Deutscher Bundestag **Drucksache 21/2072**

21. Wahlperiode

(zu Drucksache 21/1501)
08.10.2025

Unterrichtung

durch die Bundesregierung

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

– Drucksache 21/1501 –

Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung

Stellungnahme des Bundesrates

Der Bundesrat hat in seiner 1057. Sitzung am 26. September 2025 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. Zum Gesetzentwurf allgemein:

   Der Bundesrat erinnert an Ziffer 1 seiner Stellungnahme vom 27. September 2024 in BR-Drucksache 380/24 (Beschluss) und bittet, in den Entwurf des Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung insbesondere aufzunehmen:

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

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

   Der Bundesrat bittet ferner darum im weiteren Gesetzgebungsverfahren Festlegungen zu treffen, unter welchen Voraussetzungen Domänen bei Missbrauch blockiert werden können.

   Begründung:

   Der Bundesrat hat sich in Ziffer 1 seiner Stellungnahme vom 27. September 2024 in BR-Drs. 380/24 (Beschluss) anlässlich des Entwurfs für ein NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz für Regelungen ausgesprochen, mit denen zum Schutz von Verbraucherinnen und Verbrauchern die Hürden für sogenannte Fake-Shops mit „.de-Domains“ erhöht und Instrumente zur leichteren Aufdeckung und Unterbindung missbräuchlicher Aktivitäten geschaffen werden sollten. Die Bundesregierung hat in ihrer Gegenäußerung in BT-Drucksache 20/13184 zwar die Berechtigung der Anliegen anerkannt, jedoch diese nach nunmehr fast einem Jahr auch im vorliegenden Gesetzentwurf nicht berücksichtigt. Daher sollen sie wieder aufgegriffen werden.

Zu Buchstabe a:

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 (z. B. 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. Zu Artikel 1 (§ 3 Absatz 1 Nummer 18 Buchstabe a, b BSIG)

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

a) In Buchstabe a ist nach der Angabe „Bundes“ die Angabe „und der Länder“ einzufügen.

b) In Buchstabe b ist die Angabe „des Bundesamtes für Verfassungsschutz“ durch die Angabe „der Verfassungsschutzbehörden des Bundes und der Länder“ sowie die Angabe „dem Bundesverfassungsschutzgesetz“ durch die Angabe „den Verfassungsschutzgesetzen des Bundes und der Länder“ zu ersetzen.

Begründung:

Mit dieser Änderung wird die in der geltenden Fassung des BSIG bestehende Aufgabe des BSI aufrechterhalten, 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, die bei 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 bei der Beobachtung sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten anfallen.

Der vorliegende Gesetzentwurf des Bundes sieht dagegen vor, diese Unterstützungsleistung künftig auf die Bundesbehörden zu beschränken. Die Möglichkeit der Amtshilfe bleibt ausweislich der Entwurfsbegründung 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 vorliegend beabsichtigte 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.

3. Zu Artikel 1 (§ 3 Absatz 1 Nummer 20 BSIG)

In Artikel 1 § 3 Absatz 1 Nummer 20 ist nach der Angabe „Bundesverwaltung“ die Angabe „ , die Länder“ einzufügen:

Begründung:

Ausweislich der Einzelbegründung führt § 3 Absatz 1 Nummer 20 BSIG-E den bisherigen § 3 Absatz 1 Satz 2 Nummer 14 fort. Daher sollte die Möglichkeit der Leistung von Amtshilfe des Bundesamtes gegenüber den Ländern weiterhin ausdrücklich geregelt bleiben.

4. Zu Artikel 1 (§ 5 Absatz 2 Satz 2 BSIG)

In Artikel 1 § 5 Absatz 2 Satz 2 ist nach der Angabe „Meldemöglichkeiten“ die Angabe „ , einschließlich eines medienbruchfrei digitalisierten Meldeverfahrens in der Online-Plattform für den Informationsaustausch nach § 6 Absatz 1,“ einzufügen.

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.

Die in § 5 Absatz 2 Satz 5 BSIG-E normierten „geeigneten Meldemöglichkeiten“ müssen entsprechend § 1a OZG digital angeboten werden. Darüber hinaus sollte das Verfahren jedoch auch durchgehend medienbruchfrei in einem Ende-zu-Ende digitalisierten Verfahren und integriert mit der in § 6 BSIG-E geregelten Informationsplattform realisiert werden.

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

Artikel 1 § 6 ist wie folgt zu ändern:

a) Absatz 1 ist durch den folgenden Absatz 1 zu ersetzen:

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

b) Nach Absatz 2 ist der folgende Absatz 3 einzufügen:

„(3) Die Online-Plattform nach Absatz 1 ermöglicht in geeigneter Weise zugleich Zugang zu Informationen zur physischen 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.

Um den Unternehmen Planungssicherheit zu geben, ist eine klare Vorgabe hinsichtlich der Frist wünschenswert, mit der die Informationsplattform zur Verfügung gestellt werden muss.

Bei den in der Informationsplattform bereitgestellten Inhalten weicht der Gesetzentwurf vom Wortlaut der

Richtlinie ab und lässt beispielsweise die für die Unternehmen wichtigen Kompromittierungsindikatoren und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten unerwähnt. Gerade weil diese Themen in der Begründung sehr wohl erwähnt werden, erscheint ihre Auslassung im Gesetzestext unverständlich. Daher sollte die Vorschrift entsprechend ergänzt werden.

Ferner sollte klargestellt werden, dass Betroffene mit berechtigtem Interesse Zugang erhalten, soweit keine übergeordneten Bedenken entgegenstehen. Genauere Bestimmungen können dann vom BSI im Rahmen der Teilnahmebedingungen gemäß § 6 Absatz 2 BSIG-E geregelt werden.

