Bundesrat **Drucksache 380/24 (Beschluss)**

27.09.24

Stellungnahme
des Bundesrates

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

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

1. Zum Gesetzentwurf allgemein

   a) Der Bundesrat bittet, in den Entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes aufzunehmen:

      aa) den Identitätsnachweis bei der Domainregistrierung bzw. Domainübertragung und bei einer automatisierten Datenabfrage;

      bb) einer Verpflichtung zur Identitätsprüfung von Domain-Anmeldungen und Domain-Übertragungen über qualifizierte Identifizierungsverfahren, z. B. Videoidentifizierungsverfahren oder die Vorlage eines elektronischen Identitätsnachweises, sodass sich die Anbieter Gewissheit über die Person des Beteiligten verschaffen können. Dies kann insbesondere durch Vorlage eines elektronischen Identitätsnachweises beispielsweise nach § 18 PAuswG, § 12 eID-Karte-G oder eines elektronischen Identitätsnachweises, der nach der eiDAS-VO von einem anderen Mitgliedstaat der Europäischen Union ausgestellt worden ist, erfolgen;

      cc) die Vorhaltung der genauen und vollständigen Domain-Namen-Registrierungsdaten in der Datenbank für die Abfrage von Zugriffsberechtigten;

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0720-2946

dd) die Verpflichtung für Domain-Registrare und Registrierungsdienstleister, möglichst in Echtzeit einem berechtigten Zugangsnachfrager vollständige Registrierungsdaten zur Verfügung zu stellen;

b) Der Bundesrat bittet ferner, sich dafür einzusetzen, dass geregelt wird, unter welchen Voraussetzungen Domänen bei Missbrauch blockiert werden können.

Begründung:

Ein erheblicher Teil der Fake-Shops in Deutschland verfügt über eine „.de-Domain“, die bei Verbraucherinnen und Verbrauchern als besonders vertrauenswürdig gilt. Mit „.de Domains“ wird ein hohes Schutzniveau suggeriert, das tatsächlich nicht immer gewährleistet ist. Daher sollte für das wirksame Vorgehen gegen Fake-Shops eine „.de Domain“ Registrierung nur noch mit Identitätsprüfung möglich sein. Eine Vielzahl von Fakeshop-Betreibern lassen sich ältere oder nicht mehr genutzte „.de Domains“ von Unternehmen übertragen, um so von der Seriosität dieser Firmen zu profitieren. Insofern sollte auch für die Übertragung von „.de Domains“ eine Identitätsprüfung stattfinden, um die Hürde für die Registrierung von Fake-Shops unter falschen Angaben zu erhöhen.

Die Verbraucherschutzministerkonferenz (VSMK) 2024 in Regensburg hat einstimmig einen Beschluss zur Verbesserung der Bekämpfung von Fakeshops gefasst (TOP 13/20. VSMK), welcher im weiteren Gesetzgebungsverfahren berücksichtigt werden soll.

Zu Buchstabe a:

In der Bundesratsinitiative BR-Drucksche 569/19 (Beschluss) ist die Bundesregierung gebeten worden zu prüfen, wie eine mit der Datenschutz-Grundverordnung (DSGVO) in Einklang stehende öffentliche Abfrage der Domain-Inhaberdaten nach Vorbild der Who-is-Abfrage der DENIC eingeführt werden könnte. Die DENIC eG verwaltet die Top-Level-Domain „.de“ und verantwortet den Domainbetrieb.

Die Einführung qualifizierter Identifizierungsverfahren bei der Domain-Registrierung wäre für die Fake-Shop-Bekämpfung eine entscheidende Verbesserung. Für die Prüfung der Registrierungsdaten auf den Verdacht des Betreibens eines Fake-Shops ist der vollständige Datensatz der Domainregistrierung erforderlich.

Zur Fake-Shop-Bekämpfung bei Missbrauch sind die zeitnahe und vollständige Verfügbarkeit der Registrierungsdaten für die Erkennung von Vorfällen und die Reaktion darauf von wesentlicher Bedeutung. Bei gewerblichen Domänen-Anmeldungen sollten zu jedem Domänennamen alle Inhaberdaten frei zugänglich sein. Bei personenbezogenen Daten sollten alle Daten veröffentlicht werden, soweit dies von der DSGVO gedeckt ist. Besonders wichtig ist, dass berechtigte Zugriffsnachfrager auch Zugriff auf alle .de Neuregistrierungen erhalten können. Da Fake-Shops mit legitimer Adresse eines anderen Unternehmens besonders gefährlich sind, ist der DSGVO-unbedenkliche Abgleich des Ortes im Impressum des Fake-Shops mit dem in den DENIC-Registrierungsdaten hinterlegten Ort des Fake-Shop-Bertreibers zwingend erforderlich.

