimmt nicht nur eigene Trägeraufgaben der gesetzlichen Rentenversicherung wahr, sondern für alle Träger der Rentenversicherung auch die Grundsatz- und Querschnittsaufgaben. In den mit Grundsatz- und Querschnittsaufgaben befassten Organen sind die Bundes- und Regionalträger vertreten.

Mit einer Erweiterung des gesetzlich normierten Katalogs der Grundsatz- und Querschnittsaufgaben der Deutschen Rentenversicherung Bund um die Koordinierung der Informationstechnik der Rentenversicherung soll die

Grundlage für inhaltliche und organisatorische Maßnahmen geschaffen werden, die die Stärkung der IT-Sicherheit zum Ziel haben, ohne das gleichwertige Ziel der Wirtschaftlichkeit des Handelns aus den Augen zu verlieren. Zur Koordinierung der Informationstechnik gehört auch, Fortschritte in der technischen Entwicklung aufzugreifen. Die notwendige Ausgestaltung der Koordinierungstätigkeiten ergibt sich aus § 146 Satz 1 Nummer 1 bis 4. Das Regelungskonzept berücksichtigt die von den Rentenversicherungsträgern und Länderseite vorgetragenen Gesichtspunkte und die von den Trägern im Bereich der IT-Sicherheit jüngst bereits getroffenen verbindlichen Entscheidungen. Diese untergesetzlichen Regelungen werden vom Gesetzgeber bestätigt und gestärkt. Die Umsetzung der inhaltlichen und organisatorischen Maßnahmen verbleibt, soweit nicht anders bestimmt, in der Zuständigkeit und Verantwortung der einzelnen Träger der gesetzlichen Rentenversicherung. Dies gilt auch für Aufgabenstellungen aus dem Bereich der Informationstechnik, die der neuen Grundsatz- und Querschnittsaufgabe nicht zuzuordnen sind.

Die differenzierten Zuständigkeiten sollen verhindern, dass einerseits bei dezentraler Verantwortung durch abweichende Einschätzungen oder Missverständnisse wichtige Sicherheitsmaßnahmen nicht oder nur verspätet aufgegriffen werden und andererseits Entscheidungen in IT-Sicherheitsfragen, die organisatorisch weit entfernt von den jeweiligen IT-Einrichtungen gefällt werden, aufgrund einer unvollständigen Kenntnis des Sachverhalts zu unerwünschten Nebenfolgen führen.

Zu Nummer 3

Notwendige Folgeänderung zur Einfügung eines neuen Achten Unterabschnittes.

Zu Nummer 4

Zu § 146 (Verbindliche Entscheidungen zur Sicherheit in der Informationstechnik)

In § 146 Satz 1 wird die Deutsche Rentenversicherung Bund verpflichtet, die verbindlichen Entscheidungen herbeizuführen, die zur Stärkung der IT-Sicherheit als notwendig erachtet werden. Die Informationstechnik und ihre Sicherheit sind einem stetigen Wandel ausgesetzt. Die Herbeiführung weiterer verbindlicher Entscheidungen obliegt der Deutsche Rentenversicherung Bund.

Die Deutsche Rentenversicherung Bund hat erste Maßnahmen ergriffen, um die IT-Sicherheit zu stärken. Die gesetzte Frist berücksichtigt dies.

Zu § 146 Satz 1 Nummer 1

Die Deutsche Rentenversicherung Bund wird verpflichtet, einheitliche Grundsätze in der Informationstechnik und Informationssicherheit festzulegen, die für alle Träger der gesetzlichen Rentenversicherung verbindlich sind. Die Notwendigkeit, auch im Bereich der Informationssicherheit für alle Träger der gesetzlichen Rentenversicherung ein einheitliches Sicherheitsniveau zu gewährleisten, wird durch die Aufnahme in den Gesetzestext bestätigt. Ein einheitliches Sicherheitsniveau kann durch einheitliche Sicherheitsstandards und Sicherheitskonzepte erreicht werden. Bei den Grundsätzen handelt es sich um Mindestanforderungen, die die eigene Verantwortlichkeit der einzelnen Träger insbesondere als Betreiber kritischer Infrastrukturen nicht aufheben sollen.

Die Verpflichtung beinhaltet auch, Fortschritte in der Entwicklung der Informationstechnik auf Nutzen und Umsetzbarkeit in der gesetzlichen Rentenversicherung zu bewerten und Risiken für die Informationstechnik zu beobachten und zu analysieren.

Zu § 146 Satz 1 Nummer 2

Mit dieser Ergänzung wird die Deutsche Rentenversicherung Bund verpflichtet, einen einheitlichen organisatorischen Rahmen zu schaffen. Mit der Errichtung eines Gemeinsamen Rechenzentrums wurde von den Trägern der gesetzlichen Rentenversicherung in der Praxis ein erster Schritt getan. Die trägerübergreifende informationstechnische Infrastruktur der gesetzlichen Rentenversicherung soll künftig grundsätzlich bei der Deutschen Rentenversicherung Bund liegen.

Zu § 146 Satz 1 Nummer 3

Die Träger der gesetzlichen Rentenversicherung greifen zur Erfüllung ihrer Aufgaben auch auf von ihnen entwickelte Softwareanwendungen zurück. Deren Entwicklung erfolgt durch die IT-Einrichtungen verschiedener Träger. Dies erschwert die Weiterentwicklung nach einheitlichen Maßstäben und zu einheitlichen Zeitpunkten und hat zur Verwendung von untereinander nichtkompatiblen Versionen der Anwendungen geführt. Die Entwicklung

rentenversicherungsbezogener Anwendungen soll daher bei der Deutschen Rentenversicherung Bund gebündelt werden. Die Verantwortung für Anwendungsbetrieb und Nutzung der Anwendungen verbleibt bei den einzelnen Trägern.

Zu § 146 Satz 1 Nummer 4

Durch die Festlegung eines Beschaffungskonzepts soll bei Hardware, Software und Infrastrukturkomponenten eine höhere Standardisierung und eine höhere Wirtschaftlichkeit geschaffen werden. Dies muss nicht dazu führen, dass alle Rentenversicherungsträger mit einheitlichen Produkten ausgestattet sind. Solange die Produkte untereinander kompatibel sind, können die Träger mit Produkten verschiedener Anwender ausgestattet sein.

Zu § 146 Satz 2

Die Deutsche Rentenversicherung Knappschaft-Bahn-See hat neben Aufgaben aus der allgemeinen Rentenversicherung noch weitere ihr gesetzlich übertragene Aufgaben (zum Beispiel Kranken- und Pflegeversicherung, Minijob-Zentrale, Bundesfachstelle Barrierefreiheit) und besondere Leistungen (zum Beispiel Leistungszuschlag, Rente für Bergleute, Leistungen aus der Seemannskasse) wahrzunehmen. Diese machen eine besondere Regelung erforderlich. Bei den sich aus Satz 2 Nummer 17 ergebenden Grundsätzen und deren Umsetzungen sind die Interessen des Verbundsystems insgesamt und seiner besonderen Leistungen zu wahren und entsprechende Befugnisse sicherzustellen. Deshalb sind notwendige Abweichungen zulässig.

Zu Artikel 24 (Änderung der Verordnung zum Barrierefreiheitsstärkungsgesetz)

Es handelt sich um eine Folgeänderung. Der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes wird angepasst.

Zu Artikel 25 (Änderung des Elften Buches Sozialgesetzbuch)

Es handelt sich um Folgeänderungen. Die Verweise auf Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 26 (Änderung des Telekommunikationsgesetzes)

Die bisherigen Vorschriften des Telekommunikationsgesetzes (TKG) hinsichtlich der Cybersicherheit öffentlicher Telekommunikationsnetze werden entsprechend der Vorgaben der NIS-2-Richtline angepasst. Darüber hinaus werden die Verweise auf Vorschriften und die Begrifflichkeiten des bisherigen BSI-Gesetzes angepasst.

Zu Nummer 1

Es handelt sich um eine Folgeänderung.

Zu Nummer 2

Die Begriffsbestimmungen des § 3 TKG werden im Hinblick auf die NIS-2-Richtlinie angepasst: Die bereits in § 3 Nummer 53 TKG bestehende Definition des „Sicherheitsvorfalls“ wird an Artikel 6 Nummer 6 der NIS-2-Richtlinie angepasst. Darüber hinaus wird in Umsetzung von Artikel 6 Nummer 1 der NIS-2-Richtlinie die Begriffsbestimmung für ein „Netz- und Informationssystem“ ergänzt.

Zu Nummer 3

Die Änderungen dienen der Umsetzung der NIS-2-Richtlinie, nach der die Artikel 40 und 41 der Richtlinie (EU) 2018/1972 gestrichen werden (vgl. Artikel 43 der NIS-2-Richtlinie), die in den §§ 165 ff. TKG umgesetzt sind. Die Änderungen in § 165 TKG setzen Artikel 20, 21 und 23 der NIS-2-Richtlinie um. Im Übrigen werden redaktionelle Anpassungen vorgenommen.

Zu Nummer 4

Es handelt sich um rein redaktionelle Anpassungen.

Zu Nummer 5

Die Änderungen des § 168 TKG, der bislang Artikel 40 der Richtlinie (EU) 2018/1972 umsetzt, dienen der Umsetzung von Artikel 23 der NIS-2-Richtlinie.

Zu den Nummern 6 bis 8

Es handelt sich um rein redaktionelle Anpassungen.

Zu Artikel 27 (Änderung der Krankenhausstrukturfonds-Verordnung)

Zu Nummer 1

Der Anwendungsbereich des Krankenhausstrukturfonds soll für die verbleibende Laufzeit des Fonds unverändert bleiben. Um zu vermeiden, dass sich die Zahl der Krankenhäuser, die Fördermittel aus dem Fonds zur Verbesserung ihrer IT-Sicherheit erhalten können, durch künftige Änderungen der BSI-Kritisverordnung vergrößert, wird zur Abgrenzung der betroffenen Krankenhäuser auf die BSI-Kritisverordnung in ihrer aktuell geltenden Fassung Bezug genommen. Darüber hinaus handelt es sich um Folgeänderungen. Der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes wird angepasst.

Zu Nummer 2

Es handelt sich um Folgeänderungen. Die Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 28 (Änderung der Außenwirtschaftsverordnung)

Es handelt sich um Folgeänderungen. Die Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 29 (Änderung des Vertrauensdienstegesetzes)

Gemäß Artikel 42 der NIS-2-Richtlinie werden die Sicherheitsanforderungen und Meldepflichten für Vertrauensdiensteanbieter in Artikel 19 der Verordnung (EU) Nr. 910/2014 (eIDAS) gestrichen. Damit entfällt die Notwendigkeit zur Benennung einer zuständigen Stelle im Sinne des letztgenannten Artikels. Fortan gelten für Vertrauensdiensteanbieter die Vorgaben des BSI-Gesetzes.

Zu Artikel 30 (Weitere Änderung des BSI-Gesetzes)

Artikel 30 setzt die beabsichtigte Verschiebung der gesetzlichen Bestimmung kritischer Anlagen in das Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz) um. Artikel 30 tritt nach der Regelung in Artikel 33 erst mit dem Inkrafttreten einer Verordnung nach dem KRITIS-Dachgesetz in Kraft. Dabei handelt es sich um eine Nachfolgeverordnung der bisherigen BSI-Kritisverordnung. Hierdurch wird sichergestellt, dass es zu jedem Zeitpunkt immer jeweils nur eine Verordnung zur KRITIS Bestimmung gibt. Bis zum Erlass der Verordnung nach § 5 Absatz 1 in Verbindung mit § 4 Absatz 3 KRITIS-Dachgesetz ist dies übergangsweise die Rechtsverordnung nach § 56 Absatz 4 BSI-Gesetz. Die Verordnungsermächtigung in § 56 Absatz 4 BSI-Gesetz wird mit dem Inkrafttreten der Verordnung nach § 5 Absatz 1 in Verbindung mit § 4 Absatz 3 KRITIS-Dachgesetz gestrichen.

Zu den Nummern 1 bis 6

Die bisherige originäre Begriffsbestimmung wird durch einen Verweis auf die Begriffsbestimmung im KRITIS-Dachgesetz ersetzt.

Die bisherigen Vorschriften zur Bestimmung von Betreibern kritischer Anlagen entfallen aufgrund der Verweise in das KRITIS-Dachgesetz.

Die Liste der Sektoren des bisherigen § 2 Nummer 24 BSI-Gesetz wird ersetzt durch diejenige des KRITIS-Dachgesetzes.

Die Rechtsverordnung nach KRITIS-Dachgesetz tritt an die Stelle der bisherigen BSI-KritisV, der Verweis wird auf die Verordnungsermächtigung nach KRITIS-Dachgesetz geändert.