Die Aufnahme der Länder dient der Sicherstellung effizienter Informationsflüsse zwischen den zuständigen Behörden des Bundes und der Länder.

Eine solche gesetzliche Klarstellung dient nicht nur der Transparenz und Nach-vollziehbarkeit behördlicher Kommunikationsprozesse, sondern ist auch im Hinblick auf die Anforderungen der NIS-2-Richtlinie geboten.

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. Eine entsprechende Klarstellung würde eine leider auch in den unionsrechtlichen Grundlagen bestehende Lücke schließen.

6. Zu Artikel 1 (§ 8 Absatz 6 Satz 1, 2, Absatz 7 Satz 1 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren eine Änderung der in § 8 Absatz 6 Satz 1 und 2 sowie in Absatz 7 Satz 1 BSIG-E enthaltenen Kann-Bestimmungen in Soll-Bestimmungen zu prüfen.

Begründung:

Zu begrüßen ist, dass mit der Neufassung des BSIG die Voraussetzungen in § 8 Absatz 6 Satz 1 BSIG-E für eine Übermittlung der in § 8 Absatz 4 BSIG-E verwendeten personenbezogenen Daten an die Strafverfolgungsbehörden ausgeweitet werden, indem die Übermittlung nicht mehr wie bisher auf mittels eines Schadprogramms begangene Straftaten nach den §§ 202a, 202b, 303a oder 303b StGB beschränkt wird, sondern auch solche Straftaten nach den §§ 202a, 202b, 303a oder 303b StGB in Betracht kommen, die im Rahmen einer sonstigen erheblichen Gefahr für die Kommunikationstechnik des Bundes begangen werden.

Der Gesetzentwurf hält aber in § 8 Absatz 6 Satz 1 und 2 sowie in Absatz 7 Satz 1 BSIG-E daran fest, dass die Übermittlung in das Ermessen des BSI gestellt wird („kann“), obwohl Anhaltspunkte für Straftaten bzw. bestehende Gefahren vorhanden sind.

Es sollte im weiteren Gesetzgebungsverfahren geprüft werden, ob die Kann-Bestimmung in eine Soll-Bestimmung geändert wird, sodass bei Vorliegen entsprechender Erkenntnisse im Regelfall eine Information der Strafverfolgungsbehörden bzw. der genannten Nachrichtendienste erfolgt. Denn der Staat und staatliche Einrichtungen sollten mit gutem Beispiel vorangehen und bei Cyberangriffen im Regelfall die Strafverfolgungsbehörden- bzw. die genannten Nachrichtendienste informieren, so dass diese zur Strafverfolgung, Gefahrenabwehr bzw. im nachrichtendienstlichen Aufgabenbereich tätig werden können. Nur durch eine zuverlässige Weitergabe vorhandener Informationen kann sichergestellt werden, dass die Aufgabenerfüllung im Bereich der Strafverfolgung und der Gefahrenabwehr sowie die nachrichtendienstliche Aufgabenstellung vollständig wahrgenommen werden kann. Für den Bereich des Verfassungsschutzes würde die Regelungslage außerdem der Regelung in § 18 Absatz 1 Satz 1 BVerfSchG angenähert. Außerdem beinhaltet eine Soll-Vorschrift auch ein Signal gegenüber Unternehmen und Bürgerinnen und Bürgern, hier ebenso vorzugehen und die für die Strafverfolgung und Gefahrenabwehr zuständigen Behörden bzw. die Nachrichtendienste zu informieren. Dies sollte deshalb im Gesetzeswortlaut selbst zum Ausdruck kommen.

Gleiches gilt für die in § 8 Absatz 7 Satz 1 BSIG-E enthaltene Kann-Bestimmung. Wenn die in den Nummer 1 bis 4 der Vorschrift enthaltenen hohen Schwellen für eine Übermittlung der Daten nach § 8 Absatz 4 Satz 1 BSIG-E für sonstige Straftaten, Gefahren bzw. nachrichtendienstlich relevante Sachverhalte erreicht sind, sollte im Regelfall eine Übermittlung erfolgen und diese nicht in das Ermessen des BSI gestellt sein. Hierdurch wird auch der Richtervorbehalt bzw. die notwendige Anordnung des Bundesministeriums des Innern nicht tangiert, da sich die Änderung darauf bezieht, ob sich das BSI überhaupt für eine Übermittlung entscheidet und dann die notwendige Entscheidung hierfür herbeiführt.

7. Zu Artikel 1 (§ 28 Absatz 5 Satz 4 BSIG)

In Artikel 1 § 28 Absatz 5 Satz 4 ist die Angabe „vernachlässigbar ist“ durch die Angabe „eine Nebentätigkeit darstellt“ zu ersetzen.

Begründung:

Mit der Änderung soll eine Doppelregulierung für Anlagen verhindert werden, bei denen die Energieerzeugung lediglich ein Nebenzweck im Rahmen anderer Tätigkeiten darstellt. Eine solche Doppelregulierung würde keinen sicherheitsrelevanten Mehrwert bieten.

Mit der Änderung in Satz 4 wird insofern klargestellt, dass im Fall, dass der Betrieb einer Energieanlage als Geschäftstätigkeit nach Satz 1 Nummer 2 im Hinblick auf die gesamte Geschäftstätigkeit eine Nebentätigkeit darstellt, eine Regulierung nach dem EnWG entfällt und weiterhin das BSIG-E anwendbar bleibt. Eine Nebentätigkeit ist dabei weiter zu verstehen, als eine vernachlässigbare Geschäftstätigkeit nach § 28 Absatz 3 BSIG-E. Beispielhaft dafür sind im Regelfall die Energieanlagen der thermischen Abfallbehandlungsanlagen und Biovergärungsanlagen. Auch Klärwerke mit kleinen, aber nicht vernachlässigbaren PV-Anlagen würden darunterfallen.

