Referentenentwurf

des Bundesministeriums des Innern und für Heimat

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 Infrastrukturen, 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 einer Vielzahl von Herausforderungen. Europaweit und global vernetzte Prozesse führen ebenso wie die zunehmende Digitalisierung aller Lebens- und somit auch Wirtschaftsbereiche zu einer höheren Anfälligkeit durch externe, vielfach nicht steuerbare 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 zu Siedlungsabfällen. Gleiches gilt für das Funktionieren der Marktwirtschaft in Deutschland und dem Binnenmarkt der Europäischen Union. Die Vernetzung und enge Verzahnung der Wirtschaft innerhalb Deutschlands und der Europäischen Union resultieren in Interdependenzen bei der Cybersicherheit. Die vor diesem Hintergrund erforderlichen 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. Dezember 2022, S. 80, im Folgenden NIS-2-Richtlinie) in der gesamten Europäischen Union weiter angeglichen.

In Folge 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 2022 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 „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 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. 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 robust und leistungsfähig zu halten.

Für das Informationssicherheitsmanagement in der Bundesverwaltung haben sich die bisherigen Steuerungsinstrumente auf überwiegend untergesetzlicher Basis als nicht ausreichend effektiv erwiesen, um eine flächendeckende 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 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 für 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 Umsetzungsspielraums minimiert werden.

– Ausweitung des BSI Instrumentariums 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 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.

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 10 Beschäftigten und einem Jahresumsatz von mindestens einer Millionen 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 10 Beschäftigten. Unter der Annahme einer Gleichverteilung des Gesamtschadensvolumens auf die Unternehmen mit mindestens 10 Beschäftigten ergibt sich ein Schadensvolumen pro Unternehmen 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 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

[Anm. BMI CI1 – Für die formal korrekte Darstellung unter D. sind noch weitere Angaben erforderlich, die im Rahmen der laufenden Ressortabstimmung abgefragt werden. Eine Darstellung erfolgt in der nächsten Fassung des Referentenentwurfs.]

[…]

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen wird finanziell und stellenmäßig im Gesamthaushalt ausgeglichen.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Es entsteht kein Erfüllungsaufwand für die Bürgerinnen und Bürger.

E.2 Erfüllungsaufwand für die Wirtschaft

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

Davon Bürokratiekosten aus Informationspflichten

Es entfallen rund 121 Millionen Euro auf Bürokratiekosten aus Informationspflichten.

E.3 Erfüllungsaufwand der Verwaltung

[Anm. BMI CI1 – Für die formal korrekte Darstellung unter E.3 sind noch weitere Angaben erforderlich, die im Rahmen der laufenden Ressortabstimmung abgefragt werden. Eine Darstellung erfolgt in der nächsten Fassung des Referentenentwurfs. Erfüllungsaufwände nach diesem Gesetz für die Länder fallen nicht an.]

[…]

F. Weitere Kosten

Keine.

Referentenentwurf des Bundesministeriums des Innern und für Heimat

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)]

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Inhaltsübersicht

[1)] 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 1

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

(BSI-Gesetz – BSIG)

Inhaltsübersicht

Teil 2
Das Bundesamt

Kapitel 1
Aufgaben und Befugnisse

Kapitel 2
Datenverarbeitung

Teil 3
Sicherheit in der Informationstechnik von Einrichtungen

Kapitel 1
Anwendungsbereich

Kapitel 2
Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten

Kapitel 3
Informationssicherheit der Einrichtungen der Bundesverwaltung

Teil 4

Datenbanken der Domain-Name-Registrierungsdaten

Teil 5

Zertifizierung und Kennzeichen

Teil 6

Verordnungsermächtigungen, Grundrechtseinschränkungen und Berichtspflichten

Teil 7

Sanktionsvorschriften und Aufsicht

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

(1) Im Sinne dieses Gesetzes ist oder sind

1. „Beinahevorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, 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. „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 diese Ressourcen auf mehrere Standorte verteilt sind;

3. „Content Delivery Network“ ein Netz dezentraler Server zur Gewährleistung einer hohen Verfügbarkeit, Zugänglichkeit oder Zustellung digitaler Inhalte und Dienste für Internetnutzer mit möglichst niedriger Latenz im Auftrag von Inhalte- und Diensteanbietern;

4. „Cyberbedrohung“ eine Cyberbedrohung nach Artikel 2 Nummer 8 der Verordnung (EU) 2019/881;

5. „Datenverkehr“ mittels technischer Protokolle übertragene Daten; Telekommunikationsinhalte nach § 3 Absatz 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes können enthalten sein;

6. „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;

7. „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;

8. „erhebliche Cyberbedrohung“ eine Cyberbedrohung, die das Potenzial besitzt, die informationstechnischen Systeme, Komponenten und Prozesse aufgrund der besonderen technischen Merkmale der Cyberbedrohung erheblich zu beeinträchtigen; eine Beeinträchtigung ist erheblich, wenn sie erheblichen materiellen oder immateriellen Schaden verursachen kann;

9. „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,

   soweit nach Absatz 2 keine weitergehende Begriffsbestimmung erfolgt;

10. „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, die jedoch Bildungseinrichtungen nicht einschließt;

11. „Geschäftsleitung“ eine natürliche Personen, 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;

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

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

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

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

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

17. „Internet Exchange Point“ oder „IXP“ eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen Netzen (autonomen Systemen) ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr, der nur der Zusammenschaltung autonomer Systeme dient und weder voraussetzt, dass der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft; noch den betreffenden Datenverkehr verändert oder anderweitig beeinträchtigt;

18. „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; davon ausgenommen ist 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;

19. „kritische Anlage“ eine Anlage, die eine kritische Dienstleistung erbringt; welche Anlagen im Einzelnen kritische Anlagen sind, bestimmt sich nach § 28 Absatz 6;

20. „kritische Komponenten“ IKT-Produkte,

    a) die in kritischen Anlagen eingesetzt werden,

    b) bei denen Störungen der Verfügbarkeit, Integrität, Authentizität 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 Komponente bestimmt werden oder

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

    werden für einen der in § 57 Absatz 4 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, gibt es in diesem Sektor keine kritischen Komponenten im Sinne von dieser Nummer;

21. „kritische Dienstleistung“ eine Dienstleistung, die eine hohe Bedeutung für das Funktionieren des Gemeinwesens hat, da durch ihren Ausfall oder ihre Beeinträchti-gung langfristige Versorgungsengpässe oder Gefährdungen für wirtschaftliche Tätig-keiten, die öffentliche Sicherheit oder Ordnung, die öffentliche Gesundheit, wichtige gesellschaftliche Funktionen oder die Erhaltung der Umwelt eintreten;

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

23. „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;

24. „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;

25. „Online-Marktplatz“ ein Dienst nach § 312l Absatz 3 BGB;

26. „Online-Suchmaschine“ ein digitaler Dienst nach Artikel 2 Nummer 5 der Verordnung (EU) 2019/1150;

27. „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;

28. „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-Telemedien-Datenschutz-Gesetzes enthalten;

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

30. „qualifizierter Vertrauensdienst“ ein qualifizierter Vertrauensdienst nach Artikel 3 Nummer 17 der Verordnung (EU) Nr. 910/2014;

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

32. „Rechenzentrumsdienst“ ein Dienst, mit dem bereitgestellt werden:

    a) spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von IT- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie

    b) alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle (Housing oder Hosting);

33. „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;

34. „Schnittstellen der Kommunikationstechnik des Bundes“ sicherheitsrelevante Netzwerkübergänge innerhalb der Kommunikationstechnik des Bundes sowie zwischen dieser und der Informationstechnik der einzelnen Einrichtungen der Bundesverwaltung, Gruppen von Einrichtungen der Bundesverwaltung oder Dritter; nicht als Schnittstellen der Kommunikationstechnik des Bundes gelten die Komponenten an den Netzwerkübergängen, die in eigener Zuständigkeit der in Nummer 18 genannten Gerichte und Verfassungsorgane betrieben werden;

35. „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;

36. „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;

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

38. „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;

39. „Top Level Domain Name Registry“ ein Unternehmen, das 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 das Unternehmen selbst erfolgt oder ausgelagert wird; keine Top Level Domain Name Registry sind Register, die TLD-Namen nur für eigene Zwecke verwenden;

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

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

42. „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.

(2) Das Bundesministerium des Innern und für Heimat kann durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, bestimmen, wann ein Sicherheitsvorfall im Hinblick auf seine technischen oder organisatorischen Ursachen oder seine Auswirkungen auf die Einrichtung, Staat, Wirtschaft und Gesellschaft oder die Anzahl der von den Auswirkungen Betroffenen als erheblich im Sinne von Absatz 1 Nummer 9 anzusehen ist. Das Bundesministerium kann die Ermächtigung durch Rechtsverordnung auf das Bundesamt übertragen. Für den Fall, dass die Europäische Kommission einen oder mehrere Durchführungsrechtsakte gemäß Artikel 23 Absatz 11 Unterabsatz 2 der NIS-2-Richtlinie erlässt, worin näher bestimmt wird, in welchen Fällen ein Sicherheitsvorfall als erheblich anzusehen ist, geht dieser oder gehen diese der Rechtsverordnung nach Satz 1 und 2 insoweit vor.

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 zu 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 sowie Überprüfung der Einhaltung dieser Sicherheitsanforderungen festlegen;

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 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) 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, einschließlich der Bereitstellung praxisnaher Handreichungen zur Umsetzung der IT-Sicherheitsvorschriften, insbesondere der Vorgaben nach § 30 und § 44 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, dessen Unterstützung im Rahmen der Unabhängigkeit erfolgt, die ihm bei der Erfüllung 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 sowie der Bereitstellung von Handreichungen zur Umsetzung von Informationssicherheitsvorgaben, beraten und unterstützen;

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 terroristischer Bestrebungen oder nachrichtendienstlicher Tätigkeiten im Rahmen der gesetzlichen Befugnisse nach den Verfassungsschutzgesetzen des Bundes 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 bei sicherheitstechnischen Anforderungen an IT-Produkte, unter Berücksichtigung bestehender Normen und Standards sowie 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.

(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 Informationen 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 mit 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, 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 ermöglicht den Informationsaustausch zwischen besonders wichtigen Einrichtungen, wichtigen Einrichtungen, Einrichtungen der Bundesverwaltung sowie deren jeweiligen Lieferanten oder Dienstleistern zu Cyberbedrohungen, Beinahevorfällen, Schwachstellen, Techniken und Verfahren, Kompromittierungsindikatoren, gegnerischen Taktiken, bedrohungsspezifischen Informationen, Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten sowie zur Aufdeckung von Cyberangriffen. Es betreibt dazu ein geeignetes Online-Portal.

(2) Die Teilnahme am Informationsaustausch steht grundsätzlich allen besonders wichtigen Einrichtungen, wichtigen Einrichtungen, Einrichtungen der Bundesverwaltung, sowie den jeweiligen Lieferanten oder Dienstleistern dieser Einrichtungen offen. Das Bundesamt kann entsprechende Teilnahmebedingungen erstellen, die die Teilnahme am Informationsaustausch regeln. Das Bundesamt kann weiteren Stellen die Teilnahme ermöglichen.

§ 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 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 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, zu den Grundstücken und Betriebsräumen, einschließlich Datenverarbeitungsanlagen und -geräten, die für die Kommunikationstechnik des Bundes verwendet werden, Zugang 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 sowie Unterlagen und Datenträger des Betreibers einsehen und unentgeltlich Kopien, auch in elektronischer Form, anfertigen.

(4) Das Bundesamt teilt das Ergebnis seiner Kontrolle nach den Absätzen 1 bis 3 dem jeweiligen überprüften Betreiber, im Falle einer Einrichtung der Bundesverwaltung zusätzlich der oder dem Informationssicherheitsbeauftragten des Ressorts sowie der zuständigen Rechts- und Fachaufsicht sowie dem Koordinator oder der Koordinatorin für Informationssicherheit mit. 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.

(5) 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 ausschließlich 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.

(6) 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.

(7) Stellt das Bundesamt im Rahmen seiner Kontrollen fest, dass Verstöße gegen die im vorliegenden Gesetz festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur

Folge haben kann, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichten sie unverzüglich die in Artikel 55 oder 56 jener Verordnung genannten Aufsichtsbehörden.

(8) 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 Gefahren für die Kommunikationstechnik des Bundes erforderlich ist.

Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, muss die automatisierte Auswertung dieser Daten unverzüglich erfolgen und müssen diese nach erfolgtem Abgleich sofort und spurenlos gelöscht werden. 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 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 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 Gefahr für die Kommunikationstechnik des Bundes stehen oder

4. sich aus diesen Daten Hinweise auf ein Schadprogramm oder eine sonstige Gefahr für die Kommunikationstechnik des Bundesergeben können 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 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 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.

(5) Die Beteiligten des Kommunikationsvorgangs sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder seiner Wirkungen oder von sonstigen 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 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 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 beziehungsweise § 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 Zustimmung 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 Absatz 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 Satz 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 6 gilt für die Verpflichtung nach Absatz 2 Satz 1entsprechend.

§ 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 zur Berichterstattung innerhalb einer angemessenen Frist zu den nach Satz 1 angeordneten Maßnahmen auffordern. Der oder die jeweils zuständige Ressort-Informationssicherheitsbeauftragte wird über Anweisungen und Aufforderungen nach Satz 1 und 2 durch das Bundesamt entsprechend informiert. Der Bericht ist dem Bundesamt und zugleich dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts sowie dem Koordinator oder der Koordinatorin für Informationssicherheit 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 erheben und 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 weiter-

gegeben 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 KRITIS-DachG 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 Bereichen des § 57 Absatz 4 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 Telekommunikationsgesetzes). 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 und [*einfügen: andere Gesetze, die die NIS-2-Richtlinie umsetzen*] 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 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 § 60 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 der untersuchten informationstechnischen Produkte und Systeme 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 Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden

(1) Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 20 oder 24 zur Detektion von Schwachstellen und anderen Sicherheitsrisiken bei Einrichtungen der Bundesverwaltung, besonders wichtigen Einrichtungen oder wichtigen Einrichtungen Abfragen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen durchführen, um festzustellen, ob diese Schnittstellen unzureichend geschützt und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können, oder wenn die entsprechenden Einrichtungen darum ersuchen. Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, darf es diese nur zum Zwecke der Übermittlung nach § 8 Absatz 6 und 7 verarbeiten. Sofern die Voraussetzungen des

§ 8 Absatz 6 und 7 nicht vorliegen, sind Informationen, die nach Artikel 10 des Grundgesetzes geschützt sind, unverzüglich zu löschen. Abfragen nach Satz 1 dürfen nur durch eine Bedienstete oder einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet werden.

(2) Wird durch Abfragen gemäß Absatz 1 eine Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, sind die für das informationstechnische System Verantwortlichen unverzüglich darüber zu informieren. Das Bundesamt soll dabei auf bestehende Abhilfemöglichkeiten hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigem Aufwand oder über eine Bestandsdatenabfrage nach § 12 möglich, ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen, wenn überwiegende Sicherheitsinteressen nicht entgegenstehen. 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 ergriffenen Abfragen.

(3) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, welche 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 konkreter 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 Telemediendiensten

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

1. unerlaubten Zugriffen auf die für diese Telemedienangebote genutzten technischen Einrichtungen oder

2. Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

gegenüber dem jeweiligen Anbieter von Telemedien nach § 2 Absatz 2 Nummer 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes anordnen, dass dieser die jeweils zur Herstellung des ordnungsgemäßen Zustands seiner Telemedienangebote erforderlichen technischen und organisatorischen Maßnahmen ergreift, um den ordnungsgemäßen Zustand seiner Telemedienangebote 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 betroffener IKT-Produkte 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 Haushaltsordnung 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 Ordnung 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) Eine besonders wichtige Einrichtung ist

1. eine natürliche oder juristische Person oder eine rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet, die, einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen ist und die

   a) mindestens 250 Mitarbeiter beschäftigt, oder

   b) einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweist;

2. eine natürliche oder juristische Person, die, einer der in Anlage 1 bestimmten Einrichtungsarten qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registry oder DNS-Diensteanbieter zuzuordnen ist,

3. ein Anbieter von Telekommunikationsdiensten oder öffentlich zugänglichen Telekommunikationsnetzen , der

   a) mindestens 50 Mitarbeiter beschäftigt oder

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

4. ein Betreiber kritischer Anlagen .

Davon ausgenommen sind

1. Finanzunternehmen nach Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 und ein Unternehmen, für welches die Anforderungen der Verordnung (EU) 2022/2554 auf Grund von § 1a Absatz 2 Kreditwesengesetz oder § 293 Absatz 5 Versicherungsaufsichtsgesetz gelten, und

2. die Gesellschaft für Telematik nach § 306 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch, ein Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 311 Absatz 6 und § 325 des Fünften Buches Sozialgesetzbuch zugelassenen Dienste und ein Betreiber von Diensten, soweit dieser die Telematikinfrastruktur für nach § 327 Absatz 2 bis 5 des Fünften Buches Sozialgesetzbuch bestätigte Anwendungen nutzt.

(2) Eine wichtige Einrichtung ist

1. eine natürliche oder juristische Person oder eine rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet, die einer der in Anlagen 1 und 2 bestimmten Einrichtungsarten zuzuordnen ist und die

   a) mindestens 50 Mitarbeiter beschäftigt oder

   b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweist; oder

2. ein Vertrauensdiensteanbieter.

Davon ausgenommen sind

1. besonders wichtige Einrichtungen,

2. Finanzunternehmen nach Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 und ein Unternehmen, für welche die Anforderungen der Verordnung (EU) 2022/2554 auf Grund von § 1a Absatz 2 Kreditwesengesetz oder § 293 Absatz 5 Versicherungsaufsichtsgesetz gelten, und

3. die Gesellschaft für Telematik nach § 306 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch, ein Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 311 Absatz 6 und § 325 des Fünften Buches Sozialgesetzbuch zugelassenen Dienste und ein Betreiber von Diensten, soweit dieser die Telematikinfrastruktur für nach § 327 Absatz 2 bis 5 des Fünften Buches Sozialgesetzbuch bestätigte Anwendungen nutzt.

(3) Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nach den Absätzen 1 und 2 ist auf die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen und außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft die Empfehlung 2003/361/EG mit Ausnahme von Artikel 3 Absatz 4 des Anhangs anzuwenden. Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung 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 §§ 31, 32, 35 und 39 gelten nicht für:

1. Besonders wichtige Einrichtungen und wichtige Einrichtungen, soweit sie

   a) ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, und

   b) den Regelungen des Telekommunikationsgesetzes unterliegen;

2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes vom 7. Juli 2005 (BGBl. I S. 1970; 3621), das zuletzt durch Artikel 9 des Gesetzes vom 26. Juli 2023 (BGBl. 2023 I Nr. 202) geändert worden ist, soweit sie den Regelungen des § 5c des Energiewirtschaftsgesetzes unterliegen,

3. Finanzunternehmen nach Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 und Unternehmen, für welche die Anforderungen der Verordnung (EU) 2022/2554 auf Grund

von § 1a Absatz 2 Kreditwesengesetz oder § 293 Absatz 5 Versicherungsaufsichtsgesetz gelten,

(5) Ein Betreiber kritischer Anlagen ist eine natürliche oder juristische Person oder eine rechtlich unselbständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine kritische Anlage ausübt.

(6) Eine Anlage ist ab dem durch die Rechtsverordnung nach § 57 Absatz 4 festgelegten Stichtag eine kritische Anlage, wenn sie einer der durch Rechtsverordnung nach § 57 Absatz 4 festgelegten Anlagenarten in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung zuzuordnen ist und diese die durch die Rechtsverordnung nach § 57 Absatz 4 festgelegten Schwellenwerte überschreitet.

(7) Eine Anlage ist ab dem nächsten folgenden durch die Rechtsverordnung nach § 57 Absatz 4 als Stichtag festgelegten Tag keine kritische Anlage mehr, wenn sie die durch die Verordnung festgelegten Schwellenwerte unterschreitet.

(8) Eine juristische Person oder eine rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft ist keine wichtige oder besonders wichtige Einrichtung im Sinne dieses Gesetzes, wenn diese

1. im ausschließlichen mittel- oder unmittelbaren Eigentum von Gebietskörperschaften, ausgenommen des Bundes, steht,

2. ausschließlich Waren oder Dienstleistungen für Gebietskörperschaften, ausgenommen des Bundes, gegen Entgelt anbietet und

3. durch landesrechtliche Vorschriften unter Bezugnahme auf diesen Absatz reguliert wird.

§ 29

Einrichtungen der Bundesverwaltung

(1) Einrichtungen der Bundesverwaltung im Sinne dieses Gesetzes sind

1. Stellen des Bundes,

2. Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen, ungeachtet ihrer Rechtsform, auf Bundesebene, sowie

3. öffentliche Unternehmen, die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen,

die keine Institutionen der sozialen Sicherung sind.

(2) Für Einrichtungen der Bundesverwaltung finden die Regelungen für besonders wichtige Einrichtungen Anwendung. Davon ausgenommen sind die Regelungen in den §§ 38 und 64.

(3) Der Geschäftsbereich des Bundesministeriums der Verteidigung ist von den Regelungen der §§ 10, 13 Absatz 1 Nummer 1 Buchstabe e), 30, 33, 35, 38, 50 Absatz 3 und 64 ausgenommen.

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 zu ergreifen, um Störungen der Verfügbarkeit, Integrität, Authentizität 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. Dabei 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) Soweit 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.

(5) Soweit 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 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 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 § 57 Absatz 4 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) Besonders wichtige Einrichtungen sind ab dem [*einsetzen: 1 Jahr nach Inkrafttreten*] verpflichtet, am Informationsaustausch nach § 6 teilzunehmen.

(8) 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.

(9) 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.