Zu Artikel 31 (Weitere Änderung des Telekommunikationsgesetzes)

Auch dieser Artikel tritt erst mit dem Inkrafttreten der Nachfolgeverordnung nach dem KRITIS-Dachgesetz in Kraft. Auf die Begründung zu Artikel 30 wird verwiesen.

Zu Artikel 32 (Weitere Änderung der Außenwirtschaftsverordnung)

Auch dieser Artikel tritt erst mit dem Inkrafttreten der Nachfolgeverordnung nach dem KRITIS-Dachgesetz in Kraft. Auf die Begründung zu Artikel 30 wird verwiesen.

Zu Artikel 33 (Inkrafttreten, Außerkrafttreten)

Zu Absatz 1

Als Inkrafttreten wird der Tag nach Verkündung festgelegt. Im Übrigen sind die für die Verpflichtungen von wesentlichen und besonders wichtigen Einrichtungen maßgeblichen Inhalte der NIS-2-Richtlinie bereits seit dem Kommissionsentwurf vom Dezember 2020 bekannt.

Zu Absatz 2

Absatz 2 regelt die zeitliche Verknüpfung der Verschiebung bestimmter Regelungen zu kritischen Anlagen in Artikel 30, die künftig in das Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz) verschoben werden sollen. Die auf Artikel 30 folgenden Artikel enthalten entsprechende Folgeänderungen.

Anlage 2

Stellungnahme des Nationalen Normenkontrollrates (NKR) gemäß § 6 Abs. 1 NKRG

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NKR-Nr. 6824)

Der Nationale Normenkontrollrat hat den Regelungsentwurf mit folgendem Ergebnis geprüft:

I Zusammenfassung

Bürgerinnen und Bürger	keine Auswirkungen
Wirtschaft	
Jährlicher Erfüllungsaufwand:	rund 2,2 Mrd. Euro
davon aus Bürokratiekosten:	*1,9 Mio. Euro*
Einmaliger Erfüllungsaufwand:	rund 2,1 Mrd. Euro
davon aus Bürokratiekosten:	*360 000 Euro*
Verwaltung	
Bund	
Jährlicher Erfüllungsaufwand:	rund 122,3 Mio. Euro
	(rund 920 zusätzliche Planstellen)
Einmaliger Erfüllungsaufwand:	rund 38,2 Mio. Euro
Länder	
Jährlicher Erfüllungsaufwand:	rund 85 000 Euro
‘One in one out’-Regel	Der jährliche Erfüllungsaufwand der Wirtschaft in diesem Regelungsvorhaben stellt im Sinne der ‚One in one out‘-Regel der Bundesregierung kein „In“ dar, da er allein aus der Umsetzung von EU-Recht resultiert.
Digitaltauglichkeit (Digitalcheck)	Das Ressort hat Möglichkeiten zum digitalen Vollzug der Neuregelung (Digitaltauglichkeit) geprüft und hierzu einen Digitalcheck mit überwiegend nachvollziehbarem Ergebnis durchgeführt.
ggf. KMU-Betroffenheit	Das Ressort hat einen KMU-Test durchgeführt. Die Belange von KMU wurden bereits in den EU-Verhandlungen berücksichtigt.
Umsetzung von EU-Recht	Dem NKR liegen keine Anhaltspunkte dafür vor, dass mit dem Vorhaben über eine 1:1-Umsetzung von EU-Recht hinausgegangen wird.
Evaluierung	Die Neuregelung wird fünf Jahre nach Inkrafttreten evaluiert.

Ziele:	Erhöhung des gemeinsamen Cybersicherheitsniveaus
Kriterien/Indikatoren:	Ergriffene Cybersicherheitsmaßnahmen der von dem Gesetz betroffenen Einrichtungen
Datengrundlage:	Berichterstattung des BSI und freiwillige Umfragen bei den betroffenen Einrichtungen
Nutzen des Vorhabens	Vermeidung von Schäden durch Cyberangriffe Das Ressort schätzt, dass jährlich rund 3,6 Mrd. Euro Gesamtschaden bei den Unternehmen abgewehrt werden können.

Regelungsfolgen

Der Nationale Normenkontrollrat begrüßt, dass sich die Bundesregierung bereits bei der Ausarbeitung der EU-Richtlinie für aufwandsärmere Lösungen eingesetzt und hierfür früh durchgeführte Kostenfolgeschätzungen als Argumentationslinie verwendet hat.

Die Darstellung der Regelungsfolgen ist überwiegend nachvollziehbar und methodengerecht. Der NKR erhebt hiergegen im Rahmen seines gesetzlichen Auftrags keine Einwände. Allerdings hat der NKR Anhaltspunkte gefunden, dass es sich bei dem dargestellten erheblichen Mehrbedarf an Planstellen, teilweise um Sowieso-Aufwände handeln könnte, da die Bundesministerien aufgrund einer verbindlichen Richtlinie (UP Bund) bereits heute vergleichbare Cybersicherheitsmaßnahmen implementieren müssen. Der NKR hebt deshalb die Wichtigkeit einer zeitnahen Nachmessung des geschätzten Erfüllungsaufwands durch das Statistische Bundesamt hervor.

Aus Sicht des NKR sollte ein grundlegender Sicherheitsrahmen für alle Verwaltungsebenen geschaffen werden (inkl. Kommunen), weil der gesamtstaatliche Nutzen die möglichen Kosten übersteigt.

Digitaltauglichkeit

Das Ressort hat Möglichkeiten zum digitalen Vollzug der Neuregelung (Digitaltauglichkeit) geprüft. Der NKR empfiehlt darüberhinausgehend potenziell Betroffene und Sicherheitsexperten frühzeitig in die Erarbeitung der geplanten digitalen Meldeprozesse einzubeziehen und mit der Umsetzung des geplanten KRITIS-Dachgesetzes zu harmonisieren.

II Regelungsvorhaben

Das Regelungsvorhaben dient der Umsetzung der NIS-2 Richtlinie (EU) 2022/2554[*]. Ziel dieser ist die Einführung verbindlicher Maßnahmen für Verwaltung und Wirtschaft, mit denen in der gesamten Europäischen Union ein hohes gemeinsames Cybersicherheitsniveau gewährleistet werden soll. Wichtige und besonders wichtige Einrichtungen sollen dadurch vor Schäden durch Cyberangriffe geschützt und das Funktionieren des europäischen Binnenmarktes verbessert werden.

III Bewertung

III.1 Erfüllungsaufwand

Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht durch das Regelungsvorhaben kein Erfüllungsaufwand.

[*] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2555

Wirtschaft

Für die Wirtschaft erhöht sich der jährliche Erfüllungsaufwand um rund 2,2 Mrd. Euro. Davon entfallen rund 1,9 Mio. Euro auf Bürokratiekosten aus Informationspflichten. Darüber hinaus entsteht einmaliger Erfüllungsaufwand von rund 2,1 Mrd. Euro. Dieser Aufwand resultiert aus den folgenden Vorgaben:

- Einhaltung eines Mindestniveaus an IT-Sicherheit

Künftig müssen alle als besonders wichtige oder wichtige eingestuften Einrichtungen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen, um relevante IT-bezogene Störungen zu vermeiden.

Den Betreibern wichtiger und besonders wichtiger Einrichtungen entsteht dadurch jährlicher Erfüllungsaufwand in Höhe von rund 2,2 Mrd. Euro. Das Ressort geht dabei davon aus, dass künftig rund 30 000 Einrichtungen in den Anwendungsbereich des Gesetzes fallen. Weiterhin nimmt das Ressort an, dass hiervon 9 000 Einrichtungen bereits heute die nun vorgesehenen Maßnahmen – entweder aufgrund rechtlicher Verpflichtung oder aus Eigeninteresse - umsetzen. Künftig müssen so für rund 3 000 besonders wichtige und 18 000 wichtige Einrichtungen erstmalig entsprechende Cybersicherheitsmaßnahmen ergriffen werden, wobei ein fallbezogener Aufwand von 200 000 Euro für besonders wichtige und 80 000 Euro für wichtige Einrichtungen angenommen wird.

Den betroffenen Unternehmen entsteht zudem einmaliger Erfüllungsaufwand in Höhe von insgesamt rund 2,1 Mrd. Euro für die notwendige Anpassung digitaler Prozessabläufe.

- Regelmäßige Schulungen der Geschäftsführer

Das Regelungsvorhaben sieht vor, dass Geschäftsführer aller adressierten Einrichtungen regelmäßig Cybersicherheitsschulungen absolvieren müssen, die übrigen Mitarbeitenden sollen regelmäßig daran teilnehmen. Insgesamt geht das Ressort dafür von einem jährlichen Erfüllungsaufwand von rund 159 Mio. Euro aus.

- Ausweitung der Meldepflicht für Sicherheitsvorfälle

Bei Sicherheitsvorfällen sieht das Regelungsvorhaben eine Meldepflicht, in bestimmten Fällen eine Unterrichtungspflicht sowie auf Verlangen eine Auskunftspflicht vor. Insbesondere durch die Ausweitung des Kreises der melde- und auskunftspflichtigen entstehen jährliche Bürokratiekosten von rund 1 Mio. Euro.

- Ausweitung Registrierungspflicht von Einrichtungen

Durch das Regelungsvorhaben wird die bestehende Registrierungspflicht auf alle besonders wichtigen und wichtigen Einrichtungen sowie bestimmte weitere Einrichtungsarten ausgeweitet. Für die Übermittlung der notwendigen Informationen (erstmalig sowie laufend bei Änderungen) schätzt das Ressort einmalige Bürokratiekosten von rund 360 000 Euro und jährliche Bürokratiekosten von rund 48 000 Euro.

- Nachweis zur Einhaltung der IT-Sicherheitsanforderungen

Das BSI kann von den in den Anwendungsbereich der Regelung fallenden Einrichtungen Nachweise zur Einhaltung der IT-Sicherheitsmaßnahmen anfordern. Insgesamt geht das Ressort von jährlichen Bürokratiekosten von rund 850 000 Euro aus.

Verwaltung

Die Ausgestaltung des Regelungsvorhabens folgt einem Beschluss des IT-Planungsrates (2023/39), in dem der Bund aufgefordert wird, Einrichtungen der öffentlichen Verwaltung auf

lokaler Ebene und Bildungseinrichtungen aus dem Anwendungsbereich des nationalen Umsetzungsgesetzes auszunehmen. Dementsprechend fällt der Erfüllungsaufwand für dieses Vorhaben fast ausschließlich beim Bund an.

Bund

Die Bundesverwaltung ist in zweifacher Hinsicht betroffen: Zum einen muss die Bundesverwaltung als Adressat selbst neue Sicherheitsanforderungen umsetzen. Dafür geht das Ressort von jährlichem Erfüllungsaufwand von rund 61,7 Mio. Euro sowie einmaligen Erfüllungsaufwand von rund 27 Mio. Euro aus.

Zum anderen muss sie den Vollzug des Gesetzes sicherstellen. Für den Vollzug schätzt das Res-sort insgesamt einen jährlichen Erfüllungsaufwand von rund 60 Mio. Euro und einmaligen Erfüllungsaufwand von rund 11 Mio. Euro.

Bund als Adressat

Einen großen Anteil am Erfüllungsaufwand machen geschätzte Personalmehrbedarfe mit dauerhaft insgesamt ca. 380 Stellen aus. Allerdings hat der NKR Anhaltspunkte gefunden, dass der tatsächliche Aufwand geringer ausfallen könnte. So hat die Bundesregierung 2017 mit dem Umsetzungsplan Bund (UP Bund) eine Informationssicherheitsleitlinie beschlossen, die allen Ressorts verbindlich vorschreibt, wie sie sich vor Cyberangriffen zu schützen haben. Durch das Anheben der untergesetzlichen Vorschrift in Gesetzesrang müssten diese Aufwände deshalb als Sowieso-Kosten aus der Darstellung des Erfüllungsaufwands herausfallen. In der vorgelegten Darstellung lassen sich diese jedoch nicht eindeutig von neuen Pflichten abgrenzen. Der NKR hebt deshalb die Wichtigkeit einer zeitnahen Nachmessung des geschätzten Erfüllungsaufwands durch das Statistische Bundesamt hervor.

- Maßnahmen zur Gewährleistung der Informationssicherheit

Die derzeit schon bestehenden Vorgaben für Einrichtungen der Bundesverwaltung hinsichtlich der Voraussetzungen zur Gewährleistung der Sicherheit des IT-Betriebes werden ausgeweitet und verschärft. Damit ist nach Schätzungen des BMI vor allem ein erheblicher Mehrbedarf an zusätzlichen Personalstellen verbunden. Insgesamt schätzt das Ressort hierfür jährlichen Erfüllungsaufwand von rund 28,4 Mio. Euro (rund 167 Stellen) und einmaligen Erfüllungsaufwand von rund 16,3 Mio. Euro. Diese Aufwände fallen u. a. für die Etablierung und Durchführung eines Risikomanagements, die Erstellung und ständige Aktualisierung von Sicherheitskonzepten sowie Ausbau und Betrieb der notwendigen IT-Infrastruktur an.