8. Zu Artikel 1 (§ 28 Absatz 9 Nummer 2 BSIG)

In Artikel 1 § 28 Absatz 9 Nummer 2 ist die Angabe „unter Bezugnahme auf diesen Absatz“ zu streichen.

Begründung:

Nach Maßgabe des § 28 Absatz 1 Satz 1 Nummer 4 und Absatz 2 Satz 1 Nummer 3 BSIG-E sollen bestimmte natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft dem BSIG-E unterfallen. Hiervon dürfen die Länder nur unter den Voraussetzungen des § 28 Absatz 9 BSIG-E Ausnahmen zulassen. Dieser Absatz 9 basiert auf einem von Seiten der Länder eingebrachten Vorschlag, den der Bund zwar aufgenommen, aber zu ihrem Nachteil verändert hat. So müssen die Länder diesen Absatz 9 bei der abweichenden Gesetzgebung, deren Inhalt ihnen in der Vorschrift immerhin ebenfalls bundesrechtlich vorgegeben wird, zitieren. Dies schränkt sie bereits in ihrer Abweichungsmöglichkeit ein.

Zudem soll § 28 BSIG-E der Umsetzung von Artikel 3 der NIS-2-Richtlinie dienen. Diese war nach Artikel 41 Absatz 1 der NIS-2-Richtlinie bis zum 17. Oktober 2024 umzusetzen. Das BMI teilte am 9. Dezember 2024 mit, dass „die Vorgaben der NIS-2-Richtlinie … nach der Kompetenzordnung des Grundgesetzes durch [den] Bund und im Rahmen der jeweils bestehenden Zuständigkeit [durch die Länder] eigenverantwortlich umzusetzen [seien].“ Hinsichtlich der öffentlichen Unternehmen ist dabei zu berücksichtigen, dass der Bund nur über den Umfang der eigenen wirtschaftlichen Betätigung und den Status der eigenen Unternehmen befinden darf (Püttner, Die öffentlichen Unternehmen, 1985, S. 147). Wenn der Bund diese Einrichtungen nicht zu dem überwiegenden Zweck errichtet hat, im öffentlichen Auftrag Leistungen für die Verwaltungen von Ländern und Kommunen zu erbringen, ist er konsequenterweise auch nicht für die Umsetzung der NIS-2-Richtlinie im Hinblick auf diese Einrichtungen zuständig. Dementsprechend soll insbesondere § 46 Absatz 5 BSIG-E sicherstellen, dass lediglich Einrichtungen der Bundesverwaltung, die vom Anwendungsbereich der Umsetzung der NIS-2-Richtlinie zu erfassen sind, nicht von den Verpflichtungen der NIS-2-Richtlinie ausgenommen werden können. Eines solchen Zitiergebots bedarf es vor diesem Hintergrund nicht.

Vor allem wird der Sinn und Zweck der Regelung im Hinblick auf die Verpflichtungen der NIS-2-Richtlinie und die Grundsätze der Lastentragung auch ohne das Zitiergebot erreicht. Auch zur Vermeidung der negativen Folgen des laufenden Vertragsverletzungsverfahrens haben zahlreiche Länder bereits NIS-2-Umsetzungen auf den Weg gebracht. Ein solches Zitiergebot würde nicht zuletzt diejenigen Länder bestrafen, die bereits vergleichbare Regelungen erlassen haben und diese nun zum Beispiel in einem erneuten parlamentarischen Verfahren aufwändig ändern müssten. In diesem Zusammenhang ist im Bund-Länder-Verhältnis auch der Aufwand, den das Zitiergebot verursachen würde, unangemessen.

Die Voraussetzung, § 28 Absatz 9 BSIG-E explizit zu zitieren, ist deshalb zu streichen.

9. Zu Artikel 1 (§ 30 Absatz 3 Satz 2 – neu – BSIG)

Nach Artikel 1 § 30 Absatz 3 ist der folgende Satz einzufügen:

„Dies gilt nicht für Managed Service Provider und Managed Security Service Provider, wenn diese Tätigkeit im Hinblick auf die gesamte Geschäftstätigkeit dieser Einrichtung eine Nebentätigkeit darstellt."

Begründung:

Die Änderung soll eine zu erwartende übermäßige bürokratische Belastung ohne sicherheitsrelevanten Mehrwert vermeiden. Die im Gesetzentwurf vorgesehenen Regelungen würden auch Unternehmen in Gänze berühren, bei denen der eigentlich zu regulierende Bereich nur eine Nebentätigkeit darstellt.

10. Zu Artikel 1 (§ 30 Absatz 8 Satz 3, § 56 Absatz 4 Satz 1, § 56a – neu – BSIG)

Artikel 1 ist wie folgt zu ändern:

a) In § 30 Absatz 8 Satz 3 ist die Angabe „gewährleisten und" durch die Angabe „gewährleisten," zu ersetzen und nach der Angabe „Internetseite" die Angabe „und informiert hierüber die Länder" einzufügen.

b) In § 56 Absatz 4 Satz 1 ist die Angabe „nicht" zu streichen.

c) Nach § 56 ist der folgende § 56a einzufügen:

„§ 56a

Den Ländern und den Kommunen werden die durch die Rechtsverordnungen des Bundes entstehenden Kosten erstattet."

Begründung:

Die Bestimmung besonders wichtiger sowie wichtiger Einrichtungen im Gesetzentwurf orientiert sich im § 28 an den durch die Kommission definierten Größenordnungen von großen, mittleren und kleinen Betrieben. In § 30 Absatz 8 soll besonders wichtigen Einrichtungen und ihren Branchenverbänden erlaubt werden, branchenspezifische Sicherheitsstandards zur Gewährleistung der gestellten Anforderung vorzuschlagen. Der Bund kann gemäß § 56 Absatz 4 per Rechtsverordnung kritische Dienstleistungen und damit kritische Anlagen bestimmen. Diese stufenweise Konkretisierung des Gesetzeszweckes ist sinnvoll, aber bedarf wegen der vielfältigen Betroffenheiten der Länder und der Kommunen ihrer Einbindung, Mitbestimmung und Kostenerstattung.