Ein automatisiertes, digitales und datenschutzkonformes Zugriffsverfahren ist erforderlich, damit in Echtzeit auf die genauen und vollständigen Domain-Namen-Registrierungsdaten zugegriffen werden kann (z. B. über die sogenannte RDAP-Schnittstelle nach Vorbild der vorherigen Who-is-Abfrage der DENIC). Die Bekämpfung von missbräuchlichen Online-Angeboten erfordert Massenanalysen, die nach dem bisherigen Verfahren mit fallbezogenen und zeitversetzten Freigaben zeitnah nicht zu erreichen sind. Die Berechtigung sollte einmalig geprüft werden und nicht fallbezogen wie bisher mit pdf-Formularen. Als „berechtigte Zugangsnachfrager“ sollten Behörden, Verbraucherzentralen und beauftragte Sicherheitsunternehmen sowie Dienstleister, die nach einer Freischaltung generell Zugriff erhalten müssen (zum Beispiel auch die IT-Verantwortlichen des von der Verbraucherzentrale Nordrhein-Westfalen mit finanzieller Unterstützung der Bundesländer weiterentwickelten „Fake-Shop-Finder“) gelten.

Zu Buchstabe b:

Um wirksam gegen Fake-Shops vorgehen zu können, sind effektive Werkzeuge wie die Blockierung von Domänen bei Missbrauch innerhalb weniger Tage notwendig. Hierfür ist ein entsprechender Regelungsrahmen zu schaffen. Dabei sind bestehende europarechtliche Regelungen zu beachten und wenn nötig zu ergänzen. Auch sollte geprüft werden, inwieweit automatisierte Verfahren zum Einsatz kommen können.

2. Zum Gesetzentwurf allgemein

Der Bundesrat fordert, im weiteren Gesetzgebungsverfahren eine Refinanzierung der den Krankenhäusern im Rahmen der Umsetzung des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes entstehenden Kosten für Informationssicherheit sicherzustellen.

Begründung:

Die Gewährleistung von Informationssicherheit stellt auch im Krankenhausbereich einen Belang von erheblicher Bedeutung dar. Maßnahmen zur Steigerung der Informationssicherheit haben aber zwingend Mehrkosten zur Folge. Anders

als andere Einrichtungen im Anwendungsbereich des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes können Krankenhäuser diese Mehrkosten nicht weitergeben, jedenfalls sofern dies nicht in sehr eingeschränktem Umfang über den Krankenhausstrukturfonds möglich ist, der jedoch nach aktueller Rechtslage Ende 2024 ausläuft. Dies wiegt umso schwerer, als sich Krankenhäuser ohnehin bereits mit erheblich gestiegenen Betriebskosten konfrontiert sehen, die aufgrund der bundesgesetzlichen Rahmenbedingungen für die Krankenhausvergütung bislang nicht vollumfänglich von den Kostenträgern refinanziert werden konnten. Die Situation der Krankenhäuser wird sich durch das geplante Krankenhausversorgungsverbesserungsgesetz (KHVVG) insoweit nicht hinreichend verbessern. Auch bleibt die Refinanzierung notwendiger Kosten für Investitionen in Digitalisierung und Informationssicherheit im Rahmen des KHVVG außer Betracht.

3. Zu Artikel 1 (§ 2 Nummer 21 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren in geeigneter Weise klarzustellen, dass die Entwicklung, der Betrieb und die rechtliche Ausgestaltung von länderübergreifenden Verfahren nach dem IT-NetzG und dem IT-Staatsvertag zur Errichtung des IT-Planungsrates, die „im Auftrag einer oder mehrerer Einrichtungen der Bundesverwaltung betrieben“ werden, durch die Regelung des § 2 Nummer 21 BSIG-E zur „Kommunikationstechnik des Bundes“ nicht berührt wird.

Begründung:

Eine entsprechende klarstellende Erläuterung fehlt in der Begründung des Gesetzentwurfs. So sind insbesondere die Auswirkungen auf gemeinsam entwickelte und im Verbund betriebene Verfahren nach dem IT-NetzG und dem IT-Staatsvertag zur Errichtung des IT-Planungsrates nicht transparent. Offen ist insbesondere, ob sie unter den Begriff der „Kommunikationstechnik des Bundes“ fallen.

4. Zu Artikel 1 (§ 3 Absatz 1 Satz 2 Nummer 18 Buchstabe a, b BSIG)

Artikel 1 § 3 Absatz 1 Satz 2 Nummer 18 ist wie folgt zu ändern:

a) In Buchstabe a sind nach dem Wort „Bundes“ die Wörter „und der Länder“ einzufügen.

b) In Buchstabe b sind die Wörter „des Bundesamtes für Verfassungsschutz“ durch die Wörter „der Verfassungsschutzbehörden des Bundes und der Länder“ sowie die Wörter „dem Bundesverfassungsschutzgesetz“ durch die Wörter „den Verfassungsschutzgesetzen des Bundes und der Länder“ zu er-

setzen.

Begründung:

Mit dieser Änderung wird die in der geltenden Fassung des BSIG bestehende Aufgabe des BSI aufrechterhalten. Diese besteht unter anderem darin, neben den Polizeibehörden und Nachrichtendiensten des Bundes auch die Polizei- und Verfassungsschutzbehörden der Länder bei ihren gesetzlichen Aufgaben bzw. bei der Auswertung und Bewertung von Informationen zu unterstützen. Auch die bestehende Aufgabe der Beobachtung von Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand des Staates oder die Sicherheit des Bundes oder eines Landes gerichtet sind, oder Aufgaben, welche bei der Beobachtung sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten anfallen, müssen aufrechterhalten werden.