- Behandlung von Sicherheitsvorfällen

Die betroffenen Bundeseinrichtungen müssen erhebliche Sicherheitsvorfälle an das BSI melden und Maßnahmen zur Abwendung oder Behebung von Sicherheitsvorfällen ergreifen. Der hierfür notwendige Aufbau eines IT-Sicherheitsvorfall Management und Notfallmanagement verursacht einmaligen Erfüllungsaufwand von rund 5,2 Mio. Euro. Darüber hinaus nimmt das Ressort einen jährlichen Aufwand von rund 19,6 Mio. Euro an (127 Stellen).

- Regelmäßige Schulungen

Mitarbeitende und Einrichtungsleitende von Bundesbehörden sollen regelmäßig Cybersicherheitsschulungen absolvieren. Hierfür nimmt das Ressort einem einmaligen Erfüllungsaufwand von rund 940 000 Euro und jährlichem Erfüllungsaufwand von rund 5,1 Mio. Euro an.

- IT-Sicherheitsbeauftragte und IT-Infrastruktur

Für die Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes sind eigene Informationssicherheitsbeauftragte zu bestel-

len. Zudem entsteht Aufwand für die Inanspruchnahme von Dienstleistungen Dritter sowie für Ausbau und Betrieb zusätzlicher IT-Infrastruktur. Insgesamt schätzt das Ressort einen einmaligen Erfüllungsaufwand von rund 4,7 Mio. Euro und jährlichen Erfüllungsaufwand von rund 9,4 Mio. Euro (55 Stellen).

Vollzug durch den Bund

Durch das Regelungsvorhaben wird der Aufgabenbereich der betroffenen Vollzugsbehörden neu strukturiert. Wesentlicher neuer Aufwand entsteht BSI, BBK, BNetzA, BfDI und BMI. Dieser entsteht vor allem durch die stark zunehmende Anzahl der zu beaufsichtigenden Einrichtungen.

- Wahrnehmung Grundsatzaufgaben und Befugnisse (BSI, BfDI)

Bereits heute nimmt das BSI umfassende Aufgaben im Bereich Sicherheit in der Informationstechnik wahr. Mit dem Regelungsvorhaben werden die Aufgaben des BSI ausgeweitet, wobei es durch den BfDI und ITZBund unterstützt wird. Insgesamt schätzt das Ressort einen einmaligen Erfüllungsaufwand von rund 2,5 Mio. Euro und jährlichen Erfüllungsaufwand von rund 33,6 Mio. Euro.

- Bearbeitung von Meldungen erheblicher Sicherheitsvorfälle (BSI, BBK)

Bereits heute ist das BSI zentrale Anlaufstelle für Meldungen von Betreibern Kritischer Infrastrukturen zu erheblichen Sicherheitsvorfällen. Künftig werden BSI und BBK dabei zusammenarbeiten, wobei die Zahl der meldepflichtigen Einrichtungen deutlich zunehmen wird. In der Summe geht das Ressort von einem einmaligen Erfüllungsaufwand von rund 500 000 Euro und einem jährlichen Erfüllungsaufwand von rund 11 Mio. Euro aus.

- Weitere wesentliche Vorgaben mit Erfüllungsaufwand

Aus den folgenden weiteren Vorgaben ergibt sich nach Schätzungen des Ressorts insgesamt einmaliger Erfüllungsaufwand von rund 8 Mio. Euro und jährlicher Erfüllungsaufwand von rund 15,2 Mio. Euro:

Vorgabe	Jährlicher Erfüllungsaufwand (in Tsd. Euro)	Einmaliger Erfüllungsaufwand (in Tsd. Euro)
Einrichtung und Betrieb eines Registers für (besonders) wichtige Einrichtungen	2 063	8
Zentrale Melde- und Anlaufstelle (BSI, BBK, BNetzA)	4 196	12
Verschiedene Vollzugsaufgaben im Bereich der IT-Sicherheit (BMI, BSI und BBK)	5 022	12
Grundsatzaufgaben zur IT-Sicherheit im Energiesektor (BNetzA)	987	0
Grundsatzaufgaben zur IT-Sicherheit im Telekommunikationssektor (BNetzA)	2 911	8 000
Summe	15 179	8 032

Länder

Das BSI hat den zuständigen Landesbehörden wesentliche Informationen für die Abwehr von Gefahren für die Sicherheit zu übermitteln, welche dann gemeinsam mit anderen Behörden die Relevanz analysieren. Aufgrund der Ausweitung des Anwendungsbereichs geht das Ressort von laufendem Erfüllungsaufwand von rund 85 000 Euro aus.

III.2 Digitaltauglichkeit

Das Ressort hat einen Digitalcheck mit überwiegend nachvollziehbarem Ergebnis durchgeführt. Der NKR weist darüber hinaus auf folgende Sachverhalte hin:

- Meldeportal

Durch ein gemeinsames Meldeportal mit anderen Aufsichtsbehörden sollen Synergien bei den Meldepflichten der erfassten Betreiber und Einrichtungen genutzt und der Bürokratieaufwand minimiert werden. Allerdings liegen bislang nur grobe Prozessbeschreibungen vor. Für den NKR ist nicht abschließend bewertbar, ob eine effektive Harmonisierung mit dem ebenfalls zu erarbeitenden KRITIS-Dachgesetz gewährleistet wird, weil die Regelungsvorhaben zu mindestens hinsichtlich der öffentlich bekannten Referentenentwürfe und Konsultationsprozesse nicht gemeinsam weiterentwickelt wurden. Dadurch war dem NKR, der Fachöffentlichkeit und den Betroffenen eine gemeinsame Bewertung nicht möglich. Der NKR empfiehlt für die geplanten digitalen Meldeprozesse auch potenziell Betroffene und Sicherheitsexperten in die Konzeption mit einzubinden und mit der Umsetzung des KRITIS-Dachgesetzes zu harmonisieren.

III.3 Alternativenprüfung: Nutzen eines gesamtstaatlichen Cybersicherheitsrahmens

Ziel der NIS-2-Richtlinie ist es, mit verbindlichen Maßnahmen für Verwaltung und Wirtschaft ein hohes gemeinsames Cybersicherheitsniveau in der EU sicherzustellen. Sie gilt erstmals auch für öffentliche Verwaltungen auf zentraler und regionaler Ebene. Auf Beschluss des IT-Planungsrates (2023/39) wurden Länder und der Bund gebeten, kommunale Verwaltungen vom Anwendungsbereich des Regelungsvorhabens auszunehmen. Dieser Bitte folgt das Regelungsvorhaben, ohne dass erkennbar eine Alternativenprüfung für einen gesamtstaatlichen Cybersicherheitsrahmen stattgefunden hat.

Für Bürgerinnen und Bürger sowie Unternehmen wird die öffentliche Verwaltung in Deutschland in den Kommunen erlebbar. Kommunale Dienstleistungen sind von zentraler Bedeutung für das tägliche Leben der Bürgerinnen, Bürger und Unternehmen. Ein Ausfall essenzieller Dienste hat nicht nur unmittelbare und erhebliche Auswirkungen auf die betroffene Bevölkerung und Wirtschaft, sondern könnte auch das Vertrauen in die Funktionsfähigkeit staatlicher Strukturen nachhaltig erschüttern. Die anhaltenden Cyberangriffe auf Kommunen und Behörden, die teilweise weitreichende Folgen für Wirtschaft und Gesellschaft haben, verdeutlichen die Dringlichkeit. Vor diesem Hintergrund hält der NKR eine Stärkung der Cybersicherheit in diesen Bereichen ebenfalls für erforderlich. Durch verpflichtende Vorgaben für die kommunale IT-Sicherheit könnte ein Mindestmaß an Einheitlichkeit erreicht werden. Dazu könnten auch einfache, einheitliche digitale Meldewege gehören, um eine Grundlage für ein deutschlandweites, kommunales Lagebild zu erstellen. Aus Sicht des NKR sollte ein grundlegender Sicherheitsrahmen für alle Verwaltungsebenen geschaffen werden. Eine integrative Herangehensweise, die alle Verwaltungsebenen einbezieht, ist notwendig, um die Cybersicherheit in der Breite zu erhöhen.

Der gesamtstaatliche Nutzen dürfte die möglichen Kosten übersteigen.

III.4 KMU

Das Ressort hat einen KMU-Test für das Regelungsvorhaben durchgeführt, da mittelgroße Unternehmen als wichtige Einrichtungen eingestuft und damit von den Vorgaben betroffen sein können. Demnach können sich für mittlere Unternehmen Belastungen aus einer anfänglich fehlenden Routine bei der Umsetzung der Vorschriften ergeben. Durch die Differenzierung der zu ergreifenden IT-Sicherheitsmaßnahmen nach besonders wichtigen und wichtigen

Einrichtungen wurden die Belange der KMU bereits bei den Verhandlungen auf EU-Ebene eingebracht.

III.5 Umsetzung von EU-Recht

Dem NKR liegen keine Anhaltspunkte dafür vor, dass mit dem Vorhaben über eine 1:1-Umsetzung von EU-Recht hinausgegangen wird. Der NKR begrüßt, dass sich die Bundesregierung bereits bei der Ausarbeitung der EU-Richtlinie für aufwandsärmere Lösungen eingesetzt und hierfür auch frühzeitig erstellte Kostenschätzungen als Argumentationslinie verwendet hat.

III.6 Evaluierung

Das Ressort beabsichtigt spätestens nach fünf Jahren zu evaluieren, ob eine Erhöhung des gemeinsamen Cybersicherheitsniveaus erreicht wurde (Ziel). Zur Erreichung dieses Ziels stellt das Ressort auf die ergriffenen Cybersicherheitsmaßnahmen der von dem Gesetz betroffenen Einrichtungen ab (Indikatoren). Hierzu nutzt es die Berichterstattung des BSI und freiwillige Umfragen bei den betroffenen Einrichtungen (Datengrundlage). Zudem sollen die Ergebnisse der Evaluation der NIS-2-Richtlinie durch die Europäische Kommission berücksichtigt werden. Diese überprüft bis zum 17. Oktober 2027 und danach alle 36 Monate regelmäßig die Richtlinie und berichtet dem Europäischen Parlament und dem Rat.

IV Ergebnis

Der Nationale Normenkontrollrat begrüßt, dass sich die Bundesregierung bereits bei der Ausarbeitung der EU-Richtlinie für aufwandsärmere Lösungen eingesetzt und hierfür früh durchgeführte Kostenfolgeschätzungen als Argumentationslinie verwendet hat.

Die Darstellung der Regelungsfolgen ist überwiegend nachvollziehbar und methodengerecht. Der NKR erhebt hiergegen im Rahmen seines gesetzlichen Auftrags keine Einwände. Allerdings hat der NKR Anhaltspunkte gefunden, dass es sich bei dem dargestellten erheblichen Mehrbedarf an Planstellen, teilweise um Sowieso-Aufwände handeln könnte, da die Bundesministerien aufgrund einer verbindlichen Richtlinie (UP Bund) bereits heute vergleichbare Cybersicherheitsmaßnahmen implementieren müssen. Der NKR hebt deshalb die Wichtigkeit einer zeitnahen Nachmessung des geschätzten Erfüllungsaufwands durch das Statistische Bundesamt hervor.

Aus Sicht des NKR sollte ein grundlegender Sicherheitsrahmen für alle Verwaltungsebenen geschaffen werden (inkl. Kommunen), weil der gesamtstaatliche Nutzen die möglichen Kosten übersteigt.

Das Ressort hat Möglichkeiten zum digitalen Vollzug der Neuregelung (Digitaltauglichkeit) geprüft. Der NKR empfiehlt darüberhinausgehend potenziell Betroffene und Sicherheitsexperten frühzeitig in die Erarbeitung der geplanten digitalen Meldeprozesse einzubeziehen und mit der Umsetzung des geplanten KRITIS-Dachgesetzes zu harmonisieren.

Lutz Goebel	Prof. Dr. Sabine Kuhlmann
Vorsitzender	Berichterstatterin

Anlage 3

Stellungnahme der Bundesregierung zu der Stellungnahme des Nationalen Normenkontrollrates

Die Bundesregierung nimmt zur Stellungnahme des Nationalen Normenkontrollrates (NKR) vom 22. Juli 2024 wie folgt Stellung:

1.