11. Zu Artikel 1 (§ 32 Absatz 5 BSIG)

In Artikel 1 § 32 Absatz 5 ist nach der Angabe „Bundes" die Angabe „und den für Gefahrenabwehr- und Strafverfolgung originär zuständigen Behörden der Länder" einzufügen.

Begründung:

Der Gesetzentwurf sieht in § 32 BSIG-E keine Verpflichtung für besonders wichtige und wichtige Einrichtungen vor, die Straftat gegenüber den originär zuständigen polizeilichen Gefahrenabwehr- und Strafverfolgungsbehörden der Länder anzuzeigen. Ebenso wenig sind zu Cyberangriffen Meldepflichten der Bundesbehörden gegenüber den Landesbehörden bestimmt. Durch diese nicht berücksichtigten Informations- und Meldepflichten werden die Länder nicht unerheblich bei der Wahrnehmung ihrer originären Zuständigkeit zur Gefahrenabwehr und Strafverfolgung, sofern diese im Einzelfall nicht gemäß § 4 BKAG beim Bundeskriminalamt liegt, beschnitten.

Bei Cyberangriffen auf wichtige und besonders wichtige Einrichtungen besteht die Gefahr, dass diese der Polizei nicht oder erst verzögert bekannt werden, so dass Schadensbegrenzung und Tataufklärung wesentlich erschwert oder verhindert würden.

12. 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 die Angabe „aktualisieren und“ durch die Angabe „aktualisieren,“ zu ersetzen.

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

c) Nach Nummer 4 ist die folgende Nummer 5 einzufügen:

„5. besonders wichtigen und wichtigen Einrichtungen zur Erfüllung ihrer Meldepflicht nach Artikel 33 der Verordnung (EU) 2016/679 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 und diese Informationen unverzüglich den zuständigen Datenschutzaufsichtsbehörden zur Verfügung zu stellen.“

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 NIS2-Richtlinie (RL (EU) 2022/2555) nicht aufgegriffen. Danach soll der Verwaltungsaufwand für Einrichtungen verringert werden. Insbesondere wird den Mitgliedstaaten nahegelegt, die zentrale Anlaufstelle auch für Meldungen zu nutzen, die nach der DSGVO (VO (EU) 2016/679) erforderlich sind.

Durch die Verpflichtung des BSI, Online-Formulare für Meldungen nach Artikel 33 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 DSGVO an das BSI besteht dann, wenn die Einrichtung eine Meldung nach § 32 BSIG-E an das BSI 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 NIS2-Richtlinie Rechnung getragen, nach dem die Aufsichtsbehörden nach der NIS2-Richtlinie eng mit den Datenschutzaufsichtsbehörden zusammenarbeiten. Die Zurverfügungstellung 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 BSI jedoch in der Prüfung seiner Verpflichtungen nach § 7 Absatz 8 und § 61 Absatz 11 BSIG-E unterstützen.

Die vorherige Bundesregierung hat diesen Vorschlag mit unzutreffenden Argumenten abgelehnt. Dabei hat sogar der für die DSGVO zuständige Referatsleiter bei der Europäischen Kommission in einer Veranstaltung explizit darauf hingewiesen, dass die Mitgliedstaaten diese Möglichkeit zur Verfahrensvereinfachung nutzen sollten. Anders als von der Bundesregierung damals in der Gegenäußerung (vgl. BT-Drucksache 20/13184, S. 200) behauptet, steht Artikel 33 DSGVO der hier vorgeschlagenen Änderung nicht entgegen. Die Änderung zielt vielmehr darauf ab, die Vorgaben von Artikel 33 DSGVO zu erfüllen. Eine Öffnungsklausel in Artikel 33 DSGVO ist für diese nationale Verfahrensregelung nicht erforderlich. Die Änderung ist daher nach wie vor dringend angezeigt. Sie würde einen echten Beitrag zu Verfahrensvereinfachung und Bürokratieabbau leisten.

13. Zu Artikel 1 (§ 40 Absatz 3 Satz 2 – neu – BSIG)

Nach Artikel 1 § 40 Absatz 3 ist der folgende Satz einzufügen:

„Zu den Unterrichtungspflichten des Satzes 1 Nummer 4 Buchstabe d gehören insbesondere Meldungen nach § 32 von Einrichtungen in dem jeweiligen Land.“

Begründung:

Gemäß der vorliegenden Entwurfsbegründung führt Buchstabe d den bisherigen § 8b Absatz 2 Nummer 4 Buchstabe b und c BSIG fort. Der Anwendungsbereich erstreckt sich dabei auf wichtige und besonders wichtige Einrichtungen. Für die Übermittlung von Registrierungsdaten und Vorfallsmeldungen („Rot-Meldungen“) können dabei die bereits im Kontext der bisherigen Regelungen zwischen Bund und Ländern abgestimmten Übermittlungskonzepte weiter Anwendung finden.

Aufgrund der Mehrzahl an Unternehmen, die durch den vorliegenden Gesetzentwurf reguliert werden sollen, ist zum Beispiel aus Sicht des Landes Bremen in den entsprechenden Gremien zu prüfen, inwieweit die bestehenden Übermittlungskonzepte der geänderten geopolitischen Lage noch gerecht werden. Dies betrifft beispielhaft die Häufigkeit der Übermittlung der Registrierungsdaten und deren Umsetzung (z. B. Art und Weise der Übermittlung). Der bisher gewählte Wortlaut des § 40 Absatz 3 Nummer 4 Buchstabe d BSIG-E könnte so ausgelegt werden, dass dem BSI ein gewisses Ermessen obliegt, welche Informationen für die Erfüllung der Aufgaben der zentralen Kontaktstellen der Länder erforderlich sind („Informationsmonopol"). Mit dieser Auslegung wären die Länderinteressen erheblich beeinträchtigt. Durch die Ergänzung des oben aufgeführten Satzes 2 wird dieses Ermessen zumindest für die Meldungen nach § 32 soweit eingeschränkt, dass die entsprechenden Meldungen auch den zentralen Kontaktstellen übermittelt werden müssen.