Der vorliegende Gesetzentwurf sieht dagegen vor, diese Unterstützungsleistung künftig auf die Bundesbehörden zu beschränken. Die Möglichkeit der Amtshilfe bleibt ausweislich der Einzelbegründung zwar unberührt. Amtshilfe kann allerdings im Einzelfall von der ersuchten Behörde leichter abgelehnt werden, als die Durchführung einer Unterstützungsleistung, die der ersuchten Behörde als eigene Aufgabe obliegt. Insofern werden die Länder durch die geplante Neuregelung gegenüber der geltenden Gesetzesfassung schlechter gestellt – bei stetig steigender Bedeutung der Informationssicherheit von Bund und Ländern.

Die hier vorgeschlagene Änderung stellt die geltende Gesetzesfassung insofern wieder her.

Gerade mit Blick auf die aktuelle Sicherheitslage sind auch auf lokaler Ebene Ereignisse denkbar, in denen die Polizei- und Verfassungsschutzbehörden der Länder auf Unterstützungsleistungen durch das BSI angewiesen sind.

5. Zu Artikel 1 (§ 5 Absatz 2 Satz 2, § 6 Absatz 1 und 3 – neu – BSIG)

Artikel 1 ist wie folgt zu ändern:

a) In § 5 Absatz 2 Satz 2 sind nach dem Wort „Meldemöglichkeiten“ die Wörter „, einschließlich eines medienbruchfrei digitalisierten Meldeverfahrens in der Online-Plattform für den Informationsaustausch nach § 6 Absatz 1,“ einzufügen.

b) § 6 ist wie folgt zu ändern:

aa) Absatz 1 ist wie folgt zu fassen:

„(1) Das Bundesamt betreibt ab dem sechsten Monat nach Inkrafttreten dieses Gesetzes eine Online-Plattform zum Informationsaustausch mit wichtigen Einrichtungen, besonders wichtigen Einrichtungen und Einrichtungen der Bundesverwaltung. Es kann die beteiligten Hersteller,

Lieferanten oder Dienstleister zum Austausch über Cyberbedrohungen, Schwachstellen, Beinahevorfälle und IT-Sicherheitsmaßnahmen sowie zur Aufdeckung und Abwehr von Cyberangriffen mittels bedrohungsspezifischer Informationen, Cybersicherheitswarnungen, Kompromittierungsindikatoren und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten hinzuziehen. Das Bundesamt ermöglicht weiteren Stellen auf Antrag die Teilnahme, soweit ein berechtigtes Interesse vorliegt und übergeordnete Bedenken nicht entgegenstehen. Voraussetzung für den Zugang zur Online-Plattform ist eine Authentifizierung mit einem elektronischen Identitätsnachweis, der nach Artikel 6 der Verordnung (EU) Nr. 910/2014 mit dem Sicherheitsniveau „hoch“ anerkannt worden ist.“

bb) Folgender Absatz ist anzufügen:

„(3) Die Online-Plattform nach Absatz 1 ermöglicht in geeigneter Weise zugleich Zugang zu Informationen zu physischer Sicherheit und Resilienz kritischer Infrastrukturen, die vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe in Erfüllung von Vorgaben des Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 bereitgestellt werden.“

Begründung:

Dem Erfüllungsaufwand für die betroffenen Unternehmen und Einrichtungen sollte entsprechender Mehrwert für diese gegenüberstehen, um die Akzeptanz der neuen Infrastrukturen zu erhöhen und dadurch ihren Erfolg zu sichern.

Entsprechend sollte die in § 6 BSIG-E vorgesehene Möglichkeit des freiwilligen Austauschs relevanter Cybersicherheitsinformationen zwischen den in den Anwendungsbereich der Richtlinie fallenden und gegebenenfalls anderen Akteuren eine nähere Bestimmung hinsichtlich der Inhalte und organisatorischen Rahmenbedingungen bereits im Gesetz erfahren. Bei den Inhalten weicht der Gesetzentwurf vom Wortlaut der Richtlinie ab und lässt beispielsweise Kompromittierungsindikatoren und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten unerwähnt.

Erstrebenswert wäre insbesondere eine Verpflichtung der Authentifizierung der Teilnehmer mittels europäischer Identität auf Vertrauensniveau „hoch“, um die Vertraulichkeit der Nutzerbeschränkten Online-Plattform zu gewährleisten. Im Gegenzug sollte klargestellt werden, dass Betroffene mit berechtigtem Interesse Zugang erhalten, soweit keine übergeordneten Bedenken entgegenstehen. Um den Unternehmen Planungssicherheit zu geben, ist außerdem eine klare Vorgabe hinsichtlich der Frist wünschenswert, mit der die Informationsplatt-

form zur Verfügung gestellt werden muss. Schließlich sollte der im NIS-2-Umsetzungsgesetz vorgesehene Zugang der Einrichtungen zu Informationen und unterstützenden Handlungsempfehlungen zu digitalen Bedrohungen, entsprechend den Bedürfnissen der Unternehmen, mit dem Zugang zu Informationen zu physischer Sicherheit und Resilienz kritischer Infrastrukturen gemäß KRITIS-Dachgesetz verknüpft werden.