(10) Betreiber kritischer Anlagen können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach § 39 Absatz 1 vorschlagen. Absatz 9 Sätze 2 bis 4 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 anderen informationstechnischen Systemen, Komponenten und Prozessen besonders wichtiger Einrichtungen auch aufwändigere Maßnahmen nach § 30 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 sowie im Falle von Einrichtungen der Bundesverwaltung zusätzlich der jeweiligen Aufsichtsbehörde:

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 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 dann innerhalb eines Monats nach Abschluss der Bearbeitung des Sicherheitsvorfalls 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 kann die Einzelheiten zur Ausgestaltung des Meldeverfahrens und zur Konkretisierung der Meldungsinhalte nach Anhörung der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe festlegen, soweit sie möglichen Durchführungsrechtsakten der Europäischen Kommission nicht widersprechen. Die Informationen nach Satz 1 werden durch das Bundesamt auf dessen Internetseite veröffentlicht.

§ 33

Registrierungspflicht

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sowie Domain-Name-Registry-Diensteanbieter 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 soweit 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 soweit einschlägig Branche,

4. Auflistung derjenigen Mitgliedstaaten der Europäischen Union, in denen die Einrichtung Dienste der in Anlage 1 oder 2 genannten Einrichtungsarten erbringen, und

5. die für die Tätigkeiten, aufgrund derer die Registrierung erfolgt, zuständigen Aufsichtsbehörden des Bundes.

(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 § 54 Absatz 1 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-Diensteanbieter kann das Bundesamt 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 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 kann die Einzelheiten zur Ausgestaltung des Registrierungsverfahrens im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe festlegen. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamts.

§ 34

Besondere Registrierungspflicht für bestimmte Einrichtungsarten

(1) Eine Einrichtung der in § 63 Absatz 1 Satz 1 genannten Einrichtungsart ist verpflichtet, bis zum 17. Januar 2025 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 § 63 Absatz 3 benannten Vertreters;

4. aktuelle Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern der Einrichtung und soweit erforderlich, ihres nach § 63 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 § 63 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 § 33 übermittelten Angaben an die ENISA 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 wichtige Einrichtungen und wichtige Einrichtungen anweisen, die Empfänger ihrer Dienste unverzüglich über diesen erheblichen Sicherheitsvorfall zu unterrichten, der die Erbringung des jeweiligen Dienstes beeinträchtigen könnten. Das Bundesamt setzt die 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 aus den Sektoren Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, 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 diese Empfänger auch über die erhebliche Cyberbedrohung selbst. Die Unterrichtungspflicht gilt nur dann, wenn in Abwägung der Interessen der Einrichtung und des Empfängers die Interessen des Empfängers überwiegen.

§ 36

Rückmeldungen des Bundesamts gegenüber meldenden Einrichtungen

(1) Im Fall einer Meldung einer Einrichtung gemäß § 31 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 die Öffentlichkeit über den erheblichen Sicherheitsvorfall informieren oder die Einrichtung verpflichten, dies zu tun. Handelt es sich bei der betreffenden Einrichtung um eine Stelle des Bundes, 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 für Verteidigung, der Ministerien für Inneres und Justiz der Länder oder auf eigenes Betreiben besonders wichtige Einrichtungen oder wichtige Einrichtungen 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 im Benehmen mit dem jeweils zuständigen Ministerium.

(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 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 Satz 1 Nummer 1 oder Nummer 2 von einem Widerruf abgesehen werden.

§ 38

Billigungs-, 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 im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen.

(2) Ein Verzicht der Einrichtung auf Ersatzansprüche aufgrund einer Verletzung der Pflichten nach Absatz 1 oder ein Vergleich der Einrichtung über diese Ansprüche ist unwirksam. Dies gilt nicht, wenn der Ersatzpflichtige zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrens mit seinen Gläubigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.

(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 sowie Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik und die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste zu erwerben.

§ 39

Nachweispflichten für Betreiber kritischer Anlagen

(1) Betreiber kritischer Anlagen haben die Erfüllung der Anforderungen nach § 30 Absatz 1 und § 31 zu einem vom Bundesamt im Benehmen mit dem Bundesamt für

Bevölkerungsschutz und Katastrophenhilfe festgelegten Zeitpunkt frühestens drei Jahre nachdem sie erstmals oder erneut als ein Betreiber einer kritischen Anlage gelten und anschließend alle drei Jahre dem Bundesamt auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der 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 Anforderungen an die Art und Weise der Durchführung, an die Geeignetheit der zu erbringenden Nachweise sowie nach Anhörung der betroffenen Betreiber und Einrichtungen und der betroffenen Wirtschaftsverbände fachliche und organisatorische Anforderungen an die prüfenden Stellen festlegen. 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 nach § 2 Absatz 10 BSI-Gesetz 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, waren, den Zeitpunkt der Nachweiserbringung auf frühestens drei Jahre nach Erbringung des letzten Nachweises nach § 8a Absatz 3 BSI-Gesetz 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 ENISA;

2. sowie die sektorübergreifende Zusammenarbeit der in Nummer 1 genannten Länderbehörden, des Bundesamts 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 § 32 Absatz 1 Nummer 2 zu unterrichten und

   b) die zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union über nach Absatz 4 oder nach vergleichbaren Regelungen gemeldete erhebliche Störungen, die Auswirkungen in diesem Mitgliedstaat haben, zu unterrichten und

   c) das Auswärtige Amt über nach § 32 Absatz 1 gemeldete erhebliche Sicherheitsvorfälle, die von besonderer außenpolitischer Bedeutung sind, zu unterrichten und

5. im Rahmen vorab zwischen dem Bundesamt und den Empfängern abgestimmter Prozesse zur Weitergabe und Wahrung der notwendigen Vertraulichkeit den zuständigen Behörden des Bundes und der Länder Informationen zu besonders wichtigen Einrichtungen zur Verfügung zu stellen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.

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

1. Anfragen der in Absatz 1 genannten Stellen anzunehmen und an die zuständigen in Absatz 1 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 1 genannten Stellen an die in Absatz 1 genannten Stellen weiterzuleiten, nach § 31 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 ENISA über den erheblichen Sicherheitsvorfall zu unterrichten, wobei die Art der gemäß § 31 Absatz 2 erhaltenen Informationen mitzuteilen und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen zu gewahren 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 Absatz 1 Nummer 20 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 dieser 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 § 57 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 Absatz 1 Nummer 20 dürfen nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber dem Betreiber der kritischen Anlage abgeben 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 Zwecke 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 § 57 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 oder 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 dessen Organisationsstruktur, stammen. Die Sätze 1 und 2 gelten erst ab der Bekanntmachung der Allgemeinverfügung nach Satz 5 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 § 57 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 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 § 57 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 § 57 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 Einrichtungsleitung ist dafür verantwortlich, unter Berücksichtigung der Belange des IT-Betriebs die Voraussetzungen zur Gewährleistung der Informationssicherheit zu schaffen. Hierfür sind angemessene finanzielle, personelle und Sachmittel einzusetzen.

(2) Die Einrichtungsleitung nimmt regelmäßig an Schulungen teil, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

(3) Soweit mit Leistungen für Informationstechnik des Bundes privatrechtlich organisierte Stellen beauftragt werden, ist vertraglich sicherzustellen, dass diese 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 Einrichtungsleitung nach Absatz 1 bleiben hiervon unberührt.

(4) Die Registrierung von Einrichtungen der Bundesverwaltung nach § 32 obliegt der Einrichtungsleitung. Abweichend von § 64 weisen die Einrichtungen der Bundesverwaltung die Erfüllung der Anforderungen nach Absatz 1 spätestens vier Jahre nach Inkrafttreten dieses Gesetzes und anschließend regelmäßig dem Bundesamt nach dessen 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 die Sicherheit der Kommunikationstechnik des Bundes von Bedeutung sind, unterrichten diese das Bundesamt hierüber unverzüglich, soweit andere Vorschriften dem nicht entgegenstehen. Ausgenommen von den Pflichten nach Satz 1 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.

(6) Das Bundesministerium des Innern und für Heimat erlässt nach Zustimmung durch die Ressorts allgemeine Verwaltungsvorschriften zur Durchführung des Absatzes 5.

§ 44

Vorgaben des Bundesamtes

(1) Das Bundesamt legt durch den IT-Grundschutz und durch Mindeststandards für die Sicherheit in der Informationstechnik des Bundes die nach § 30 zu erfüllenden Anforderungen für Einrichtungen der Bundesverwaltung fest. Dabei berücksichtigt es, ob Einrichtungen der Bundesverwaltung gleichzeitig Betreiber kritischer Anlagen sind. Die Mindeststandards legt das Bundesamt im Benehmen mit den Ressorts fest. Durch die Umsetzung der in Satz 1 genannten Anforderungen ist die Erfüllung der Vorgaben nach § 30 gewährleistet. Das Bundesamt berät die Einrichtungen der Bundesverwaltung auf Ersuchen bei der Umsetzung und Einhaltung dieser Anforderungen, stellt Handreichungen zur Verfügung und unterstützt die Bereitstellung entsprechender Lösungen durch die IT-Dienstleister des Bundes über den gesamten Lebenszyklus. Insbesondere berücksichtigt es die Erfahrungen aus dieser Mitwirkung bei der Fortschreibung der Vorschriften nach Satz 1.

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

(3) Für die Einrichtungen der Bundesverwaltung kann der Koordinator oder die Koordinatorin für Informationssicherheit im Einvernehmen mit den Ressorts festlegen, dass sie verpflichtet sind, nach § 19 bereitgestellte IT-Sicherheitsprodukte beim Bundesamt abzurufen. Eigenbeschaffungen sind in diesem Fall nur zulässig, wenn das spezifische Anforderungsprofil den Einsatz abweichender Produkte erfordert. Dies gilt nicht für die in § 2 Absatz 1 Nummer 18 genannten Gerichte und Verfassungsorgane sowie die Einschränkungen gemäß § 7 Absatz 6.

§ 45

Informationssicherheitsbeauftragte der Einrichtungen der Bundesverwaltung

(1) Die Einrichtungsleitungen der Bundesverwaltung bestellen jeweils eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten sowie mindestens eine zur Vertretung berechtigte Person.

(2) Für die Erfüllung ihrer Aufgaben sind neben Personal- und Sachausstattung in angemessenem Umfang auch finanzielle Mittel zur Verfügung zu stellen, die sie zur Erfüllung ihrer Aufgaben eigenständig verwalten. Die Informationssicherheitsbeauftragen der Einrichtungen müssen die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde erwerben. Sie sowie ihre Vertreter unterstehen der Fachaufsicht des oder der jeweils zuständigen Informationssicherheitsbeauftragten des Ressorts.

(3) Die Informationssicherheitsbeauftragten sind für den Aufbau und die Aufrechterhaltung des Informationssicherheitsprozesses der Einrichtung zuständig. Sie erstellen ein Informationssicherheitskonzept, welches mindestens die Vorgaben des Bundesamtes nach § 44 Absatz 1 erfüllt. Sie wirken auf die operative Umsetzung des Informationssicherheitskonzepts hin und kontrollieren diese innerhalb der Einrichtung. Die Informationssicherheitsbeauftragen beraten die Einrichtungsleitung in allen Fragen der Informationssicherheit und unterrichten die Einrichtungsleitung 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 angemessene Mittel- und Personalausstattung nach § 43 Absatz 1 Satz 2 sowie über Sicherheitsvorfälle.

(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 Einrichtungsleitung sowie bei dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts.

§ 46

Informationssicherheitsbeauftragte der Ressorts

(1) Die Ressortleitungen sowie weitere oberste 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 bzw. innerhalb der obersten Bundesbehörde und ihres Geschäftsbereichs obliegt, sowie mindestens eine zur Vertretung berechtigte Person. Er oder sie wirkt auf eine angemessene Umsetzung der Informationssicherheit in ihrem oder seinem Ressort hin.

(2) Für die Erfüllung seiner oder ihrer Aufgaben sind neben Personal- und Sachausstattung in angemessenem Umfang auch angemessene finanzielle Mittel zur Verfügung zu stellen, die der oder die Informationssicherheitsbeauftragte des Ressorts zur Erfüllung seiner oder ihrer Aufgaben eigenständig verwaltet. Der oder die Informationssicherheitsbeauftragte des Ressorts muss die zur Erfüllung seiner oder ihrer Aufgaben erforderliche Fachkunde besitzen.

(3) Der oder die Informationssicherheitsbeauftragte koordiniert jeweils die Fortschreibung von Informationssicherheitsleitlinien für sein oder ihr Ressort. Er oder sie unterrichtet die Ressortleitung über seine oder ihre Tätigkeit und über den Stand der Informationssicherheit innerhalb des Ressorts, über die angemessene Mittel- und Personalausstattung nach § 43 Absatz 1 Satz 2 sowie über Sicherheitsvorfälle. In begründeten Einzelfällen kann der 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 der Koordinator oder die Koordinatorin für Informationssicherheit zu unterrichten. Im Falle des § 29 Absatz 1 Nummer 3 ist der oder die Informationssicherheitsbeauftragte des für das Bundesunternehmen beteiligungsführenden Ressorts für die Erteilung des Ausnahmebescheides zuständig.

(4) Der oder die Informationssicherheitsbeauftragte des Ressorts kann im Benehmen mit dem Koordinator oder der Koordinatorin für Informationssicherheit Einrichtungen der Bundesverwaltung innerhalb des Ressorts, soweit diese nicht besonders wichtige Einrichtungen oder wichtige Einrichtungen nach § 28 sind, von Verpflichtungen nach diesem Teil teilweise oder insgesamt durch Erteilung eines Ausnahmebescheides befreien. Voraussetzung hierfür ist, dass sachliche Gründe für die Erteilung einer Ausnahme vorliegen und durch die Befreiung keine nachteiligen Auswirkungen für die Informationssicherheit des Bundes zu befürchten sind. Über erteilte Ausnahmebescheide ist das Bundesamt zu unterrichten, hierbei gilt § 43 Absatz 4 Satz 2 entsprechend.

(5) Der oder die Informationssicherheitsbeauftragte des Ressorts ist bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben innerhalb des Ressorts zu beteili-

gen, soweit diese Fragen der Informationssicherheit berühren. Er oder sie hat ein unmittelbares Vortragsrecht bei der jeweiligen Ressortleitung sowie bei dem Koordinator oder der Koordinatorin für Informationssicherheit.

§ 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. 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. Soweit bei ressortübergreifenden Digitalisierungsvorhaben oder Kommunikationsinfrastrukturen eine Bestellung durch Einrichtungen in verschiedenen beteiligten Ressorts und weiteren obersten Bundesbehörden in Betracht kommt und Einvernehmen darüber nicht innerhalb einer angemessenen Frist hergestellt werden kann, entscheidet der Koordinator oder die Koordinatorin für Informationssicherheit, durch welche Einrichtung die Bestellung erfolgt. Die Informationssicherheitsbeauftragten nach Satz 1 unterstehen in einer obersten Bundesbehörde der Einrichtungsleitung und in einer nachgeordneten Behörde der Fachaufsicht des oder der jeweils zuständigen Informationssicherheitsbeauftragten des Ressorts.

(2) Zur Gewährleistung der Informationssicherheit bei der Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben sind angemessene Mittel für die Informationssicherheit einzusetzen. Die jeweils verantwortliche Einrichtung soll das Bundesamt frühzeitig beteiligen und dem Bundesamt Gelegenheit zur Stellungnahme geben.

§ 48

Amt des Koordinators für Informationssicherheit

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

(2) Für die Erfüllung der Aufgaben sind neben Personal- und Sachausstattung auch finanzielle Mittel in angemessenem Umfang zur Verfügung zu stellen, die der Koordinator oder die Koordinatorin zur Erfüllung seiner oder ihrer Aufgaben eigenständig verwaltet.

§ 49

Aufgaben des Koordinators

Dem Koordinator oder der Koordinatorin für Informationssicherheit obliegt die zentrale Koordinierung des Informationssicherheitsmanagements des Bundes. Zu diesem Zweck wirkt er oder sie auf ein angemessenes Verhältnis zwischen dem Einsatz von Informationstechnik und Informationssicherheit hin. Er oder sie koordiniert die Erstellung und Aktualisierung von Informationssicherheitsleitlinien des Bundes und unterstützt die Ressorts bei der Umsetzung der Vorgaben zur Informationssicherheit. Er oder sie überwacht die angemessene Mittelverwendung nach § 43 Absatz 1 Satz 2 und unterrichtet hierüber kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Haushaltsausschuss des Deutschen Bundestages.

§ 50

Befugnisse des Koordinators

(1) Zur Wahrnehmung der Aufgaben nach § 49 beteiligen die Ressorts den Koordinator oder die Koordinatorin für Informationssicherheit bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben, soweit sie Fragen der Informationssicherheit berühren. Er oder sie kann der Bundesregierung Vorschläge machen und Stellungnahmen zuleiten. Die Ressorts unterstützen den Koordinator oder die Koordinatorin bei der Erfüllung seiner oder ihrer Aufgaben.

(2) Zur Wahrnehmung seiner oder ihrer Aufgaben hat der Koordinator oder die Koordinatorin ein direktes Vortragsrecht vor dem Ausschuss für Inneres und Heimat und dem Haushaltsausschuss des Deutschen Bundestages zu allen Themen der Informationssicherheit in Einrichtungen der Bundesverwaltung.

(3) Der Koordinator oder die Koordinatorin kann im Benehmen mit dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts Einrichtungen anweisen, innerhalb von drei Monaten nach der Vorlage der Ergebnisse von Kontrollen gemäß § 7 ein Sofortprogramm vorzulegen, welches die Einhaltung der Anforderungen innerhalb einer angemessenen Umsetzungsfrist sichert.

Teil 4

Datenbanken der Domain-Name-Registrierungsdaten

§ 51

Pflicht zum Führen einer Datenbank

(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domain Name Systems zu leisten, sind Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister verpflichtet, genaue und vollständige Domain-Namen-Registrierungsdaten in einer eigenen Datenbank im Einklang mit dem Datenschutzrecht in Bezug auf personenbezogene Daten 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 sind verpflichtet, Vorgaben und Verfahren, einschließlich Überprüfungsverfahren, vorzuhalten,

mit denen sichergestellt wird, dass die Datenbank genaue und vollständige Angaben enthält. Diese Vorgaben und Verfahren sind öffentlich zugänglich zu machen.

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

§ 52

Verpflichtung zur Zugangsgewährung

(1) Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister sind verpflichtet,

1. einem berechtigten Zugangsnachfrager auf rechtmäßigen und hinreichend begründeten Antrag im Einklang mit dem Datenschutzrecht Zugang zu bestimmten Domain-Namen-Registrierungsdaten zu gewähren und

2. alle Anträge auf Zugang unverzüglich und in jedem Fall innerhalb von 72 Stunden nach Eingang eines Antrags auf Zugang zu beantworten.

(2) Die in Absatz 1 genannten Vorgaben und Verfahren im Hinblick auf die Offenlegung der Domain-Namen-Registrierungsdaten sind öffentlich zugänglich zu machen. Das Auskunftsverfahren bei Bestandsdaten gemäß § 22 des Telekommunikation-Telemedien-Datenschutz-Gesetzes bleibt unberührt.

§ 53

Kooperationspflicht

Um zu vermeiden, dass die Einhaltung der in § 51 und § 52 festgelegten Verpflichtungen zu einer doppelten Erhebung von Domain-Namen-Registrierungsdaten führt, sind Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister insoweit zur Kooperation verpflichtet.

Teil 5

Zertifizierung und Kennzeichen

§ 54

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 die Unterlagen vorzulegen und die Auskünfte zu erteilen, deren Kenntnis für die Prüfung und Bewertung des Systems oder der Komponente oder der Eignung der Person sowie für die Erteilung des Zertifikats erforderlich ist.

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

(4) Das Sicherheitszertifikat wird erteilt, wenn

1. informationstechnische 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 eine Zertifikatserteilung 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 Anerkennung nach Absatz 3 wird erteilt, 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, soweit sie eine den Sicherheitszertifikaten des Bundesamtes gleichwertige Sicherheit ausweisen und die Gleichwertigkeit vom Bundesamt festgestellt worden ist.

§ 55

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 § 54 dieses Gesetzes tätig werden, eine Befugnis erteilen, als solche tätig zu werden, wenn die Voraussetzungen des maßgeb-

lichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 oder des § 54 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 § 54 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 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 dieser das Bundesamt bei der Wahrnehmung seiner Befugnisse nach Absatz 4 oder im Falle eines Inhabers eines europäischen Cybersicherheitszertifikats auch nach Absatz 5 behindert hat.

(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 Verordnung (EU) 2019/881 oder des § 54 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 diese das Bundesamt bei der Wahrnehmung seiner Befugnisse nach den Absätzen 4 und 5 behindert hat.

§ 56

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 § 57 Absatz 3 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 § 57 Absatz 3 bestimmt wird. Den genauen Ablauf des Antragsverfahrens und die beizufügenden Unterlagen regelt die Rechtsverordnung nach § 57 Absatz 3.

(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 § 57 Absatz 3 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

§ 57

Ermächtigung zum Erlass von Rechtsverordnungen

(1) Das Bundesministerium des Innern und für Heimat bestimmt nach Anhörung der betroffenen Wirtschaftsverbände und 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 § 54 und deren Inhalt.

(2) Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung der betroffenen Wirtschaftsverbände 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 § 52, 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, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Einrichtungen und der betroffenen Wirtschaftsverbände 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, 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, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und Wirtschaftsverbände 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 den jeweiligen Sektoren wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Anlagen als kritische Anlagen im Sinne dieses Geset-

zes 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.