Daher ist § 40 Absatz 3 BSIG-E um den oben genannten Satz 2 zu ergänzen.

14. Zu Artikel 1 (§ 44 Absatz 2 Satz 4 BSIG)

Artikel 1 § 44 Absatz 2 Satz 4 ist zu streichen.

Begründung:

Die Frist zur Modernisierung und Fortentwicklung „des IT-Grundschutzes" vom absehbar frühestmöglichen Zeitpunkt des Inkrafttretens der Novellierung des BSIG bis zum 1. Januar 2026 ist nicht sachgerecht einhaltbar. Hiervon wären auch die Länder betroffen, die aufgrund der bestehenden rechtsverbindlichen Beschlussfassung des IT-Planungsrates (Informationssicherheitsleitlinie für die öffentliche Verwaltung) ihr Informationssicherheitsmanagement auf Basis der BSI-Standards und der IT-Grundschutz-Methodik aufgebaut haben und betreiben. Die derzeit bereits stattfindende Modernisierung und Fortentwicklung des sogenannten BSI-Kompendiums unter dem Arbeitstitel „Grundschutz++" umfasst nur einen Teil „des IT-Grundschutzes", namentlich die Konsolidierung bestehender Maßnahmen-Bausteine samt deren Überführung in ein maschinenlesbares Format. Weitere zwingend erforderliche Bestandteile „des IT-Grundschutzes" wie etwa eine Fortschreibung der BSI-Standards oder die Festlegung verbindlicher Mindestniveaus fehlen hingegen noch und lassen sich absehbar nicht bis zum 1. Januar 2026 ergänzen. Zudem enthält § 44 Absatz 2 Satz 3 BSIG-E bereits die entsprechende Verpflichtung des BSI: „Der IT-Grundschutz wird durch das Bundesamt regelmäßig evaluiert und entsprechend dem Stand der Technik sowie unter Berücksichtigung der Erfahrungen aus der Praxis und aus der Beratung und Unterstützung nach Absatz 4 fortentwickelt; dabei wird der Umsetzungsaufwand soweit möglich minimiert".

15. Zu Artikel 1 (§ 49 Absatz 3 Satz 3 – neu – BSIG), Artikel 30 (Inkrafttreten)

a) Nach Artikel 1 § 49 Absatz 3 Satz 2 ist der folgende Satz einzufügen:

„Das Überprüfungsverfahren nach Satz 1 beinhaltet eine Identitätsüberprüfung bei Registrierung und Übertragung einer Registrierung entsprechend den Anforderungen nach den §§ 11 und 12 des Geldwäschegesetzes."

b) Artikel 30 ist durch den folgenden Artikel 30 zu ersetzen:

„Artikel 30

Inkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach der Verkündung in Kraft.

(2) Artikel 1 § 49 Absatz 3 Satz 3 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen tritt am 1. Juli 2026 in Kraft."

Begründung:

Zu Buchstabe a:

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 lässt 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 vorgeschlagene Konkretisierung der Überprüfungsverfahren steht im Einklang mit Artikel 28 Absatz 3 der NIS-2-Richtlinie.

Zu Buchstabe b:

Für die Einführung der Identitätsprüfung wird eine Übergangsfrist bis 30. Juni 2026 eingeräumt.

16. 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. Es wird daher darum gebeten, im weiteren Gesetzgebungsverfahren eine Erweiterung des BSI-Sicherheitskennzeichen zu prüfen 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-Sicherheitskennzeichen eine Sicherheitsgarantie entnehmen, die das Zeichen tatsächlich nicht gibt.

17. Zu Artikel 1 (§ 56 Absatz 4 BSIG)

Der Bundesrat stellt fest, dass die Länder im Hinblick auf die Cyber- und Informationssicherheit einer besonderen Bedrohungslage ausgesetzt sind. Zur Gewährleistung eines hohen Sicherheitsniveaus ist es daher unabdingbar, dass den Ländern angemessene Mitwirkungsrechte eingeräumt werden. Hierbei gilt es sicherzustellen, dass die Länder frühzeitig, umfassend und verpflichtend in für sie relevante Entscheidungsprozesse eingebunden werden und die Interessen der Länder somit gewahrt werden können. Die Berücksichtigung dieses Erfordernisses hält der Bundesrat deshalb auch im Rahmen der Ermächtigung zum Erlass von Rechtsverordnungen für geboten. Der vorliegende Gesetzentwurf enthält umfangreiche Ermächtigungen zur Festlegung technischer Detailregelungen sowie von Systematik und Methodik zur Identifizierung von KRITIS. Besonders hervorzuheben ist § 56 Absatz 4 BSIG-E, der dem BMI im Einvernehmen mit den Fachressorts erlaubt, durch Rechtsverordnung kritische Dienstleistungen sowie sektorale Versorgungskennzahlen (Anlagenkategorien und Schwellenwerte) festzulegen. Eine solche Festlegung ist jedoch nur möglich, wenn Erfahrungswerte aus den Ländern hinreichende Berücksichtigung finden. Maßgeblich ist mithin ein Zusammenwirken von Bund und Ländern. Der Bundesrat fordert daher, dass die Länder, vor einem Gebrauchmachen der Verordnungsermächtigung in § 56 BSIG-E, hinreichend informiert und eingebunden werden.