Der NKR habe Anhaltspunkte gefunden, dass es sich bei dem dargestellten erheblichen Mehrbedarf an Planstellen, teilweise um Sowieso-Aufwände handeln könnte, da die Bundesministerien aufgrund einer verbindlichen Richtlinie (UP Bund) bereits heute vergleichbare Cybersicherheitsmaßnahmen implementieren müssen. Es wird daher die Wichtigkeit einer zeitnahen Nachmessung des geschätzten Erfüllungsaufwands durch das Statistische Bundesamt hervorgehoben

Stellungnahme der Bundesregierung:

In Bezug auf die infrage gestellte Plausibilität des gemeldeten Mehrbedarfs an Planstellen für die Verwaltung ist darauf hinzuweisen, dass die Bundesverwaltung – auch aufgrund des verfassungsrechtlich verankerten Ressortprinzips – keine homogene IT-Sicherheitslandschaft darstellt. Zutreffend ist, dass bestehende Pflichten in der Darstellung der Haushaltsausgaben und des Erfüllungsaufwands keine Berücksichtigung finden können. Gleichwohl erfolgte durch jedes Ressort eine Einzelfallbewertung hinsichtlich der sich aus dem Gesetz ergebenden Mehraufwände. Angleichungen wurden im Rahmen der zur Verfügung stehenden Zeit vorgenommen. Abschließend ist darauf hinzuweisen, dass zukünftige Bedrohungen im Bereich der Cybersicherheit nur sehr begrenzt vorhersehbar sind und insoweit eine gewisse Unsicherheit in der Natur der Regelungsmaterie liegt.

2.

Anhaltende Cyberangriffe auf Kommunen und Behörden, die teilweise weitreichende Folgen für Wirtschaft und Gesellschaft haben, verdeutlichen die Dringlichkeit und Notwendigkeit einer Stärkung der Cybersicherheit auch in den Kommunen. Durch verpflichtende Vorgaben für die kommunale IT-Sicherheit könnte ein Mindestmaß an Einheitlichkeit erreicht werden. Aus Sicht des NKR sollte ein grundlegender Sicherheitsrahmen für alle Verwaltungsebenen geschaffen werden. Eine integrative Herangehensweise, die alle Verwaltungsebenen einbezieht, sei notwendig, um die Cybersicherheit in der Breite zu erhöhen.

Stellungnahme der Bundesregierung:

Die Bundesregierung sieht die Entwicklung der Cybersicherheit von Kommunen mit Sorge. Hinsichtlich des aus Sicht des NKR zu schaffenden grundlegenden Sicherheitsrahmens für alle Verwaltungsebenen (inklusive Kommunen) verweist die Bundesregierung auf den verfassungsrechtlichen Rahmen. Vorgaben für die Cybersicherheit von Kommunen konnten aus verfassungsrechtlichen Gründen im Gesetzentwurf keine Berücksichtigung finden. Nach dem Kompetenzgefüge des Grundgesetzes ist dem Bund keine Gesetzgebungskompetenz für die Cybersicherheit von Kommunen zugewiesen, diese liegt bei den Ländern. Damit obliegt den Ländern auch die Entscheidung der optionalen Ausweitung des Anwendungsbereichs der Umsetzung der NIS-2-Richtlinie auf die lokale Ebene. Mit Beschluss 2023/39 des IT-Planungsrates vom 3. November 2023 wurde den Ländern empfohlen, keinen Gebrauch von der vorgenannten Option zu machen. Die Bundesregierung hat sich dem Beschluss nicht entgegengestellt, da es sich bei dem Beschlussgegenstand ausschließlich um eine Frage in der Zuständigkeit der Länder handelte. Unabhängig von dem vorliegenden Gesetzentwurf hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem sogenannten „Weg in die Basisabsicherung“ niedrigschwellige Leitfäden erstellt, wie auch Kommunen ihre Systeme sicherer machen können.

3.

Für den NKR ist nicht abschließend bewertbar, ob eine effektive Harmonisierung mit dem ebenfalls zu erarbeitenden KRITIS-Dachgesetz gewährleistet wird, weil die Regelungsvorhaben zu mindestens hinsichtlich der öffentlich bekannten Referentenentwürfe und Konsultationsprozesse nicht gemeinsam weiterentwickelt wurden. Dadurch war dem NKR, der Fachöffentlichkeit und den Betroffenen eine gemeinsame Bewertung nicht möglich.

Der NKR empfiehlt zudem für die geplanten digitalen Meldeprozesse auch potenziell Betroffene und Sicherheitsexperten in die Konzeption mit einzubinden.

Stellungnahme der Bundesregierung:

Hinsichtlich der vom NKR geforderten Kohärenz des Gesetzentwurfs mit dem zukünftigen Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz) ist darauf hinzuweisen, dass dies fortlaufend im Rahmen der Erstellung des Gesetzentwurfs und während der Ressortabstimmung berücksichtigt wurde.

Die Bundesregierung teilt die Bewertung des NKR zur Funktionalität des Meldeportals, welches das Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) einrichten werden. Um den Bürokratieaufwand so gering wie möglich und den betroffenen Unternehmen eine leichte Erfüllung der Meldepflichten nach dem KRITIS-Dachgesetz und dem BSI-Gesetz zu ermöglichen, soll ein gemeinsames Meldeportal für beide Gesetze genutzt werden. Eine Einbeziehung von potenziell Betroffenen und Sicherheitsexperten bei der Erarbeitung des Meldeportals wird als sinnvoll erachtet. Im Übrigen sind die unionsrechtlichen Vorgaben in Bezug auf den Zeitpunkt der nationalen Festlegung des jeweiligen persönlichen Anwendungsbereichs unterschiedlich. Der Anwendungsbereich der Umsetzung der NIS-2-Richtlinie ist bereits mit Ablauf der Richtlinienumsetzungsfrist (17. Oktober 2024) im Gesetz festzulegen, wohingegen die entsprechende Festlegung nach der CER-Richtlinie bis zum 17. Juli 2026 zu erfolgen hat. Insoweit wird die finale Kohärenz erst mit dem Inkrafttreten der nach dem KRITIS-Dachgesetz vorgesehenen Rechtsverordnung herzustellen sein. Gegebenenfalls sind auch im parlamentarischen Verfahren noch Angleichungen vorzunehmen.

Anlage 4

Stellungnahme des Bundesrates

Der Bundesrat hat in seiner 1047. Sitzung am 27. September 2024 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. Zum Gesetzentwurf allgemein

   a) Der Bundesrat bittet, in den Entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes aufzunehmen:

      aa) den Identitätsnachweis bei der Domainregistrierung bzw. Domainübertragung und bei einer automatisierten Datenabfrage;

      bb) einer Verpflichtung zur Identitätsprüfung von Domain-Anmeldungen und Domain-Übertragungen über qualifizierte Identifizierungsverfahren, z. B. Videoidentifizierungsverfahren oder die Vorlage eines elektronischen Identitätsnachweises, sodass sich die Anbieter Gewissheit über die Person des Beteiligten verschaffen können. Dies kann insbesondere durch Vorlage eines elektronischen Identitätsnachweises beispielsweise nach § 18 PAuswG, § 12 eID-Karte-G oder eines elektronischen Identitätsnachweises, der nach der eiDAS-VO von einem anderen Mitgliedstaat der Europäischen Union ausgestellt worden ist, erfolgen;

      cc) die Vorhaltung der genauen und vollständigen Domain-Namen-Registrierungsdaten in der Datenbank für die Abfrage von Zugriffsberechtigten;

      dd) die Verpflichtung für Domain-Registrare und Registrierungsdienstleister, möglichst in Echtzeit einem berechtigten Zugangsnachfrager vollständige Registrierungsdaten zur Verfügung zu stellen;

   b) Der Bundesrat bittet ferner, sich dafür einzusetzen, dass geregelt wird, unter welchen Voraussetzungen Domänen bei Missbrauch blockiert werden können.

   Begründung:

   Ein erheblicher Teil der Fake-Shops in Deutschland verfügt über eine „.de-Domain“, die bei Verbraucherinnen und Verbrauchern als besonders vertrauenswürdig gilt. Mit „.de Domains“ wird ein hohes Schutzniveau suggeriert, das tatsächlich nicht immer gewährleistet ist. Daher sollte für das wirksame Vorgehen gegen Fake-Shops eine „.de Domain“ Registrierung nur noch mit Identitätsprüfung möglich sein. Eine Vielzahl von Fakeshop-Betreibern lassen sich ältere oder nicht mehr genutzte „.de Domains“ von Unternehmen übertragen, um so von der Seriosität dieser Firmen zu profitieren. Insofern sollte auch für die Übertragung von „.de Domains“ eine Identitätsprüfung stattfinden, um die Hürde für die Registrierung von Fake-Shops unter falschen Angaben zu erhöhen.

   Die Verbraucherschutzministerkonferenz (VSMK) 2024 in Regensburg hat einstimmig einen Beschluss zur Verbesserung der Bekämpfung von Fakeshops gefasst (TOP 13/20. VSMK), welcher im weiteren Gesetzgebungsverfahren berücksichtigt werden soll.

   Zu Buchstabe a:

   In der Bundesratsinitiative BR-Drucksche 569/19 (Beschluss) ist die Bundesregierung gebeten worden zu prüfen, wie eine mit der Datenschutz-Grundverordnung (DSGVO) in Einklang stehende öffentliche Abfrage der Domain-Inhaberdaten nach Vorbild der Who-is-Abfrage der DENIC eingeführt werden könnte. Die DENIC eG verwaltet die Top-Level-Domain „.de“ und verantwortet den Domainbetrieb.

Die Einführung qualifizierter Identifizierungsverfahren bei der Domain-Registrierung wäre für die Fake-Shop-Bekämpfung eine entscheidende Verbesserung. Für die Prüfung der Registrierungsdaten auf den Verdacht des Betreibens eines Fake-Shops ist der vollständige Datensatz der Domainregistrierung erforderlich.

Zur Fake-Shop-Bekämpfung bei Missbrauch sind die zeitnahe und vollständige Verfügbarkeit der Registrierungsdaten für die Erkennung von Vorfällen und die Reaktion darauf von wesentlicher Bedeutung. Bei gewerblichen Domänen-Anmeldungen sollten zu jedem Domänennamen alle Inhaberdaten frei zugänglich sein. Bei personenbezogenen Daten sollten alle Daten veröffentlicht werden, soweit dies von der DSGVO gedeckt ist. Besonders wichtig ist, dass berechtigte Zugriffsnachfrager auch Zugriff auf alle .de Neuregistrierungen erhalten können. Da Fake-Shops mit legitimer Adresse eines anderen Unternehmens besonders gefährlich sind, ist der DSGVO-unbedenkliche Abgleich des Ortes im Impressum des Fake-Shops mit dem in den DENIC-Registrierungsdaten hinterlegten Ort des Fake-Shop-Bertreibers zwingend erforderlich.

Ein automatisiertes, digitales und datenschutzkonformes Zugriffsverfahren ist erforderlich, damit in Echtzeit auf die genauen und vollständigen Domain-Namen-Registrierungsdaten zugegriffen werden kann (z. B. über die sogenannte RDAP-Schnittstelle nach Vorbild der vorherigen Who-is-Abfrage der DENIC). Die Bekämpfung von missbräuchlichen Online-Angeboten erfordert Massenanalysen, die nach dem bisherigen Verfahren mit fallbezogenen und zeitversetzten Freigaben zeitnah nicht zu erreichen sind. Die Berechtigung sollte einmalig geprüft werden und nicht fallbezogen wie bisher mit pdf-Formularen. Als „berechtigte Zugangsnachfrager“ sollten Behörden, Verbraucherzentralen und beauftragte Sicherheitsunternehmen sowie Dienstleister, die nach einer Freischaltung generell Zugriff erhalten müssen (zum Beispiel auch die IT-Verantwortlichen des von der Verbraucherzentrale Nordrhein-Westfalen mit finanzieller Unterstützung der Bundesländer weiterentwickelten „Fake-Shop-Finder“) gelten.

Zu Buchstabe b:

Um wirksam gegen Fake-Shops vorgehen zu können, sind effektive Werkzeuge wie die Blockierung von Domänen bei Missbrauch innerhalb weniger Tage notwendig. Hierfür ist ein entsprechender Regelungsrahmen zu schaffen. Dabei sind bestehende europarechtliche Regelungen zu beachten und wenn nötig zu ergänzen. Auch sollte geprüft werden, inwieweit automatisierte Verfahren zum Einsatz kommen können.

2. Zum Gesetzentwurf allgemein

Der Bundesrat fordert, im weiteren Gesetzgebungsverfahren eine Refinanzierung der den Krankenhäusern im Rahmen der Umsetzung des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes entstehenden Kosten für Informationssicherheit sicherzustellen.