§ 58

Einschränkung von Grundrechten

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

§ 59

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 übermittelt bis zum 9. November 2018 und danach alle zwei Jahre bis zum 17. Oktober 2024 die folgenden Informationen an die Europäische Kommission:

1. die nationalen Maßnahmen zur Ermittlung der Betreiber kritischer Anlagen;

2. eine Aufstellung der im in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, die in der Rechtsverordnung nach § 57 Absatz 4 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrad;

3. eine zahlenmäßige Aufstellung der Einrichtungen der in Nummer 2 genannten Sektoren, die in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren ermittelt werden, einschließlich eines Hinweises auf ihre Bedeutung für den jeweiligen Sektor.

Die Übermittlung darf keine Informationen enthalten, die zu einer Identifizierung einzelner Betreiber führen können. Das Bundesamt übermittelt die nach Satz 1 übermittelten Informationen unverzüglich dem Bundesministerium des Innern und für Heimat, dem Bundeskanzleramt, 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 und nukleare Sicherheit und Verbraucherschutz.

(5) Sobald bekannt wird, dass eine Einrichtung oder Anlage nach § 2 Absatz 1 Nummer 19 oder Teile einer Einrichtung oder Anlage eine wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistung in einem der in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren in einem anderen Mitgliedstaat der Europäischen Union bereitstellt, nimmt das Bundesamt zum Zweck der gemeinsamen Ermittlung der Einrichtungen, die kritische Dienstleistungen in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Teilsektoren erbringen, mit der zuständigen Behörde dieses Mitgliedstaats Konsultationen auf.

(6) Das Bundesamt übermittelt bis zum 9. August 2018 und danach jährlich bis zum Berichtszeitraum Kalenderjahr 2023 an die Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 einen zusammenfassenden Bericht zu den Meldungen, die die in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren oder digitale Dienste betreffen. Der Bericht enthält auch die Zahl der Meldungen und die Art der gemeldeten Sicherheitsvorfälle sowie die ergriffenen Maßnahmen. Der Bericht darf keine Informationen enthalten, die zu einer Identifizierung einzelner Meldungen oder einzelner Einrichtungen führen können.

(7) Das Bundesamt legt der ENISA erstmalig 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 § 31 und § 5 Absatz 2 gemeldet wurden. Der erstmalige Bericht nach Satz 1 enthält auch die Daten, die für das Jahr 2024 gemäß Absatz 6 übermitteln zu gewesen wären.

(8) Das Bundesamt übermittelt erstmalig 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 § 32 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

Sanktionsvorschriften und Aufsicht

§ 60

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer entgegen § 39 Absatz 1 Satz 1 in Verbindung mit der Rechtsverordnung nach § 57 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 § 34 Absatz 1 Satz 6,

b) § 14 Absatz 2 Satz 1 oder § 64 Absatz 8 Satz 1 und 2 oder Absatz 9 Satz 1 oder in Verbindung mit § 65

c) § 18 oder § 64 Absatz 6 Satz 1 und 2 oder in Verbindung mit § 65

d) § 40 Absatz 4 Satz 1

zuwiderhandelt,

2. entgegen § 30 Absatz 1 in Verbindung mit einer Rechtsverordnung nach § 57 Absatz 4 Satz 1 eine dort genannte Maßnahme nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig ergreift,

3. entgegen § 32 Absatz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

4. entgegen § 33 Absatz 1 oder Absatz 5 jeweils in Verbindung mit einer Rechtsverordnung nach § 57 Absatz 4 Satz 1 oder entgegen § 34 Absatz 1 eine Angabe oder Änderung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,,

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

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

7. entgegen § 39 Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 57 Absatz 4 Satz 1 oder § 64 Absatz 3 Satz 1 oder in Verbindung mit § 65, einen Nachweis nicht oder nicht rechtzeitig erbringt,

8. entgegen § 51 Absatz 1 gegenüber dem Bundesamt nicht vorweisen kann, dass er eine vollständige Datenbank vorhält oder entgegen § 52 Satz 1 auf Anträge nicht oder nicht rechtzeitig antwortet oder den Zugang gewährt oder entgegen § 51 Absatz 3 und 4, § 52 Satz 2 die erforderlichen Angaben nicht öffentlich macht,

9. vorgibt, Inhaber einer Zertifizierung nach § 54 Absatz 2 zu sein, ohne dass diese besteht,

10. entgegen § 55 Absatz 2 Satz 2 als Konformitätsbewertungsstelle tätig wird,

11. entgegen § 56 Absatz 4 Satz 1 das IT-Sicherheitskennzeichen verwendet,

12. entgegen § 64 Absatz 5 Satz 3 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,

13. einer Anordnung nach § 64 Absatz 7 Satz 2 oder in Verbindung mit § 65 nicht nachkommt.

(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 Schwachstelle oder Unregelmäßigkeit gibt.

3. vorgibt, Inhaber eines europäischen Cybersicherheitszertifikats gemäß Artikel 56 oder Aussteller einer EU-Konformitätserklärung gemäß Artikel 53 Absatz 2 zu sein, obwohl diese nicht besteht, widerrufen oder für ungültig erklärt wurde.

(5) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 1 Buchstabe a mit einer Geldbuße bis zu zwei Millionen Euro, wobei § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten anzuwenden ist, sowie in den Fällen des Absatzes 2 Nummer 1 Buchstabe c, Nummern 4, 6, 7 Variante 2 und 3, 8, 9, 10 und 11 und des Absatzes 4 mit einer Geldbuße bis zu fünfhunderttausend Euro und in den Fällen des Absatzes 2 Nummer 1 Buchstabe b , der Nummer 13 und des Absatzes 3 mit einer Geldbuße bis zu einhunderttausend Euro geahndet werden.

(6) Handelt es sich bei dem Betroffenen um eine wichtige Einrichtung kann die Ordnungswidrigkeit in den Fällen des Absatzes 2 Nummer 2 und 3 mit einer Geldbuße bis zu 7 Millionen Euro oder mit einem Höchstbetrag von mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört geahndet werden.

(7) Handelt es sich bei dem Betroffenen um eine besonders wichtige Einrichtung, kann die Ordnungswidrigkeit in den Fällen des Absatzes 2 Nummer 2 und 3 mit einer Geldbuße bis zu 10 Millionen Euro oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört, in den Fällen des Absatzes 1 und des Absatzes 2 Nummer 7 Variante 1 mit einer Geldbuße bis zu 10 Millionen Euro, in den Fällen des Absatzes 2 Nummer 12 mit einer Geldbuße bis zu fünfhunderttausend Euro und in den Fällen des Absatzes 2 Nummer 1 Buchstabe d und Nummer 5 mit einer Geldbuße bis zu einhunderttausend Euro geahndet werden.

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

(9) 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 ein weiteres Bußgeld für einen Verstoß nach diesem Gesetz, der sich aus demselben Verhalten ergibt wie jener Verstoß, nicht verhängt werden.

§ 61

Zuwiderhandlungen durch Institutionen der sozialen Sicherung

Bei Zuwiderhandlungen gegen eine in § 60 Absatz 1 bis 4 genannte Vorschrift, die von Körperschaften gemäß § 29 des Vierten Buches Sozialgesetzbuch, Arbeitsgemeinschaften gemäß § 94 des Zehnten Buches Sozialgesetzbuch sowie der Deutschen Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist (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.

§ 62

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.

§ 63

Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten

(1) Abweichend von § 62 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 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 hat. 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, 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, 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 Mitgliedsstaats 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, Komponente oder Prozess betreibt. Satz 1 gilt entsprechend bei Amtshilfeersuchen eines anderen Mitgliedsstaats 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 Komponente oder einen Prozess betreibt.

§ 64

Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

(1) Das Bundesamt kann einzelne besonders wichtige Einrichtungen verpflichten, Audits, Prüfungen oder Zertifizierungen von unabhängigen Stellen zur Prüfung der Erfüllung der Anforderungen nach den §§ 30, 31 und 32 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, neben der nach § 39 für Betreiber einer kritischen Anlage bestimmten Frist, auch gegenüber anderen besonders wichtigen Einrichtungen frühestens drei Jahre nach Inkrafttreten dieses Gesetzes die Vorlage von Nachweisen über die Erfüllung einzelner oder aller Anforderungen nach den §§ 30, 31 und 32anordnen. 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.

(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 Maßnahmen anordnen, die zur Verhütung oder Behebung eines Sicherheitsvorfalls oder eines Mangels erforderlich sind. Ferner kann das Bundesamt die Berichterstattung zu den nach Satz 1 angeordneten Maßnahmen verlangen.

(7) Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen verbindliche Anordnungen zur Umsetzung der Verpflichtungen nach diesem Gesetz erlassen. Es kann die Umsetzung von im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen 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 Verpflichtungen nach diesem Gesetz nach durch das Bundesamt bestimmten Vorgaben öffentlich bekannt zu machen.

(9) Das Bundesamt kann für besonders wichtige Einrichtungen einen Überwachungsbeauftragten benennen, der die Einhaltung der Verpflichtungen nach den §§ 28, 29 und 37 überwacht. Die Benennung erfolgt für einen bestimmten Zeitraum. In der Benennung müssen die Aufgaben des Überwachungsbeauftragten genau festgelegt sein.

(10) Sofern besonders wichtige Einrichtungen den Anordnungen des Bundesamtes nach diesem Gesetz trotz Fristsetzung nicht nachkommen, kann das Bundesamt dies der jeweils zuständigen Aufsichtsbehörde mitteilen.

1. Die Genehmigung für einen Teil oder alle Dienste oder Tätigkeiten dieser Einrichtung ist vorübergehend auszusetzen und

2. den natürlichen Personen, die als Geschäftsführung oder gesetzliche Vertreter für Leitungsaufgaben in der besonders wichtigen Einrichtung zuständig sind, ist die Wahrnehmung der Leitungsaufgaben vorübergehend zu untersagen.

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

(11) Soweit das Bundesamt Aufsichtsmaßnahmen gegenüber besonders wichtigen Einrichtungen durchführt, die gleichzeitig Betreiber kritischer Anlagen sind, informiert es die zuständige Aufsichtsbehörde des Bundes darüber.

(12) Stellt das Bundesamt im Zuge der Beaufsichtigung einer Einrichtung oder Durchsetzung einer Maßnahme fest, dass der Verstoß einer besonders wichtigen Einrichtung gegen Verpflichtungen aus § 30 oder 31 eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur Folge haben kann, die gemäß Artikel 33 der vorgenannten Verordnung zu melden ist, unterrichtet das Bundesamt unverzüglich die in Artikel 55 oder 56 der Verordnung (EU) 2016/679 genannten Aufsichtsbehörden.

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

§ 65

Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen

Rechtfertigen Tatsachen die Annahme, dass eine wichtige Einrichtung die Anforderungen aus den §§ 30, 31 und 32 nicht oder nicht richtig umsetzt, so kann das Bundesamt die Einhaltung der Anforderungen nach den §§ 30, 31 und 32 überprüfen und Maßnahmen nach § 64 treffen.

§ 66

Verwaltungszwang

(1) Soweit das Bundesamt Zwangsgelder verhängt, beträgt deren Höhe abweichend von § 11 Absatz 3 des Verwaltungsvollstreckungsgesetzes bis zu 100.000 Euro.

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 gemäß § 3 Nr. 31a EnWG
1.1.2			Betreiber von Elektrizitätsverteilernetzen gemäß §3 Nr. 3 EnWG
1.1.3			Betreiber von Übertragungsnetzen gemäß § 3 Nr. 10 EnWG
1.1.4			Betreiber von Erzeugungsanlagen gemäß § 3 Nr. 18d EnWG
1.1.5			Nominierte Strommarktbetreiber nach Artikel 2 Nummer 8 der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates
1.1.6			Aggregatoren gemäß § 3 Nr. 1a EnWG
1.1.7			Betreiber von Energiespeicheranlagen gemäß § 3 Nr. 15d EnWG
1.1.8			Anbieter von Ausgleichsleistungen im Sinne von § 3 Nr. 1b EnWG
1.1.9			Ladepunktbetreiber gemäß § 2 Nr. 8 LSV
1.2		Fernwärme und -kälteversorgung	
1.2.1			Betreiber von Fernwärme- bzw. Fernkälteversorgung im Sinne § 3 Nr. 19 und 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
1.4		Gasversorgung	
1.4.1			Betreiber von Gasverteilnetzen gemäß § 3 Nr. 8 EnWG
1.4.2			Betreiber von Fernleitungsnetzen gemäß § 3 Nr. 5 EnWG
1.4.3			Betreiber von Gasspeicheranlagen gemäß § 3 Nr. 6 EnWG
1.4.4			Betreiber von LNG-Anlagen gemäß § 3 Nr. 9 EnWG
1.4.5			Gaslieferanten gemäß § 3 Nr. 19b EnWG

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
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, 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, 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 aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben
2.1.3			Flugverkehrskontrolldienste im Sinne von § 27c Abs. 2 Nr. 1 lit. a) LuftVG
2.2		Schienenverkehr	
2.2.1			Eisenbahninfrastrukturbetreiber nach § 2 Nummer 6 und 6a des Allgemeinen Eisenbahngesetz (AEG) einschließlich zentraler Einrichtungen, die den Zugbetrieb vorausschauend und bei unerwartet eintretenden Ereignissen disponiert
2.2.2			Eisenbahnverkehrsunternehmen nach § 2 Nummer 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 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, 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 nach § 1 Absatz 6 Nummer 1 des Bundeswasserstraßengesetzes.

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
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 des Bundesfernstraßengesetzes 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 intelligentes Verkehrssystem nach § 2 Nummer 1 des Intelligente Verkehrssysteme Gesetz.
3	**Finanz- und Versicherungswesen**		
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 Abs. 22 WpHG
3.2.2			Zentrale Gegenparteien, die zwischen die Gegenparteien der auf einem oder mehreren Märkten gehandelten Kontrakte tritt und somit als Käufer für jeden Verkäufer bzw. als Verkäufer für jeden Käufer fungiert
4	**Gesundheit**		
4.1.1			Erbringer von Gesundheitsdienstleistungen
4.1.2			EU-Referenzlaboratorien nach Artikel 15 der Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates
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 („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden
5	**Wasser**		
5.1		Trinkwasserversorgung	

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
5.1.1			Betreiber von Wasserversorgunsanlagen nach § 2 Nr. 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 Abs. 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.
6	**Informationstechnik und Telekommunikation**		
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			Anbieter öffentlicher elektronischer Kommunikationsnetze
6.1.9			Anbieter öffentlich zugänglicher elektronsicher Kommunikationsdienste
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 § 4 Nr. 1 PostG, einschließlich Anbieter von Kurierdiensten
2	**Abfallbewirtschaftung**		
2.1.1			Unternehmen der Abfallbewirtschaftung nach § 3 Abs. 14 KrWG, ausgenommen Unternehmen, für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist.
3	**Produktion, Herstellung und Handel mit chemischen Stoffen**		
3.1.1			Unternehmen nach Artikel 3 Nummern 9 und 14 der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates , die Stoffe herstellen und mit Stoffen oder Gemischen handeln, und Unternehmen, die Erzeugnisse nach Artikel 3 Nummer 3 der genannten Verordnung aus Stoffen oder Gemischen produzieren
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, die im Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind
5	**Verarbeitendes Gewerbe/Herstellung von Waren**		
5.1.1			Unternehmen, die Medizinprodukte nach Artikel 2 Nummer 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates(4)herstellen, und Unternehmen, die In-vitro-Diagnostika nach Artikel 2 Nummer 2 der Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates(5)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 („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
5.2		Herstellung von Medizinprodukten und In-vitro-Diagnostika	
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 Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	
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
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 BSI-Gesetzes (FNA 206-2)

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

1. § 2 Absatz 1 Nummer 18 wird wie folgt neu gefasst:

   „18. „kritische Anlage“ eine Anlage im Sinne von § 2 Nummer 3 des Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen“.

2. In § 28 werden die Absätze 5 bis 8 gestrichen.

3. § 54 Absatz 4 wird gestrichen.

Artikel 3

Änderung des BND-Gesetzes (FNA 12-6)

In § 24 des BND-Gesetzes vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch Artikel 3 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2274) geändert worden ist, wird die Angabe „§ 5 Absatz 7 Satz 2 bis 8 des BSI-Gesetzes“ durch die Angabe „§ 8 Absatz 8 Satz 2 bis 8 des BSI-Gesetzes“ ersetzt.

Artikel 4

Änderung der Sicherheitsüberprüfungsfeststellungsverordnung (FNA 12-10-3)

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

Artikel 5

Änderung des Telekommunikation-Telemedien-Datenschutz-Gesetzes (FNA 204-5)

In § 19 des Telekommunikation-Telemedien-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 4 des Gesetzes vom 12. August

2021 (BGBl. I S. 3544; 2022 I 1045) geändert worden ist, wird die Angabe „§ 7d Satz 1 BSI-Gesetz“ durch die Angabe „§ 17 Satz 1 des BSI-Gesetzes“ ersetzt.

Artikel 6

Änderung der Gleichstellungsbeauftragtenwahlverordnung (FNA 205-3-1)

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, wird die Angabe „§ 9 des BSI-Gesetzes“ durch die Angabe „§ 54 des BSI-Gesetzes“ ersetzt.

Artikel 7

Änderung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (FNA 206-2)

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“, das nach der Angabe „(Artikel 1)“ folgt, wird durch einen Punkt „.“ ersetzt.

2. Nummer 2 wird aufgehoben.

Artikel 8

Änderung der BSI-Zertifizierungs- und Anerkennungsverordnung (FNA 206-2-1)

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 neu gefasst:

   „Auf Grund des § 57 Absatz 2 des BSI-Gesetzes in der Fassung der Bekanntmachung vom [*einfügen: Verkündungsdatum*] (BGBl. I S. [*einfügen: Seite im Bundesgesetzblatt*]) 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 wird die Angabe „§ 9 des BSI-Gesetzes“ durch die Angabe „§ 54 des BSI-Gesetzes“ ersetzt.

3. In § 12 Absatz 1 wird die Angabe „§ 9 Absatz 4 des BSI-Gesetzes“ durch die Angabe „§ 54 Absatz 4 des BSI-Gesetzes“ ersetzt.

4. In § 15 Absatz 1 und § 18 Absatz 1 wird die Angabe „§ 9 Absatz 5 des BSI-Gesetzes“ durch die Angabe „§ 54 Absatz 6 des BSI-Gesetzes“ und die Angabe „§ 9 Absatz 4 Nummer 2 des BSI-Gesetzes“ durch die Angabe „§ 54 Absatz 4 Nummer 2 des BSI-Gesetzes“ ersetzt.

5. § 21 wird wie folgt geändert:

   a) In Absatz 1 wird die Angabe „§ 9 Absatz 6 des BSI-Gesetzes“ durch die Angabe „§ 54 Absatz 7 des BSI-Gesetzes“ ersetzt.

   b) In Absatz 1 Nummer 2 wird die Angabe „§ 9 Absatz 6 Nummer 2 des BSI-Gesetzes“ durch die Angabe „§ 54 Absatz 7 Satz 1 Nummer 2 des BSI-Gesetzes“ ersetzt.

   c) In Absatz 4 Satz 1 wird die Angabe „§ 9 Absatz 6 Satz 2 des BSI-Gesetzes“ durch die Angabe „§ 54 Absatz 7 Satz 2 des BSI-Gesetzes“ ersetzt.

Artikel 9

Änderung der BSI IT-Sicherheitskennzeichenverordnung (FNA 206-2-3)

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

1. Die Eingangsformel wird wie folgt neu gefasst:

   „Auf Grund des § 57 Absatz 3 des BSI-Gesetzes in der Fassung der Bekanntmachung vom [*einfügen: Verkündungsdatum*] (BGBl. I S. [*einfügen: Seite im Bundesgesetzblatt*]) 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 wird die Angabe „§ 9c Absatz 3 Satz 1 des BSI-Gesetzes“ durch die Angabe „§ 56 Absatz 3 Satz 1 des BSI-Gesetzes“ ersetzt.

3. In § 3 Absatz 1 Satz 1 wird die Angabe „§ 9c Absatz 2 des BSI-Gesetzes“ durch die Angabe „§ 56 Absatz 2 des BSI-Gesetzes“ ersetzt.

4. In § 5 wird wie folgt geändert:

   a) In Absatz 4 wird die Angabe „§ 9c Absatz 5 BSIG“ durch die Angabe „§ 56 Absatz 5 des BSI-Gesetzes“ ersetzt.

   b) In Absatz 5 Satz 1 wird die Angabe „§§ 7 oder 7a des BSI-Gesetzes“ durch die Angabe „§ 13 oder 14 des BSI-Gesetzes“ und die Angabe „§ 9c Absatz 8 des BSI-Gesetzes“ durch die Angabe „§ 56 Absatz 8 des BSI-Gesetzes“ ersetzt.

5. In § 6 Absatz 1 wird die Angabe „§ 9 des BSI-Gesetzes“ durch die Angabe „§ 54 des BSI-Gesetzes“ ersetzt.

6. In § 7 Absatz 3 und § 9 Absatz 1 Satz 1 wird die Angabe „§ 9c des BSI-Gesetzes“ durch die Angabe „§ 56 des BSI-Gesetzes“ ersetzt.

7. § 13 wird wie folgt geändert:

   a) In Satz 1 wird die Angabe „§ 9c Absatz 2 des BSI-Gesetzes“ durch die Angabe „§ 56 Absatz 2 des BSI-Gesetzes“ ersetzt.

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

8. In § 14 wird die Angabe „§ 10 Absatz 3 Satz 1 des BSI-Gesetzes“ durch die Angabe „§ 57 Absatz 3 Satz 1 des BSI-Gesetzes“ ersetzt.

Artikel 10

Änderung des De-Mail-Gesetzes (FNA 206-4)

In § 18 Absatz 3 Nummer 3 des De-Mail-Gesetzes vom 28. April 2011 (BGBl. I S. 666), das zuletzt durch Artikel 7 des Gesetzes vom 10. August 2021 (BGBl. I S. 3436) geändert worden ist, werden wie Wörter „§ 9 Absatz 2 Satz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik“ durch die Wörter „§ 54 Absatz 2 Satz 1 des BSI-Gesetzes“ ersetzt.