Begründung:

Nach aktuellen Planungen des Bundes sollen die o. g. Detailregelungen durch eine gemeinsame KRITIS-Verordnung erfolgen, die sich auf die Ermächtigungen aus dem BSIG-E und dem KRITIS-Dachgesetz-E stützt. Allerdings sind die geplanten Detailregelungen derzeit weder den Ländern bekannt noch sind deren Auswirkungen auf die Länder abschätzbar. Deshalb ist die Ermächtigung zum Erlass solcher Verordnungen ohne Beteiligung der Länder abzulehnen.

Es wird deshalb eine stärkere Einbindung der Länder in die Festlegung von KRITIS-Detailregelungen sowie die Entwicklung einer einheitlichen, an den tatsächlichen Versorgungssicherheiten orientierten Identifikationsmethodik, die den Schutz Kritischer Infrastrukturen erheblich verbessert, gefordert. Diese Methodik sollte eine Gesamtbetrachtung unter Einbeziehung mehrerer Faktoren vorsehen, wobei der grundlegende Maßstab die tatsächliche Sicherstellung der Versorgung im jeweiligen Bereich sein muss.

Denn die bloße Übernahme der bisherigen Systematik zur KRITIS-Identifizierung mit einem Regelschwellenwert von 500 000 zu versorgenden Personen, wie sie im BSIG-E bzw. der bestehenden BSI-KritisV verankert ist, ist nicht ausreichend. Diese Regelung schließt wesentliche Bereiche Kritischer Infrastrukturen aus und erfüllt somit nicht den tatsächlichen Schutzbedarf.

18. Zu Artikel 1 (§ 62 BSIG)

a) Der Bundesrat begrüßt die mit dem Gesetzentwurf vorgesehene Umsetzung der NIS-2-Richtlinie in nationales Recht. Hierbei 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.

b) 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 § 62 BSIG-E aufgenommen werden kann.

Begründung:

Der Gesetzentwurf dient der Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Entsprechend der unionsrechtlichen Vorgaben wird der mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I 2015, S. 1324) und dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021 (BGBl. I 2021, S. 1122) geschaffene Ordnungsrahmen durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz auf den Bereich bestimmter Unternehmen erweitert, zusätzlich werden entsprechende Vorgaben für die Bundesverwaltung eingeführt.

Schwerpunktmäßig 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
– über zehn Millionen Euro Jahresumsatz.

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

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 gegebenenfalls nicht mehr einhalten können.

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

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

In Artikel 1 Anlage 1 Nummer 5.2.1 Spalte D ist die Angabe „Unternehmen, die Abwasser nach § 54 Absatz 1 WHG“ durch die Angabe „Abwasserbeseitigungspflichtige im Sinne von § 56 WHG, die Abwasser“ zu ersetzen.

Begründung:

Die im aktuellen Gesetzentwurf verwendete Definition von Abwasser gemäß § 54 Absatz 1 WHG, lässt eine breite Branchenbeschreibung und damit einen großen Interpretationsspielraum zu. Die vorgesehene Fassung adressiert zunächst jedes Unternehmen, in dem Abwasser – also Schmutzwasser oder Niederschlagswasser – anfällt und gesammelt wird. Die zu betrachtenden Unternehmen sollten auf die Abwasserbeseitigungspflichtigen eingeschränkt werden, die im § 56 WHG definiert werden. Dies dient der Klarstellung, der Rechtssicherheit und kommt einer möglicherweise ungewollten Ausweitung des Adressatenkreises zuvor.

Vor dem Hintergrund der Kosten, die mit der Umsetzung der Anforderungen an besonders wichtige und wichtige Unternehmen einhergeht, ist eine unbeabsichtigte Ausweitung der Unternehmen zu vermeiden.

Der Antrag knüpft an Ziffer 16 des Bundesratsbeschlusses in der BR-Drucksache 380/24 (Beschluss) an, da mit der im Gesetzesentwurf gemäß Drucksache 369/25 verwendeten Formulierung das seinerzeit intendierte Ziel nicht erreicht wird.

20. Zu Artikel 17 Nummer 2 (§ 5c Absatz 3 Satz 3 Nummer 2a – neu – EnWG)

Nach Artikel 17 § 5c Absatz 3 Satz 3 Nummer 2 ist die folgende Nummer 2a einzufügen:

„2a. die Eigenschaft als eine wichtige Einrichtung, eine besonders wichtige Einrichtung oder als Betreiber einer kritischen Anlage,“.

Begründung:

Die Änderung stellt ausdrücklich klar, dass bei der Erstellung der IT-Sicherheitskataloge die unterschiedlichen Kategorien der betroffenen Unternehmen explizit zu berücksichtigen sind. Diese Klarstellung verhindert eine mögliche Überbürokratisierung und schafft die notwendige Rechtssicherheit durch eindeutige gesetzliche Vorgaben. Grundlegende Entscheidungen über die Ausgestaltung der IT-Sicherheitsanforderungen werden somit nicht vollständig auf die behördliche Ebene verlagert.

Im Bereich des BSIG-E ist bereits klar festgelegt, dass alle drei Stufen der von der NIS-2-Regulierung betroffenen Unternehmen (Betreiber kritischer Anlagen, besonders wichtige Einrichtungen und wichtige Einrichtungen) unterschiedlich und damit risikoangemessen reguliert werden.

Die entsprechende Klarstellung im EnWG stellt sicher, dass dieser dreistufige Ansatz auch in den IT-Sicherheitskatalogen konsequent umgesetzt wird. Die bisher im Gesetz nur angedeutete Differenzierung wir damit eindeutig und rechtssicherer ausgestaltet.

21. Zu Artikel 30 (Inkrafttreten)

Artikel 30 wird durch den folgenden Artikel 30 ersetzt:

„Artikel 30

Inkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach der Verkündung in Kraft.

