Diskussionspapier

des Bundesministeriums des Innern und für Heimat

Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland

Inhaltsübersicht

Artikel 1

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

(BSI-Gesetz – BSIG)

Inhaltsübersicht

Teil 3
Sicherheit der Informationstechnik von Einrichtungen

Kapitel 1
Anwendungsbereich

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

Teil 4
Datenbanken der Domain-Name-Registrierungsdaten

Teil 6
Verordnungsermächtigungen, Grundrechtseinschränkungen und Berichtspflichten

Teil 7
Sanktionsvorschriften und Aufsicht

Teil 1

Allgemeine Vorschriften

§ 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 wurde oder auf andere Weise nicht eingetreten ist;

2. „Cloud Computing-Dienst“ ein digitaler Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen 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 im Sinne des 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 ihrer besonderen technischen Merkmale 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. „Geschäftsleiter“ eine natürliche Personen, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer Einrichtung berufen ist; Leiterinnen und Leiter von Einrichtungen der Bundesverwaltung im Sinne des § 29 gelten nicht als Geschäftsleiter.;

12. „IKT-Dienst“ ein IKT-Dienst im Sinne des Artikels 2 Nummer 13 der Verordnung (EU) 2019/881;

13. „IKT-Produkt“ ein IKT-Produkt im Sinne des Artikels 2 Nummer 12 der Verordnung (EU) 2019/881;

14. „IKT-Prozess“ ein IKT-Prozess im Sinne des Artikels 2 Nummer 14 der Verordnung (EU) 2019/881;

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

16. „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;

17. […];

18. „kritische Anlage“ eine Anlage, die von hoher Bedeutung für das Funktionieren des Gemeinwesens ist, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden; welche Anlagen im Einzelnen kritische Anlagen sind, bestimmt sich nach § 28 Absatz 6;

19. […];

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

21. „Managed Service Provider“ oder „MSP“ jemand, der Dienste 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 erbringt;

22. „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;

23. „Online-Marktplatz“ ein Dienst im Sinne des § 312l Absatz 3 BGB;

24. „Online-Suchmaschine“ ein digitaler Dienst im Sinne des Artikels 2 Nummer 5 der Verordnung (EU) 2019/1150;

25. „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;

26. „Protokolldaten“ Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind; Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes können enthalten sein;

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

28. „qualifizierter Vertrauensdienst“ ein qualifizierter Vertrauensdienst im Sinne des Artikels 3 Nummer 17 der Verordnung (EU) Nr. 910/2014;

29. „qualifizierter Vertrauensdiensteanbieter“ ein qualifizierter Vertrauensdiensteanbieter im Sinne des Artikels 3 Nummer 20 der Verordnung (EU) Nr. 910/2014;

30. „Rechenzentrumsdienst“ ein Dienst, mit dem 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 alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden;

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

32. […];

33. „Schwachstelle“ eine Eigenschaft von IKT-Produkten oder IKT-Diensten durch deren Au[snutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden IKT-Produkten oder IKT-Diensten verschaffen oder die Funktion von IKT-Produkten oder IKT-Diensten beeinflussen können;

34. „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 von informationstechnischen Systemen, Komponenten oder Prozessen;

35. „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;

36. „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;

37. „Top Level Domain Name Registry“ eine Einrichtung, welche 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, zuständig ist, unabhängig davon, ob der Betrieb durch die Einrichtung selbst erfolgt oder ausgelagert wird, jedoch mit Ausnahme von Situationen, in denen TLD-Namen von einem Register nur für seine eigenen Zwecke verwendet werden;

38. „Vertrauensdienst“ ein Vertrauensdienst im Sinne des Artikels 3 Nummer 16 der Verordnung (EU) Nr. 910/2014;

39. „Vertrauensdiensteanbieter“ ein Vertrauensdiensteanbieter im Sinne des Artikels 3 Nummer 19 der Verordnung (EU) Nr. 910/2014;

40. „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 10 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

§ 6

Informationsaustausch

(1) Das Bundesamt ermöglicht den Informationsaustausch besonders wichtiger Einrichtungen und wichtiger Einrichtungen, Einrichtungen der Bundesverwaltung sowie deren jeweiligen Lieferanten oder Dienstleistern untereinander zu Cyberbedrohungen, Beinahevorfällen, Schwachstellen, Techniken und Verfahren, Kompromittierungsindikatoren, gegnerische Taktiken, bedrohungsspezifische 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 deren jeweiligen Lieferanten oder Dienstleistern offen. Das Bundesamt kann entsprechende Teilnahmebedingungen erstellen, die die Teilnahme am Informationsaustausch regeln. Das Bundesamt kann weiteren Stellen die Teilnahme ermöglichen.

§ 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 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 weitergegeben worden sind, darf das Bundesamt die Daten abweichend von Satz 2 bis zur Beendigung der Unterstützung dieser Behörden weiterverarbeiten. Eine Nutzung zu anderen Zwecken ist unzulässig. § 8 Absatz 8 ist entsprechend anzuwenden.