Die in § 6 BSIG-E geregelte Informationsplattform sollte zugleich eine der in § 5 normierten „geeigneten Meldemöglichkeiten“ integrieren. Die allgemeine Meldestelle für die Sicherheit in der Informationstechnik sollte die Meldung, entsprechend der relevanten OZG/XÖV-Standards, in einem Ende-zu-Ende digitalisierten Verfahren realisieren.

6. Zu Artikel 1 (§ 7 Absatz 8, § 61 Absatz 11 BSIG)

In Artikel 1 § 7 Absatz 8 und § 61 Absatz 11 ist jeweils das Wort „offensichtliche“ zu streichen und sind die Wörter „Folge hat“ durch die Wörter „Folge haben kann“ zu ersetzen.

Begründung:

Die aktuelle Fassung der Verpflichtungen des Bundesamts die zuständigen Datenschutzaufsichtsbehörden über eine Verletzung des Schutzes personenbezogener Daten zu unterrichten, bleibt hinter Artikel 35 Absatz 1 der NIS-2-Richtlinie zurück. § 7 Absatz 8 und § 61 Absatz 11 BSIG-E sollen laut Einzelbegründung allerdings Artikel 35 der NIS-2-Richtlinie umsetzen.

Mit der Änderung wird eine Anpassung an den Wortlaut von Artikel 35 Absatz 1 der NIS-2-Richtlinie vorgenommen: Danach besteht die Unterrichtungspflicht, wenn die zuständigen IT-Sicherheitsbehörden im Zuge ihrer Aufgabenwahrnehmung feststellen, dass der Verstoß gegen Risikomanagementmaßnahmen oder Berichtspflichten eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 DSGVO zur Folge haben kann.

Artikel 35 Absatz 1 der NIS-2-Richtlinie fordert gerade keine Offensichtlichkeit oder das Feststehen der Datenschutzverletzung, sondern nur deren Möglichkeit.

Um die Richtlinie ordnungsgemäß umzusetzen und den Zwecken des Schutzes personenbezogener Daten und der Effektivität der Zusammenarbeit (wie sie Artikel 31 Absatz 3 der NIS-2-Richtlinie vorsieht) gerecht zu werden, sind in § 7 Absatz 8 und § 61 Absatz 11 BSIG-E die Einschränkungen zu streichen.

7. Zu Artikel 1 (§ 28 Absatz 8 Nummer 2 BSIG)

In Artikel 1 § 28 Absatz 8 Nummer 2 ist das Wort „vergleichbare“ durch die Wörter „die NIS-2-Richtlinie umsetzende“ zu ersetzen.

Begründung:

Mit dieser Norm wird für die Länder die Möglichkeit geschaffen, in eigener Verantwortung wirtschaftlich tätige rechtlich unselbstständige Organisationseinheiten von Gebietskörperschaften und juristische Personen, an denen ausschließlich Gebietskörperschaften, ausgenommen der Bund, beteiligt sind, vom Anwendungsbereich des BSIG-E auszunehmen. Eine Voraussetzung hierfür ist, dass die Einrichtungen „durch vergleichbare landesrechtliche Vorschriften“ reguliert werden (§ 28 Absatz 8 Nummer 2 BSIG-E).

Die bislang gewählte Formulierung „durch vergleichbare landesrechtliche Vorschriften“ in § 28 Absatz 8 Nummer 2 BSIG-E erweckt gemeinsam mit der Einzelbegründung den Eindruck, dass die jeweilige Einrichtung Gegenstand einer mit den Regelungen des BSIG-E vergleichbaren NIS-2-Umsetzung durch das betreffende Land sein muss.

Maßstab für vergleichbare Regelungen in den Ländern hat indes nicht die bundesrechtliche Regelung des BSIG-E zu sein, sondern vielmehr das unmittelbare EU-Recht, mithin die NIS-2-Richtlinie selbst. Die in diesem Antrag vorgeschlagene Änderung gewährleistet, dass Anpassungen der Regelungen in den Ländern nach möglichen Änderungen im BSIG-E vermieden werden und Maßstab stets die Vorgaben der NIS-2-Richtlinie sind und nicht etwa gegebenenfalls über die Mindestharmonisierung hinausgehende Vorgaben des Bundes.

8. Zu Artikel 1 (§ 30 Absatz 7 BSIG)

In Artikel 1 § 30 Absatz 7 sind nach dem Wort „Straftaten“ die Wörter „sowie der Unabhängigkeit der Datenschutzaufsichtsbehörden“ einzufügen.

Begründung:

Eine Einschränkung der Unabhängigkeit der Datenschutzaufsichtsbehörden wäre nur auf europarechtlicher Grundlage zulässig. Aus der NIS-2-Richtlinie ergibt sich jedoch indirekt, dass die Datenschutzaufsichtsbehörden zur Verhängung von Geldbußen (uneingeschränkt) befugt sind: Gem. Artikel 35 Absatz 2 der NIS-2-Richtlinie darf bei einer Geldbußenverhängung durch die Datenschutzaufsichtsbehörde keine zusätzliche Geldbuße nach Artikel 34 NIS-2-Richtlinie verhängt werden. Das setzt voraus, dass die Datenschutzaufsichtsbehörden weiterhin Geldbußen verhängen dürfen.