Begründung:

Die Gewährleistung von Informationssicherheit stellt auch im Krankenhausbereich einen Belang von erheblicher Bedeutung dar. Maßnahmen zur Steigerung der Informationssicherheit haben aber zwingend Mehrkosten zur Folge. Anders als andere Einrichtungen im Anwendungsbereich des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes können Krankenhäuser diese Mehrkosten nicht weitergeben, jedenfalls sofern dies nicht in sehr eingeschränktem Umfang über den Krankenhausstrukturfonds möglich ist, der jedoch nach aktueller Rechtslage Ende 2024 ausläuft. Dies wiegt umso schwerer, als sich Krankenhäuser ohnehin bereits mit erheblich gestiegenen Betriebskosten konfrontiert sehen, die aufgrund der bundesgesetzlichen Rahmenbedingungen für die Krankenhausvergütung bislang nicht vollumfänglich von den Kostenträgern refinanziert werden konnten. Die Situation der Krankenhäuser wird sich durch das geplante Krankenhausversorgungsverbesserungsgesetz (KHVVG) insoweit nicht hinreichend verbessern. Auch bleibt die Refinanzierung notwendiger Kosten für Investitionen in Digitalisierung und Informationssicherheit im Rahmen des KHVVG außer Betracht.

3. Zu Artikel 1 (§ 2 Nummer 21 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren in geeigneter Weise klarzustellen, dass die Entwicklung, der Betrieb und die rechtliche Ausgestaltung von länderübergreifenden Verfahren nach dem

IT-NetzG und dem IT-Staatsvertag zur Errichtung des IT-Planungsrates, die „im Auftrag einer oder mehrerer Einrichtungen der Bundesverwaltung betrieben“ werden, durch die Regelung des § 2 Nummer 21 BSIG-E zur „Kommunikationstechnik des Bundes“ nicht berührt wird.

Begründung:

Eine entsprechende klarstellende Erläuterung fehlt in der Begründung des Gesetzentwurfs. So sind insbesondere die Auswirkungen auf gemeinsam entwickelte und im Verbund betriebene Verfahren nach dem IT-NetzG und dem IT-Staatsvertag zur Errichtung des IT-Planungsrates nicht transparent. Offen ist insbesondere, ob sie unter den Begriff der „Kommunikationstechnik des Bundes“ fallen.

4. Zu Artikel 1 (§ 3 Absatz 1 Satz 2 Nummer 18 Buchstabe a, b BSIG)

Artikel 1 § 3 Absatz 1 Satz 2 Nummer 18 ist wie folgt zu ändern:

a) In Buchstabe a sind nach dem Wort „Bundes“ die Wörter „und der Länder“ einzufügen.

b) In Buchstabe b sind die Wörter „des Bundesamtes für Verfassungsschutz“ durch die Wörter „der Verfassungsschutzbehörden des Bundes und der Länder“ sowie die Wörter „dem Bundesverfassungsschutzgesetz“ durch die Wörter „den Verfassungsschutzgesetzen des Bundes und der Länder“ zu ersetzen.

Begründung:

Mit dieser Änderung wird die in der geltenden Fassung des BSIG bestehende Aufgabe des BSI aufrechterhalten. Diese besteht unter anderem darin, neben den Polizeibehörden und Nachrichtendiensten des Bundes auch die Polizei- und Verfassungsschutzbehörden der Länder bei ihren gesetzlichen Aufgaben bzw. bei der Auswertung und Bewertung von Informationen zu unterstützen. Auch die bestehende Aufgabe der Beobachtung von Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand des Staates oder die Sicherheit des Bundes oder eines Landes gerichtet sind, oder Aufgaben, welche bei der Beobachtung sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten anfallen, müssen aufrechterhalten werden.

Der vorliegende Gesetzentwurf sieht dagegen vor, diese Unterstützungsleistung künftig auf die Bundesbehörden zu beschränken. Die Möglichkeit der Amtshilfe bleibt ausweislich der Einzelbegründung zwar unberührt. Amtshilfe kann allerdings im Einzelfall von der ersuchten Behörde leichter abgelehnt werden, als die Durchführung einer Unterstützungsleistung, die der ersuchten Behörde als eigene Aufgabe obliegt. Insofern werden die Länder durch die geplante Neuregelung gegenüber der geltenden Gesetzesfassung schlechter gestellt – bei stetig steigender Bedeutung der Informationssicherheit von Bund und Ländern.

Die hier vorgeschlagene Änderung stellt die geltende Gesetzesfassung insofern wieder her.

Gerade mit Blick auf die aktuelle Sicherheitslage sind auch auf lokaler Ebene Ereignisse denkbar, in denen die Polizei- und Verfassungsschutzbehörden der Länder auf Unterstützungsleistungen durch das BSI angewiesen sind.

5. Zu Artikel 1 (§ 5 Absatz 2 Satz 2, § 6 Absatz 1 und 3 – neu – BSIG)

Artikel 1 ist wie folgt zu ändern:

a) In § 5 Absatz 2 Satz 2 sind nach dem Wort „Meldemöglichkeiten“ die Wörter „, einschließlich eines medienbruchfrei digitalisierten Meldeverfahrens in der Online-Plattform für den Informationsaustausch nach § 6 Absatz 1,“ einzufügen.

b) § 6 ist wie folgt zu ändern:

aa) Absatz 1 ist wie folgt zu fassen:

„(1) Das Bundesamt betreibt ab dem sechsten Monat nach Inkrafttreten dieses Gesetzes eine Online-Plattform zum Informationsaustausch mit wichtigen Einrichtungen, besonders wichtigen

Einrichtungen und Einrichtungen der Bundesverwaltung. Es kann die beteiligten Hersteller, Lieferanten oder Dienstleister zum Austausch über Cyberbedrohungen, Schwachstellen, Beinahevorfälle und IT-Sicherheitsmaßnahmen sowie zur Aufdeckung und Abwehr von Cyberangriffen mittels bedrohungsspezifischer Informationen, Cybersicherheitswarnungen, Kompromittierungsindikatoren und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten hinzuziehen. Das Bundesamt ermöglicht weiteren Stellen auf Antrag die Teilnahme, soweit ein berechtigtes Interesse vorliegt und übergeordnete Bedenken nicht entgegenstehen. Voraussetzung für den Zugang zur Online-Plattform ist eine Authentifizierung mit einem elektronischen Identitätsnachweis, der nach Artikel 6 der Verordnung (EU) Nr. 910/2014 mit dem Sicherheitsniveau „hoch“ anerkannt worden ist.“

bb) Folgender Absatz ist anzufügen:

„(3) Die Online-Plattform nach Absatz 1 ermöglicht in geeigneter Weise zugleich Zugang zu Informationen zu physischer Sicherheit und Resilienz kritischer Infrastrukturen, die vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe in Erfüllung von Vorgaben des Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 bereitgestellt werden.“

Begründung:

Dem Erfüllungsaufwand für die betroffenen Unternehmen und Einrichtungen sollte entsprechender Mehrwert für diese gegenüberstehen, um die Akzeptanz der neuen Infrastrukturen zu erhöhen und dadurch ihren Erfolg zu sichern.

Entsprechend sollte die in § 6 BSIG-E vorgesehene Möglichkeit des freiwilligen Austauschs relevanter Cybersicherheitsinformationen zwischen den in den Anwendungsbereich der Richtlinie fallenden und gegebenenfalls anderen Akteuren eine nähere Bestimmung hinsichtlich der Inhalte und organisatorischen Rahmenbedingungen bereits im Gesetz erfahren. Bei den Inhalten weicht der Gesetzentwurf vom Wortlaut der Richtlinie ab und lässt beispielsweise Kompromittierungsindikatoren und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten unerwähnt.

Erstrebenswert wäre insbesondere eine Verpflichtung der Authentifizierung der Teilnehmer mittels europäischer Identität auf Vertrauensniveau „hoch“, um die Vertraulichkeit der Nutzerbeschränkten Online-Plattform zu gewährleisten. Im Gegenzug sollte klargestellt werden, dass Betroffene mit berechtigtem Interesse Zugang erhalten, soweit keine übergeordneten Bedenken entgegenstehen. Um den Unternehmen Planungssicherheit zu geben, ist außerdem eine klare Vorgabe hinsichtlich der Frist wünschenswert, mit der die Informationsplattform zur Verfügung gestellt werden muss. Schließlich sollte der im NIS-2-Umsetzungsgesetz vorgesehene Zugang der Einrichtungen zu Informationen und unterstützenden Handlungsempfehlungen zu digitalen Bedrohungen, entsprechend den Bedürfnissen der Unternehmen, mit dem Zugang zu Informationen zu physischer Sicherheit und Resilienz kritischer Infrastrukturen gemäß KRITIS-Dachgesetz verknüpft werden.

Die in § 6 BSIG-E geregelte Informationsplattform sollte zugleich eine der in § 5 normierten „geeigneten Meldemöglichkeiten“ integrieren. Die allgemeine Meldestelle für die Sicherheit in der Informationstechnik sollte die Meldung, entsprechend der relevanten OZG/XÖV-Standards, in einem Ende-zu-Ende digitalisierten Verfahren realisieren.

6. Zu Artikel 1 (§ 7 Absatz 8, § 61 Absatz 11 BSIG)

In Artikel 1 § 7 Absatz 8 und § 61 Absatz 11 ist jeweils das Wort „offensichtliche“ zu streichen und sind die Wörter „Folge hat“ durch die Wörter „Folge haben kann“ zu ersetzen.

Begründung:

Die aktuelle Fassung der Verpflichtungen des Bundesamtes die zuständigen Datenschutzaufsichtsbehörden über eine Verletzung des Schutzes personenbezogener Daten zu unterrichten, bleibt hinter Artikel 35 Absatz 1 der NIS-2-Richtlinie zurück. § 7 Absatz 8 und § 61 Absatz 11 BSIG-E sollen laut Einzelbegründung

allerdings Artikel 35 der NIS-2-Richtlinie umsetzen.

Mit der Änderung wird eine Anpassung an den Wortlaut von Artikel 35 Absatz 1 der NIS-2-Richtlinie vorgenommen: Danach besteht die Unterrichtungspflicht, wenn die zuständigen IT-Sicherheitsbehörden im Zuge ihrer Aufgabenwahrnehmung feststellen, dass der Verstoß gegen Risikomanagementmaßnahmen oder Berichtspflichten eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 DSGVO zur Folge haben kann.

Artikel 35 Absatz 1 der NIS-2-Richtlinie fordert gerade keine Offensichtlichkeit oder das Feststehen der Datenschutzverletzung, sondern nur deren Möglichkeit.

Um die Richtlinie ordnungsgemäß umzusetzen und den Zwecken des Schutzes personenbezogener Daten und der Effektivität der Zusammenarbeit (wie sie Artikel 31 Absatz 3 der NIS-2-Richtlinie vorsieht) gerecht zu werden, sind in § 7 Absatz 8 und § 61 Absatz 11 BSIG-E die Einschränkungen zu streichen.

7. Zu Artikel 1 (§ 28 Absatz 8 Nummer 2 BSIG)

In Artikel 1 § 28 Absatz 8 Nummer 2 ist das Wort „vergleichbare“ durch die Wörter „die NIS-2-Richtlinie umsetzende“ zu ersetzen.

Begründung:

Mit dieser Norm wird für die Länder die Möglichkeit geschaffen, in eigener Verantwortung wirtschaftlich tätige rechtlich unselbstständige Organisationseinheiten von Gebietskörperschaften und juristische Personen, an denen ausschließlich Gebietskörperschaften, ausgenommen der Bund, beteiligt sind, vom Anwendungsbereich des BSIG-E auszunehmen. Eine Voraussetzung hierfür ist, dass die Einrichtungen „durch vergleichbare landesrechtliche Vorschriften“ reguliert werden (§ 28 Absatz 8 Nummer 2 BSIG-E).

Die bislang gewählte Formulierung „durch vergleichbare landesrechtliche Vorschriften“ in § 28 Absatz 8 Nummer 2 BSIG-E erweckt gemeinsam mit der Einzelbegründung den Eindruck, dass die jeweilige Einrichtung Gegenstand einer mit den Regelungen des BSIG-E vergleichbaren NIS-2-Umsetzung durch das betreffende Land sein muss.

Maßstab für vergleichbare Regelungen in den Ländern hat indes nicht die bundesrechtliche Regelung des BSIG-E zu sein, sondern vielmehr das unmittelbare EU-Recht, mithin die NIS-2-Richtlinie selbst. Die in diesem Antrag vorgeschlagene Änderung gewährleistet, dass Anpassungen der Regelungen in den Ländern nach möglichen Änderungen im BSIG-E vermieden werden und Maßstab stets die Vorgaben der NIS-2-Richtlinie sind und nicht etwa gegebenenfalls über die Mindestharmonisierung hinausgehende Vorgaben des Bundes.