(4) Das Bundesamt darf Informationen, von denen es im Rahmen dieser Vorschrift Kenntnis erlangt, nur mit Einwilligung des Ersuchenden weitergeben, es sei denn, die Informationen lassen keine Rückschlüsse auf die Identität des Ersuchenden zu oder die Informationen können entsprechend § 8 Absatz 6 und 7 übermittelt werden. 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 es darum ersucht wurde und es sich um einen herausgehobenen Fall im Sinne des Absatzes 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.

Teil 3

Sicherheit 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;

   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. ein qualifizierter Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter,

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 oder

5. eine Einrichtung, die gemäß Anlage 3 dem Teilsektor Zentralregierung des Sektors öffentliche Verwaltung angehört.

Ausgenommen sind Finanzunternehmen im Sinne des 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.

(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.

Ausgenommen sind besonders wichtige Einrichtungen sowie Finanzunternehmen im Sinne des 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.

(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 seinem Partner oder verbundenen Unternehmen ist.

(4) §§ 30 und 31 gelten nicht für

1. Besonders wichtige Einrichtungen und wichtige Einrichtungen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,

2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetz 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. die Gesellschaft für Telematik nach § 306 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch, Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 311 Absatz 6 und § 325 des Fünften Buches Sozialgesetzbuch zugelassenen Dienste und Betreiber von Diensten, soweit sie die Telematikinfrastruktur für nach § 327 Absatz 2 bis 5 des Fünften Buches Sozialgesetzbuch bestätigte Anwendungen nutzen.

(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 kritische Anlage ist eine Anlage, die den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum sowie Siedlungsabfallentsorgung angehört und die von hoher Bedeutung für das Funktionieren des Gemeinwesens ist, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden; welche Anlagen im Einzelnen kritische Anlagen sind, bestimmt sich nach der Rechtsverordnung nach § 57 Absatz 4.

(7) Eine Anlage ist ab dem durch die Rechtsverordnung nach § 57 Absatz 4 festgelegten Stichtag eine kritische Anlage, wenn sie einer der durch die Rechtsverordnung

festgelegten Anlagenarten zuzuordnen ist und die durch Verordnung festgelegten Schwellenwerte erreicht oder überschreitet.

(8) 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.

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.

(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 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 informationstechnischen Systemen, Komponenten und Prozessen, 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 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 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 der 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 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 diese 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.

Das Bundesamt kann zudem feststellen, ob die branchenspezifischen Sicherheitsstandards zur Gewährleistung der Anforderungen nach § 39 Absatz 1 geeignet sind.

§ 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, 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 übermitteln dem Bundesamt über einen vom Bundesamt im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichteten Meldeweg 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;

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

(3) Betreiber kritischer Anlagen sind zusätzlich verpflichtet, Angaben zur Art der betroffenen Anlage, der kritischen Dienstleistung und 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 festlegen, soweit sie möglichen Durchführungsrechtsakten der Europäischen Kommission nicht widersprechen.

§ 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 die folgenden Angaben zu übermitteln:

1. der Name der Einrichtung, einschließlich der Rechtsform und soweit einschlägig der Handelsregisternummer,

2. die Anschrift und aktuellen Kontaktdaten, einschließlich E-Mail-Adresse, IP-Adressbereiche und Telefonnummern,

3. der relevante in Anlage 1 oder 2 genannte Sektor oder soweit einschlägig Teilsektor,

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

(2) Betreiber kritischer Anlagen übermitteln mit den Angaben nach Absatz 1 die IP-Adressbereiche der von ihnen betriebenen Anlagen sowie die für die von ihnen betriebenen kritischen Anlagen ermittelte Anlagenkategorie und Versorgungskennzahlen gemäß der Rechtsverordnung nach § 54 Absatz 1. Die Betreiber stellen sicher, dass sie über ihre in Absatz 1 genannten Kontaktdaten 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 geänderte Versorgungskennzahlen einmal jährlich, alle anderen Angaben unverzüglich, spätestens jedoch zwei Wochen ab dem Zeitpunkt, zu dem die Einrichtung Kenntnis von der Änderung erhalten hat, dem Bundesamt zu übermitteln.

(6) Das Bundesamt kann die Einzelheiten zur Ausgestaltung des Registrierungsverfahrens festlegen.