Die Änderung stellt klar, dass keine Einschränkung der Unabhängigkeit der Datenschutzaufsichtsbehörden geregelt wird. Diese Klarstellung soll bereits im Gesetzestext erfolgen.

9. Zu Artikel 1 (§ 38 Absatz 2 Satz 3 – neu – BSIG)

Dem Artikel 1 § 38 Absatz 2 ist folgender Satz anzufügen:

„Rechtsvorschriften im Hinblick auf die für öffentliche Einrichtungen geltenden Haftungsregelungen sowie die Haftung von öffentlichen Bediensteten und gewählten und ernannten Amtsträgerinnen und Amtsträgern bleibt unberührt."

Begründung:

Ziel ist eine konsequente 1:1-Umsetzung der NIS-2-Richtlinie.

Die Änderung führt zu einem Gleichlauf von NIS-2-Richtlinie und Umsetzungsgesetz. Die Bundesregierung selbst hat sich bei der Umsetzung von EU-Recht zum Ziel gesetzt, dass diese „effektiv, bürokratiearm und im Sinne des einheitlichen Europäischen Binnenmarktes erfolgt." An diesem selbstgesteckten Ziel muss sich die Bundesregierung messen lassen.

Es soll daher klargestellt werden, dass – wie in Artikel 20 Absatz 1 Satz 2 NIS-2-Richtlinie geregelt – die bestehenden Haftungsregelungen für öffentliche Einrichtungen sowie die Haftung von öffentlichen Bediensteten und gewählten und ernannten Amtsträgern unberührt bleiben.

Zur Rechtsklarheit trägt das Weglassen dieser Klarstellung – in Abweichung von der NIS-2-Richtlinie – nicht bei und führt im Gegenteil ggf. eher zu Rechtsunsicherheiten und Bürokratie- und Begründungsaufwand.

10. Zu Artikel 1 (§ 38 Absatz 3 Satz 2 – neu – BSIG)

Dem Artikel 1 § 38 Absatz 3 ist folgender Satz anzufügen:

„Die Geschäftsleitungen wirken daraufhin, dass allen Mitarbeiterinnen und Mitarbeitern besonders wichtiger und wichtiger Einrichtungen regelmäßig entsprechende Schulungen angeboten werden."

Folgeänderungen:

a) In der Inhaltsübersicht ist die Angabe zu Artikel 1 § 38 wie folgt zu fassen:

„§ 38 Governance“.

b) In Artikel 1 § 38 ist die Überschrift wie folgt zu fassen:

„§ 38

Governance“.

Begründung:

Ziel ist eine konsequente 1:1-Umsetzung der NIS-2-Richtlinie.

Die Änderung führt zu einem Gleichlauf von NIS-2-Richtlinie und Umsetzungsgesetz. Die Bundesregierung selbst hat sich bei der Umsetzung von EU-Recht zum Ziel gesetzt, dass diese „effektiv, bürokratiearm und im Sinne des einheitlichen Europäischen Binnenmarktes erfolgt.“ An diesem selbstgesteckten Ziel muss sich die Bundesregierung messen lassen.

Es kann mit Blick auf die Einzelbegründung zu § 38 Absatz 3 BSIG-E davon ausgegangen werden, dass bereits nach aktuellem Stand allen Mitarbeiterinnen und Mitarbeitern besonders wichtiger und wichtiger Einrichtungen regelmäßig entsprechende Schulungen anzubieten sind („Wichtige und besonders wichtige Einrichtungen werden aufgefordert, derartige Schulungen für alle Beschäftigten anzubieten“). Zur Klarstellung sollte dies auch aufgrund Artikel 20 Absatz 2 der NIS-2-Richtlinie in das beabsichtigte Gesetz übernommen werden, um Rechtssicherheit zu schaffen.

Die Folgeänderung trägt dieser Klarstellung Rechnung. Bislang stellt die Überschrift nur auf die Schulungspflicht für Geschäftsleitungen ab. Bei einer Anfügung des oben aufgeführten Satzes passt die Überschrift nicht mehr. Deshalb sollte diese – auch hier in 1:1 Umsetzung der NIS-2-Richtlinie – auf den übergeordneten Begriff der „Governance“ geändert werden, um auch die Schulungen der Mitarbeiterinnen und Mitarbeiter erfassen zu können.

11. Zu Artikel 1 (§ 40 Absatz 3 Nummer 5 – neu – BSIG)

Artikel 1 § 40 Absatz 3 ist wie folgt zu ändern:

a) In Nummer 3 ist das Wort „und“ am Ende durch ein Komma zu ersetzen.

b) In Nummer 4 Buchstabe d ist das Wort „unterrichten.“ durch die Wörter „unterrichten und“ zu ersetzen.

c) Folgende Nummer ist anzufügen:

„5. besonders wichtigen und wichtigen Einrichtungen geeignete Online-Formulare zur Verfügung zu stellen, welche es ermöglichen, zeitgleich mit einer Meldung nach § 32 die in Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 angegebenen Informationen mitzuteilen. Die Einrichtungen können ihrer Meldepflicht nach Artikel 33 der Verordnung (EU) 2016/679 durch eine Meldung an das Bundesamt mittels des nach Satz 1 genannten Online-Formulars nachkommen. Das Bundesamt stellt die Meldungen unverzüglich den zuständigen Datenschutzaufsichtsbehörden zur Verfügung. § 7 Absatz 8 und § 61 Absatz 11 bleibt unberührt."