Artikel 11

Änderung des E-Government-Gesetz (FNA 206-6)

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 gestrichen.

Artikel 12

Änderung der Passdatenerfassungs- und Übermittlungsverordnung (FNA 210-5-11)

In § 4 der Passdatenerfassungs- und Übermittlungsverordnung vom 9. Oktober 2007 (BGBl. I S. 2312), die zuletzt durch Artikel 79 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821)“ durch die Angabe „§ 54 des BSI-Gesetzes in der Fassung der Bekanntmachung vom [*einfügen: Verkündungsdatum*] (BGBl. I S. [*einfügen: Seite im Bundesgesetzblatt*])“ ersetzt.

Artikel 13

Änderung der Personalausweisverordnung (FNA 210-6-1)

In § 3 der Personalausweisverordnung vom 1. November 2010 (BGBl. I S. 1460), die zuletzt durch Artikel 3 der Verordnung vom 20. August 2021 (BGBl. I S. 3682) geändert worden ist, wird die Angabe „§ 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 Angabe „§ 54 des BSI-Gesetzes in der Fassung der Bekanntmachung vom [*einfügen: Verkündungsdatum*] (BGBl. I S. [*einfügen: Seite im Bundesgesetzblatt*])" ersetzt.

Artikel 14

Änderung der Kassensicherungsverordnung (FNA 610-1-26)

In § 11 Absatz 1 der Kassensicherungsverordnung vom 26. September 2017 (BGBl. I S. 3515), die durch Artikel 2 des Gesetzes vom 30. Juli 2021 (BGBl. I S. 3295) geändert worden ist, wird die Angabe „§ 9 des BSI-Gesetzes" durch die Angabe „§ 54 des BSI-Gesetzes" ersetzt.

Artikel 15

Änderung des Atomgesetzes (FNA 751-1)

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, wird die Angabe „§ 8b Absatz 1, 2 Nummer 1 bis 3, Nummer 4 Buchstabe a bis c und Absatz 7 des BSI-Gesetzes" durch die Angabe „§ 40 Absatz 1, 2 Nummer 1 bis 3, Nummer 4 Buchstabe a, Nummer 5 und Absatz 5 des BSI-Gesetzes" ersetzt.

Artikel 16

Änderung des Energiewirtschaftsgesetzes (FNA 752-6)

Das Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970; 3621), das zuletzt durch Artikel 2 des Gesetzes vom 12. Juli 2023 (BGBl. 2023 I Nr. 184) geändert worden ist, wird wie folgt geändert:

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

   „5c IT-Sicherheit im Anlagen- und Netzbetrieb".

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

„§ 5c

IT-Sicherheit im Anlagen und Netzbetrieb

(1) Betreiber von Energieversorgungsnetzen haben einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und 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 der IT-Sicherheitskatalog eingehalten und dies vom Betreiber dokumentiert worden ist

(2) Betreiber von Energieanlagen, die besonders wichtige Einrichtungen nach § 28 Absatz 6 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von kritischen Anlagen und Einrichtungen (BSI-Gesetz) vom […] oder wichtige Einrichtungen nach § 28 Absatz 7 des BSI-Gesetzes sind und an ein Energieversorgungsnetz angeschlossen sind, haben einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind.. Der angemessene Schutz nach Satz 1 ist auch durch Berücksichtigung erforderlicher An-forderungen 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 nach Satz 1 und deren Branchenverbände. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf. Für Telekommunikations- und 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 1 des Gesetzes vom 4. Dezember 2022 (BGBl. I S. 2153) geändert worden ist, haben Vorgaben auf Grund des Atomgesetzes Vorrang vor den Anforderungen des Katalogs nach Satz 1. Die für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder sind bei der Erarbeitung des Katalogs von Sicherheitsanforderungen zu beteiligen. Ein angemessener Schutz nach Satz 1 liegt vor, wenn der IT-Sicherheitskatalog eingehalten und dies vom Betreiber dokumentiert worden ist.

(3) Die IT-Sicherheitskataloge nach den Absätzen 1 und 2 sollen den Stand der Technik einhalten und unter Berücksichtigung der einschlägigen europäischen und internationalen Normen sowie der Umsetzungskosten ein Sicherheitsniveau 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. Die IT-Sicherheitskataloge nach den Absätzen 1 und 2 umfassen zumindest:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme

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 Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen,

6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit,

7. Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit,

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 innerhelb der Einrichtung,

11. Einsatz von Systemen zur Angriffserkennung nach § 2 Absatz 1 Nummer 38 des BSI-Gesetzes.

Die Bundesnetzagentur kann in den IT-Sicherheitskatalogen nach den Absätzen 1 und 2 nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation sowie Behebung der Sicherheitsmängel treffen. Die Sicherheitskataloge nach den Absätzen 1 und 2 enthalten auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen.

(4) Betreiber von Energieversorgungsnetzen und solche Betreiber von Energieanlagen, die kritische Anlagen nach § 2 Absatz 1 Nummer 19 28 Absatz 6 des BSI-Gesetzes sind, übermitteln der Bundesnetzagentur die Dokumentation nach Absatz 3 Satz 4. Bei Bedarf kann die Bundesnetzagentur die Vorlage des Mängelbeseitigungsplans anfordern. Die Bundesnetzagentur kann bei Sicherheitsmängeln aus dem Mängelbeseitigungsplan die Beseitigung dieser innerhalb einer durch die Bundesnetzagentur gesetzten Frist verlangen. Die Betreiber nach Satz 1 haben der Bundesnetzagentur und den in deren 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 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 von Energieanlagen, der eine wichtige Einrichtung nach § 28 Absatz 7 des BSI-Gesetzes ist, die Anforderungen aus Absatz 2 nicht oder nicht richtig umsetzt, so kann sie Maßnahmen nach Absatz 4 durchführen. Die Bundesnetzagentur

kann Informationen anfordern, um die Einhaltung der Sicherheitsanforderungen nach Absatz 2 zu überprüfen.

(6) Betreiber von Energieversorgungsnetzen und solche Betreiber von Energieanlagen, die besonders wichtige Einrichtungen nach § 28 Absatz 6 des BSI-Gesetzes oder wichtige Einrichtungen nach § 28 Absatz 7 des BSI-Gesetzes sind, übermitteln an das Bundesamt für Sicherheit in der Informationstechnik über eine vom Bundesamt für Sicherheit in der Informationstechnik im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Meldemöglichkeit:

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 des Bundesamtes für Sicherheit in der Informationstechnik eine Zwischenmeldung über relevante Statusaktualisierungen;

4. spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Nummer 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 zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;

   c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;

   d) Gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

§§ 2 Absatz 1 Nummer 10 und 31 Absatz 2 bis 5 des BSI-Gesetzes gelten entsprechend.

(7) Das Bundesamt für Sicherheit in der Informationstechnik hat die Meldungen nach Absatz 6 und solche Meldungen über Sicherheitsvorfälle nach § 31 des BSI-Gesetzes, bei welchen das Bundesamt für Sicherheit in der Informationstechnik Kenntnis von einer Relevanz für die Energieversorgungssicherheit und Erfüllung der Ziele nach § 1 erlangt, unverzüglich an die Bundesnetzagentur weiterzuleiten. Die Bundesnetzagentur führt unverzüglich eine Bewertung der Auswirkungen des nach Satz 1 übermittelten Sicherheitsvorfalls 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 deshalb 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- und Fernleitungsnetzen einbeziehen und ist befugt, ihnen die hierzu erforderlichen personenbezogenen Daten zu übermitteln. Die Betreiber von Übertragungs- und Fernleitungsnetzen 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- und Fernleitungsnetzen unverzüglich zu löschen. Das Bundesamt für Sicherheit in der Informationstechnik berücksichtigt die Bewertung der Bundesnetzagentur bei der Erfüllung der Aufgaben nach § 40 Absatz 2 Nummer 2 des BSI-Gesetzes. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben 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 § 5c Absatz 1 bis Absatz 7 wird nicht gewährt. § 29 des Verwaltungsverfahrensgesetzes bleibt unberührt.

(8) Betreiber von Energieversorgungsnetzen und solche Betreiber von Energieanlagen, die besonders wichtige Einrichtungen nach § 28 Absatz 6 des BSI-Gesetzes oder wichtige Einrichtungen nach § 28 Absatz 7 des BSI-Gesetzes sind, sind verpflichtet, spätestens bis zum 1. April, erstmalig oder erneut, sich beim Bundesamt für Sicherheit in der Informationstechnik zu registrieren. Dabei sind Angaben nach § 32 Absatz 1 Nummer 1 – 4 des BSI-Gesetzes zu übermitteln. Für Betreiber von Energieversorgungsnetzen und Betreiber von Energieanlagen, die kritische Anlagen nach § 28 Absatz 3 des BSI-Gesetzes sind, gilt § 32 Absatz 3 des BSI-Gesetzes entsprechend. Das Bundesamt für Sicherheit in der Informationstechnik übermittelt die Registrierungen einschließlich der damit verbundenen Kontaktdaten an die Bundesnetzagentur. Die Registrierungen nach Satz 1 und Satz 3, 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 die Bundesnetzagentur darüber und übermittelt die damit verbundenen Kontaktdaten. Die Betreiber haben sicherzustellen, dass sie über die benannte oder durch das Bundesamt für Sicherheit in der Informationstechnik festgelegte Kontaktstelle jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt für Sicherheit in der Informationstechnik nach § 40 Absatz 2 Nummer 4 Buchstabe a des BSI-Gesetzes erfolgt an diese Kontaktstelle.

(9) Die Bundesnetzagentur legt bis zum 22. Mai 2023 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 Absatz 1 Nummer 20 Buchstabe c Ziffer aa des BSI-Gesetzes sind oder

2. welche Funktionen kritisch bestimmte Funktionen nach § 2 Absatz 1 Nummer 20 Buchstabe c Ziffer bb des BSI-Gesetzes sind.

Die Betreiber von Energieversorgungsnetzen und Energieanlagen, die kritische Anlagen nach § 28 Absatz 3 des BSI-Gesetzes sind, haben die Vorgaben des Katalogs spätestens sechs Monate nach dessen Inkrafttreten zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden. Der Katalog wird mit den IT-Sicherheitskatalogen nach Absätzen 1 und 2 verbunden.

(10) Betreiber von Energieversorgungsnetzen und Betreiber von Energieanlagen, die besonders wichtige Einrichtungen nach § 28 Absatz 6 des BSI-Gesetzes sind, sind ab dem [einsetzen: 1 Jahr nach Inkrafttreten] verpflichtet, am Informationsaustausch nach § 6 des BSI-Gesetzes teilzunehmen.

(11) Die Bundesnetzagentur erstellt im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik bis zum 1. Juni jeden Jahres einen zusammenfassenden Bericht über die im vergangenen Kalenderjahr an sie nach Absatz 6 übermittelten Meldungen über Sicherheitsvorfälle und deren Auswirkungen und legt ihn dem Bundesministerium für Wirtschaft und Klimaschutz vor.“

3. In § 11 werden die Absätze 1a bis 1g aufgehoben.

4. In § 91 Absatz 1 Nummer 4 wird der Angabe „7c“ die Angabe „5c Absatz 4“ vorangestellt.

5. § 95 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Nummer 2a wird die Angabe „§ 11 Absatz 1a oder 1b den Katalog von Sicherheitsanforderungen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig einhält“ durch „§ 5c Absatz 1 oder 2 den Sicherheitskatalog nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig einhält“ ersetzt.

bb) In Nummer 2b wird die Angabe „§ 11 Absatz 1 c“ durch die Angabe „§ 5c Absatz 6“ ersetzt.

b) Nach Absatz 2 wird folgender Absatz 2a eingefügt:

„(2a) Die Ordnungswidrigkeit kann in Fällen des Absatzes 1 Nummer 2a und Nummer 2b mit einer Geldbuße bis zu einer Million Euro geahndet werden. Handelt es sich bei dem Betroffenen um eine wichtige Einrichtung nach § 28 Absatz 7 des BSI-Gesetzes kann die Ordnungswidrigkeit mit einer Geldbuße bis zu 7 Millionen Euro oder mit einem Höchstbetrag von mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört geahndet werden. Handelt es sich bei dem Betroffenen um eine besonders wichtige Einrichtung nach § 28 Absatz 7 des BSI-Gesetzes, kann die Ordnungswidrigkeit mit einer Geldbuße bis zu 10 Millionen Euro oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört, geahndet werden. Die Höhe des Gesamtumsatzes kann geschätzt werden.“

Artikel 17

Änderung des Messstellenbetriebsgesetzes (FNA 752-10)

In § 24 des Messstellenbetriebsgesetz vom 29. August 2016 (BGBl. I S. 2034), das zuletzt durch Artikel 11 des Gesetzes vom 20. Juli 2022 (BGBl. I S. 1237) geändert worden

ist, wird die Angabe „§ 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821)“ durch die Angabe „§ 54 des BSI-Gesetzes in der Fassung der Bekanntmachung vom [*einfügen: Verkündungsdatum*] (BGBl. I S. [*einfügen: Seite im Bundesgesetzblatt*])“ ersetzt.

Artikel 18

Änderung des Energiesicherungsgesetzes (FNA 754-3)

Das Energiesicherungsgesetz vom 20. Dezember 1974 (BGBl. I S. 3681), das zuletzt durch Artikel 7 des Gesetzes vom 20. Dezember 2022 (BGBl. I S. 2560) geändert worden ist, wird wie folgt geändert:

1. In den §§ 17 Absatz 1, 18 Absatz 2 Satz 1 Nummer 1 und 29 Absatz 1 werden die Wörter „Kritische Infrastrukturen“ durch die Wörter „kritische Anlagen“ und die Angabe „§ 2 Absatz 10 des BSI-Gesetzes“ durch die Angabe „§ 2 Absatz 1 Nummer 19 des BSI-Gesetzes“ ersetzt.

2. § 10 Absatz 1 Satz 3 wird wie folgt gefasst:

   „Die zuständigen Behörden, der Marktgebietsverantwortliche und die Betreiber von Elektrizitätsversorgungsnetzen übermitteln die nach den Sätzen 1 und 2 sowie nach § 2b Absatz 1 erlangten Daten einschließlich personenbezogener Daten und Betriebs- und Geschäftsgeheimnisse

   1. an andere Behörden, den Marktgebietsverantwortlichen und die Betreiber von Elektrizitätsversorgungsnetzen, soweit dies für die Vorbereitung und Wahrnehmung der Aufgaben nach diesem Gesetz sowie aufgrund dieses Gesetzes erlassenen Rechtsverordnungen erforderlich ist, sowie

   2. auf deren Ersuchen an die Bundesanstalt für Finanzdienstleistungsaufsicht, soweit dies für die Erfüllung ihrer Aufgaben erforderlich ist. Die Bundesanstalt für Finanzdienstleistungsaufsicht hat die Gründe für ihr Ersuchen zu dokumentieren. Die Verwendung der Daten ist nach Maßgabe der allgemeinen datenschutzrechtlichen Vorschriften vorzunehmen und auf das zur Erfüllung der Aufgaben dieser Stellen jeweils erforderliche Maß zu beschränken.“

[Anm. BMI CI 3 für BMWK – Zum vorstehenden Satz: Der erste Satzteil erscheint nur deklaratorisch und sollte besser in die Begründung passen. Der zweite Satzteil ist eine Wiederholung von „soweit dies für die Erfüllung ihrer Aufgaben erforderlich ist“. Ich bitte um Bestätigung, dass der markierte Teil gestrichen werden kann und bitte zudem um eine Formulierung für die Gesetzesbegründung.]

Artikel 19

Änderung des Fünften Buches Sozialgesetzbuch (FNA 860-5)

Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 1b des Gesetzes vom 20. Dezember 2022 (BGBl. I S. 2793) geändert worden ist, wird wie folgt geändert:

1. In § 75b Absatz 4 wird die Angabe „§ 8a Absatz 1 des BSI-Gesetzes“ durch die Angabe „§ 39 Absatz 1 des BSI-Gesetzes“ ersetzt.

2. § 75c wird wie folgt geändert:

   a) In Absatz 2 wird die Angabe „§ 8a Absatz 2 des BSI-Gesetzes“ durch die Angabe „§ 30 Absatz 12 des BSI-Gesetzes“ ersetzt.

   b) In Absatz 3 werden die Wörter „Kritische Infrastrukturen“ durch die Wörter „kritischer Anlagen“ und die Angabe „§ 8a des BSI-Gesetzes“ durch die Angabe „§§ 30 und 39 des BSI-Gesetzes“ ersetzt.

Artikel 20

Änderung der Digitale Gesundheitsanwendungen-Verordnung (FNA 860-5-55)

In der Tabellenzelle in der Spalte Anforderung und der Zeile Nummer 5 der Überschrift „Datensicherheit“, der Unterüberschift „Basisanforderungen, die für alle digitalen Gesundheitsanwendungen gelten“ der Tabelle in Anlage 1 (Fragebogen gemäß § 4 Absatz 6) der Digitale Gesundheitsanwendungen-Verordnung vom 8. April 2020 (BGBl. I S. 768), die zuletzt durch Artikel 3 des Gesetzes vom 20. Dezember 2022 (BGBl. I S. 2793) geändert worden ist, wird die Angabe „§ 8 Absatz 1 Satz 1 des BSI-Gesetzes“ durch die Angabe „§ 44 Absatz 1 Satz 1 des BSI-Gesetzes“ ersetzt.

Artikel 21

Änderung des Sechsten Buches Sozialgesetzbuch (FNA 860-6)

[Anm. BMI CI 1 – Ergänzungsbitte BMAS]

§ 138 Absatz 1 Satz 2 des Sechsten Buches Sozialgesetzbuch – Gesetzliche Rentenversicherung – in der Fassung der Bekanntmachung vom 19. Februar 2002 (BGBl. I S. 754, 1404, 3384), das zuletzt durch Artikel 13 des Gesetzes vom 2. März 2023 (BGBl. 2023 I Nr. 56) geändert worden ist, wird wie folgt geändert:

1. In Nummer 15 wird das Wort „und“ durch ein Komma ersetzt.

2. In Nummer 16 wird der Punkt am Ende durch das Wort „und“ ersetzt.

3. Folgende Nummer 17 wird angefügt:

   „17. Koordinierung einer an den Zielen von Wirtschaftlichkeit und Sicherheit ausgerichteten Informationstechnik der Rentenversicherung, insbesondere durch

      a) die Festlegung von einheitlichen Grundsätzen für die Informationstechnik und Informationssicherheit der Rentenversicherung,

      b) den Betrieb der informationstechnischen Infrastruktur und des Netzwerkes der Rentenversicherung,

c) die Entwicklung rentenversicherungsbezogener Anwendungen und

d) die Festlegung eines Beschaffungskonzepts.“

Artikel 22

Änderung der Verordnung zum Barrierefreiheitsstärkungsgesetz (FNA 860-9-4-1)

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 Absatz 1 Nummer 36 des BSI-Gesetzes in der Fassung der Bekanntmachung vom [*einfügen: Verkündungsdatum*] (BGBl. I S. [*einfügen: Seite im Bundesgesetzblatt*])“.

Artikel 23

Änderung des Telekommunikationsgesetzes (FNA 900-17)

Das Telekommunikationsgesetz vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 5 des Gesetzes vom 14. März 2023 (BGBl. 2023 I Nr. 71) geändert worden ist, wird wie folgt geändert:

1. § 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 bzw. zugänglich sind, beeinträchtigt;“.

   b) In Nummer 79 wird der „.“ durch ein „;“ ersetzt.

   c) Es wird folgende Nummer 80 eingefügt:

      „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.“

2. § 165 wird wie folgt geändert:

a) Absatz 2 Satz 3 wird gestrichen.

b) In Absatz 2 wird der Satz „Bei diesen Maßnahmen ist der Stand der Technik zu berücksichtigen“ gestrichen und stattdessen folgender Satz angefügt:

„Diese Maßnahmen sollen den Stand der Technik einhalten und unter Berücksichtigung der einschlägigen europäischen und internationalen Normen sowie der Umsetzungskosten ein Sicherheitsniveau Netz- und Informationssysteme gewährleisten, 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.“

c) Nach Absatz 2 wird folgender Absatz 2a eingefügt:

„(2a) Maßnahmen nach Absatz 2 von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 6 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 7 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.“

d) In Absatz 3 wird die Angabe „§ 2 Absatz 9b„ durch die Angabe „§ 2 Absatz 1 Nummer 38„ ersetzt.

e) In Absatz 4 wird Angabe „§ 2 Absatz 13“ durch die Angabe „§ 2 Absatz 1 Nummer 20“ ersetzt.

f) In Absatz 11 wird die Angabe „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; L33 vom 7.2.2018, S.5)“ durch die Angabe „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.

3. § 167 Absatz 1 Nummer 2 wird wie folgt geändert:

a) Die Angabe „§ 2 Absatz 13 Satz 1 Nummer 3 Buchstabe b“ wird durch die Angabe „§ 2 Absatz 1 Nummer 20 Buchstabe c Doppelbuchstabe bb“ ersetzt.

b) Die Angabe „§ 2 Absatz 13“ wird durch die Angabe „§ 2 Absatz 1 Nummer 20“ ersetzt.

4. § 168 wird wie folgt geändert:

a) 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 siener 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.

(2) Dauert der erhebliche Sicherheitsvorfall im Zeitpunkt des Absatz 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.“

b) Absatz 6 wird die Angabe „§ 8e“ durch die Angabe „§ 42“ ersetzt.

5. In § 174 Absatz 3 und 5 wird die Angabe „§ 2 Absatz 10 Satz 1 Nummer 1“ durch die Angabe „§ 57 Absatz 4 Nummer 1“ ersetzt.