§ 34

Besondere Registrierungspflicht für bestimmte Einrichtungsarten

(1) Eine Einrichtung der in § 63 Absatz 1 Satz 1 genannten Einrichtungsart übermittelt bis zum 17. Januar 2025 dem Bundesamt folgende Angaben:

1. Name der Einrichtung;

2. einschlägiger Sektor, Teilsektor und Einrichtungsart wie in Anlage 1 bestimmt;

3. Anschrift der Hauptniederlassung in der Europäischen Union im Sinne des § 60 Absatz 2 und seiner 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, seines nach § 63 Absatz 3 benannten Vertreters;

5. die Mitgliedstaaten der Europäischen Union, in denen die Einrichtung Dienste erbringt, und

6. die 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 diese erheblichen Sicherheitsvorfälle zu unterrichten, die die Erbringung

des jeweiligen Dienstes beeinträchtigen könnten. Die Unterrichtung nach Satz 1 kann, soweit sinnvoll, auch durch eine Veröffentlichung im Internet erfolgen.

(2) Einrichtungen im Sinne des 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 im Sinne des Absatz 1 informieren diese Empfänger auch über die erhebliche Cyberbedrohung selbst. Die Unterrichtungspflicht nach diesem Absatz gilt nur dann, wenn in Abwägung der Interessen der Einrichtung im Sinne des Absatz 1 und derjenigen des Empfängers letztere 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 nach Eingang der Meldung eine erste Rückmeldung zu dem Sicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operative Beratung für die Durchführung möglicher 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. Soweit es sich bei der betreffenden Einrichtung um eine Stelle des Bundes handelt, gilt für die Information der Öffentlichkeit § 4 Absatz 3 entsprechend.

§ 38

Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Geschäftsleiter 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 Geschäftsleiter 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 Cybersicherheit und deren Auswirkungen 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 nach Inkrafttreten dieses Gesetzes 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 Bundesamts.

§ 40

Zentrale Melde- und Anlaufstelle

(1) Das Bundesamt ist die zentrale Meldestelle für besonders wichtige Einrichtungen und wichtige Einrichtungen in Angelegenheiten der Sicherheit in der Informationstechnik und zentrale Anlaufstelle für die Aufsicht in Angelegenheiten der Sicherheit in der Informationstechnik über besonders wichtige Einrichtungen und wichtige Einrichtungen und fungiert dabei als nationale Verbindungsstelle um:

1. die grenzüberschreitende Zusammenarbeit von Behörden der Länder, die diese als zuständige Behörde für die Aufsicht von Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene im Sinne des Artikels 2 Absatz 2 Buchstabe f Nummer ii der NIS-2-Richtlinie bestimmt haben, Bundesnetzagentur und 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 mit in Nummer 1 genannten Behörden der Länder, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bundesnetzagentur und Bundesanstalt für Finanzdienstleistungsaufsicht

zu gewährleisten.

(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe

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, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise,

2. deren potentielle Auswirkungen auf die Verfügbarkeit der kritischen Anlagen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zu analysieren,

3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der kritischen Anlagen oder besonders wichtigen Einrichtungen oder wichtigen Einrichtungen kontinuierlich zu aktualisieren und

4. unverzüglich

   a) die besonders wichtigen Einrichtungen und wichtigen Einrichtungen über sie betreffende Informationen nach den Nummern 1 bis 3 durch Übermittlung an die Kontaktdaten nach § 32 Absatz 1 Nummer 2 sowie

   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

5. soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, im Rahmen vorab 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.

(3) Das Bundesamt hat zur Wahrnehmung seiner Aufgabe als zentrale Anlaufstelle

1. Anfragen von den in Absatz 1 genannten Stellen anzunehmen oder soweit zutreffend an eine oder mehrere in Absatz 1 genannten Stellen weiterzuleiten,

2. Antworten auf die in Absatz 2 Nummer 2 genannten Anfragen zu erstellen und dabei soweit zutreffend die in Absatz 1 genannten Stellen zu beteiligen oder Antworten der in Absatz 1 genannten Stellen an die in Absatz 1 genannten Stellen weiterzuleiten,

3. auf eigenes Betreiben nach § 31 eingegangene Meldungen an zentrale Anlaufstellen der anderen betroffenen Mitgliedstaaten der Europäischen Union weiterzuleiten,

4. gegebenenfalls und insbesondere, wenn der erhebliche Sicherheitsvorfall zwei oder mehr Mitgliedstaaten der Europäischen Union betrifft, die anderen betroffenen Mitgliedstaaten und die ENISA über den erheblichen Sicherheitsvorfall zu unterrichten, wobei diese Informationen umfassen die Art der gemäß § 31 Absatz 2 erhaltenen Informationen und das Bundesamt dabei das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen wahrt.

(4) Während einer erheblichen Störung gemäß § 31 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 einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2 erforderlich ist.

(5) 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.

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 im Sinne des Absatzes 1 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 Datenbanken im Sinne des Absatz 1 genaue und vollständige Angaben enthalten. 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

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

1. auf rechtmäßige und hinreichend begründete Anträge berechtigten Zugangsnachfragern 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.