Begründung:

§ 40 BSIG-E regelt, dass das BSI zentrale Meldestelle ist und welche Aufgaben es insoweit zu erfüllen hat. Hierbei wird jedoch der Erwägungsgrund 106 der NIS-2-Richtlinie nicht aufgegriffen. Danach soll der Verwaltungsaufwand für Einrichtungen verringert werden. Insbesondere wird den Mitgliedstaaten nahegelegt die zentrale Anlaufstelle auch für Meldung zu nutzen, die nach der DSGVO erforderlich sind.

Durch die Verpflichtung des Bundesamts, Online-Formulare für Meldungen nach Artikel 33 der DSGVO zur Verfügung zu stellen, wird der Impuls aus Erwägungsgrund 106 aufgegriffen und den Einrichtungen die Möglichkeit eröffnet, ihre Meldeverpflichtungen durch Meldung an eine Stelle zu erfüllen. Diese Möglichkeit einer Meldung nach Artikel 33 der DSGVO an das Bundesamt besteht dann, wenn die Einrichtung eine Meldung nach § 32 BSIG-E an das Bundesamt vornimmt. Durch die Bündelung beider Meldungen an eine Stelle wird Bürokratieentlastung erreicht und ein Impuls zur Vereinheitlichung der Anforderungen für eine Meldung nach Artikel 33 DSGVO gegeben. Außerdem wird mit der neuen Nummer 5 auch Artikel 31 Absatz 3 der NIS-2-Richtlinie Rechnung getragen, nach dem die Aufsichtsbehörden nach der NIS-2-Richtlinie eng mit den Datenschutzaufsichtsbehörden zusammenarbeiten.

Das zur Verfügung stellen der Online Formulare lässt die Verpflichtungen des Bundesamts nach § 7 Absatz 8 und § 61 Absatz 11 BSIG-E unberührt. Die Bündelung der Meldung kann das Bundesamt jedoch in der Prüfung seiner Verpflichtungen nach § 7 Absatz 8 und § 61 Absatz 11 BSIG-E unterstützen.

12. Zu Artikel 1 (§ 43 Absatz 3 BSIG)

Der Bundesrat regt mit Blick auf § 43 Absatz 3 BSIG-E an, Musterverträge, vergleichbar dem EVB-IT, zu schaffen bzw. diese zu ergänzen, damit die IT-Dienstleister der Länder frühzeitig über die Erwartungshaltung und Auflagen des Auftraggebers „Bundesverwaltung“ informiert sind.

Begründung:

Erbringen öffentlich-rechtlich oder privatrechtlich organisierte Stellen im Auftrag des Bundes Leistungen der Informationstechnik, sind die Verträge zur Einhaltung der Voraussetzungen zur Gewährleistung der Informationssicherheit von besonderer Bedeutung. Betroffen von § 43 Absatz 3 BSIG-E können auch IT-Dienstleister der Länder über die Deutsche Verwaltungscloud und den Marktplatz sein, über den künftig auch die Bundesverwaltung Leistungen abrufen kann. Ebenfalls wäre im Bereich des statistischen Verbundes, in dem das Bundesamt entsprechende Aufträge für Statistiken an die Länder erteilt, eine derartige Konstellation zu erwarten.

Musterverträge unterstützen die vorstehend genannten Stellen dabei, sich frühzeitig auf die Anforderungen dieses Auftraggebers einzustellen.

13. Zu Artikel 1 (§ 44 Absatz 5 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren, in geeigneter Weise den Ländern den Zugriff auf die technischen Richtlinien und Referenzarchitekturen im Sinne des § 44 Absatz 5 BSIG-E unter Wahrung der Vorschriften des Vergaberechts und des Geheimschutzes zu ermöglichen.

Begründung:

Im Sinne einer ganzheitlichen Architektur trägt der Zugriff zur länderübergreifenden Standardisierung bei und kann gleichzeitig dazu dienen, Aufwände in der öffentlichen Verwaltung zu reduzieren.

14. Zu Artikel 1 (§ 55 BSIG)

Der Bundesrat begrüßt das Bestreben der Bundesregierung, die Cybersicherheit im Rahmen der Umsetzung der NIS-2-Richtlinie zu erhöhen. Es wird jedoch auf die Notwendigkeit hingewiesen, die Transparenz von Sicherheitseigenschaften von verbrauchernahen Produkten mit digitalen Elementen bereits beim Kauf für Verbraucherinnen und Verbraucher zu verbessern. Die Bundesregierung wird daher um Prüfung einer Erweiterung des BSI-Sicherheitskennzeichens gebeten mit dem Ziel, dass

a) das BSI-Sicherheitskennzeichen auch Fragen des Datenschutzes berücksichtigt,

b) eine Ausweitung des Produktkatalogs auf alle verbrauchernahen Produkte und Dienstleistungen mit digitalen Elementen erfolgt und

c) das BSI-Sicherheitskennzeichen um eine Skala (in Sternen) erweitert wird, die eine einfache und intuitive Botschaft zur Sicherheit des Produktes mit digitalen Elementen transportiert, um insbesondere weniger digitalaffine Verbraucherinnen und Verbraucher bei ihrer Kaufentscheidung zu unterstützen und das IT-Sicherheitsniveau in der Gesellschaft insgesamt weiter zu erhöhen.