6. In § 214 Absatz 3 werden die Wörter „Kritische Infrastrukturen“ durch die Wörter „kritische Anlagen“ und die Angabe „§ 2 Absatz 10“ durch die Angabe „§ 2 Absatz 1 Nummer 19“ ersetzt.

Artikel 24

Änderung der Krankenhausstrukturfonds-Verordnung (FNA 2126-9-19)

In § 11 Absatz 1 Nummer 4 Buchstabe a und § 14 Absatz 2 Nummer 8 der 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 wird die Angabe „§ 8a des BSI-Gesetzes“ durch die Angabe „§ 39 des BSI-Gesetzes“ ersetzt.

Artikel 25

Änderung der Mess- und Eichverordnung (FNA 7141-8-1)

In § 40 Absatz 4 Nummer 2 der Mess- und Eichverordnung vom 11. Dezember 2014 (BGBl. I S. 2010, 2011), die zuletzt durch Artikel 1 der Verordnung vom 26. Oktober 2021 (BGBl. I S. 4742) geändert worden ist, werden die Wörter „§ 3 Absatz 1 Nummer 5 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 3 Absatz 7 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist, in der jeweils geltenden Fassung“ durch die Angabe „§ 3 Absatz 1 Satz 2 Nummer 8 des BSI-Gesetzes in der Fassung der Bekanntmachung vom [*einfügen: Verkündungsdatum*] (BGBl. I S. [*einfügen: Seite im Bundesgesetzblatt*])“ ersetzt.

Artikel 26

Änderung der Außenwirtschaftsverordnung (FNA 7400-4-1)

In § 55a der Außenwirtschaftsverordnung vom 2. August 2013 (BGBl. I S. 2865; 2021 I S. 4304), die zuletzt durch Artikel 10 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2632) geändert worden ist, wird wie folgt geändert:

1. In Absatz 1 Nummer 1 werden die Wörter „Kritischen Infrastruktur“ durch die Wörter „kritischen Anlage“ ersetzt.

2. In Absatz 1 Nummer 2 wird die Angabe „§ 2 Absatz 13 des BSI-Gesetzes“ durch die Angabe „§ 2 Absatz 1 Nummer 19 des BSI-Gesetzes“ und die Wörter „Kritischen Infrastrukturen“ durch die Wörter „kritischen Anlagen“ ersetzt.

Artikel 27

Änderung des Vertrauensdienstegesetzes (FNA 9020-13)

In § 2 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 Absatz 3 gestrichen.

Artikel 28

Evaluierung

Das Bundesministerium des Innern und für Heimat berichtet dem Deutschen Bundestag unter Einbeziehung von wissenschaftlichem Sachverstand über die Wirksamkeit der in diesem Gesetz nach Artikel 1 enthaltenen Maßnahmen für die Erreichung der mit diesem Gesetz verfolgten Ziele bis zum *[einsetzen: Datum des ersten Tages des achtundvierzigsten auf die Verkündung folgenden Kalendermonats]* hinsichtlich Artikel 1 Teil 2 Kapitel 1, Teil 3 Kapitel 3 sowie Teil 5 dieses Gesetzes.

Artikel 29

Inkrafttreten, Außerkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich der Absätze 2 und 3 am 1. Oktober 2024 in Kraft. Gleichzeitig tritt das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821) außer Kraft.

(2) Artikel 2 tritt an dem Tag in Kraft, an dem das Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen vom [*einsetzen*] 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.

(3) Artikel 27 tritt am 18. Oktober 2024 in Kraft.

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 Infrastrukturen, 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 einer Vielzahl von Herausforderungen. Europaweit und global vernetzte Prozesse führen ebenso wie die zunehmende Digitalisierung aller Lebens- und somit auch Wirtschaftsbereiche zu einer höheren Anfälligkeit durch externe, vielfach nicht steuerbare Faktoren. Informationstechnik in kritischen Anlagen sowie in bestimmten Unternehmen spielt dabei eine zentrale Rolle. Ihre Sicherheit und Resilienz bilden die Grundlage für die Versorgungssicherheit, von der Versorgung mit Strom und Wasser bis hin zu Siedlungsabfällen. Gleiches gilt für das Funktionieren der Marktwirtschaft in Deutschland und dem Binnenmarkt der Europäischen Union. Die Vernetzung und enge Verzahnung der Wirtschaft innerhalb Deutschlands und der Europäischen Union resultieren in Interdependenzen bei der Cybersicherheit. Die vor diesem Hintergrund erforderlichen 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. Dezember 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.

In Folge des 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 2022 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 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 „Zeitenwende“ auch neue Bedrohungen oder die Einschätzungen zu bereits bekannten Bedrohungen mussten aufgrund veränderter Rahmenbedingungen geändert werden. Beispiele hierfür bestehen beispielsweise 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. Eine Erhöhung der Resilienz der Wirtschaft gegenüber diesen neuen Bedrohungen ist daher eine zentrale Aufgabe für die beteiligten Akteure in Staat, Wirtschaft und Gesellschaft, um den Wirtschaftsstandort Deutschland robust und leistungsfähig zu halten.

Für das Informationssicherheitsmanagement in der Bundesverwaltung haben sich die bisherigen Steuerungsinstrumente auf überwiegend untergesetzlicher Basis als nicht ausreichend effektiv erwiesen, um eine flächendeckende wirksame Steigerung des Sicherheitsniveaus zu erreichen. Dies haben insbesondere Sachstandserhebungen zum Umsetzungsplan Bund sowie Prüfungen des 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 für den Bereich kritischer Anlagen und 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 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 BSIG 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 KRITIS-Dachgesetzes – 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 BSIG in Artikel 1, die Änderung des BSIG in Artikel 2, die Änderung des IT-Sicherheitsgesetzes 2.0 in Artikel 7,die Änderung des EnWG in Artikel 16, die Änderung des Energiesicherungsgesetzes in Artikel 18 und die Änderung des Telekommunikationsgesetzes in Artikel 23, 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) Grundgesetz (GG) sowie aus Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft, einschließlich gefahrenabwehrrechtlicher Annexkompetenz) in Verbindung mit Artikel 72 Absatz 2 GG.

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 Einrichtungen 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.

FürRegelungen in Artikel 1 und 2 zum 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 21 ergibt sich aus Artikel 74 Absatz 1 Nummer 12 GG.

Die Gesetzgebungskompetenzen des Bundes für die Folgeänderungen zum BSIG 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 um eine nationale Regelung, die nicht Bestandteil der Umsetzung der NIS-2-Richtlinie ist.

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 Bundesamts 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“. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

3. 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 2,3 Milliarden Euro. . Insgesamt entsteht einmaliger Aufwand von rund zwei Milliarden Euro. Dieser ist fast ausschließlich der Kategorie Einführung oder Anpassung digitaler Prozessabläufe zuzuordnen.

Davon entfallen rund 121 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.

Vorgabe 4.2.1 (Weitere Vorgabe): Einhaltung eines Mindestniveaus an IT-Sicherheit (Besonders wichtige und wichtige Einrichtungen); §§ 30 und 38 Absatz 1 in Verbindung mit § 28 BSIG-E

Bereits heute sind Betreiber kritischer Infrastrukturen und Anbieter digitaler Dienste verpflichtet, ein Mindestniveau an IT-Sicherheit zu gewährleisten (vgl. §§ 8a und 8c BSIG, § 11 EnWG und § 165 TKG). Der Regelungsentwurf führt mit §§ 30 und 38 Absatz 1 in Verbindung mit § 28 BSIG-E eine vergleichbare Norm ein, in deren Anwendungsbereich deutlich mehr Unternehmen fallen werden. Demnach sollen künftig alle besonders wichtigen und wichtigen Einrichtungen geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der für die erbrachten Dienste notwendigen Netz- und Informationssysteme zu beherrschen (§ 30 Absatz 1 BSIG-E). Hinsichtlich der Verhältnismäßigkeit benennt § 30 Absatz 2 BSIG-E als Bewertungskriterien etablierte IT-Standards, Umsetzungskosten und bestehende Risiken. Letztere werden bestimmt durch die Risikoexposition, die Größe der Einrichtung bzw. des Betreibers sowie der

Eintrittswahrscheinlichkeit und 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 8 100 Unternehmen als besonders wichtige und rund 20 900 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 Infrastrukturen, die bereits heute nach geltender Rechtslage entsprechende Maßnahmen implementiert haben (vgl. Online-Datenbank des Erfüllungsaufwands des StBA (OnDEA), ID 2015030909595401, 2017052913283301, 2020093009264301 und 2020093009264401). Folglich konstituiert die Rechtsänderung nur für die übrigen rund 3 400 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. Mangels amtlicher Statistiken kann dieser Anteil nur anhand von sonstigen öffentlich zu-gänglichen Informationen geschätzt werden. So zeigt eine empirische Studie, dass rund 21 Prozent der vom IT-Sicherheitsgesetz 2.0 betroffenen Betreiber kritischer Infrastruktur bereits zum Inkrafttreten des Gesetzes die gesetzlich vorgegebenen Systeme der Angriffserkennung eingesetzt hatten (vgl. Hayvali (2023), https://www.secunet.com/ueber-uns/news-events/artikel/kritis-studie-cybersecurity-bedrohung-fuer-unternehmen-waechst). Laut einer anderen Studien sahen sich im Jahr 2023 17 Prozent der befragten Unternehmen (auch aus dem nicht kritischen Infrastrukturbereich) als sehr gut gegen Cyberangriffe aufgestellt (s. eco – Verband der Internetwirtschaft e. V. (2023),: https://www.eco.de/presse/eco-it-sicherheitsumfrage-2023-viele-unternehmen-unterschaetzen-noch-immer-bedrohungslage/). Angesichts dieser Erkenntnisse wird angenommen, dass rund 17 Prozent der potenziell betroffenen Unternehmen bereits heute im Grundsatz ausreichende Maßnahmen 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.

Laut OnDEA (vgl. ID 2015030909595401 und 2017052913283301) beträgt der Personalaufwand der Betreiber kritischer Infrastrukturen für die Einhaltung eines Mindestniveau an IT-Sicherheit nach geltender Rechtslage durchschnittlich 2 752 Stunden und 60 000 Euro Sachkosten. Die Daten wurden vom StBA 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 erhoben und für die Verwendung in der vorliegenden Schätzung an die Inflation der letzten drei Jahre angepasst. 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 und aufgrund der entfallenden ex ante Nachweisverfahren 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 Euroentspricht. 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 Unternehmen mit wichtigen Einrichtungen 70 Prozent der Aufwände der besonders wichtigen Einrichtungen und der Aufwand mittlerer Unternehmen mit wichtigen 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 jährliche Personalkosten in der Höhe von rund 288 Millionen Euro (= 2 000 Unternehmen * 2 752 Stunden * 52,30 Euro) und jährliche Sachkosten in der Höhe 104 Millionen Euro entstehen (= 2 000 Unternehmen * 52 000 Euro pro Unternehmen). Für die wichtigen Einrichtungen entstehen jährliche Personalkosten von 720 Millionen Euro (= 12 500 Unternehmen * 1 101 Stunden * 52,30 Euro). Die jährlichen Sachkosten belaufen sich auf knapp 263 Millionen Euro (= 12 500 Unternehmen * 21 000 Euro/Unternehmen). Insgesamt erhöht sich der jährliche Erfüllungsaufwand um über zwei Milliarden Euro.

Hinsichtlich des einmaligen Aufwands liegen keine Anhaltspunkte für eine Schätzung vor. Nach einer freien Annahme wird davon ausgegangen, 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. Insofern ist von einem einmaligen Erfüllungsaufwand von rund zwei Milliarden Euro auszugehen.

Gemäß dem Konzept zur Erhöhung der Transparenz über den Umstellungsaufwand für die Wirtschaft und zu dessen wirksamer und verhältnismäßiger Begrenzung ist der einmalige Erfüllungsaufwand der Kostenkategorie der Einführung und Anpassung digitaler Prozessabläufe zuzuordnen.

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 ist zum jetzigen Zeitpunkt aber 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 Zuge den nun in Artikel 21 und dem Erwägungsgrund 15 vorgesehenen Bewertungskriterien bezüglich der Angemessenheit der zu treffenden Maßnahmen ist eine solche Unterscheidung möglich – sie findet ihre bundesrechtliche Entsprechung in §§ 30 und 34 in Verbindung mit § 28 BSIG-E. 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. Zusammenfassend kann festgehalten werden, dass im Vergleich zum Richtlinienvorschlag der einmalige Erfüllungsaufwand der geltenden EU-Richtlinie aufgrund der beschriebenen Änderungen um geschätzt rund 1,1 Milliarden Euro niedriger ausfallen wird.

Vorgabe 4.2.2 (Informationspflicht): Nachweis der Einhaltung eines Mindestniveaus an IT-Sicherheit (Besonders wichtige Einrichtungen); § 34 BSIG-E in Verbindung mit §§ 28 und 30 BSIG-E

Besonders wichtige Einrichtungen haben die Einhaltung der Anforderungen an das Risikomanagement dem BSI auf geeignete Weise nachzuweisen; wichtige Einrichtungen unterliegen dieser Nachweispflicht nicht (vgl. § 34 BSIG-E). Bereits heute gibt es nationale Regelungen, durch welche ein Teil der betroffenen Einrichtungen vergleichbaren Dokumentations- und Nachweispflichten unterliegt (vgl. 11 Absatz 1b EnWG, §§ 8a Absatz 3 und 8c Absatz 4 sowie § 8f Absatz 1 BSIG). Nennenswerter Mehraufwand wird insofern nur für rund 3 550 (≈ 8 250 - 4 693) besonders wichtige Einrichtungen ausgelöst, die bisher noch nicht in den Anwendungsbereich vergleichbarer nationaler Regelungen fallen (vgl. Vorgabe 4.2.1).

Laut OnDEA (ID 2015030909595501 und 2020093009264402) beträgt der durchschnittliche Zeitaufwand zur Erbringung der Nachweispflicht inklusive notwendiger Dokumentationen und Prüfungen im Mittel 282 Stunden und die Sachkosten im Mittel 19 300 Euro. Bei einem mittleren Lohnsatz von 56,90 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), ergeben sich jährliche Personalkosten in der Höhe rund 57 Millionen Euro. Hinzu kommen jährliche Sachkosten in der Höhe von 69 Millionen Euro. Der gesamte jährliche Erfüllungsaufwand aus dieser Informationspflicht beträgt demnach rund 125 Millionen Euro.

Vorgabe 4.2.3 (Informationspflicht): Meldung erheblicher Sicherheitsvorfälle (Besonders wichtige und wichtige Einrichtungen); § 31 in Verbindung mit § 28 BSIG-E

Der Regelungsentwurf sieht im Zusammenhang mit Sicherheitsvorfällen Meldepflichten besonders wichtiger und wichtiger Einrichtungen gegenüber dem BSI vor (vgl. § 31 BSIG-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, § 169 TKG) eine Meldepflicht von Sicherheitsvorfällen.

Die Anzahl der gemeldeten Sicherheitsvorfälle betrug im Zeitraum 1. Juni 2021 bis 31. Mai 2022 laut BSI insgesamt 452 (vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2022, S. 68, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8). Bei bisher 4 693 meldepflichtigen Unter-nehmen ergibt dies je Unternehmen ca. 0,0963 Meldungen pro Jahr. Geht man von einer ähnlich strengen Meldepflicht der geplanten Rechtsänderungen aus, werden die neu hin-zukommenden 25 157 (= 29 850 - 4 693) meldepflichtigen Unternehmen pro Jahr zusätz-lich rund 2 400 erhebliche Sicherheitsvorfälle melden.

Der fallbezogene Zeitaufwand beträgt rund 4,5 Stunden für Meldungen nach geltender Rechtslage (vgl. OnDEA, ID 2017052913283701 und 2015030909595201). Der Regelungsentwurf sieht ein mehrstufiges Meldeverfahren vor (vgl. § 31 Abs. 1 BSIG-E). Dieses umfasst unter anderem eine obligatorische Kurzmeldung innerhalb von 24 Stunden und eine obligatorische Vorfallmeldung innerhalb von 72 Stunden. Gemäß § 8b Absatz 4 Satz 2 BSIG ist derzeit lediglich eine Meldung vorgesehen, weswegen davon auszugehen ist, dass der Aufwand pro gemeldetem Sicherheitsvorfall künftig höher sein wird. Hierfür wird vereinfacht ein Aufschlag von 50 Prozent angesetzt, so dass von einer Gesamtdauer von 6,75 Stunden je Sicherheitsvorfall ausgegangen wird.

Bei 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 946 000 Euro.

Vorgabe 4.2.4 (Informationspflicht): Registrierungspflichten (Besonders wichtige und wichtige Einrichtungen sowie bestimmte Einrichtungsarten); §§ 32 und 33 in Verbindung mit § 28 BSIG-E

Durch den Regelungsentwurf wird die bestehende Registrierungspflicht (vgl. §§ 8b und 8f BSIG) auf alle besonders wichtigen und wichtigen Einrichtungen sowie für bestimmte Einrichtungsarten ausgeweitet. Als registerführende Stelle kann BSI Einzelheiten des Registrierungsverfahrens bestimmen. Durch die erstmalige Übermittlung der Informationen entsteht einmaliger Erfüllungsaufwand. Jährlicher Erfüllungsaufwand entsteht aus der Pflicht, Änderungen der registerpflichtigen Angaben melden zu müssen (vgl. §§ 32 und 33 in Verbindung mit § 28 BSIG-E).

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 In-formationspflicht 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 wichtigen und wesentlichen Einrichtungen haben die zuständige Behörde über etwaige Änderungen zu informieren (vgl. §§ 32 Absatz 6, 33 Absatz 2 BSIG-E). Es wird davon ausgegangen, dass sich pro Jahr in einem Drittel der Einrichtungen mindestens eine An-gabe 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 4.2.5 (Weitere Vorgabe): Regelmäßige Schulungen (Besonders wichtige und wichtige Einrichtungen); § 38 Absatz 4 in Verbindung mit § 28 BSIG-E

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 4 BISG-E).

Der Regelungsentwurf lässt wesentliche Angaben, die zur Herleitung des Erfüllungsaufwands notwendig sind, offen. 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 werden müssen. Dies liegt der freien Annahme zu Grunde, dass einmal im Jahr zehn Be-schäftigte je Unternehmen an einer solchen Schulung teilnehmen müssen (29 850 Unter-nehmen * 10). Es ist jedoch davon auszugehen, dass Unternehmen aus eigenem Interesse zum Teil bereits heute ihren führenden Mitarbeitenden Cybersicherheitsschulungen anbie-ten. Es wird frei angenommen, dass dies für 50 Prozent der Unternehmen zutrifft, sodass davon auszugehen ist, dass sich für rund 150 000 Mitglieder der Leitungsorgane eine Ver-änderung 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 (= 150 000 * 4 Stunden * 58,40 Euro).

Werden je teilnehmender Person zusätzliche Schulungskosten in Höhe von 100 Euro angenommen, fallen zusätzlich jährliche Sachkosten in Höhe von 15 Millionen Euro an (= 150 000 * 100 Euro Schulungskosten).

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 werden (= insgesamt knapp 6 Millionen Beschäftigte). Wie bei den Geschäftsleitern wird davon ausgegangen, dass rund 50 Prozent der Unternehmen ihren Mitarbeitenden bereits heute die Teilnahme an entsprechenden Cybersicherheitsschulungen ermöglichen (= knapp 3 Millionen Beschäftigte). 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, https://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 (Lohn-kosten der Gesamtwirtschaft A-S ohne O; durchschnittliches Qualifikationsniveau) zusätz-licher 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.

KMU-Test

Ein KMU-Test ist für den Gesetzentwurf durchgeführt worden. Das Regelungsvorhaben betrifft kleine und mittlere Unternehmen, da diese unter § 28 Abs. 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

[Anm. BMI CI1 – Für die formal korrekte Darstellung unter D. sind noch weitere Angaben erforderlich, die im Rahmen der laufenden Ressortabstimmung abgefragt werden. Eine Darstellung erfolgt in der nächsten Fassung des Referentenentwurfs.]

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen wird finanziell und stellenmäßig im Gesamthaushalt ausgeglichen.

4. Weitere Kosten

Keine.

5. 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. § 1 Absatz 2 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. Befristung; Evaluierung

Art. 28 sieht eine Evaluierungsklausel vor. Da der Gesetzentwurf in weiten Teilen der Umsetzung der NIS-2-Richtlinie dient und gemäß Artikel 40 der NIS-2-Richtlinie bereits Gegenstand einer Evaluierung durch die Europäische Kommission ist, wird vorliegend eine beschränkte Evaluierung vorgesehen.

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 Betreibern und 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)

Bis auf redaktionelle Änderungen unverändert im Vergleich zu § 1 BSI-Gesetz a.F.

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 Absatz 1

Zu Nummer 1

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 5 der NIS-2-Richtlinie.

Zu Nummer 2

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.

Zu Nummer 3

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 32 30 der NIS-2-Richtlinie.

Zu Nummer 4

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 10 32 der NIS-2-Richtlinie.

Zu Nummer 5

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 9 fort.

Zu Nummer 6

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 20 der NIS-2-Richtlinie.

Zu Nummer 7

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 22 der NIS-2-Richtlinie.

Zu Nummer 8

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 11 der NIS-2-Richtlinie.

Zu Nummer 9

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 10

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 % der Gesamttätigkeit gegeben sein.

Zu Nummer 11

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 12

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 13

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 14

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 15

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 16

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 1 fort.

Zu Nummer 17

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 18 der NIS-2-Richtlinie.

Zu Nummer 18

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 19

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.

Zu Nummer 20

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 13 fort.

Zu Nummer 21

Die Begriffsbestimmung der kritischen Dienstleistung wurde neu aufgenommen.

Zu Nummer 22

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 40 der NIS-2-Richtlinie.

Zu Nummer 23

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 39 der NIS-2-Richtlinie.