Diese Vorgaben und Verfahren im Hinblick auf die Offenlegung solcher Daten 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 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 wichtige Einrichtung eingesetzten Produkte, Dienste oder Prozesse gemäß § 30 Absatz 9 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 Gesetzes gelten. Der als bedeutend anzusehende Versorgungsgrad ist anhand branchenspezifischer Schwellenwerte für jede als kritisch anzusehende Dienstleistung zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.

Teil 7

Sanktionsvorschriften und Aufsicht

§ 60

Sanktionsvorschriften

(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 oder Absatz 9 Satz 1 oder § 65

   c) § 18

   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, einen Nachweis nicht oder nicht rechtzeitig erbringt

8. 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,

9. vorgibt, Inhaber einer Zertifizierung nach § 54 Absatz 2 Satz 1 zu sein, ohne dass diese besteht,

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

11. vorgibt, Inhaber eines europäischen Cybersicherheitszertifikats oder Aussteller einer EU-Konformitätserklärung zu sein, obwohl diese nicht besteht, widerrufen oder für ungültig erklärt wurde,

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

13. einer verbindlichen Anweisung nach § 64 Absatz 7 oder § 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.

(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, 9, 10, 11 und 12 mit einer Geldbuße bis zu fünfhunderttausend Euro und in den Fällen des Absatzes 2 Nummer 1 Buchstabe b 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 der Absatz 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, in den Fällen des Absatzes 2 Nummer 1 Buchstabe d, Nummer 4 mit einer Geldbuße bis zu fünfhunderttausend Euro und in dem Fall des Absatzes 2 Nummer 13 mit einer Geldbuße bis zu einhunderttausend Euro geahndet werden.

(7) Handelt es sich bei dem Betroffenen um eine besonders wichtige Einrichtung, kann die Ordnungswidrigkeit in den Fällen der Absätze 1 und 2 Nummer 2, 3 und 7 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 2 Nummer 1 Buchstabe d, Nummern , 4, 8 und 13 mit einer Geldbuße bis zu fünfhunderttausend Euro und in den Fällen des Absatzes 2 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.

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

§ 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 von besonders wichtigen Einrichtungen Nachweise über die Erfüllung einzelner oder aller Anforderungen nach den §§ 30, 31 und 32 verlangen. 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 Anweisungen in Bezug auf Maßnahmen erlassen, die zur Verhütung oder Behebung eines Sicherheitsvorfalls erforderlich sind. Ferner kann das Bundesamt die Einrichtungen zur Berichterstattung zu den nach Satz 1 angeordneten Maßnahmen auffordern.

(7) Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen verbindliche Anweisungen zur Umsetzung der Verpflichtungen nach diesem Gesetz erlassen.

(8) Das Bundesamt kann besonders wichtige Einrichtungen anweisen, 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 besonders wichtige Einrichtungen anweisen, Informationen zu Verstößen gegen diese Richtlinie nach bestimmten Vorgaben öffentlich bekannt zu machen.

(9) Das Bundesamt kann für besonders wichtige Einrichtungen einen Überwachungsbeauftragten benennen, der die Einhaltung der Verpflichtungen aus §§ 28, 29 und 37 überwacht. Die Benennung erfolgt für einen bestimmten Zeitraum und muss die Aufgaben des Überwachungsbeauftragten genau festlegen.

(10) Sofern besonders wichtige Einrichtungen den Anordnungen des Bundesamtes nach diesem Gesetz trotz Fristsetzung nicht nachkommen, kann das Bundesamt die jeweils zuständige Aufsichtsbehörde des Bundes auffordern

1. die Genehmigung für einen Teil oder alle Dienste oder Tätigkeiten dieser Einrichtung vorübergehend auszusetzen

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

Die Aussetzung nach Buchstabe a und die Untersagung nach Buchstabe b sind nur solange zulässig, bis die Besonders wichtige Einrichtung den Anordnungen des Bundesamtes nachkommt, wegen deren Nichtbefolgung sie verhängt ausgesprochen wurden.

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

(12) Stellt das Bundesamt im Zuge der Beaufsichtigung oder Durchsetzung 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.

§ 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.

Anlage 1

Sektoren mit hoher Kritikalität

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Teilsektor	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 im Sinne des Artikels 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 im Sinne des Artikels 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	Teilsektor	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 im Sinne des Artikels 3 Nummer 4 der Verordnung (EG) Nr. 300/2008, die für gewerbliche Zwecke genutzt werden
2.1.2			Flughafenleitungsorgane im Sinne des Artikels 2 Nummer 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates, Flughäfen im Sinne des Artikels 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 im Sinne des § 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 im Sinne des § 2 Nummer 3 des Allgemeinen Eisenbahngesetz (AEG), einschließlich Betreiber einer Serviceeinrichtung im Sinne des § 2 Nummer 9 jenes Gesetzes
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 im Sinne des Artikels 3 Nummer 1 der Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates, einschließlich ihrer Hafenanlagen im Sinne des Artikels 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