(2) Artikel 1 gilt für rechtlich unselbstständige Organisationseinheiten von Gebietskörperschaften und juristische Personen, an denen ausschließlich Gebietskörperschaften, ausgenommen der Bund, beteiligt sind, und die zu dem Zweck errichtet wurden, überwiegend im öffentlichen Auftrag Leistungen für Verwaltungen zu erbringen, mit Wirkung vom [einsetzen: Datum des ersten Tages des zwölften auf die Verkündung folgenden Monats].“

Begründung:

Da das Landesrecht nach Artikel 1 (§ 28 Absatz 9 Nummer 2 BISG-E) ausdrücklich auf die Öffnungsklausel Bezug nehmen und vergleichbare Vorschriften vorsehen muss, müssen bestehende oder bereits im parlamentarischen Verfahren befindliche Landesregelungen erneut angepasst werden. Dies ist zum gegenwärtigen Zeitpunkt nicht möglich, da das Landesrecht nicht auf eine noch nicht existierende Norm des Bundesgesetzes Bezug nehmen kann. Dies ist erst möglich, wenn der vorliegende Gesetzentwurf in Kraft getreten ist. Hierzu bedarf es einer Übergangsfrist von mindestens zwölf Monaten, in denen das Bundesgesetz keine Anwendung auf die in der Öffnungsklausel genannten Einrichtungen in den Ländern findet. Diesen Zeitraum benötigen die Länder, um dem in § 28 Absatz 9 Nummer 2 BISG-E genannten expliziten Bezug auch landesrechtlich Rechnung tragen und ein entsprechendes parlamentarisches Verfahren in den Ländern durchführen zu können. Dafür ist Artikel 30 entsprechend anzupassen.

Gegenäußerung der Bundesregierung

Die Bundesregierung äußert sich zur Stellungnahme des Bundesrates wie folgt:

Zu Nummer 1. [Zum Gesetzentwurf allgemein]

Die Bundesregierung lehnt den Vorschlag für dieses Gesetzgebungsverfahren ab.

Die Bundesregierung teilt die Einschätzung, dass die Bekämpfung von Fake-Shops im Interesse der Verbraucherinnen und Verbraucher wichtig ist. Maßnahmen sollten jedoch eingeordnet werden in die bestehenden Rechtsgrundlagen und Strategien nach Landesrecht, laufende Arbeitsprozesse auf internationaler Ebene und den Empfehlungen der NIS-Kooperationsgruppe. Insbesondere sollten neue Maßnahmen auf ihre Wirksamkeit hin im gesamten Kontext untersucht werden, bevor Regelungen hierzu beschlossen werden. Zu berücksichtigen sind dabei auch die wirtschaftlichen Folgen etwaiger nationaler Eingriffe in die grenzüberschreitenden Strukturen des Domainmarkts für Domaininhaber und die Einrichtungen im Zuständigkeitsbereich des BSI nach § 60 BSIG-E. Aus Sicht der Bundesregierung ist der Vorschlag insoweit noch nicht ausgereift und sollte noch entsprechend ergänzend ausgearbeitet, unter Einbeziehung kriminalistischer Erfahrung diskutiert und geprüft werden. Für den anschließenden Bund-Länder-Dialog kommen verschiedene Foren in Betracht und die Bundesregierung sieht einer entsprechenden Initiative der Länder entgegen. Das vorliegende Gesetzgebungsvorhaben gibt dafür leider keine Gelegenheit mehr, denn die Umsetzung der NIS-2-Richtlinie eilt sehr. §§ 49-51 BSIG-E dienen einer 1:1-Umsetzung des Artikels 28 der NIS-2-Richtlinie und sind unverzichtbar, auch um eine EU-weit möglichst harmonisierte Anwendung der Vorschriften des Artikel 28 NIS-2-Richtlinie entlang der Empfehlungen der NIS-Kooperationsgruppe zu gewährleisten.

Zu Nummer 2. [Zu Artikel 1 (§ 3 Absatz 1 Nummer 18 Buchstabe a und b]

Die Bundesregierung lehnt den Vorschlag ab.

Durch die Änderung wird die Möglichkeit zur Leistung von Amtshilfe durch das Bundesamt nicht eingeschränkt. Die bisherige Regelung stellte ohnehin lediglich eine einfachgesetzliche Ausgestaltung der Amtshilfe dar.

Zu Nummer 3. [Zu Artikel 1 (§ 3 Absatz 1 Nummer 20)]

Die Bundesregierung lehnt den Vorschlag ab.

Durch die Änderung wird die Möglichkeit zur Leistung von Amtshilfe durch das Bundesamt nicht eingeschränkt. Die bisherige Regelung stellte ohnehin lediglich eine einfachgesetzliche Ausgestaltung der Amtshilfe dar.

Zu Nummer 4. [Zu Artikel 1 (§ 5 Absatz 2 Satz 2 BSIG)]

Die Bundesregierung lehnt den Vorschlag ab.

Die Meldemöglichkeit nach § 5 Absatz 2 Satz 2 BSIG-E existiert bereits in digitalisierter Form, eine zusätzliche gesetzliche Regelung ist daher nicht notwendig.

Zu Nummer 5. [Zu Artikel 1 (§ 6 Absatz 1, Absatz 3 – neu – BSIG)]

Die Bundesregierung lehnt den Vorschlag ab.

Die in § 6 Absatz 1 BSIG-E genannten Informationen umfassen die des Artikel 29 der NIS-2-Richtlinie (vgl. dazu auch die entsprechende Gesetzesbegründung), insofern wird die Richtlinie vollständig umgesetzt. Die Authentifizierungsmodalitäten für die Online-Plattform zum Informationsaustausch nach § 6 BSIG-E können im Rahmen der Teilnahmebedingungen gemäß § 6 Absatz 2 BSIG-E festgelegt werden.