Begründung:

Eine Erweiterung des IT-Sicherheitskennzeichens könnte die Transparenz von Sicherheitseigenschaften von verbrauchernahen Produkten mit digitalen Elementen erhöhen und würde es Verbraucherinnen und Verbrauchern erleichtern, eine informierte Kaufentscheidung zu treffen. Unter anderem könnte der statische Teil des IT-Sicherheitskennzeichens um eine Skala ergänzt werden, die es Verbraucherinnen und Verbrauchern ermöglicht, direkt zu erkennen, wie sicher ein Produkt im Vergleich zu anderen ist. Dies ist vor allem vor dem Hintergrund notwendig, dass Verbraucherinnen und Verbraucher nach einer Studie zum Thema „Untersuchung zum Thema Verbrauchersicherheitswissen und -verhalten im Digitalen Raum“ (2022) (abrufbar unter https://www.conpolicy.de/data/user_upload/Pdf_von_Publikationen/studie-des-din-vr-zu-verbrauchersicherheitswissen-und-verhalten-im-digitalen-raum--data.pdf) teilweise dem statischen Teil des IT-Sicherheitskennzeichens eine Sicherheitsgarantie entnehmen, die das Zeichen tatsächlich nicht gibt.

15. Zu Artikel 1 (§ 56 Absatz 4, § 62 BSIG)

a) Der Bundesrat begrüßt grundsätzlich die im Gesetzentwurf vorgesehenen Regelungen zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundsätze des Informationssicherheitsmanagements in der Bundesverwaltung.

b) Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob neben dem anhand branchenspezifischer Schwellenwerte festzusetzenden Versorgungsgrad, weitere Kriterien in Ergänzung zu der Rechtsverordnung zur Bestimmung Kritischer Anlagen beziehungsweise Kritischer Dienstleistungen festzulegen sind.

c) Bei der vorgesehenen Umsetzung der NIS-2-Richtlinie in nationales Recht handelt es sich um einen wichtigen nächsten Schritt hin zu einer kohärenten Gesetzgebung zum Schutz der kritischen Infrastruktur. Wichtige und besonders wichtige Einrichtungen sollen vor Schäden durch Cyberangriffe geschützt und das Funktionieren des europäischen Binnenmarktes verbessert werden.

d) Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob die Frist zur Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in § 61 Absatz 1 BSIG-E genannten Verpflichtungen wie sie in § 61 Absatz 3 Satz 5 BSIG-E für Krankenhäuser vorgesehen ist, auch für wichtige Einrichtungen im Bereich des Gesundheitssektors gemäß der Bestimmung in § 28 Absatz 2 Nummer 3 BSIG-E vorgesehen und in die Regelung des § 61 BSIG-E aufgenommen werden kann.

Begründung:

Zu Buchstaben a und b:

Grundsätzlich sollte der vorliegende Gesetzentwurf auch die stetig steigende Sicherheitsbedrohung für die Krankenhäuser durch die zunehmende Digitalisierung des öffentlichen Lebens sowie der Wirtschaft sachgerecht abbilden. In jüngster Vergangenheit sahen sich auch vermehrt Krankenhäuser einer steigenden Sicherheitsbedrohung durch Hackerangriffe auf ihre IT- Infrastruktur ausgesetzt.

Es wird jedoch das Risiko gesehen, dass nach dem vorliegenden Gesetzentwurf die weit überwiegende Zahl der Krankenhäuser zumindest in Nordrhein-Westfalen nicht vom Anwendungsbereich dieses Gesetzes umfasst sind und somit der bestehenden Sicherheitsbedrohung keine Rechnung getragen werden

würde.

Zwar sieht § 56 Absatz 4 BSIG-E die Festsetzung der als kritisch anzusehenden Dienstleistungen beziehungsweise kritischen Anlagen anhand eines branchenspezifischen Schwellenwerts vor, jedoch bildet alleine ein solcher Schwellenwert die Bedeutung gerade von Krankenhäusern im ländlichen Raum nur unzureichend ab. Aufgrund des engen Zusammenhangs zum KRITIS-DachG sowie aufgrund des Artikels 30 des Gesetzentwurfs, ist derzeit davon auszugehen, dass der Schwellenwert für den Krankenhausbereich – wie auch im KRITIS-DachG – bei 500 000 zu versorgenden Einwohnern liegen wird. Mit Blick auf die besondere Stellung der Daseinsvorsorge im Gesundheitsbereich sind die Schwellenwerte grundsätzlich zu hinterfragen. Es wird daher gebeten, die Sinnhaftigkeit der alleinig entscheidenden Schwellenwerte vor diesem Hintergrund erneut zu prüfen.