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Teilsektor	Einrichtungsart
			nach § 1 Absatz 6 Nummer 1 des Bundeswasserstraßengesetzes.
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 im Sinne des § 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 im Sinne des Artikels 15 der Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates
4.1.3			Unternehmen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des § 2 AMG ausüben.
4.1.4			Unternehmen, die pharmazeutische Erzeugnisse im Sinne des Abschnitts 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 im Sinne des Artikels 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	Teilsektor	Einrichtungsart
5	**Wasser und Abwasser**		
5.1		Trinkwasserversorgung	
5.1.1			Betreiber von Wasserversorgunsanlagen im Sinne von § 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 im Sinne des § 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-Knoten (Internet Exchange Points)
6.1.2			DNS-Dienstanbieter, ausgenommen Betreiber von Root-Nameservern
6.1.3			TLD-Namensregister
6.1.4			Anbieter von Cloud-Computing-Diensten
6.1.5			Anbieter von Rechenzentrumsdiensten
6.1.6			Betreiber von Inhaltszustellnetzen (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

Sonstige kritische Sektoren

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Teilsektor	Einrichtungsart
1	**Transport und Verkehr**		
1.1		Post- und Kurierdienste	
1.1.1			Anbieter von Postdienstleistungen im Sinne des § 4 Nr. 1 PostG, einschließlich Anbieter von Kurierdiensten
2	**Siedlungsabfallentsorgung**		
2.1.1			Unternehmen der Abfallbewirtschaftung im Sinne des § 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 im Sinne des Artikels 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 im Sinne des Artikels 3 Nummer 3 der genannten Verordnung aus Stoffen oder Gemischen produzieren
4	**Produktion, Verarbeitung und Vertrieb von Lebensmitteln**		
4.1.1			Lebensmittelunternehmen im Sinne des Artikels 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 im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates(4)herstellen, und Einrichtungen, die In-vitro-Diagnostika im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates(5)herstellen, mit Ausnahme der unter Anhang I Nummer 5 fünfter Gedankenstrich dieser Richtlinie aufgeführten Einrichtungen, die Medizinprodukte herstellen

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Teilsektor	Einrichtungsart
5.2		Herstellung von Medizinprodukten und In-vitro-Diagnostika	
5.2.1			Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts 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 im Sinne des Abschnitts 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 im Sinne des Abschnitts 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 im Sinne des Abschnitts 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 worten 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 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 [*die KRITIS-Dachgesetz-Verordnung*] in Kraft tritt, aber nicht vor dem Inkrafttretenstermin nach Absatz 1. Das Bundesministerium des Innern und für Heimat gibt den Tag des Inkrafttretens nach diesem Absatz im Bundesgesetzblatt bekannt.

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

Begründung

B. Besonderer Teil

Zu Artikel 1 (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Informationssicherheit 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 § 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 30 der NIS-2-Richtlinie.

Zu Nummer 3

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

Zu Nummer 4

Die Begriffsbestimmung dient der Umsetzung von Artikel 6 Nummer 10 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.

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 im Sinne des § 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 informationstechnischen Systemen, 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.

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

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 1 fort.

Zu Nummer 16

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

Zu Nummer 17

[…]

Zu Nummer 18

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 19

[…].

Zu Nummer 20

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

Zu Nummer 21

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

Zu Nummer 22

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

Zu Nummer 23

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

Zu Nummer 24

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

Zu Nummer 25

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

Zu Nummer 26

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 8 fort.

Zu Nummer 27

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

Zu Nummer 28

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

Zu Nummer 29

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

Zu Nummer 30

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

Zu Nummer 31

Die Begriffsbestimmung führt den bisherigen § 2 Absatz 5 fort.

Zu Nummer 32

[…]

Zu Nummer 33

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 34

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

Zu Nummer 35

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

Zu Nummer 36

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

Zu Nummer 37

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

Zu Nummer 38

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

Zu Nummer 39

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

Zu Nummer 40

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.

Zu Teil 2 (Das Bundesamt)

Zu Kapitel 1 (Aufgaben und Befugnisse)

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 und ermöglicht den Teilnehmern 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 § 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 Teil 3 (Sicherheit 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 Nummer 5

Nummer 5 dient der Umsetzung von Artikel 3 Absatz 1 Buchstabe d in Verbindung mit Artikel 2 Absatz 2 Buchstabe f Nummer i der NIS-2-Richtlinie. Unter dem von der NIS-2-Richtlinie vorgegebenen Begriff der „Zentralregierung“ werden in Anlehnung an die deutsche Definition von „zentrale Regierungsbehörden“ in der Richtlinie 2014/24/EU die Bundesministerien und das Bundeskanzleramt ausgenommen der jeweiligen Geschäftsbereichsbehörden gefasst werden. Die genaue Festlegung erfolgt in Anlage 3.

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. 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.

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.

Zu Absatz 5

Absatz 5 dient der Definition von Betreibern kritischer Anlagen.