8. Zu Artikel 1 (§ 30 Absatz 7 BSIG)

In Artikel 1 § 30 Absatz 7 sind nach dem Wort „Straftaten“ die Wörter „sowie der Unabhängigkeit der Datenschutzaufsichtsbehörden“ einzufügen.

Begründung:

Eine Einschränkung der Unabhängigkeit der Datenschutzaufsichtsbehörden wäre nur auf europarechtlicher Grundlage zulässig. Aus der NIS-2-Richtlinie ergibt sich jedoch indirekt, dass die Datenschutzaufsichtsbehörden zur Verhängung von Geldbußen (uneingeschränkt) befugt sind: Gem. Artikel 35 Absatz 2 der NIS-2-Richtlinie darf bei einer Geldbußenverhängung durch die Datenschutzaufsichtsbehörde keine zusätzliche Geldbuße nach Artikel 34 NIS-2-Richtlinie verhängt werden. Das setzt voraus, dass die Datenschutzaufsichtsbehörden weiterhin Geldbußen verhängen dürfen.

Die Änderung stellt klar, dass keine Einschränkung der Unabhängigkeit der Datenschutzaufsichtsbehörden geregelt wird. Diese Klarstellung soll bereits im Gesetzestext erfolgen.

9. Zu Artikel 1 (§ 38 Absatz 2 Satz 3 – neu – BSIG)

Dem Artikel 1 § 38 Absatz 2 ist folgender Satz anzufügen:

„Rechtsvorschriften im Hinblick auf die für öffentliche Einrichtungen geltenden Haftungsregelungen sowie die Haftung von öffentlichen Bediensteten und gewählten und ernannten Amtsträgerinnen und Amtsträgern bleibt unberührt."

Begründung:

Ziel ist eine konsequente 1:1-Umsetzung der NIS-2-Richtlinie.

Die Änderung führt zu einem Gleichlauf von NIS-2-Richtlinie und Umsetzungsgesetz. Die Bundesregierung selbst hat sich bei der Umsetzung von EU-Recht zum Ziel gesetzt, dass diese „effektiv, bürokratiearm und im Sinne des einheitlichen Europäischen Binnenmarktes erfolgt." An diesem selbstgesteckten Ziel muss sich die Bundesregierung messen lassen.

Es soll daher klargestellt werden, dass – wie in Artikel 20 Absatz 1 Satz 2 NIS-2-Richtlinie geregelt – die bestehenden Haftungsregelungen für öffentliche Einrichtungen sowie die Haftung von öffentlichen Bediensteten und gewählten und ernannten Amtsträgern unberührt bleiben.

Zur Rechtsklarheit trägt das Weglassen dieser Klarstellung – in Abweichung von der NIS-2-Richtlinie – nicht bei und führt im Gegenteil ggf. eher zu Rechtsunsicherheiten und Bürokratie- und Begründungsaufwand.

10. Zu Artikel 1 (§ 38 Absatz 3 Satz 2 – neu – BSIG)

Dem Artikel 1 § 38 Absatz 3 ist folgender Satz anzufügen:

„Die Geschäftsleitungen wirken daraufhin, dass allen Mitarbeiterinnen und Mitarbeitern besonders wichtiger und wichtiger Einrichtungen regelmäßig entsprechende Schulungen angeboten werden."

Folgeänderungen:

a) In der Inhaltsübersicht ist die Angabe zu Artikel 1 § 38 wie folgt zu fassen:

„§ 38

Governance".

b) In Artikel 1 § 38 ist die Überschrift wie folgt zu fassen:

„§ 38

Governance".

Begründung:

Ziel ist eine konsequente 1:1-Umsetzung der NIS-2-Richtlinie.

Die Änderung führt zu einem Gleichlauf von NIS-2-Richtlinie und Umsetzungsgesetz. Die Bundesregierung selbst hat sich bei der Umsetzung von EU-Recht zum Ziel gesetzt, dass diese „effektiv, bürokratiearm und im Sinne des einheitlichen Europäischen Binnenmarktes erfolgt." An diesem selbstgesteckten Ziel muss sich die Bundesregierung messen lassen.

Es kann mit Blick auf die Einzelbegründung zu § 38 Absatz 3 BSIG-E davon ausgegangen werden, dass bereits nach aktuellem Stand allen Mitarbeiterinnen und Mitarbeitern besonders wichtiger und wichtiger Einrichtungen regelmäßig entsprechende Schulungen anzubieten sind („Wichtige und besonders wichtige Einrichtungen werden aufgefordert, derartige Schulungen für alle Beschäftigten anzubieten"). Zur Klarstellung sollte dies auch aufgrund Artikel 20 Absatz 2 der NIS-2-Richtlinie in das beabsichtigte Gesetz übernommen werden, um Rechtssicherheit zu schaffen.

Die Folgeänderung trägt dieser Klarstellung Rechnung. Bislang stellt die Überschrift nur auf die Schulungspflicht für Geschäftsleitungen ab. Bei einer Anfügung des oben aufgeführten Satzes passt die Überschrift nicht mehr. Deshalb sollte diese – auch hier in 1:1 Umsetzung der NIS-2-Richtlinie – auf den übergeordneten Begriff der „Governance“ geändert werden, um auch die Schulungen der Mitarbeiterinnen und Mitarbeiter erfassen zu können.

11. Zu Artikel 1 (§ 40 Absatz 3 Nummer 5 – neu – BSIG)

Artikel 1 § 40 Absatz 3 ist wie folgt zu ändern:

a) In Nummer 3 ist das Wort „und“ am Ende durch ein Komma zu ersetzen.

b) In Nummer 4 Buchstabe d ist das Wort „unterrichten.“ durch die Wörter „unterrichten und“ zu ersetzen.

c) Folgende Nummer ist anzufügen:

„5. besonders wichtigen und wichtigen Einrichtungen geeignete Online-Formulare zur Verfügung zu stellen, welche es ermöglichen, zeitgleich mit einer Meldung nach § 32 die in Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 angegebenen Informationen mitzuteilen. Die Einrichtungen können ihrer Meldepflicht nach Artikel 33 der Verordnung (EU) 2016/679 durch eine Meldung an das Bundesamt mittels des nach Satz 1 genannten Online-Formulars nachkommen. Das Bundesamt stellt die Meldungen unverzüglich den zuständigen Datenschutzaufsichtsbehörden zur Verfügung. § 7 Absatz 8 und § 61 Absatz 11 bleibt unberührt.“

Begründung:

§ 40 BSIG-E regelt, dass das BSI zentrale Meldestelle ist und welche Aufgaben es insoweit zu erfüllen hat. Hierbei wird jedoch der Erwägungsgrund 106 der NIS-2-Richtlinie nicht aufgegriffen. Danach soll der Verwaltungsaufwand für Einrichtungen verringert werden. Insbesondere wird den Mitgliedstaaten nahegelegt die zentrale Anlaufstelle auch für Meldung zu nutzen, die nach der DSGVO erforderlich sind.

Durch die Verpflichtung des Bundesamtes, Online-Formulare für Meldungen nach Artikel 33 der DSGVO zur Verfügung zu stellen, wird der Impuls aus Erwägungsgrund 106 aufgegriffen und den Einrichtungen die Möglichkeit eröffnet, ihre Meldeverpflichtungen durch Meldung an eine Stelle zu erfüllen. Diese Möglichkeit einer Meldung nach Artikel 33 der DSGVO an das Bundesamt besteht dann, wenn die Einrichtung eine Meldung nach § 32 BSIG-E an das Bundesamt vornimmt. Durch die Bündelung beider Meldungen an eine Stelle wird Bürokratieentlastung erreicht und ein Impuls zur Vereinheitlichung der Anforderungen für eine Meldung nach Artikel 33 DSGVO gegeben. Außerdem wird mit der neuen Nummer 5 auch Artikel 31 Absatz 3 der NIS-2-Richtlinie Rechnung getragen, nach dem die Aufsichtsbehörden nach der NIS-2-Richtlinie eng mit den Datenschutzaufsichtsbehörden zusammenarbeiten.

Das zur Verfügung stellen der Online Formulare lässt die Verpflichtungen des Bundesamtes nach § 7 Absatz 8 und § 61 Absatz 11 BSIG-E unberührt. Die Bündelung der Meldung kann das Bundesamt jedoch in der Prüfung seiner Verpflichtungen nach § 7 Absatz 8 und § 61 Absatz 11 BSIG-E unterstützen.

12. Zu Artikel 1 (§ 43 Absatz 3 BSIG)

Der Bundesrat regt mit Blick auf § 43 Absatz 3 BSIG-E an, Musterverträge, vergleichbar dem EVB-IT, zu schaffen bzw. diese zu ergänzen, damit die IT-Dienstleister der Länder frühzeitig über die Erwartungshaltung und Auflagen des Auftraggebers „Bundesverwaltung“ informiert sind.

Begründung:

Erbringen öffentlich-rechtlich oder privatrechtlich organisierte Stellen im Auftrag des Bundes Leistungen der Informationstechnik, sind die Verträge zur Einhaltung der Voraussetzungen zur Gewährleistung der Informationssicherheit von besonderer Bedeutung. Betroffen von § 43 Absatz 3 BSIG-E können auch IT-Dienstleister der Länder über die Deutsche Verwaltungscloud und den Marktplatz sein, über den künftig

auch die Bundesverwaltung Leistungen abrufen kann. Ebenfalls wäre im Bereich des statistischen Verbundes, in dem das Bundesamt entsprechende Aufträge für Statistiken an die Länder erteilt, eine derartige Konstellation zu erwarten.

Musterverträge unterstützen die vorstehend genannten Stellen dabei, sich frühzeitig auf die Anforderungen dieses Auftraggebers einzustellen.

13. Zu Artikel 1 (§ 44 Absatz 5 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren, in geeigneter Weise den Ländern den Zugriff auf die technischen Richtlinien und Referenzarchitekturen im Sinne des § 44 Absatz 5 BSIG-E unter Wahrung der Vorschriften des Vergaberechts und des Geheimschutzes zu ermöglichen.

Begründung:

Im Sinne einer ganzheitlichen Architektur trägt der Zugriff zur länderübergreifenden Standardisierung bei und kann gleichzeitig dazu dienen, Aufwände in der öffentlichen Verwaltung zu reduzieren.

14. Zu Artikel 1 (§ 55 BSIG)

Der Bundesrat begrüßt das Bestreben der Bundesregierung, die Cybersicherheit im Rahmen der Umsetzung der NIS-2-Richtlinie zu erhöhen. Es wird jedoch auf die Notwendigkeit hingewiesen, die Transparenz von Sicherheitseigenschaften von verbrauchernahen Produkten mit digitalen Elementen bereits beim Kauf für Verbraucherinnen und Verbraucher zu verbessern. Die Bundesregierung wird daher um Prüfung einer Erweiterung des BSI-Sicherheitskennzeichens gebeten mit dem Ziel, dass

a) das BSI-Sicherheitskennzeichen auch Fragen des Datenschutzes berücksichtigt,

b) eine Ausweitung des Produktkatalogs auf alle verbrauchernahen Produkte und Dienstleistungen mit digitalen Elementen erfolgt und

c) das BSI-Sicherheitskennzeichen um eine Skala (in Sternen) erweitert wird, die eine einfache und intuitive Botschaft zur Sicherheit des Produktes mit digitalen Elementen transportiert, um insbesondere weniger digitalaffine Verbraucherinnen und Verbraucher bei ihrer Kaufentscheidung zu unterstützen und das IT-Sicherheitsniveau in der Gesellschaft insgesamt weiter zu erhöhen.

Begründung:

Eine Erweiterung des IT-Sicherheitskennzeichens könnte die Transparenz von Sicherheitseigenschaften von verbrauchernahen Produkten mit digitalen Elementen erhöhen und würde es Verbraucherinnen und Verbrauchern erleichtern, eine informierte Kaufentscheidung zu treffen. Unter anderem könnte der statische Teil des IT-Sicherheitskennzeichens um eine Skala ergänzt werden, die es Verbraucherinnen und Verbrauchern ermöglicht, direkt zu erkennen, wie sicher ein Produkt im Vergleich zu anderen ist. Dies ist vor allem vor dem Hintergrund notwendig, dass Verbraucherinnen und Verbraucher nach einer Studie zum Thema „Untersuchung zum Thema Verbrauchersicherheitswissen und -verhalten im Digitalen Raum“ (2022) (abrufbar unter www.conpolicy.de/data/user_upload/Pdf_von_Publikationen/studie-des-din-vr-zu-verbrauchersicherheitswissen-und-verhalten-im-digitalen-raum--data.pdf) teilweise dem statischen Teil des IT-Sicherheitskennzeichens eine Sicherheitsgarantie entnehmen, die das Zeichen tatsächlich nicht gibt.