Zu Nummer 24

Die Begriffsbestimmung dient der Vereinfachung der zahlreichen Zitate der NIS-2-Richtlinie im BSI-Gesetz.

Zu Nummer 25

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 28 der NIS-2-Richtlinie.

Zu Nummer 26

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 29 der NIS-2-Richtlinie.

Zu Nummer 27

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 33 der NIS-2-Richtlinie.

Zu Nummer 28

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 8 fort.

Zu Nummer 29

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 8a fort.

Zu Nummer 30

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 26 der NIS-2-Richtlinie.

Zu Nummer 31

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 27 der NIS-2-Richtlinie.

Zu Nummer 32

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 31 der NIS-2-Richtlinie.

Zu Nummer 33

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 5 fort.

Zu Nummer 34

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 35

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 36

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 2 Satz 2 fort.

Zu Nummer 37

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

Zu Nummer 38

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 9b fort.

Zu Nummer 39

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 21 der NIS-2-Richtlinie.

Zu Nummer 40

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 24 der NIS-2-Richtlinie.

Zu Nummer 41

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 25 der NIS-2-Richtlinie.

Zu Nummer 42

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 7 fort.

Zu Absatz 2

Absatz 2 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 RVO sinnvoll ist. Da hierzu bis Oktober 2024 auch ein Durchführungsrechtsakt der EU-KOM 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 BSIG stünden, aber ggf. aufgrund anderweitiger Festlegungen im Durchführungsrechtsakt ungültig wären. Durch die Möglichkein, mit einer nachgelagerten RVO hier auch ergänzend zum Durchführungsrechtsakt weitergehende Klarstellungen zu geben, ergibt sich dieses Problem nicht.

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 Absatz 1 Nummer 36 definierten Begriff handelt, welche die bereinigten Worte bereits beinhaltet, handelte es sich hier um einen Zirkelschluss.

Zu Nummer 1

Nummer 1 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 1 fort.

Zu Nummer 2

Nummer 2 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 2 fort.

Zu Nummer 3

Nummer 3 dient der Umsetzung von Artikel 14 und 15 der NIS-2-Richtlinie in Form einer Aufgabe des Bundesamtes.

Zu Nummer 4

Nummer 4 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 3 fort.

Zu Nummer 5

Nummer 5 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 4 fort.

Zu Nummer 6

Nummer 6 dient der Umsetzung von Artikel 19 der NIS-2-Richtlinie in Form einer Aufgabe des Bundesamtes.

Zu Nummer 7

In Nummer 7 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 BSI bei der dort geregelten Aufgabe der 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

Nummer 8 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 5 fort.

Zu Nummer 9

Nummer 9 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 5a fort.

Zu Nummer 10

Nummer 10 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 6 fort.

Zu Nummer 11

Nummer 11 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 7 fort.

Zu Nummer 12

Nummer 12 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 8 fort.

Zu Nummer 13

Nummer 13 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 9 fort.

Zu Nummer 14

Nummer 14 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 10 fort.

Zu Nummer 15

Nummer 15 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.

Zu Nummer 16

Nummer 16 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

Nummer 17 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.

Zu Nummer 18

Nummer 18 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

Nummer 19 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 13a fort.

Zu Nummer 20

Nummer 20 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

Nummer 21 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 14a fort.

Zu Nummer 22

Nummer 22 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 15 fort.

Zu Nummer 23

Nummer 23 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 16 fort.

Zu Nummer 24

Nummer 24 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

Nummer 25 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

Nummer 26 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 19 fort.

Zu Nummer 27

Nummer 27 führt den bisherigen § 3 Absatz 1 Satz 2 Nummer 20 fort.

Zu Nummer 28

Die neue Aufgabe des Bundesamtes in Nummer 28 dient der Umsetzung von Artikel 10 Absatz 8 der NIS-2-Richtlinie.

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 zum Umgang mit den identifizierten Gefahren bereitstellen muss.

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 Absatz 1 Nummer 4), Beinahevorfällen (§ 2 Absatz 1 Nummer 1), Schwachstellen (§ 2 Absatz 1 Nummer 35), 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 BSI 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 Absatz 1 bis Absatz 6

Die Vorschrift führt § 4a BSI-Gesetz a.F. 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. Zudem wird eine Sachverhaltsklärung ergänzt, um Missverständnissen und Fehlern vorzubeugen. Darüber hinaus steht es jeder geprüften Einrichtung frei, zum Prüfbericht des BSI eine eigene Stellungnahme gegenüber denjenigen Stellen abzugeben, die den Prüfbericht des BSI erhalten haben, also insbesondere gegenüber dem eigenen Ressort-ISB und der eigenen Fach- und Rechtsaufsicht. Im Übrigen erfolgen redaktionelle Änderungen.

Zu Absatz 7

Absatz 7 dient der Umsetzung von Artikel 35 der NIS-2-Richtlinie.

Zu Absatz 8

Die neue Vorschrift dient dem Ziel, mehr Umsetzungsverantwortung zu schaffen. Bislang sind die Prüfungen nach § 4a BSI-Gesetz a.F. 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 BMI 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 § 59 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.

Zu Absatz 7

Absatz 7 führt den bisherigen § 5 Absatz 6 fort. Ergänzt wird die Möglichkeit, dass BSI 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 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. Die Anweisung des Bundesamtes gegenüber Einrichtungen der Bundesverwaltung können sowohl die jeweilige Informationssicherheitsbeauftragte oder den jeweiligen Informationssicherheitsbeauftragten der Einrichtung gem. § 45 betreffen, als auch die Informationssicherheitsbeauftragte oder den Informationssicherheitsbeauftragten für wesentliche Digitalisierungsvorhaben und Kommunika-

tionsinfrastrukturen des Bundes gem. § 47. Mögliche Beispiele für BSI-Anweisungen können lageabhängig nach sachlicher und rechtlicher Einzelfallprüfung sein: Übergabe von Systemen oder Daten zur Analyse an das BSI; erhöhte Protokollierung zur Anomaliedetektion; Verlängerung von Speicherfristen; Verhindern von Datenlöschung; Installation eines BSI-Netzwerksensors 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 Die Durchsetzung allgemeiner präventiver Maßnahmen bleibt dagegen Aufgabe der Informationssicherheitsbeauftragten der Ressorts und des Koordinators oder der Koordinatorin für Informationssicherheit (vgl. §§ 46, 49 und 50 Absatz 3). Entsprechend der unterschiedlichen Rollen im Aufsichtsgefüge ist eine Berichterstattung gleichermaßen vorgesehen an BSI als operativer Aufsichtsbehörde, Ressort-ISB als zuständiger Fachaufsicht sowie CISO Bund als koordinierender Stelle für die Informationssicherheit in der Bundesverwaltung insgesamt, die zur effektiven Wahrnehmung ihrer jeweiligen Aufgaben auf aktuelle Lageinformationen angewiesen sind..

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.

Zu Absatz 4

Absatz 4 führt den bisherigen § 5b Absatz 4 fort.

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.

Zu Absatz 2

Absatz 1 führt den bisherigen § 5b Absatz 1 und 2 fort.

Zu Absatz 3

Absatz 2 führt den bisherigen § 5b Absatz 3 fort.

Zu Absatz 4

Absatz 3 führt den bisherigen § 5b Absatz 4 fort. Die Begriffe werden an die neuen Kategoriebezeichnungen angepasst.

Zu Absatz 5

Absatz 4 führt den bisherigen § 5b Absatz 5 fort.

Zu Absatz 6

Absatz 5 führt den bisherigen § 5b Absatz 6 fort.

Zu Absatz 7

Absatz 6 führt den bisherigen § 5b Absatz 7 fort.

Zu Absatz 8

Absatz 7 führt den bisherigen § 5b Absatz 8 fort.

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.

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

§ 15 führt den bisherigen § 7b fort.

Zu Absatz 1

Absatz 1 führt den bisherigen § 7b Absatz 1 fort. Die Änderungen dienen 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. Einschränkungen auf bestimmte Arten von Scans oder einen Anlass als Voraussetzungen für diese Schwachstellenscans sehen die Regelungen der NIS-2-Richtlinie nicht vor, so dass der bisher in § 7b Absatz 1 enthaltene Verweis auf bloße Portscans ebenso zu streichen war, wie die Annahme eines ungeschützten Systems als Voraussetzung. Dabei war eine Einschränkung auf bloße Portscans auch deswegen nicht angezeigt, da die Detektion von Sicherheitslücken ist nicht nur über Portscans, sondern auch über weitere webseiten-/ domainbasierte Methoden möglich ist. Da sich die Art von Sicherheitsscans durch den technischen Fortschritt verändern kann, war eine ebenso entwicklungsoffene Formulierung zu wählen, wie sie die NIS-2-Richtlinie enthält. Die Regelung ermöglicht auch Scans bei den von den IT-Dienstleistern für die Einrichtung betriebenen Systemen. Der gewählte Begriff der Abfrage bezeichnet eine entwicklungsoffene Art einer informationstechnischen Abfrage an die öffentlich erreichbaren Schnittstellen, die im Rahmen der technischen Spezifikation der Schnittstelle grundsätzlich vorgesehen ist. 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 ist 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. § 7b Absatz 2 war zu streichen, da eine entsprechende einschränkende Definition z.B. auf öffentlich bekannte Schwachstellen von der NIS-2-Richtlinie nicht vorgesehen ist.

Zu Absatz 2

Absatz 2 führt den bisherigen § 7b Absatz 3 fort. § 7b Absatz 3 Satz 5 entfällt in Folge der Änderungen in Absatz 1.

Zu Absatz 3

Absatz 3 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.

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 Telemediendiensten)

§ 17 führt den bisherigen § 7d fort.

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

§ 18 führt den bisherigen § 8b Absatz 6 fort.

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. Zudem wird auf Wunsch des BMF die Einhaltung der Haushaltsordnung hinzugefügt.

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 a der NIS-2-Richtlinie.

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 Vereinheitlichungen der in diesem Gesetz genutzten und durch die NIS-2-Richtlinie vorgesehenen Einrichtungsarten.

Zu Absatz 2

Absatz 2 dient der Definition wichtiger Einrichtungen. Die obenstehenden Hinweise in der Begründung zu Absatz 1 gelten entsprechend.

Zu Nummer 1

Nummer 1 dient der Umsetzung von Artikel 3 Absatz 2 der NIS-2-Richtlinie.

Zu Nummer 2

Nummer 2 dient der Umsetzung von Artikel 2 Absatz 2 Buchstabe a Nummer ii der NIS-2-Richtlinie. Während qualifizierte Vertrauensdiensteanbieter besonders wichtige Einrichtungen sind, sind die übrigen Vertrauensdiensteanbieter wichtige Einrichtungen.

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 Kommissionsempfehlung 2003/361/EG mit Ausnahme von Artikel 3 Absatz 4 der Empfehlung anzuwenden. 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. Allerdings beziehen sich die diesbezüglichen spezialgesetzlichen Regelungen im TKG und im EnWG jeweils aufgrund der entsprechenden Zuständigkeit der Bundesnetzagentur jeweils nur auf die Erbringung der kritischen Versorgungsdienstleistung maßgeblichen IT-Systeme. Dies sind im Energiesektor die IT-Systeme, die für einen sicheren Netz- bzw. Anlagenbetrieb maßgeblich sind und im TK-Sektor die Datenverarbeitungssysteme für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten.

Für alle anderen informationstechnischen Systeme Komponenten und Prozesse, die diese Betreiber für die Erbringung ihrer Dienste nutzen, die jedoch nicht von den vorgenannten IT-Sicherheitskatalogen der Bundesnetzagentur erfasst sind, gelten somit nach wie vor die allgemeinen Anforderungen für wichtige und besonders wichtige Einrichtungen mit einer entsprechenden allgemeinen Zuständigkeit des Bundesamts.

Hierbei ist zu beachten, dass gemäß Absatz 4 die Anwendung der § 31, 32, 35 und 39 nur jeweils ausgeschlossen ist, soweit die Unternehmen den Regelungen des TKG bzw. des EnWG unterliegen. Für Querverbundsunternehmen, die in unterschiedlichen Sektoren gleichzeitig tätig sind, ergeben sich daher mitunter mehrere gesetzliche Vorschriften, die parallel für den jeweiligen Tätigkeitsbereich gelten. Somit gelten beispielsweise für ein Stadtwerk, dass im TK-Bereich, im Energiesektor und im Wasser-/Abwasserbereich tätig ist, jeweils für den TK-Bereich die Anforderungen des TKG, für den Energiesektor die Anforderungen des EnWG und für den Wasser/Abwasserbereich sowie für die sonstige IT, welche für die Erbringung der Dienste genutzt wird, die Vorgaben des BSIG.

Zu Nummer 1

Nummer 1 führt den bisherigen § 8d Absatz 2 Nummer 1 fort. Die Vorschrift dient der Umsetzung von Erwägungsgrund 92 und 95 der NIS-2-Richtlinie.

Zu Nummer 2

Nummer 2 führt den bisherigen § 8d Absatz 2 Nummer 2 fort.

Zu Nummer 3

Nummer 3 führt den bisherigen § 8d Absatz 2 Nummer 3 fort und setzt die Bereichsausnahme für Finanzunternehmen, die unmittelbar unter die DORA-VO fallen, um.

Zu Absatz 5

Absatz 5 dient der Definition von Betreibern kritischer Anlagen.

Zu Absatz 6

Absatz 6 dient der Definition kritischer Anlagen und regelt den Stichtag, ab dem eine Anlage als kritische Anlage gilt.

Zu Absatz 7

Absatz 8 regelt den Stichtag, ab dem eine Anlage nicht mehr als kritische Anlage gilt.

Zu Absatz 8

Mit dieser Öffnungsklausel werden solche Unternehmen aus dem Anwendungsbereich der Umset-zung der NIS-2-Richtline auf Bundesebene ausgenommen, die zu 100% im Eigentum von Ländern und Kommunen stehen und ausschließlich Waren oder Dienstleistungen an Länder oder Kommunen anbieten. Beteiligungsstrukturen (auch gemischte mehrerer Länder oder Kommunen) sind zulässig. Schließlich ist notwendig, dass das Unternehmen Gegenstand einer landesrechtlichen NIS-2-Umsetzung ist und das Land mit der Bezugnahme auf die Öffnungsklausel auch – bewusst – Gebrauch macht. Letzteres soll gewährleisten, dass keine Unternehmen regulierungsfrei gestellt werden, die durch den Mitgliedstaat zu regulieren 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. Vor dem Hintergrund des Schutzzwecks der Informationssicherheit des Bundes und zum Zwecke der Begriffskonsolidierung ist die Definition 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. Damit wird auch dem Umstand begegnet, dass in der Vergangenheit mitunter Unklarheiten bestanden, ob und für welche Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts die Geltung der Mindeststandards angeordnet war. Mit dem Ziel der möglichst einheitlichen Regelung eines möglichst hohen Niveaus an Sicherheit wird das bisherige Anordnungserfordernis ("Opt-In“) für die Mindeststandards im Bereich der mittelbaren Bundesverwaltung nach der bisherigen § 8 Absatz 1 Satz 1 Nr. 2 durch eine allgemeine Anforderung mit der Möglichkeit zum Opt-Out abgelöst: Zur Vermeidung von Unverhältnismäßigkeiten können die Ressorts gemäß § 46 Absatz 4 Ausnahmebescheide erlassen.

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, 13 Absatz 1 Nummer 1 e), 32, 33, 35, 36, 37, 57, 62. Folgende Regelungen für besonders wichtige oder wichtige Einrichtungen finden keine Anwendung: §§ 38, und 64, da stattdessen folgende abweichende Regelungen Anwendung finden: §§ 7, 10, 43 (1), 43 (2), 43 (4), 50 (3).

Zu Absatz 3

Absatz 3 dient der Festlegung der in der NIS-2-Richtlinie angelegten Ausnahme für den Verteidigungsbereich.

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) Versorgungs-

dienstleistungen 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, obob es sich um eine wichtige Einrichtungen, eine besonders wichtige im Vergleich zu wesentlichen Einrichtung oder einen Betreiber einer kritischen 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.

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 Bundesamts gemäß § 64 Abs. 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 BSI 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 Abs. 2 der NIS-2-Richtlinie ist die EU Kommission ebenfalls befugt, delegierte Rechtsakte nach Art. 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 BMI.

Vor Erlass einer solchen Rechtsverordnung ist durch BMI 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 BSI (BISP) umgesetzt wird, soll durch diesen Absatz 7 der bidirektionale Austausch sichergestellt werden.

Zu Absatz 8

Absatz 8 dient der Umsetzung von Artikel 30 der NIS-2-Richtlinie.

Zu Absatz 9

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 Abs. 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 Abs. 1 durch Betreiber kritischer Anlagen geeignet. Sofern das Bundesamt gemäß § 64 Abs. 3 BSIG 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.

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.

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, kann das BSI Einzelheiten des Meldeverfahrens nach Anhörung der betroffenen Betreiber und Wirt-schaftsverbände festlegen. Soweit die Europäische Kommission einen Durchführungs-rechtsakt 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 § 33 (Registrierungspflicht)

§ 32 dient der Umsetzung von Artikel 3 Absatz 3 der NIS-2-Richtlinie. Registrierungspflichten für Einrichtungen der Bundesverwaltung werden in § 43 Absatz 4 abweichend geregelt.

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 3 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

[…]

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 5 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 festlegen kann.

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 BSI 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.

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 Bundesamts beispielsweise zu Auswirkungen des Sicherheitsvorfalls, Auskunft erteilen oder einen Ansprechpartner benennen können.

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 Bundesamts 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 Mitgliedsstaaten 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 Mitgliedsstaatsinteresse 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 die Möglichkeit zur Schaffung von Ausnahmen ergänzend in § 46 Absatz 4 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 (Billigungs-, 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. 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 Vorsehung einer zwingenden Norm ist zwar nicht ausdrücklich in der umzusetzenden Richtlinienbestimmung enthalten. Jedoch wird hiermit der bestehende Umsetzungsspielraum unionsrechtskonform ausgeübt. Denn soweit eine Richtlinie den Mitgliedsstaaten keine zwingenden Vorgaben macht, sondern Spielräume für die Umsetzung lässt, sind diese durch die Mitgliedsstaaten eigenständig so auszufüllen, dass die Ziele der Richtlinie vollständig erreicht werden. Diesen Zielen würde es widersprechen, wenn es sich hier um eine disponible Haftung handeln würde.

Die Binnenhaftung des Geschäftsleitungsorgans bei Verletzung von Pflichten nach dem BSIG ergibt sich aus den allgemeinen Grundsätzen (bspw. § 93 AktG). 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 Geschäftsleiter. Wichtige und besonders wichtige Einrichtungen werden aufgefordert, derartige Schulungen für alle Beschäftigten anzubieten. 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 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 (Zentrale Melde- und Anlaufstelle)

§ 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 Artikel 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 Artikel 8 Absatz 3 bis 5 der NIS-2-Richtlinie.

Zu Absatz 2

Absatz 1 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 1 führt den bisherigen § 8b Absatz 2 Nummer 2 fort.

Zu Nummer 3

Nummer 1 führt den bisherigen § 8b Absatz 2 Nummer 3 fort.

Zu Nummer 4

Zu Buchstabe a

Buchstabe a führt den bisherigen § 8b Absatz 2 Nummer 1 Buchstabe a fort. Die Vorschrift wird an die neuen Kategorien angepasst.

Zu Buchstabe b

Buchstabe b führt den bisherigen § 8b Absatz 2 Nummer 1 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 besonderer außenpolitischer Bedeutung sind, angewiesen. Das Bundesamt ist verpflichtet, das Auswärtige Amt über solche Sicherheitsvorfälle, an deren Informationen das Auswärtige Amt ein berechtigtes Interesse hat, unverzüglich zu unterrichten. Die besondere außenpolitische Bedeutung im Sinne der Vorschrift liegt insbesondere dann vor, wenn (i) der Sicherheitsvorfall informationstechnische Systeme betrifft, die besonders weit verbreitet sind, (ii) die Auswirkungen des erheblichen Sicherheitsvorfalls für die auswärtigen Beziehungen oder die nationale Sicherheit eine unmittelbare Relevanz aufweist, und (iii) die Auswirkungen des Sicherheitsvorfalls absehbar in mehreren Mitgliedstaaten der Europäischen Union oder in Bündnispartnern des Nordatlantikvertrags zu erheblichen Versorgungsengpässen oder Gefährdungen der öffentlichen Sicherheit führen würde.

Zu Nummer 5

Nummer 5 enthält eine Neuregelung. Aufgrund der hohen Sicherheitsrelevanz der Angaben von Betreibern kritischer Anlagen, ist eine restriktivere Behandlung angezeigt. Die bisherigen § 8b Absatz 2 Nummer 1 Buchstaben b und c entfallen.

Zu Absatz 3

Zu Nummer 1

Nummer 1 dient der Umsetzung von Artikel 8 Absatz 3-5 der NIS-2-Richtlinie.

Zu Nummer 2

Nummer 3 dient der Umsetzung von Artikel 23 Absatz 8 der NIS-2-Richtlinie.

Zu Nummer 3

Nummer 4 dient der Umsetzung von Artikel 23 Absatz 6 der NIS-2-Richtlinie.

Zu Absatz 4

Absatz 4 führt den bisherigen § 8b Absatz 4a fort.

Zu Absatz 5

Absatz 5 führt den bisherigen § 8b Absatz 5 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 1 der vom BSI 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, sowie die BSI-Mindeststandards. 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. Die Vorgabe, angemessene finanzielle und personelle Mittel zur Verfügung zu stellen, erlaubt abstrakt-generell 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. Wenngleich die tatsächliche Angemessenheit des Mitteleinsatzes (d.h. die Ausgaben für die Informationssicherheit) je nach den konkreten Umständen zu beurteilen ist, gilt die Vermutung, dass – als grober Richtwert – der finanzielle Mitteleinsatz als angemessen bewertet werden kann, wenn er mindestens 20 Prozent der Ausgaben des IT-Betriebs innerhalb der Einrichtung beträgt. Die Verwendungs-Berichtspflicht als regelmäßige Rechtfertigungspflicht soll als Mittel der Compliance-Förderung die tatsächliche Umsetzung sicherstellen.