Zu Absatz 6

Absatz 6 dient der Definition kritischer Anlagen.

Zu Absatz 7

Absatz 7 regelt den Stichtag, ab dem eine Anlage als kritische Anlage gilt.

Zu Absatz 8

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

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. 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 Belastungen für besonders wichtige und wichtige Einrichtungen entstehen, sollen die genannten Risikomanagementmaßnahmen in einem angemessenen Verhältnis zu den Risiken stehen, denen das betroffene Netz- und Informationssystem ausgesetzt wird. Hierbei werden u.a. auch den Kosten der Umsetzung sowie der Größe der Einrichtung Rechnung getragen. In die Bewertung der Angemessenheit und Verhältnismäßigkeit kann ebenfalls einfließen, ob wichtige Einrichtungen im Vergleich zu wesentlichen Einrichtungen 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.

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.

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.

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 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.

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.

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.

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.

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 1 dient der Umsetzung von Artikel 3 Absatz 4 Unterabsatz 1 Buchstabe b der NIS-2-Richtlinie.

Zu Nummer 3

Nummer 1 dient der Umsetzung von Artikel 3 Absatz 4 Unterabsatz 1 Buchstabe c der NIS-2-Richtlinie.

Zu Nummer 4

Nummer 1 dient der Umsetzung von Artikel 3 Absatz 4 Unterabsatz 1 Buchstabe d der NIS-2-Richtlinie.

Zu Absatz 2

Absatz 3 regelt für Betreiber kritischer Anlagen zusätzlich zu übermittelnde 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.

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.

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 krimineller 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 § 38 (Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter 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 Geschäftsleiter. 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.

Zu Absatz 1

Absatz 1 führt den bisherigen § 8a Absatz 3 fort.

Zu Absatz 2

Absatz 2 führt den bisherigen § 8a Absatz 5 fort.

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

Zu Nummer 3

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

Zu Nummer 4

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 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 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 Infrastrukturen mit einem Fokus auf die Versorgungsrelevanz erfolgen sollte. Gemäß dieser Verordnung als KRITIS-Betreiber bestimmte Unternehmen gelten gleichzeitig als besonders wichtige Einrichtungen.

KRITIS-Betreiber werden in Zukunft weiterhin mit Schwellenwerten anhand ihrer Versorgungsrelevanz bestimmt.

Für den in der Rechtsverordnung festzusetzenden als bedeutend anzusehenden Versorgungsgrad anhand von branchenspezifischen Schwellenwerten soll das bereits in mehrjähriger Verwaltungspraxis etablierte Verfahren der Verordnung zu Bestimmung Kritischer Infrastrukturen (BSI-KritisV) weiter fortgeführt werden. Hierbei werden durch BMI gemeinsam mit den jeweils zuständigen Ressorts sowie unter Beteiligung der KRITIS-Betreiber und ihrer Branchenverbände geeignete Bemessungsgrößen für kritische Anlagen bestimmt, anhand derer der Versorgungsgrad im Sinne der durch die Anlage versorgten Personen näherungsweise bestimmt werden kann. Diese Bemessungsgrößen stellen typischerweise quantitative oder qualitative anlagenspezifische Eigenschaften wie Kapazitäten, Größen, Typ oder Art der Anlage dar, die entweder den Betreibern bereits bekannt sind oder zumindest mit möglichst geringem Aufwand für die jeweiligen Anlagen ermittelt werden können. Anschließend werden für die so gefundenen Bemessungsgrößen Schwellenwerte bestimmt, bei deren Überschreitung der Versorgungsgrad der betreffenden Anlage als bedeutend im Sinne dieses Gesetzes gilt und damit die Anlage eine kritische Anlage darstellt.

Zu Teil 7 (Sanktionsvorschriften und Aufsicht)

Zu § 60 (Sanktionsvorschriften)

§ 60 führt den bisherigen § 14 fort. Da der § 60 nunmehr auch einen Absatz betreffend des Verwaltungszwangs umfasst, wird die Überschrift entsprechend geändert. 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 zu erbringenden Nachweisen, Nachforderungen, Auskünfte und Kennzahlen vorsätzlich nicht richtig oder nicht vollständig erbracht werden.

In § 60 Absatz 1 wurden lediglich die Verweise angepasst. Besonders wichtige Einrichtungen haben die Erfüllung der Anforderungen nach § 30 Absatz 1 spätestens zu einem vom Bundesamt festgelegten Zeitpunkt anschließend alle zwei Jahre nachzuweisen. § 8a Absatz 3 Satz 1 betraf die früheren Betreiber kritischer Infrastruktur, sodass hier eine Ersetzung mit dem neu eingeführten Einrichtungsäquivalent der besonders wichtigen Einrichtungen erfolgten musste. Die Betreiber kritischer Infrastrukturen sind als Einrichtungskategorie mit einem Mehr an Pflichten ebenfalls erfasst.