Zu Buchstaben c und d:

Der Gesetzentwurf dient der Umsetzung der NIS-2-Richtlinie und der Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Entsprechend der unionsrechtlichen Vorgaben wird der mit dem IT-Sicherheitsgesetz und dem IT-Sicherheitsgesetz 2.0 geschaffene Ordnungsrahmen durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz auf den Bereich bestimmter Unternehmen erweitert, zusätzlich werden entsprechende Vorgaben für die Bundesverwaltung eingeführt.

Schwerpunktmäßig wird eine Novellierung des BSI-Gesetzes vorgenommen. Dabei sollen die Vorgaben der NIS-2-Richtlinie 1:1 im Bereich Wirtschaft umgesetzt werden. Dadurch erweitert sich der Kreis der Unternehmen, die Risikomanagementmaßnahmen im Bereich der IT-Sicherheit und Meldepflichten bei IT-Sicherheitsvorfällen zu erfüllen haben.

Für den Bereich des Gesundheitswesens könnten künftig große Praxen, Berufsausübungsgemeinschaften (BAG) und Medizinische Versorgungszentren (MVZ) von den Vorschriften zu den kritischen Sektoren betroffen sein, wenn sie eines von zwei Kriterien erfüllen

- mindestens 50 Mitarbeiter oder
- über zehn Millionen Euro Jahresumsatz.

Davon könnten große ambulante Einrichtungen, umsatzstarke Praxen aus der Radiologie und Nuklearmedizin, Nephrologie oder Laboratoriumsmedizin betroffen sein (§ 28 Absatz 2 Nummer 3 BSIG-E).

Auf diese Einrichtungen kommen mit dem Gesetzentwurf neue Pflichten zu.

§ 61 BSIG-E beschreibt die Vorgehensweise gegenüber besonders wichtigen Einrichtungen. Zudem bestehen auch für bestimmte besonders wichtige Einrichtungen Ausnahmen betreffend die Umsetzungspflicht. So schreibt § 61 Absatz 3 Satz 5 BSIG-E fest, dass für Krankenhäuser nach § 108 SGB V eine Übergangsfrist von fünf Jahren nach Inkrafttreten des Gesetzes zur Vorlage von Nachweisen anzunehmen ist.

In Anbetracht der auch auf die wichtigen Einrichtungen mit dem Gesetzentwurf zukommenden Verpflichtungen wird die Notwendigkeit gesehen, eine entsprechende Übergangfrist auch für diese in § 62 BSIG-E vorzusehen.

Aus den vorgesehenen Verpflichtungen können sich weitere Aufwände und Kosten für die betroffenen Einrichtungen ergeben, die bisher nicht einkalkuliert sind. Der Umsetzungs- und Dokumentationsaufwand für die gesetzlich vorgeschriebenen Maßnahmen ist nicht unerheblich. Betroffene Einrichtungen, die erst jetzt beginnen, sich mit NIS-2-Vorschriften zu befassen, werden die Umsetzungsfrist ggf. nicht mehr einhalten können.

Zudem müssten diese Ausnahmetatbestände doch erst recht für (weniger) wichtige Einrichtungen gelten.

16. Zu Artikel 1 (Anlage 1 Nummer 5.2.1 Spalte D BSIG)

In Artikel 1 sind in Anlage 1 Nummer 5.2.1 Spalte D die Wörter „Unternehmen, die Abwasser nach § 2 Absatz 1 AbwAG“ durch die Wörter „Abwasserbeseitigungspflichtige im Sinne von § 56 WHG, die Abwasser“ zu ersetzen.

Begründung:

In der NIS-2-Richtlinie Artikel 1 § 2 wird in der Begriffsdefinition der Begriff Unternehmen nicht definiert. Die Auslegung des Begriffes Unternehmen kann dementsprechend sehr weitläufig gefasst werden. Entsprechend des Statistischen Bundesamtes wird ein Unternehmen als „[…] kleinste rechtlich selbstständige Einheit definiert, die aus handels- bzw. steuerrechtlichen Gründen Bücher führt und eine jährliche Feststellung des Vermögensbestandes bzw. des Erfolgs der wirtschaftlichen Tätigkeit vornehmen muss. […]“ (siehe: https://www.destatis.de/DE/Themen/ Branchen-Unternehmen/Handwerk/Glossar/unternehmen.html). In der Anlage 1 werden die Sektoren besonders wichtiger und wichtiger Einrichtungen aufgeführt. Hierbei werden unter Nummer 5.2.1 die Adressaten in der Abwasserbeseitigung bestimmt. Jedoch wird mit Verweis auf „§ 2 Absatz 1 AbwAG“ lediglich der Begriff „Abwasser“ an sich definiert. Da in jedem Unternehmen Abwasser anfällt und gesammelt wird (Regen- wie Sanitärabwasser), wird der Adressatenkreis überproportional erweitert. Entsprechend der Definition vom Statistischen Bundesamt kann hierunter z. B. auch ein Kleingartenverein oder Straßenbaulastträger fallen. Zielführender ist es, die Abwasserbeseitigungspflichtigen gemäß § 56 WHG direkt zu adressieren. Die gewählte Formulierung dient auch der einheitlichen Darstellung der Anlage 1 Nummer 5.