Zu Absatz 2

Absatz 2 dient der Umsetzung Artikel 20 Absatz 2 der NIS-2-Richtlinie. Ein weiterer Bestandteil dieses Absatzes der NIS2-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 1 mit Bezug zum IT-Grundschutz berücksichtigt. Angebote des zentralen Fortbildungsdienstleisters der Bundesverwaltung, der Bundesakademie für öffentliche Verwaltung im Bundesministerium 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 2 ist eine Generalklausel zum Zweck der Verantwortungszuweisung an Einrichtungsleitungen im Falle der Beauftragung privater Dienstleister, wie sie bisher bereits nach Kapitel 7 des Umsetzungsplans Bund gilt. Er regelt die Notwendigkeit, dass 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, AG). Die Verpflichtung hat im notwendigen und angemessenen Umfang abhängig vom konkreten Auftragsgegenstand bzw. der beauftragten Leistung zu erfolgen. Die Verpflichtung umfasst i.d.R. die Umsetzung des IT-Grundschutzes und relevanter Mindeststandards. Es sind außerdem notwendige Einsichts-/Kontrollrechte und die Zusammenarbeit mit dem AG oder BSI 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 BSI, die die beauftragende Einrichtung treffen, vertraglich entsprechend auf die Dienstleister zu erstrecken.

Zu Absatz 4

Satz 1 stellt klar, dass die Registrierungspflicht aus § 32 gemäß § 29 auch Einrichtungen der Bundesverwaltung trifft. Die in Satz 2 vorgesehene Abweichung von § 34 sieht vor, dass Nachweise nicht nur „auf geeignete Weise“ zu erbringen sind, sondern Einrichtungen der Bundesverwaltung hierzu „nach Vorgaben des BSI“ 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 BSI 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 BSI 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. 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 5 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

Absatz 1 knüpft an den bisherigen § 8 Absatz 1 an und verankert neben den dort bereits geregelten Mindeststandards gleichrangig für die in § 29 etablierte Kategorie der Einrichtungen der Bundesverwaltung auch den IT-Grundschutz, der bereits bisher durch Kabinettsbeschluss zum Umsetzungsplan Bund verpflichtend umzusetzen ist. Damit erhalten beide für das Informationssicherheitsmanagement des Bundes maßgeblichen Regelwerke gemeinsam an zentraler Stelle dasselbe Niveau an Verbindlichkeit. Die Formulierung zielt darauf ab klarzustellen, dass die Vorgaben, die das Bundesamt mit dem IT-Grundschutz und mit den Mindeststandards für die Einrichtungen der Bundesverwaltung festlegt, materiell die Vorgaben von § 30 konkretisieren: 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 BSI 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. Die im bisherigen § 8 Absatz 1 Satz 3 vorgesehene Möglichkeit zur Abweichung wird abgelöst durch die Kompetenz der Ressort-ISBs, Ausnahmebescheide gemäß § 46 Absatz 4 zu erlassen. Die vom bisherigen § 8 Absatz 1 Satz 5 vorgesehene Sonderregelung für die Streitkräfte und den Militärischen Abschirmdienst ist nun-

mehr in § 29 Absatz 3 enthalten. Die Beratung des Bundesamtes wird ergänzt um die Erstellung von Handreichungen 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 2

Absatz 2 führt den bisherigen § 8 Absatz 2 fort, ergänzt um die Bereitstellung von Referenzarchitekturen.

Zu Absatz 3

Absatz 3 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 BSI zur Bereitstellung von IT-Sicherheitsprodukten verbleibt mit § 19 in Teil 2. Die Zuständigkeit für die Nutzungsvorgaben wird aus sachlichen Gründen auf CISO Bund im Einvernehmen mit den 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 BSI 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 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. Personal- und Sachausstattung richten sich nach dem Gesamterfüllungsaufwand in der jeweiligen Einrichtung sowie nach dem Schadenspotenzial von Sicherheitsvorfällen oder Störungen. Angemessene finanzielle Mittel sind in der Regel etwa 20 % der entsprechenden Ausgaben für den IT-Betrieb (vgl. Erläuterungen zu § 43 Absatz 1); im Einzelfall bei z.B. IT-Dienstleistern kann diese Quote höher ausfallen. Fachkunde ist nicht Voraus-

setzung für die Übertragung der Tätigkeit, muss jedoch wenigstens tätigkeitsbegleitend erworben werden. Dadurch wird einerseits die Besetzung entsprechender Funktionen 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 Informationssicherheitskonzepten 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.

Zu Absatz 4

Absatz 4 räumt den Einrichtungs-ISBs Beteiligungs- und Vortragsrechte ein. 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, informell auch „Ressort-CISOs“ genannt), wie sie schon bisher im Rahmen des Umsetzungsplans Bund angelegt sind, eine gesetzliche Grundlage. Zur Umsetzung von Art. 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) Fachkunde besitzen müssen, es sich also nicht um politische Funktionen handelt, sondern der Fokus bei der Aufgabenausübung auf der fachlichen Expertise liegt und b) ein eigenes Budgetrecht besitzen, um handlungsfähig zu sein, und c) 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, und die teilweise auch einen Geschäftsbereich mit nachgeordneten Behörden haben, ist auch für „ressort-unabhängige“ oberste Bundesbehörden die Rolle eines Ressort-ISB einzurichten. In obersten Bundesbehörden ohne Geschäftsbereich bzw. nachgeordnete Behörden werden die Rollen des Einrichtungs-ISB und des Ressort-ISB in Personalunion wahrgenommen. Weitere Regelungen in diesem Paragraphen, die für das jeweilige Ressort des oder der Informationssicherheitsbeauftragten getroffen werden, sind entsprechend auf die oberste Bundesbehörde und falls vorhanden ihren Geschäftsbereich anzuwenden.

Zu Absatz 1

Absatz 1 regelt Bestellung und Zuständigkeit von Ressort-ISBs. Sie tragen die Verantwortung 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. Damit Ressort-ISBs die für die Erfüllung ihrer Aufgaben notwendige organisatorische Unabhängigkeit besitzen, benötigen sie angemessene Ausstattung und Mittel, die nicht auf organisatorischer Ebene anderen Zwecken zufließen können dürfen. Fachkunde ist erforderlich, da die Ressort-ISBs die Fachaufsicht über die ISBs der Einrichtungen in ihrem Zuständigkeitsbereich führen können müssen.

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 unterstehen, sind die Ressort-ISBs insoweit weisungsbefugt. Die Berichtspflicht dient als Mittel der Compliance-Förderung. 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 4

Absatz 4 regelt die Möglichkeit für Ressort-ISBs, Ausnahmebescheide für Einrichtungen innerhalb ihres Zuständigkeitsbereichs zu erlassen. Besonders wichtige und wichtige Einrichtungen können hiervon nicht umfasst werden, für diese wären Ausnahmebescheide nach § 37 zu erlassen. Mit einem Ausnahmebescheid kann ein Ressort-ISB beispielsweise wie bisher nach dem Umsetzungsplan Bund für sehr kleine Einrichtungen zulassen, dass dort kein eigener ISB bestellt werden muss, wenn ein anderer ISB des Geschäftsbereichs die Rolle für diese Einrichtung wahrnimmt. Sachliche Gründe zur Erteilung eines Ausnahmebescheids können sich insbesondere auch aus Geheimschutzinteressen ergeben.

Zu Absatz 5

Absatz 5 räumt den Ressort-ISBs Beteiligungs- und Vortragsrechte ein. 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 solcher Vorhaben und Strukturen ist fachlich erforderlich, dass Informationssicherheit dort durch eigene ISBs umgesetzt wird. Bei ressortübergreifenden Digitalisierungsvorhaben ist grundsätzlich von einer wesentlichen Bedeutung für allgemeine Sicherheitsbelange auszugehen, und die ressortübergreifenden Kommunikationsinfrastrukturen haben für die Regierungskommunikation insgesamt eine herausgehobene Bedeutung. Die Entscheidungskompetenz des CISO Bund in Zweifelsfällen, wenn eine Einigung 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 2

Absatz 2 führt den bisherigen § 8 Absatz 4 fort. Die Ergänzung erfolgt, um auch hier angemessene Mittel sicherzustellen. Der Koordinator oder die Koordinatorin für Informationssicherheit ist gemäß § 50 Absatz 1 zuständigkeitshalber ebenfalls zu beteiligen.

Zu § 48 (Amt des Koordinators für Informationssicherheit)

Die neue Vorschrift schafft die Funktion eines Koordinators oder einer Koordinatorin der Bundesregierung für Informationssicherheit (CISO Bund). Die zugehörigen Aufgaben und Befugnisse werden in den folgenden Paragraphen geregelt.

Zu Absatz 1

Absatz 1 regelt die Bestellung des CISO Bund. Die konkrete organisatorische Anbindung bleibt dem umsetzenden Kabinettbeschlusses vorbehalten. Um Interessenskonflikte zu vermeiden, sollte die Funktion möglichst unabhängig organisiert werden.

Zu Absatz 2

Absatz 2 stellt klar, dass auch der CISO Bund die mit dieser Funktion verbundenen Aufgaben und Befugnisse nur ausüben kann, wenn hierfür angemessene Mittel zur Verfügung gestellt werden.

Zu § 49 (Aufgaben des Koordinators)

§ 49 regelt die allgemeinen Aufgaben des CISO Bund.

Zu § 50 (Befugnisse des Koordinators)

Zu Absatz 1

Absatz 1 sieht Beteiligungsrechte für den CISO Bund zur effektiven Wahrnehmung der Aufgaben vor.

Zu Absatz 2

Absatz 2 räumt dem CISO Bund Vortragsrechte zur effektiven Wahrnehmung der Aufgaben ein.

Zu Absatz 3

Absatz 3 dient der Umsetzung von Artikel 32 Absatz 4 Buchstabe d) der NIS-2-Richtlinie im Hinblick auf Einrichtungen der Zentralregierung sowie im Sinne eines kohärenten Regelungsregimes zu einer entsprechenden Anwendung auf Einrichtungen der Bundesverwaltung insgesamt im Einklang mit § 29. Aus Rücksicht auf das Ressortprinzip bedarf es des Benehmens mit dem oder der jeweiligen Ressort-ISB. Die Möglichkeit, die Vorlage von Sofortprogrammen anzuweisen, bildet ein wirksames Element für effektive Nachsteuerung, wenn Anlass dafür gegeben ist. Anlässe können etwa sein, wenn im Rahmen einer Überprüfung nach § 7 z. B. eine erhebliche Unterschreitung der Anforderungen an das Informationssicherheitsmanagement deutlich wird.

Zu Teil 4 (Datenbanken der Domain-Name-Registrierungsdaten)

Teil 4 dient der Umsetzung von Artikel 28 der NIS-2-Richtlinie.

Zu § 51 (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 1 dient der Umsetzung von Artikel 28 Absatz 2 Buchstabe b der NIS-2-Richtlinie.

Zu Nummer 3

Nummer 1 dient der Umsetzung von Artikel 28 Absatz 2 Buchstabe c der NIS-2-Richtlinie.

Zu Nummer 4

Nummer 1 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 § 52 (Verpflichtung zur Zugangsgewährung)

§ 52 dient der Umsetzung von Artikel 28 Absatz 5 der NIS-2-Richtlinie.

Zu § 53 (Kooperationspflicht)

§ 53 dient der Umsetzung von Artikel 28 Absatz 6 der NIS-2-Richtlinie.

Zu Teil 5 (Zertifizierung und Kennzeichen)

Zu § 54 (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 IT-Sicherheitsbeauftragten 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 5 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 § 55 (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 § 56 (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 § 57 Absatz 3 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 § 57 (Ermächtigung zum Erlass von Rechtsverordnungen)

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 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.

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 Infrastruk-

turen 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 § 58 (Einschränkung von Grundrechten)

§ 58 führt den bisherigen § 11 fort.

Zu § 59 (Berichtspflichten des Bundesamtes)

In der Überschrift von § 59 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

Zu Nummer 1

Nummer 1 führt den bisherigen § 13 Absatz 4 Nummer 1 fort.

Zu Nummer 2

Nummer 2 führt den bisherigen § 13 Absatz 4 Nummer 2 fort.

Zu Nummer 3

Nummer 3 führt den bisherigen § 13 Absatz 4 Nummer 3 fort.

Zu Absatz 5

Absatz 5 führt den bisherigen § 13 Absatz 5 fort.

Zu Absatz 6

Absatz 6 führt den bisherigen § 13 Absatz 6 fort. Gemäß Artikel 44 der NIS-2-Richtlinie tritt die Richtlinie (EU) 2016/1148 am 18. Oktober 2024 außer Kraft, damit entfällt die Übermittlungspflicht nach deren Artikel 11 wodurch die Daten für das Kalenderjahr 2023 nach dieser Vorschrift die letztmalige Übermittlung darstellen.

Zu Absatz 7

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. Als Übergangsregelung sind Daten für das gesamte Kalenderjahr 2024 Teil der erstmaligen Übermittlung im von der NIS-2-Richtlinie vorgegebenen Dreimonatszeitraum.

Zu Absatz 8

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 (Sanktionsvorschriften und Aufsicht)

Zu § 60 (Bußgeldvorschriften)

§ 60 führt den bisherigen § 14 fort. Im Katalog der Bußgeldvorschriften wurden die Verweise angepasst, Bußgeldtatbestände entsprechend der Anforderungen durch die NIS2-Richtlinie ergänzt sowie der Bußgeldrahmen angepasst.

Zu Absatz 1

§ 60 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.

In § 60 Absatz 1 führt den bisherigen § 14 Absatz 1 fort.

Der Verweis auf § 10 Absatz 1 Satz 1, nunmehr § 57 Absatz 4 Satz 1 wurde ebenfalls angepasst.

Zu Absatz 2

Mit § 60 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

In Nummer 1 Buchstabe a) wurden die Verweise angepasst und inhaltlich keine Änderungen vorgenommen.

§ 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 6 den bisherigen § 8a Absatz 3 Satz 5 fort.

Zu Buchstabe b

In Buchstabe b wurde einerseits der Verweis angepasst: § 14 Absatz 2 Satz führt den bisherigen § 7a Absatz 2 Satz 1 fort.

Zum anderen wurden zwei neue Varianten ergänzt:

§ 64 Absatz 8 Satz 1 und 2 oder Absatz 9 Satz 1 oder auch in Verbindung mit § 65 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. Ebenso wird eine Bußgeldbewehrung bei einem Verstoß gegen § 64 Absatz 5, der vorsieht, dass das Bundesamt für besonders wichtige Einrichtungen einen Überwachungsbeauftragten benennen kann, der die Einhaltung der Verpflichtungen aus §§ 30, 31 und 39 überwacht, geschaffen. Mit der Schaffung dieses Bußgeldtatbestandes wird den Anforderungen aus Artikel 32 Absatz 4 Buchstabe i in Verbindung mit Buchstabe g der NIS-2-Richtlinie nachgekommen.

Artikel 34 Absatz 4 der NIS2 Richtlinie sieht vor, dass Geldbußen zusätzlich zu jeglichen der Maßnahmen nach Artikel 32 Absatz 2 Buchstaben a bis h, Artikel 32 Absatz 5 und Artikel 33 Absatz 4 Buchstaben a bis g verhängt werden. Artikel 32 Absatz 4 Buchstabe g sieht dabei eine Bebußung Zuwiderhandlung gegen einen für einen bestimmten Zeitraum einen mit genau festgelegten Aufgaben betrauten Überwachungsbeauftragten vor. Artikel 32 Absatz 4 Buchstabe h sieht eine Bebußung bei Zuwiderhandlung gegen Anweisungen, Aspekte der Verstöße gegen diese Richtlinie entsprechend bestimmten Vorgaben öffentlich bekannt zu machen, vor.

Zu Buchstabe c

§ 18 führt den bisherigen § 8b Absatz 6 Satz 1 fort. Satz 2 entfällt aufgrund obiger Anpassungen. § 8c Absatz 4 Satz 1 entfällt, da die Kategorie „Anbieter digitaler Dienste“ in den neuen Einrichtungskategorien aufgeht.

Ferner wurde eine neue Variante ergänzt: §§ 64 Absatz 6 Satz 1 und 2 in Verbindung mit § 65 sieht eine Bebußung bei Verstößen besonders wichtiger und wichtiger Einrichtungen gegen Anordnungen nach § 64 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 wird hiermit den Anforderungen aus Artikel 32 Absatz 4 Buchstabe h nachgekommen. Demnach ist eine Bebußung bei Zuwiderhandlung nach Artikel 32 Absatz 4 Buchstabe b vorzunehmen. Zu Buchstabe d

Es wird mit Buchstabe d ein neuer Bußgeldtatbestand geschaffen, der die Weigerung der Herausgabe notwendiger Informationen zur Bewältigung einer Störung bei Betreibern kritischer Anlagen ahnden soll (siehe § 40 Absatz 4 Satz 1).

Zu Nummer 2

In Nummer 2 wurden die Verweise angepasst. Der vormalige 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 den neugeschaffenen § 30 (Risikomanagementmaßnahmen), der § 8a Absatz 1 Satz 1 entspricht. Zudem wird hiermit den Anforderungen der NIS2 Richtlinie (Artikel 21 NIS2-Richtlinie) nach einer Bebußung bei Verstößen gegen Risikomanagementmaßnahmen nachgekommen.

Zu Nummer 3

§ 32 Absatz 1 BSIG nF definiert die Meldepflichten für besonders wichtige und wichtige Einrichtungen (Umsetzung des Artikels 23 der NIS-2-Richtlinie).

§ 8c und 8f entfallen, da die Regelungsadressaten in den neuen Einrichtungskategorien aufgehen.

Zu Nummer 4

Nach Nummer 4 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, 3 ersetzt und auf die neugeschaffenen Einrichtungskategorien angepasst: § 33 Absatz 1 definiert die Registrierungspflichten für wichtige und besonders wichtige Einrichtungen, Absatz 3 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, 2, der Registrierungspflichten für andere Einrichtungsarten vorsieht.

Zu Nummer 5

Nummer 5 sieht eine Bebußung für Betreiber kritischer Anlagen vor. Diese haben nach § 32 Absatz 2 Satz 2 sicherzustellen, dass sie über ihre in Absatz 1 genannten Kontaktdaten jederzeit erreichbar sind.

Zu Nummer 6

In Nummer 6 wurde ein neuer Bußgeldtatbestand geschaffen. § 34 Absatz 2 sieht vor, dass Änderungen der nach § 33 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 7

Hier wurde der Verweis zur Aktualisierung der Nachweispflichten (siehe bereits unter Absatz 1) angepasst und eine Aktualisierung der Nachweispflichten entsprechend der neuen Einrichtungskategorien vorgenommen: Hier bestimmt § 39 Absatz 2 Satz 1 die für kritische Einrichtungen.

Ebenfalls wurde entsprechend Anforderungen der NIS2-Richtlinie nach Artikel 32 Absatz 4 Buchstabe d für besonders wichtige sowie Artikel 33 Absatz 4 Buchstabe d für wichtige Einrichtungen 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.

Zu Nummer 8

Mit der Nummer 8 wird die in Artikel 36 der NIS2-Richtline vorgesehene Möglichkeit, 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. Ebenso erfasst wird das vorgeschriebene Vorhalten eines öffentlichen Zugangs zu den nicht personenbezogenen Domain-Namen-Registrierungsdaten sowie zu den Vorgaben und Verfahren für die Aufrechterhaltung der vollständigen Datenbank oder der Offenlegung bestimmter weiterer Registrierungsdaten.

Zu Nummer 9

Mit Nummer 9 wurde ein neuer Bußgeldtatbestand geschaffen: § 54 Absatz 2 bestimmt, dass für bestimmte Produkte oder Leistungen beim Bundesamt eine Sicherheits- oder Personenzertifizierung beantragt werden kann. Eine Ahndung im Rahmen eines Bußgeldes bei Vorgabe über die Inhabereigenschaft einer solchen Zertifizierung ist aufgrund des Missbrauchspotentials sowie damit einhergehender unbefugter Nutzung erforderlich; auch da hier keine effektive Verwaltungszwangsmöglichkeit besteht.

Zu Nummer 10

§ 55 Absatz 2 Satz 2 führt den bisherigen § 9a Absatz 2 Satz 2 fort.

Zu Nummer 11

§ 56 Absatz 4 Satz 1 führt den bisherigen § 9c Absatz 4 Satz 1 fort.

Zu Nummer 12

Der vormalige § 14 Absatz 2 Nummer 8 mit einer Bußgeldahndung für Verstöße gegen § 8c Absatz 1 Satz 1 wird gestrichen, da dieser in den neuen Einrichtungskategorien aufgeht.

Die neue Nummer 12 sieht eine Bebußung bei besonders wichtigen Einrichtungen wie folgt vor: 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 (§ 64 Absatz 5 Satz 3).

Zu Nummer 13

In Nummer 13 wurde ein neuer Bußgeldtatbestand geschaffen, der ein Zuwiderhandeln gegen eine verbindliche Anweisung nach § 64 Absatz 7 Satz 2 oder § 65 ahnden sollen. § 64 Absatz 7 und § 65 bestimmen, dass das Bundesamt gegenüber besonders wichtigen, respektive wichtigen Einrichtungen verbindliche Anweisungen zur Umsetzung der Verpflichtungen nach diesem Gesetz erlassen kann. Mit der Schaffung dieses Bußgeldtatbestandes werden Artikel 32, 33 Absatz 4 Buchstaben f, i der NIS 2 Richtlinie umgesetzt, die eine respektive Bebußung von wichtigen und besonders wichtigen Einrichtungen vorsehen, wenn diese sie sich einer verbindlichen Anweisung die im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen innerhalb einer angemessenen Frist umzusetzen, widersetzen.