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 lit. 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.

§ 5b Absatz 6 entspricht nunmehr dem § 11 Absatz 6. § 7c Absatz 1 entspricht dem § 16 Absatz 1 Satz 1, § 7d entspricht § 17 und § 8a Absatz 3 Satz 5 entspricht § 34 Absatz 1 Satz 6

Zu Buchstabe b

In Buchstabe b) wurde der Verweis angepasst.

§ 64 Absatz 8 Satz 1 oder Absatz 9 Satz 1 oder § 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 wesentliche 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, 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.

Zu Buchstabe c

In Buchstabe c) wurde der Verweis angepasst. Satz 2 entfällt aufgrund obiger Anpassungen. § 8c Absatz 4 Satz 1 entfällt, da die Kategorie „Anbieter digitaler Dienste“ in den neuen Einrichtungskategorien aufgeht.

Zu Buchstabe d

Die alte Nummer 8 mit einer Bußgeldahndung für Verstöße gegen Streichung des § 8c Absatz 1 Satz 1 wird gestrichen, da dieser in den neuen Einrichtungskategorien aufgeht. 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

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 nach einer Bebußung bei Verstößen gegen Risikomanagementmaßnahmen nachgekommen.

Zu Nummer 3

In Nummer 3 wurden die Verweise angepasst und entsprechend der Einführung der neuen Einrichtungskategorien aktualisiert. Anpassung der Verweise und Aktualisierung – Meldepflichten:

§ 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

In Nummer 4 wurden die Verweise angepasst und aktualisiert:

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 § 32 Absatz 1, 3 ersetzt und auf die neugeschaffenen Einrichtungskategorien angepasst: § 32 Absatz 1 definiert die Registrierungspflichten für wichtige und besonders wichtige Einrichtungen, Absatz 3 die Anforderungen für kritische Einrichtungen.

§ 8f Absatz 5 Satz 1 entfällt, da dieser in den neuen Einrichtungskategorien aufgeht.

Ein Ersatz erfolgt jedoch durch § 33 Absatz 1, 2, der Registrierungspflichten für andere Einrichtungsarten vorsieht.

§ 32 Absatz 6 sieht vor, dass Änderungen der nach § 32 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 5

In Nummer 5 wurden die Verweise angepasst und aktualisiert:

Zu Nummer 6

Anpassung des Verweises

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 § 34 Absatz 1 Satz 1 die Anforderungen für besonders wichtige und wichtige Einrichtungen, § 39 Absatz 2 Satz 1 die für kritische Einrichtungen.

Zu Nummer 8

In Nummer 8 wurden inhaltlich ebenfalls keine Änderungen vorgenommen und die Verweise lediglich angepasst. § 64 Absatz 5 Satz 3 bestimmt die Zutrittsverschaffungspflicht bei besonders wichtigen Einrichtungen.

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

Lediglich Anpassung des Verweises

Zu Nummer 11

In Nummer 11 wurde ein neuer Bußgeldtatbestand geschaffen, der das Vorgeben Inhaber eines europäischen Cybersicherheitszertifikats oder Aussteller einer EU-Konformitätserklärung zu sein, obgleich diese nicht besteht, widerrufen oder für ungültig erklärt wurde, ahnden. 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 Nummer 12

Lediglich Anpassung des Verweises.

Zu Nummer 13

In Nummer 13 wurde ein neuer Bußgeldtatbestand geschaffen, der ein Zuwiderhandeln gegen eine verbindliche Anweisung § 64 Absatz 7 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 diese Bußgeldtatbestandes werden Neuer Bußgeldtatbestand: Umsetzung NIS 2

Es werden hierbei Artikel 32, 33 Absatz 4 lit. 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 widersetzen.

Zu Absatz 3

Redaktionelle Änderung von „Sicherheitslücke“ auf „Schwachstelle“.

Zu Absatz 4

Zu Nummer 1

Redaktionelle Änderung von „Sicherheitslücke“ auf „Schwachstelle“.

Zu Nummer 2

Redaktionelle Änderung von „Sicherheitslücke“ auf „Schwachstelle“.

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 ergab sich hierbei keine Veränderung. Auf der zweithöchsten Stufe wurde ein Verstoß gegen Absatz 2 Nummer 4 und 6 aufgenommen. Bei diesem handelt es sich um einen Verstoß gegen die Registrierungspflichten für andere Einrichtungsarten nach § 32 Absatz 1 s.Domain-Name Registry Diensteanbieter oder Anbieter nach §§ 33 Absatz 1, 64 Absatz 1).

Für einen Verstoß gegen Absatz 2 Nummer 10 und 12 ergaben sich keine Veränderungen in der Bußgeldhöhe.