15. Zu Artikel 1 (§ 56 Absatz 4, § 62 BSIG)

a) Der Bundesrat begrüßt grundsätzlich die im Gesetzentwurf vorgesehenen Regelungen zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundsätze des Informationssicherheitsmanagements in der Bundesverwaltung.

b) Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob neben dem anhand branchenspezifischer Schwellenwerte festzusetzenden Versorgungsgrad, weitere Kriterien in Ergänzung zu der Rechtsverordnung zur Bestimmung Kritischer Anlagen beziehungsweise Kritischer Dienstleistungen festzulegen sind.

c) Bei der vorgesehenen Umsetzung der NIS-2-Richtlinie in nationales Recht handelt es sich um einen wichtigen nächsten Schritt hin zu einer kohärenten Gesetzgebung zum Schutz der kritischen Infrastruktur. Wichtige und besonders wichtige Einrichtungen sollen vor Schäden durch Cyberangriffe geschützt und das Funktionieren des europäischen Binnenmarktes verbessert werden.

d) Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob die Frist zur Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in § 61 Absatz 1 BSIG-E genannten Verpflichtungen wie sie in § 61 Absatz 3 Satz 5 BSIG-E für Krankenhäuser vorgesehen ist, auch für wichtige Einrichtungen im Bereich des Gesundheitssektors gemäß der Bestimmung in § 28 Absatz 2 Nummer 3 BSIG-E vorgesehen und in die Regelung des § 61 BSIG-E aufgenommen werden kann.

Begründung:

Zu den Buchstaben a und b:

Grundsätzlich sollte der vorliegende Gesetzentwurf auch die stetig steigende Sicherheitsbedrohung für die Krankenhäuser durch die zunehmende Digitalisierung des öffentlichen Lebens sowie der Wirtschaft sachgerecht abbilden. In jüngster Vergangenheit sahen sich auch vermehrt Krankenhäuser einer steigenden Sicherheitsbedrohung durch Hackerangriffe auf ihre IT- Infrastruktur ausgesetzt.

Es wird jedoch das Risiko gesehen, dass nach dem vorliegenden Gesetzentwurf die weit überwiegende Zahl der Krankenhäuser zumindest in Nordrhein-Westfalen nicht vom Anwendungsbereich dieses Gesetzes umfasst sind und somit der bestehenden Sicherheitsbedrohung keine Rechnung getragen werden würde.

Zwar sieht § 56 Absatz 4 BSIG-E die Festsetzung der als kritisch anzusehenden Dienstleistungen beziehungsweise kritischen Anlagen anhand eines branchenspezifischen Schwellenwerts vor, jedoch bildet alleine ein solcher Schwellenwert die Bedeutung gerade von Krankenhäusern im ländlichen Raum nur unzureichend ab. Aufgrund des engen Zusammenhangs zum KRITIS-DachG sowie aufgrund des Artikels 30 des Gesetzentwurfs, ist derzeit davon auszugehen, dass der Schwellenwert für den Krankenhausbereich – wie auch im KRITIS-DachG – bei 500 000 zu versorgenden Einwohnern liegen wird. Mit Blick auf die besondere Stellung der Daseinsvorsorge im Gesundheitsbereich sind die Schwellenwerte grundsätzlich zu hinterfragen. Es wird daher gebeten, die Sinnhaftigkeit der alleinig entscheidenden Schwellenwerte vor diesem Hintergrund erneut zu prüfen.

Zu den Buchstaben c und d:

Der Gesetzentwurf dient der Umsetzung der NIS-2-Richtlinie und der Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Entsprechend der unionsrechtlichen Vorgaben wird der mit dem IT-Sicherheitsgesetz und dem IT-Sicherheitsgesetz 2.0 geschaffene Ordnungsrahmen durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz auf den Bereich bestimmter Unternehmen erweitert, zusätzlich werden entsprechende Vorgaben für die Bundesverwaltung eingeführt.

Schwerpunktmäßig wird eine Novellierung des BSI-Gesetzes vorgenommen. Dabei sollen die Vorgaben der NIS-2-Richtlinie 1:1 im Bereich Wirtschaft umgesetzt werden. Dadurch erweitert sich der Kreis der Unternehmen, die Risikomanagementmaßnahmen im Bereich der IT-Sicherheit und Meldepflichten bei IT-Sicherheitsvorfällen zu erfüllen haben.

Für den Bereich des Gesundheitswesens könnten künftig große Praxen, Berufsausübungsgemeinschaften (BAG) und Medizinische Versorgungszentren (MVZ) von den Vorschriften zu den kritischen Sektoren betroffen sein, wenn sie eines von zwei Kriterien erfüllen

– mindestens 50 Mitarbeiter oder
– über zehn Millionen Euro Jahresumsatz.

Davon könnten große ambulante Einrichtungen, umsatzstarke Praxen aus der Radiologie und Nuklearmedizin, Nephrologie oder Laboratoriumsmedizin betroffen sein (§ 28 Absatz 2 Nummer 3 BSIG-E).

Auf diese Einrichtungen kommen mit dem Gesetzentwurf neue Pflichten zu.

§ 61 BSIG-E beschreibt die Vorgehensweise gegenüber besonders wichtigen Einrichtungen. Zudem bestehen auch für bestimmte besonders wichtige Einrichtungen Ausnahmen betreffend die Umsetzungspflicht. So schreibt § 61 Absatz 3 Satz 5 BSIG-E fest, dass für Krankenhäuser nach § 108 SGB V eine Übergangsfrist von fünf Jahren nach Inkrafttreten des Gesetzes zur Vorlage von Nachweisen anzunehmen ist.

In Anbetracht der auch auf die wichtigen Einrichtungen mit dem Gesetzentwurf zukommenden Verpflichtungen wird die Notwendigkeit gesehen, eine entsprechende Übergangfrist auch für diese in § 62 BSIG-E vorzusehen.

Aus den vorgesehenen Verpflichtungen können sich weitere Aufwände und Kosten für die betroffenen Einrichtungen ergeben, die bisher nicht einkalkuliert sind. Der Umsetzungs- und Dokumentationsaufwand für die gesetzlich vorgeschriebenen Maßnahmen ist nicht unerheblich. Betroffene Einrichtungen, die erst jetzt beginnen, sich mit NIS-2-Vorschriften zu befassen, werden die Umsetzungsfrist ggf. nicht mehr einhalten können.

Zudem müssten diese Ausnahmetatbestände doch erst recht für (weniger) wichtige Einrichtungen gelten.

16. Zu Artikel 1 (Anlage 1 Nummer 5.2.1 Spalte D BSIG)

In Artikel 1 sind in Anlage 1 Nummer 5.2.1 Spalte D die Wörter „Unternehmen, die Abwasser nach § 2 Absatz 1 AbwAG“ durch die Wörter „Abwasserbeseitigungspflichtige im Sinne von § 56 WHG, die Abwasser“ zu ersetzen.

Begründung:

In der NIS-2-Richtlinie Artikel 1 § 2 wird in der Begriffsdefinition der Begriff Unternehmen nicht definiert. Die Auslegung des Begriffes Unternehmen kann dementsprechend sehr weitläufig gefasst werden. Entsprechend des Statistischen Bundesamtes wird ein Unternehmen als „[…] kleinste rechtlich selbstständige Einheit definiert, die aus handels- bzw. steuerrechtlichen Gründen Bücher führt und eine jährliche Feststellung des Vermögensbestandes bzw. des Erfolgs der wirtschaftlichen Tätigkeit vornehmen muss. […]“ (siehe: www.destatis.de/DE/Themen/ Branchen-Unternehmen/Handwerk/Glossar/unternehmen.html). In der Anlage 1 werden die Sektoren besonders wichtiger und wichtiger Einrichtungen aufgeführt. Hierbei werden unter Nummer 5.2.1 die Adressaten in der Abwasserbeseitigung bestimmt. Jedoch wird mit Verweis auf „§ 2 Absatz 1 AbwAG“ lediglich der Begriff „Abwasser“ an sich definiert. Da in jedem Unternehmen Abwasser anfällt und gesammelt wird (Regen- wie Sanitärabwasser), wird der Adressatenkreis überproportional erweitert. Entsprechend der Definition vom Statistischen Bundesamt kann hierunter z. B. auch ein Kleingartenverein oder Straßenbaulastträger fallen. Zielführender ist es, die Abwasserbeseitigungspflichtigen gemäß § 56 WHG direkt zu adressieren. Die gewählte Formulierung dient auch der einheitlichen Darstellung der Anlage 1 Nummer 5.

Anlage 5

Gegenäußerung der Bundesregierung zu der Stellungnahme des Bundesrates

Die Bundesregierung äußert sich zur Stellungnahme des Bundesrates wie folgt:

Zum Gesetzentwurf allgemein

Die Bundesregierung lehnt den Vorschlag für dieses Gesetzgebungsverfahren ab.

Die Bundesregierung teilt die Einschätzung, dass die Bekämpfung von Fake-Shops im Interesse der Verbraucherinnen und Verbraucher wichtig ist. Maßnahmen sollten jedoch eingeordnet werden in die bestehenden Rechtsgrundlagen und Strategien nach Landesrecht und insbesondere sollten neue Maßnahmen auf ihre Wirksamkeit hin im gesamten Kontext untersucht werden, bevor Regelungen hierzu beschlossen werden. Aus Sicht der Bundesregierung ist der Vorschlag insoweit noch nicht ausgereift und sollte noch entsprechend ergänzend ausgearbeitet, unter Einbeziehung kriminalistischer Erfahrung diskutiert und geprüft werden. Für den anschließenden Bund-Länder-Dialog kommen verschiedene Foren in Betracht und die Bundesregierung sieht einer entsprechenden Initiative der Länder entgegen. Das vorliegende Gesetzgebungsvorhaben gibt dafür leider keine Gelegenheit mehr, denn die Umsetzung der NIS-2-Richtlinie eilt sehr. §§ 49-51 BSIG-E dienen einer 1:1-Umsetzung des Artikels 28 der NIS-2-Richtlinie[1] und sind daher unverzichtbar.

Zum Gesetzentwurf allgemein

Die Bundesregierung lehnt den Vorschlag ab.

Die Finanzierung von Investitionsmaßnahmen im Krankenhausbereich ist nach dem Prinzip der dualen Finanzierung Aufgabe der Länder. Durch fehlende Investitionen der Länder ist in den vergangenen Jahren eine Lücke entstanden, so dass Krankenhäuser hier vermehrt Eigenmittel aufwenden müssen.

Aus diesen Gründen wurde der Krankenhausstrukturfonds (KHSF) als zeitlich befristetes Förderprogramm errichtet, um die Länder bei Investitionen zur Verbesserung der Bedarfsgerechtigkeit der Krankenhausstruktur zu unterstützen. Im Zuge der Verlängerung des KHSF wurde auch die Förderung von Investitionen in die informationstechnische Sicherheit als Fördertatbestand für diejenigen Krankenhäuser ergänzt, die als kritische Infrastrukturen anzusehen sind, weil die entsprechenden Aufwendungen durch die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) bundesrechtlich induziert waren. Im Rahmen der geplanten Krankenhausreform ist vorgesehen, den KHSF bis Ende 2025 zu verlängern.

Der Krankenhauszukunftsfonds (KHZF) wurde im Jahr 2020 ebenfalls als einmaliges und befristetes Förderprogramm für die Förderung von Digitalisierungsmaßnahmen in Krankenhäusern errichtet. Es handelt sich somit bei beiden Programmen um eine Anschubfinanzierung in Bezug auf Digitalisierungsmaßnahmen, und nicht um die Etablierung einer dauerhaften Finanzierung. Eine Fortsetzung dieser Förderprogramme ist – auch mangels verfügbarer bundesseitiger Haushaltsmittel – nicht geplant.

Soweit auch nach Auslaufen der Fördermöglichkeiten KHSF II und KHZF weiterer Investitionsbedarf im Bereich der Digitalisierung von Krankenhäusern besteht, wäre es Aufgabe der Länder, die hierfür erforderlichen Mittel zur Verfügung zu stellen; soweit es sich um pflegesatzfähige Kosten handelt (z. B. für zusätzliches Personal, pflegesatzfähige Instandhaltungskosten), werden diese im Rahmen der geltenden Regelungen der pauschalierten Entgelte von den Kostenträgern refinanziert. Eine Erhöhung der pauschal berücksichtigten pflegesatzfähigen Instandhaltungskosten für Anlagegüter in Höhe von 1,1 Prozent der für die allgemeinen Krankenhausleistungen

[1] 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 Richt-linie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148.

vereinbarten Vergütung, die systematisch eigentlich von den Ländern zu tragen sind und bis Anfang der 1990er Jahre auch getragen wurden, ist nicht beabsichtigt. Soweit die Investitionsfördermittel der Länder weiter auf einem niedrigen Niveau bleiben und die Länder diese Mittel nicht substanziell erhöhen, führt dies dazu, dass in der Praxis die Krankenhäuser einen Großteil der Kosten tragen werden müssen.