Zu Absatz 3

Redaktionelle Änderung von „Sicherheitslücke“ auf „Schwachstelle“.

Zu Absatz 4

§ 60 Absatz 4 Nummer 1 und 2 führt den bisherigen § 14 Absatz 4 Nummer 1 und 2 fort. Zu Nummer 1

Redaktionelle Änderung von „Sicherheitslücke“ auf „Schwachstelle“.

Zu Nummer 2

Redaktionelle Änderung von „Sicherheitslücke“ auf „Schwachstelle“.

Zu Nummer 3

In Absatz 4 wurde ein neuer Bußgeldtatbestand in der Nummer 3 geschaffen, der das Vorgeben der Inhaberschaft eines europäischen Cybersicherheitszertifikats oder Aussteller einer EU-Konformitätserklärung zu sein, obgleich diese nicht besteht, widerrufen oder für ungültig erklärt wurde, ahndet. Eine Notwendigkeit für die Ahndung ergibt sich anliegend an den Nummer 9 aus dem Missbrauchspotential, Folgen einer unbefugten Nutzung und der fehlenden effektiven Verwaltungszwangsmöglichkeit.

Zu Absatz 5

§ 60 Absatz 5 regelt die Höhe der jeweiligen Bußgelder in einem allgemeinem Bußgeldtatbestand. Das Stufensystem wurde beibehalten, wobei die Stufen vorliegend angepasst wurden. Die Stufen sind auf den Werten 20 Millionen Euro (höchste Stufe), 500.000 Euro (zweite Stufe) und 100.000 Euro (dritte Stufe) angesetzt.

Die höchste Stufe wird auf 20 Millionen Euro angesetzt. Für die Stufe von 20 Millionen Euro bei einem Verstoß gegen Absatz 2 Nummer 1 Buchstabe a wurde keine Veränderung der Bußgeldhöhe vorgenommen, da durch den Verweis auf § 30 Absatz 2 Satz 3 OWiG in § 14 Absatz 5 alte Fassung eine Anhebung der Bußgeldhöhe ebenfalls erfolgte.

Für die zweithöchste Stufe wurde ein Wert von 500.000 Euro angesetzt. Für einen Verstoß gegen Absatz 2 Nummer 1 Buchstabe c Variante 1 ergab sich hierbei keine Veränderung . Ein Verstoß gegen Absatz 2 Nummer 1 Buchstabe c Variante 2 und 3 wurde auf dieser Höhe vorgesehen, da die Abstellung *bestehender, bekannterweise offener Lücken*, für Übergriffe genutzt werden können und hiermit in seiner Bedeutung signifikant ist. Auf der zweithöchsten Stufe wurde ebenfalls ein Verstoß gegen Absatz 2 Nummer 4 und 6 aufgenommen. Bei diesem handelt es sich um einen Verstoß gegen die Registrierungspflichten für Einrichtungsarten nach § 32 Absatz 1 s.Domain-Name Registry Diensteanbieter oder Anbieter nach §§ 33 Absatz 1, 64 Absatz 1).

Ein Verstoß gegen Absatz 2 Nummer 7 Variante 2 und 3 wurde ebenfalls auf dieser Stufe angesiedelt wegen der Nähe zu den Risikomanagementmaßnahmen, die auf höchster Stufe bebußt sind.

Ein Verstoß gegen Absatz 2 Nummer 8 für Nichtbefolgung der Vorgaben für Maßnahmen auch für Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister fällt ebenfalls unter diese Einstufung. Für einen Verstoß gegen Absatz 2 Nummer 10 und 11 ergaben sich keine Veränderungen in der Bußgeldhöhe.

Auf der zweithöchsten Stufe wurden zudem Verstöße gegen den neueingeführten Absatz 2 Nummer 9 aufgenommen. Bei diesem handelt es sich um Vorgabe der Inhaberschaft einer Zertifizierung nach § 54 Absatz 2. Bei der Einstufung wurde sich an der Bußgeldhöhe von Nummern 10 und 11, die in der vormaligen und jetzigen Fassung ebenfalls in dieser Höhe angesiedelt sind und im Unrechtsgehalt eine Entsprechung finden, orientiert.

Ebenfalls auf dieser Stufe sind Verstöße gegen Absatz 4 angesiedelt. Für die Nummern 1 und 2 ergaben sich keine Veränderungen. Neu wurde auf dieser Stufe die Nummer 3 aufgrund einer Vergleichbarkeit zu den Bußgeldtatbeständen aus Absatz 2 Nummern 10 und 11 aufgenommen.

Als niedrigste Stufe wurde die frühere 100.000 Euro Stufe übernommen. Hierbei ergaben sich für einen Verstöße gegen Absatz 2 Nummer 1 Buchstabe b Variante 1 und Absatz 3 keine Veränderungen. Ebenfalls auf dieser Stufe wurden Verstöße gegen Absatz 2 Nummer 1 Buchstabe b Varianten 2, 3 und 4 und gegen Nummer 13 aufgenommen. Die neu geschaffenen Nummer 13 wurde auf dieser untersten Stufe angesetzt, da im Falle von Nummer 13 erstmals eine Bebußung von Verstößen gegen Anordnungen zur Umsetzung von im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen innerhalb einer bestimmten Frist vorgesehen wird.

Zu Absatz 6

Mit § 60 Absatz 6 wurde ein Bußgeldtatbestand für die Einrichtungskategorie der wichtigen Einrichtungen geschaffen. Eine Separierung erfolgte zur besseren Übersichtlichkeit und angesichts der Änderungen in der Stufung aufgrund der Anforderungen der NIS 2 Richtlinie. Die Stufen stellen sich wie folgt dar: Es wird ein Wert von 7 Millionen Euro oder 1,4 Prozent des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens angesetzt.

Dies bestimmt Artikel 34 Absatz 4 der NIS 2 Richtlinie, der eine derartige Bußgeldhöhe bei Verstößen gegen Risikomanagementmaßnahmen und Meldepflichten (hier den Absätzen 2 Nummern 2 und 3) vorsieht.

.

Zu Absatz 7

Mit § 60 Absatz 7 wurde ein separater Bußgeldtatbestand für die Kategorie des Betreibers kritischer Anlagen und besonders wichtige Einrichtungen geschaffen. Erwägungen waren auch hier eine Übersichtlichkeit angesichts der unterschiedlichen Bußgeldhöhen zu schaffen und den Anforderungen nach der Verhängung eines von an den Einrichtungskategorien angelehnten abgestuften Systems gerecht zu werden.

Eine Unterscheidung zwischen den beiden Kategorien der besonders wichtigen Einrichtung und dem Betreiber kritischer Anlagen, in der Bußgeldhöhe wurde hier nicht vorgenommen wegen marginaler Differenzen im Pflichtenkatalog. Eine entsprechende Differenzierung der Bußgeldhöhe entsprechend des Verhältnismäßigkeitsgrundsatzes kann nach Schwere des Verstoßes und Einrichtungsart durch das Bundesamt vorgenommen werden. So ist bei Betreibern kritischer Anlagen der Bußgeldrahmen am oberen Rande auszuschöpfen.

Höchste Stufe ist hier die Stufe von 10 Millionen Euro oder mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört. Auf dieser Stufe werden Verstöße gegen Absatz 2 Nummern 2 und 3 geahndet.

Ein Verstoß gegen Absatz 2 Nummer 2 wurde auf dieser höchsten Stufe angesetzt. Dieser sieht die Ahndung von Verstößen gegen Risikomanagementmaßnahmen iSd § 30 Absatz 1 vor. Hier traf Artikel 34 Absatz 4 NIS2 Richtlinie dezidierte Vorgaben (10 Millionen Euro oder mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört) die übernommen wurden. Gleiches gilt für Nummer 3.

Auf einer separaten Unterstufe in Höhe von 10 Millionen Euro, ohne prozentuale Alternative, werden zwei Verstöße geahndet.

Bei einem Verstoß gegen Absatz 1 tritt keine Veränderung der Bußgeldhöhe ein, da der frühere Verweis auf § 30 Absatz 2 Satz 3 OWiG zu einer Verzehnfachung führte, die hier ebenfalls erreicht wird.

Ein Verstoß gegen Absatz 2 Nummer 7 Variante 1 (Nachweispflichten) ist auf der höchsten Stufe bei Betreibern kritischer Anlagen angesiedelt. Die Bußgeldhöhe wurde entsprechend Absatz 1 angepasst (vormals ebenso hoch durch den Verweis des § 30 Absatz 2 Satz 3 OWiG).

Zweithöchste Stufe ist die Stufe von 500.000 Euro

Die neu geschaffene Nummer 12 wurde auf der zweiten Stufe angesetzt für Verstöße wenn bei besonders wichtigen Einrichtungen 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

Unterste Stufe ist die Stufe von 100.000 Euro. Ein Verstoß gegen Absatz 2 Nummer 1 Buchstabe d, der die Herausgabe von notwendigen Informationen zur Bewältigung der Störung betrifft, wurde auf dieser Stufe angesiedelt, um die Dringlichkeit der Herausgabe derartiger Informationen zu verdeutlichen. Bei einem Verstoß gegen Absatz 2 Nummer 5 wurde die bisherige Bußgeldhöhe übernommen..

Zu Absatz 8

§ 60 Absatz 8 führt den bisherigen § 14 Absatz 6 fort.

Zu Absatz 9

Absatz 9 dient der Umsetzung von Artikel 35 Absatz 2 NIS-2-Richtlinie.

Zu § 61 (Zuwiderhandlungen durch Institutionen der sozialen Sicherung)

§ 61 führt den bisherigen § 14a fort.

Zu § 62 (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 § 63 (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 2 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 § 64 (Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen)

Zu Absatz 1

§ 64 dient der Umsetzung von Artikel 32 der NIS-2-Richtlinie. Da eine regelmäßige Nachweispflicht für die Umsetzung von Risikomanagementmaßnahmen ausschließlich für Betreiber kritischer Anlagen gilt, ist in § 64 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.

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 Bundesamts 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 4 Buchstabe g der NIS-2-Richtlinie.

Zu Absatz 10

Zu Nummer 1

Nummer 1 dient der Umsetzung von Artikel 32 Absatz 5 Unterabsatz 1 Buchstabe a der NIS-2-Richtlinie.

Zu Nummer 2

Nummer 2 dient der Umsetzung von Artikel 32 Absatz 5 Unterabsatz 1 Buchstabe b der NIS-2-Richtlinie.

Zu Absatz 11

Absatz 11 dient der Umsetzung von Artikel 32 Absatz 9 der NIS-2-Richtlinie.

Zu Absatz 12

Absatz 12 dient der Umsetzung von Artikel 35 der NIS-2-Richtlinie.

Zu Absatz 13

Absatz 13 regelt in Umsetzung von Artikel 37 der NIS-2-Richtlinie Einzelheiten zur Amtshilfe für zuständige Aufsichtsbehörden in anderen Mitgliedsstaaten der Europäischen Union, wenn Einrichtungen Dienstleistungen in mehreren Mitgliedsstaaten erbringen, und hierfür beispielsweise IT-Systeme, Komponenten oder Prozesse eingesetzt werden, die sich in Deutschland befinden.

Zu § 65 (Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen)

§ 65 dient der Umsetzung von Artikel 33 der NIS-2-Richtlinie. Für wichtige Einrichtungen sind gemäß dieser Vorschrift grundsätzlich die gleichen Aufsichtsmaßnahmen des Bundesamts vorgesehen, wie in § 64 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 Anforderungen aus den §§ 30, 31 oder 32 nicht oder nicht richtig umgesetzt hat.

Zu § 66 (Verwaltungszwang)

Mit § 66 wird Artikel 34 Absatz 6 NIS 2 umgesetzt.

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: Die NIS-2-Richtlinie stellt für die einzubeziehenden Einrichtungskategorien in Anhang 1 Nr. 5 auf Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie (EU) 2011/24 des Europäischen Parlaments und des Rates ab. Gemäß Artikel 3 Absatz 3 Buchstabe a) der Richtlinie (EU) 2011/24 (Patientenmobilitätsrichtlinie) 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.

Zu Artikel 2 (Änderung des BSI-Gesetzes (FNA 206-2))

Artikel 2 setzt die beabsichtigte Verschiebung der gesetzlichen Bestimmung kritischer Anlagen in das Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz) um. Artikel 2 tritt nach der Regelung in Artikel 29 erst mit dem Inkrafttreten einer Verordnung nach dem KRITIS-Dachgesetz in Kraft. Dabei handelt es sich um eine Nachfolgeverordnung der bisherigen BSI-Kritisverordnung.

Zu Artikel 3 (Änderung des BND-Gesetzes (FNA 12-6))

Es handelt sich um eine Folgeänderung. Der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes wird angepasst.

Zu Artikel 4 (Änderung der Sicherheitsüberprüfungsfeststellungsverordnung (FNA 12-10-3))

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 5 (Änderung des Telekommunikation-Telemedien-Datenschutz-Gesetzes (FNA 204-5))

Es handelt sich um eine Folgeänderung. Der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes wird angepasst.

Zu Artikel 6 (Änderung der Gleichstellungsbeauftragtenwahlverordnung (FNA 205-3-1))

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 (FNA 206-2))

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. Da die NIS-2-Richtlinie bereits einer Evaluierung durch die Europäische Kommission unterliegt (Artikel 40 der NIS-2-Richtlinie) ist eine (auf den Mitgliedstaat Deutschland isolierte) Evaluierung der Umsetzung nicht zielführend.

Zu Artikel 8 (Änderung der BSI-Zertifizierungs- und Anerkennungsverordnung (FNA 206-2-1))

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 9 (Änderung der BSI IT-Sicherheitskennzeichenverordnung (FNA 206-2-3))

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 10 (Änderung des De-Mail-Gesetzes (FNA 206-4))

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 (FNA 206-6))

Löschung des Verweises auf das BSI-Gesetzes wegen Entfernung IT-Rat als Entscheidungsgremium, welches auf untergesetzlicher Ebene eingerichtet wird.

Zu Artikel 12 (Änderung der Passdatenerfassungs- und Übermittlungsverordnung (FNA 210-5-11))

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 13 (Änderung der Personalausweisverordnung (FNA 210-6-1))

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 14 (Änderung der Kassensicherungsverordnung (FNA 610-1-26))

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 15 (Änderung des Atomgesetzes (FNA 751-1))

Es handelt sich um eine Folgeänderung. Der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes wird angepasst.

Zu Artikel 16 (Änderung des Energiewirtschaftsgesetzes (FNA 752-6))

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

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 5

Die Vorschrift zur Meldung von Sicherheitsvorfällen wird unter Berücksichtigung der neuen Mindestvorgaben aus Artikel 23 der NIS-2 Richtlinie neu gefasst.

Zu Artikel 17 (Änderung des Messstellenbetriebsgesetzes (FNA 752-10))

Es handelt sich um eine Folgeänderung. Der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes wird angepasst.

Zu Artikel 18 (Änderung des Energiesicherungsgesetzes (FNA 754-3))

Es handelt sich um Folgeänderungen. Die Begrifflichkeiten und der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 19 (Änderung des Fünften Buches Sozialgesetzbuch (FNA 860-5))

Es handelt sich um Folgeänderungen. Die Verweise auf Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 20 (Änderung der Digitale Gesundheitsanwendungen-Verordnung (FNA 860-5-55))

Es handelt sich um Folgeänderungen. Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 21 (Änderung des Sechsten Buches Sozialgesetzbuch (FNA 860-6))

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 nähere Ausgestaltung der Koordinierungstätigkeiten ergibt sich aus den Buchstaben a bis d. Die Aufzählung ist nicht abschließend, um insbesondere dem stetig voranschreitenden Wandel in der Informationstechnik und ihrer Sicherheit entsprechen zu können.

Die Umsetzung der inhaltlichen und organisatorischen Maßnahmen verbleibt, soweit nicht anders bestimmt, in der Zuständigkeit und Verantwortung der einzelnen Träger der 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 Buchstabe a

Mit dieser Befugnis soll es möglich werden, einheitliche Grundsätze in der Informationstechnik und Informationssicherheit festzulegen, die für alle Träger der Rentenversicherung verbindlich sind. Die Notwendigkeit, auch im Bereich der Informationssicherheit für alle Träger der Rentenversicherung ein einheitliches Sicherheitsniveau sicherzustellen, wird durch die Aufnahme in den Gesetzestext betont. 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.

Der eingeräumten Befugnis entspricht die Verpflichtung, Fortschritte in der Entwicklung der Informationstechnik auf Nutzen und Umsetzbarkeit in der Rentenversicherung zu bewerten und Risiken für die Informationstechnik zu beobachten und zu analysieren.

Mit der Befugnis kann nur der Gestaltungsspielraum der Rentenversicherung ausgefüllt werden, den die bestehenden gesetzlichen Regelungen für die Informationssicherheit wesentlicher Einrichtungen und Einrichtungen der Bundesverwaltung belassen.

Zu Nummer 3 Buchstabe b

Mit dieser Ergänzung erhält die Deutsche Rentenversicherung Bund die gesetzliche Befugnis, einen einheitlichen organisatorischen Rahmen zu schaffen. Mit der Errichtung eines Gemeinsamen Rechenzentrums wurde von den Trägern der Rentenversicherung ein erster

Schritt getan. Die gesamte informationstechnische Infrastruktur der gesetzlichen Rentenversicherung wird künftig bei der Deutschen Rentenversicherung Bund liegen.

Zu Nummer 3 Buchstabe c

Die Träger der gesetzlichen Rentenversicherung greifen zur Erfüllung ihrer Aufgaben auf von ihnen entwickelte Softwareanwendungen zurück. Deren Entwicklung erfolgt arbeitsteilig 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 Betrieb und Nutzung der Anwendungen verbleibt bei den einzelnen Trägern.

Zu Nummer 3 Buchstabe d

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 Artikel 22 (Änderung der Verordnung zum Barrierefreiheitsstärkungsgesetz (FNA 860-9-4-1))

Es handelt sich um eine Folgeänderung. Der Verweis auf die Vorschrift des bisherigen BSI-Gesetzes wird angepasst.

Zu Artikel 23 (Änderung des Telekommunikationsgesetzes (FNA 900-17))

Es handelt sich um Folgeänderungen. Die Verweise auf Vorschriften und die Begrifflichkeiten des bisherigen BSI-Gesetzes werden angepasst.

Zu Nummer 1

Zu Buchstabe a

Zu Buchstabe b

[…]

Zu Buchstabe c

Zu Nummer 2

Zu Buchstabe a

[…]

Zu Buchstabe b

[…]

Zu Buchstabe c

Zu Buchstabe d

[…]

Zu Buchstabe f

[…]

Zu Nummer 4

Zu Buchstabe a

Zu Buchstabe b

[…]

Zu Artikel 24 (Änderung der Krankenhausstrukturfonds-Verordnung (FNA 2126-9-19))

Es handelt sich um Folgeänderungen. Die Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 25 (Änderung der Mess- und Eichverordnung (FNA 7141-8-1))

Es handelt sich um Folgeänderungen. Die Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 26 (Änderung der Außenwirtschaftsverordnung (FNA 7400-4-1))

Es handelt sich um Folgeänderungen. Die Verweise auf die Vorschriften des bisherigen BSI-Gesetzes werden angepasst.

Zu Artikel 27 (Änderung des Vertrauensdienstegesetzes (FNA 9020-13))

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 28 (Evaluierung)

Artikel 28 sieht eine Evaluierungsklausel vor.

Mit der Evaluierungsklausel soll überprüft werden, ob die Zielsetzung des NIS2UmsuCG in Bezug auf die Bundesverwaltung erreicht wird. Gemäß Artikel 40 der NIS2-Richtlinie nimmt die EU-Kommission eine eigene Evaluierung der Richtlinie vor. Sie legt den ersten Bericht bis zum 17.Oktober 2027 vor. Um eine Doppelevaluierung zu vermeiden, ist vorliegend eine beschränkte Evaluierung hinsichtlich des Teil 2 Kapitel 1, Teil 3 Kapitel 3 sowie Teil 5 des BSI-Gesetzes (Artikel 1) vorgesehen.

Evaluiert werden sollen, die Aufgaben und Befugnisse des BSI, die Informationssicherheit der Einrichtungen der Bundesverwaltung und die Zertifizierung und Kennzeichen.

Zu Artikel 29 (Inkrafttreten, Außerkrafttreten)

Zu Absatz 1

Bei einer Verkündung im März 2024 stehen den Einrichtungen noch sechs Monate für die Umsetzung der in diesem Gesetz enthaltenen Verpflichtungen zur Verfügung. Der hier genannte Zeitpunkt ist der letzte Quartalsbeginn vor Ablauf der Umsetzungsfrist des Artikel 41 NIS-2-Richtlinie am 17. Oktober 2024. Im Übrigen sind die für die Verpflichtungen von wesentlichen und wichtigen Einrichtungen maßgeblichen Inhalte der NIS-2-Richtlinie bereits seit dem Kommissionsentwurf aus Dezember 2020 bekannt.

Zu Absatz 2

Absatz 2 regelt die zeitliche Verknüpfung der Verschiebung bestimmter Regelungen zu kritischen Anlagen in Artikel 2, die künftig in das Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz) verschoben werden sollen. Die überarbeitete Ermächtigung zum Erlass einer Rechtsverordnung nach § 10 Absatz 1b BSI-Gesetz muss bereits zuvor in Kraft treten, damit diese zum Tag des Inkrafttretens des Gesetzes im Übrigen bereits erlassen sein kann.

Zu Absatz 3

Der Artikel 19 der Verordnung (EU) Nr. 910/2014 wird durch Artikel 42 der NIS-2-Richtlinie mit Wirkung für den 17. Oktober 2024 gelöscht, daher tritt dieser Änderungsbefehl verzögert in Kraft.