Auf der zweithöchsten Stufe wurden zudem Verstöße gegen die neueingeführten Absatz 2 Nummern 9 und 11 aufgenommen. Bei diesen handelt es sich um Vorgabe der Inhaberschaft einer Zertifizierung nach § 54 Absatz 2 oder eines europäischen Cybersicherheitszertifikats. Bei der Einstufung wurde sich an der Bußgeldhöhe von Nummern 10 und 12,

die in der vormaligen und jetzigen Fassung ebenfalls in dieser Höhe angesiedelt sind und im Unrechtsgehalt eine Entsprechung finden, orientiert.

Als niedrigste Stufe wurde die frühere 100.000 Euro übernommen. Hierbei ergaben sich für einen Verstoß gegen Absatz 3 keine Veränderungen.

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: Auf höchster Stufe wird ein Wert von 7 Millionen Euro oder 1,4 Prozent des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens angesetzt. Auf zweiter Stufe wird ein Wert von 500.000 Euro, auf niedrigster Stufe ein Wert von 100.000 Euro angesetzt.

Eine erste Bußgeldstufe in Höhe von 7 Millionen Euro oder einem Höchstbetrag von mindestens § 1,4 Prozent des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens 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.

Auf einer zweiten Stufe, in Höhe von 500.000 Euro, werden die Verstöße gegen Absatz 2 Nummern 1 Buchstabe d und Nummern 4, geahndet. 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. Gleiches gilt für einen Verstoß gegen Absatz 2 Nummer 4 und 6, der Verstöße gegen die Registrierungspflichten betrifft

Die unterste Stufe in Höhe von 100.000 Euro bei wichtigen Einrichtungen ahndet Verstöße gegen Absatz 2 Nummern Nummer 4 und 13. Die neu geschaffene Nummer 4 betrifft Verstöße gegen die Nichtmitteilung von Änderungen nach § 32. Hierbei wurde in Nummer 4 die Bußgeldhöhe im Vergleich zu besonders wichtigen und kritischen Einrichtungen in ein Verhältnis gesetzt und auf unterster Ebene angegliedert. Die neu geschaffenen Nummern 13 wurde ebenfalls auf dieser untersten Stufe angesetzt, da im Falle von Nummer 13 erstmals eine Bebußung von Verstößen gegen Anweisungen geahndet.

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 geleiteten 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 1 und Absatz 2 Nummern 2, 3 und 7 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 2 wurde ebenfalls 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.

Ein Verstoß gegen Absatz 2 Nummer 7 (Nachweispflichten) ist auf der höchsten Stufe bei besonders wichtigen Einrichtungen und Betreibern kritischer Anlagen angesiedelt. Die Bußgeldhöhe wurde entsprechend Absatz 1 angepasst (vormals ebenso hoch durch den Verweis des § 30 Absatz 2 Satz 3 OWiG). Ein Verstoß gegen Absatz 2 Nummer 8 (Meldepflichten) musste auf höchster Bußgeldstufe angesetzt werden, da Artikel 34 Absatz 4 NIS2 Richtlinie hier ebenfalls Vorgaben für die Bußgeldhöhe, die hier umgesetzt wurde, schuf.

Zweithöchste Stufe ist die Stufe von 500.000 Euro. Absatz 2 Nummer 8, der den Verstoß gegen eine Weigerung der Zutrittsgestattung bebußt, wurde auf eine Bußgeldhöhe von 500.000 Euro entsprechend der Bedeutung der besonders wichtigen Einrichtung und Betreiber kritischer Anlagen gesetzt. Bei Absatz 2 Nummer 4 erfolgte keine Änderung der vorherigen Bußgeldhöhe.

Ein Verstoß gegen die neugeschaffene Nummer 4 (Nichtmitteilung von Änderungen nach § 32) wurde auf eine Bußgeldhöhe auf zweiter Stufe gesetzt und somit in der Höhe von Verstößen bei wichtigen Einrichtungen höhergestuft.. Die neu geschaffene Nummer 13 wurde auf der zweiten Stufe angesetzt, da im Falle vor Nummer 13 erstmals eine Bebußung von Verstößen gegen Anweisungen geahndet wird, jedoch im Vergleich zu einem Verstoß bei einer wichtigen Einrichtung eine Abstufung bestehen sollte.

Unterste Stufe ist die Stufe von 100.000 Euro. Bei einem Verstoß gegen Absatz 2 Nummer 5 wurde die bisherige Bußgeldhöhe übernommen.

Zu Absatz 8

Keine Veränderung

Zu Absatz 9

Mit Absatz 9 wird Artikel 35 Absatz 2 NIS-2 umgesetzt.

Zu Absatz 10

Mit Absatz 10 wird Artikel 34 Absatz 6 NIS 2 umgesetzt.

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 Anfoderungen 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 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 1 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 § 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 Anlage 1 (Sektoren mit hoher Kritikalität)

Die Anlage dient der Umsetzung von Anhang I der NIS-2-Richtlinie.

Zu Anlage 2 (Sonstige kritische Sektoren)

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 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.

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.