Zu Artikel 1 (§ 2 Nummer 21 BSIG-E)

Die Bundesregierung lehnt den Vorschlag ab.

Bereits in der aktuell geltenden Fassung des BSI-Gesetzes ist geregelt, dass „Informationstechnik, die von einer oder mehreren Bundesbehörden oder im Auftrag einer oder mehrerer Bundesbehörden betrieben wird und der Kommunikation oder dem Datenaustausch innerhalb einer Bundesbehörde, der Bundesbehörden untereinander oder der Bundesbehörden mit Dritten dient“ von der Regelung umfasst ist. „Im Auftrag einer oder mehrerer Bundesbehörden“ betriebene IT kann also schon jetzt länderübergreifende Verfahren berühren. Die Regelung wird lediglich von „Bundesbehörden“ auf „Einrichtungen der Bundesverwaltung“ erweitert. Die Definition der „Einrichtungen der Bundesverwaltung“ gemäß § 29 BSIG-E umfasst zusätzlich zu den Bundesbehörden die öffentlich-rechtlichen IT-Dienstleister der Bundesverwaltung sowie Körperschaften, Anstalten und Stiftungen öffentlichen Rechts, soweit durch das Bundesamt für Sicherheit in der Informationstechnik (im Folgenden BSI oder Bundesamt) im Einvernehmen mit dem zuständigen Ressort angeordnet.

Zu Artikel 1 (§ 3 Absatz 1 Nummer 18 BSIG-E)

Die Bundesregierung lehnt den Vorschlag ab.

Durch die Änderung wird die Möglichkeit zur Leistung von Amtshilfe durch das Bundesamt nicht eingeschränkt. Die bisherige Regelung stellte ohnehin lediglich eine einfachgesetzliche Ausgestaltung der Amtshilfe dar.

Zu Artikel 1 (§ 5 Absatz 2 Satz 2, § 6 Absatz 1 und 3 – neu – BSIG-E)

Die Bundesregierung lehnt den Vorschlag ab.

Zu a)

Die Meldemöglichkeit nach § 5 Absatz 2 Satz 2 BSIG-E existiert bereits in digitalisierter Form, eine zusätzliche gesetzliche Regelung ist daher nicht notwendig.

Zu aa)

Die in § 6 Absatz 1 BSIG-E genannten Informationen umfassen die des Artikel 29 der NIS-2-Richtlinie (vgl. dazu auch die entsprechende Gesetzesbegründung), insofern wird die Richtlinie vollständig umgesetzt.

Die Authentifizierungsmodalitäten für die Online-Plattform zum Informationsaustausch nach § 6 BSIG-E können im Rahmen der Teilnahmebedingungen gemäß § 6 Absatz 2 BSIG-E festgelegt werden.

Eine mögliche Erweiterung des Teilnehmerkreises ist bereits in § 6 Absatz 1 Satz 3 BSIG-E vorgesehen, eine weitere Qualifizierung zusätzlicher Teilnehmer erscheint entbehrlich.

Zu bb)

Der Austausch von Informationen zur physischen Sicherheit geht über die angestrebte 1:1-Umsetzung der NIS-2-Richtlinie hinaus und ist auch nicht Gegenstand der CER-Richtlinie[1]. Zur Umsetzung der Registrierungs- und Meldevorschriften der NIS-2-Richtlinie sieht der Regierungsentwurf in § 32 Absatz 1 und § 33 Absatz 2 BSIG-E jedoch bereits ein gemeinsames Meldeportal von BSI und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) vor, das gegebenenfalls zukünftig als Ausgangspunkt für ein solches Angebot dienen kann.

[1] 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.

Zu Artikel 1 (§ 7 Absatz 8, § 61 Absatz 11 BSIG-E)

Die Bundesregierung wird den Vorschlag prüfen.

Zu Artikel 1 (§ 28 Absatz 8 Nummer 2 BSIG-E)

Die Bundesregierung lehnt den Vorschlag ab.

Mit dem vorliegenden Gesetzentwurf wird eine bundeseinheitliche Umsetzung für die wirtschaftsbezogenen Regelungen der NIS-2-Richtlinie geschaffen. Diese Einheitlichkeit soll auch dann gewährleistet werden, wenn einzelne wirtschaftlich tätige Unternehmen – die sonst vom Anwendungsbereich des § 28 BSIG-E erfasst würden – aufgrund der Öffnungsklausel durch Landesrecht reguliert werden. Durch die 1:1-Umsetzung der NIS-2-Richtlinie im Bereich der Wirtschaft ist dabei keine Mehrbelastung der Länder zu erwarten.

Zu Artikel 1 (§ 30 Absatz 7 BSIG-E)

Die Bundesregierung lehnt den Vorschlag ab.

Die Unabhängigkeit der Datenschutzaufsichtsbehörden nach Artikel 52 Absatz 1 der Datenschutz-Grundverordnung (DSGVO) gilt unionsrechtlich unbedingt und kann durch nationales Recht nicht eingeschränkt werden.

Zu Artikel 1 (§ 38 Absatz 2 Satz 3 BSIG-E)

Die Bundesregierung wird den Vorschlag prüfen.

Es bestehen Zweifel, ob die unveränderte Übernahme des Wortlauts in Artikel 20 Absatz 1 Satz 2 der NIS-2-Richtlinie tatsächlich der mit dem Vorschlag bezweckten Klarstellung dient. Insbesondere ist zu prüfen, ob der im nationalen Recht unbestimmte Rechtsbegriff der „öffentlichen Einrichtung“ nicht zu einer unionsrechtswidrigen Einschränkung der Umsetzung der Richtlinienvorgabe führt.

Zu Artikel 1 (§ 38 Absatz 3 BSIG-E)

Die Bundesregierung lehnt den Vorschlag ab.

Artikel 20 Absatz 2 der NIS-2-Richtlinie verpflichtet die Mitgliedstaaten lediglich, wichtige und besonders wichtige Einrichtungen aufzufordern, „allen Mitarbeitern regelmäßige Schulungen anzubieten“. Einer gesetzlichen Regelung bedarf es dafür nicht. Der Vorschlag würde durch die Schaffung neuer Pflichten für die Geschäftsleitungen wichtiger und besonders wichtiger Einrichtungen vielmehr über eine 1:1-Umsetzung der Richtlinie hinausgehen.

Im Übrigen wird darauf hingewiesen, dass § 30 Absatz 2 Nummer 7 BSIG-E (als Umsetzung von Artikel 21 Absatz 2 Buchstabe g der NIS-2-Richtlinie) „Schulungen im Bereich der Cybersicherheit“ als Teil der von den Einrichtungen zu ergreifenden Cybersicherheitsmaßnahmen vorsieht.

Zu Artikel 1 (§ 40 Absatz 3 Nummer 3, Nummer 4 Buchstabe d, Nummer 5 – neu – BSIG-E)

Die Bundesregierung lehnt den Vorschlag ab.

Die Vereinbarkeit des Vorschlags mit Artikel 33 der DSGVO ist nicht gegeben. Die DSGVO enthält im Übrigen auch keine Öffnungsklausel für abweichende nationale Verfahrensregelungen.

Zu Artikel 1 (§ 43 Absatz 3 BSIG-E)

Die Bundesregierung wird die Erstellung von Musterverträgen prüfen. Durch den Vorschlag entsteht jedoch kein Änderungsbedarf am Gesetzentwurf.

Zu Artikel 1 (§ 44 Absatz 5 BSIG-E)

Die Bundesregierung wird den Zugriff der Länder auf technische Richtlinien und Referenzarchitekturen des Bundes im Rahmen der Vorschriften prüfen. Durch den Vorschlag entsteht jedoch kein Änderungsbedarf am Gesetzentwurf.

Zu Artikel 1 (§ 55 BSIG-E)

Die Bundesregierung lehnt den Vorschlag zu a) ab, stimmt dem Vorschlag zu b) zu und wird den Vorschlag zu c) prüfen.

Zu a)

Das IT-Sicherheitskennzeichen wurde bewusst nur mit dem Fokus auf IT-Sicherheit entwickelt. Im Hinblick auf den künftigen Cyber Resilience Act (CRA) soll das IT-Sicherheitskennzeichen den Herstellern eine Hilfestellung zur Erfüllung der CRA-Schutzziele bieten. Eine Aufnahme des Datenschutzes würde dieser Strategie entgegenstehen.

Zu b)

Das BSI arbeitet bereits an der Aufnahme von weiteren Produktkategorien (zuletzt „Mobile Endgeräte“). Für die Aufnahme von neuen Kategorien bedarf es aber erst die Verfügbarkeit von angemessenen IT-Sicherheitsanforderungen sowie korrespondierenden Prüfspezifikationen. Die Entwicklung dieser ist zeitintensiv, sodass eine Ausweitung nicht sofort erfolgen kann. Gesetzliche Änderungen sind nicht erforderlich.

Zu c)

Das IT-Sicherheitskennzeichen wird derzeit evaluiert mit dem Ziel, es für die Zukunft zu verbessern. Eine Erweiterung des IT-Sicherheitskennzeichens um eine Skala oder unterschiedliche Level (bspw. ähnlich wie das Label von Singapur) kann ein mögliches Evaluierungsergebnis sein.

Zu Artikel 1 (§ 56 Absatz 4, 62 BSIG-E)

Die Bundesregierung nimmt die Ausführungen zu a) und c) erfreut zur Kenntnis und lehnt den Vorschlag zu b) und d) ab.

Zu b)

Die bestehende Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) soll im Wesentlichen unverändert fortgeführt werden. Eine Anpassung von Schwellenwerten ist im Rahmen dieses Gesetzes nicht geplant. Es wird jedoch darauf hingewiesen, dass die BSI-KritisV lediglich der Identifizierung kritischer Infrastrukturen dient. Die Identifizierung wichtiger und besonders wichtiger Einrichtungen ist dagegen in § 28 BSIG-E abschließend geregelt, wobei hierzu Unternehmenskennzahlen wie etwa Mitarbeiterzahl und Jahresbilanzsumme zugrunde gelegt werden. Der Versorgungsgrad spielt hierbei keine Rolle. Die Einschätzung, dass Krankenhäuser vielfach nicht unter den Anwendungsbereich des Gesetzes fallen würden, kann daher nicht geteilt werden, vielmehr werden Krankenhäuser regelmäßig zumindest als wichtige oder besonders wichtige Einrichtungen von den wesentlichen Vorgaben des BSIG-E – unter anderem zur Einhaltung der nach § 30 BSIG-E verpflichtenden Risikomanagementmaßnahmen – erfasst werden.

Zu d)

Wie in Artikel 33 der NIS-2-Richtlinie vorgesehen, gilt für wichtige Einrichtungen eine *ex post*-Aufsicht. So kann das BSI bei einer wichtigen Einrichtung z. B. im Fall des Auftretens eines IT-Sicherheitsvorfalls die Einhaltung der gesetzlichen Verpflichtungen überprüfen und Maßnahmen nach § 61 BSIG-E ergreifen, vgl. § 62 BSIG-E. Eine Ex-ante-Aufsicht – wie bei besonders wichtigen Einrichtungen – oder gar eine allgemeine Nachweispflicht – wie bei Betreibern kritischer Anlagen – ist gerade nicht vorgesehen. Da hierdurch die Verhältnismäßigkeit der

Aufsichtsmaßnahmen bereits ausreichend sichergestellt ist, wird der Änderungsbedarf im Sinne des Vorschlags nicht geteilt.

Zu Artikel 1 (Anlage 1 Nummer 5.2.1 BSIG-E)

Die Bundesregierung lehnt den Vorschlag ab.

Anlage 1 Nummer 5.2.1 BSIG-E stellt eine 1:1-Umsetzung der NIS-2-Richtlinie dar (dort Anhang 1 Nummer 7). Im Übrigen wird darauf hingewiesen, dass die Einrichtungsart jedoch nicht solche Unternehmen erfasst, „für die das Sammeln, die Entsorgung oder die Behandlung solchen Abwassers ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist.“. Mit einer Identifizierung der in der Vorschlagsbegründung genannten Beispiele („Kleingartenverein“, „Straßenbaulastträger“) als wichtige oder besonders wichtige Einrichtung ist nach Auffassung der Bundesregierung daher nicht zu rechnen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333