Eine mögliche Erweiterung des Teilnehmerkreises ist bereits in § 6 Absatz 1 Satz 3 BSIG-E vorgesehen, eine weitere Qualifizierung zusätzlicher Teilnehmer erscheint entbehrlich. Der Austausch von Informationen zur physischen Sicherheit geht über die angestrebte 1:1-Umsetzung der NIS-2-Richtlinie hinaus und ist auch nicht Gegenstand der CER-Richtlinie. Zur Umsetzung der Registrierungs- und Meldevorschriften der NIS-2-Richtlinie sieht der Regierungsentwurf in § 32 Absatz 1 und § 33 Absatz 2 BSIG-E jedoch bereits ein gemeinsames Melde-

portal von BSI und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) vor, das gegebenenfalls zukünftig als Ausgangspunkt für ein solches Angebot dienen kann.

Zu Nummer 6. [Zu Artikel 1 (§ 8 Absatz 6 Satz 1, 2, Absatz 7 Satz 1 BSIG)]

Die Bundesregierung lehnt den Vorschlag ab.

Bei § 8 Absatz 6 bzw. 7 BSIG-E handelt es sich um Bestandsvorschriften der § 5 Absatz 5 bzw. 6 BSIG. Dies sind ebenfalls Ermessensvorschriften mit der Formulierung „kann“. Das BSI benötigt in Abwägung gegenseitiger Interessen von beispielsweise Hinweisgebern maximale Flexibilität bzw. Ermessen zur Entscheidung der Weiterleitung.

Zu Nummer 7. [Zu Artikel 1 (§ 28 Absatz 5 Satz 4 BSIG)]

Die Bundesregierung wird den Antrag prüfen.

Zu Nummer 8. [Zu Artikel 1 (§ 28 Absatz 9 Nummer 2 BSIG)]

Die Bundesregierung lehnt den Vorschlag ab. Eine entsprechende Regelung war bereits Gegenstand des Gesetzentwurfs aus der letzten Legislaturperiode (Artikel 1 § 28 Absatz 8 Nummer 2 des Gesetzentwurfs auf Bundesratsdrucksache 380/24). Eine ausdrückliche Inbezugnahme ist aus Gründen der rechtlichen Klarheit geboten.

Zu Nummer 9. [Zu Artikel 1 (§ 30 Absatz 3 Satz 2 – neu – BSIG)]

Die Bundesregierung lehnt den Vorschlag ab. Die vorgeschlagene Änderung stellt keine richtlinienkonforme Umsetzung der NIS-2-Richtlinie dar.

Zu Nummer 10. [Zu Artikel 1 (§ 30 Absatz 8 Satz 3, § 56 Absatz 4 Satz 1, § 56a – neu – BSIG)]

Die Bundesregierung lehnt den Vorschlag ab.

Zu a)

Die Bundesregierung lehnt den Vorschlag ab. Es wird insoweit auf § 40 Absatz 3 Nummer 4 Buchstabe d) BSIG-E hingewiesen, wonach im Rahmen vorab zwischen dem BSI und den Empfängern abgestimmter Prozesse zur Weitergabe und Wahrung der notwendigen Vertraulichkeit die zu diesem Zweck dem Bundesamt von den Ländern als zentrale Kontaktstellen benannten Behörden des Bundes über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen zu unterrichten hat. Im Übrigen sind die betreffenden Informationen auch für die Länder auf der Internetseite jederzeit abrufbar.

Zu b)

Die Bundesregierung lehnt den Vorschlag ab. Eine sachgerechte Einbindung der Länder ist bereits durch andere Regelungen im BSIG sichergestellt.

Zu c)

Die Bundesregierung lehnt den Vorschlag ab. Auf Artikel 104a GG wird hingewiesen.

Zu Nummer 11. [Zu Artikel 1 (§ 32 Absatz 5 BSIG)]

Die Bundesregierung lehnt den Vorschlag ab. Es wird insoweit auf § 40 Absatz 3 Nummer 4 Buchstabe d) BSIG-G hingewiesen, wonach das BSI im Rahmen vorab zwischen dem BSI und den Empfängern abgestimmter Prozesse zur Weitergabe und Wahrung der notwendigen Vertraulichkeit die zu diesem Zweck von den Ländern als zentrale Kontaktstellen benannten Behörden oder die zuständigen Behörden des Bundes über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen zu unterrichten hat.

Zu Nummer 12. [Zu Artikel 1 (§ 40 Absatz 3 Nummer 5 – neu – BSIG)]

Die Bundesregierung lehnt den Vorschlag ab.

Vorliegend werden vorrangig die NIS-2 Vorgaben umgesetzt. Unbenommen dessen werden Vereinfachungsmaßnahmen – auch vor dem Hintergrund noch laufender europäischer Entwicklungen – in Bezug auf Meldepflichten für Sicherheitsvorfälle und Datenschutzverletzungen geprüft. Eine Konkretisierung der europäischen Abstimmung ist indes abzuwarten.

Zu Nummer 13. [Zu Artikel 1 (§ 40 Absatz 3 Satz 2 – neu – BSIG)]

Die Bundesregierung lehnt den Vorschlag ab. Es wird insoweit auf den Wortlaut von § 40 Absatz 3 Nummer 4 Buchstabe d) BSIG-E hingewiesen, wonach das BSI zur Wahrnehmung seiner Aufgabe als zentrale Meldestelle die von den Ländern als zentrale Kontaktstellen benannten Behörden über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen zu unterrichten „hat“. Eine Beeinträchtigung der Länderinteressen ist insoweit nicht zu erkennen.

Zu Nummer 14. [Zu Artikel 1 (§ 44 Absatz 2 Satz 4 BSIG)]

Die Bundesregierung lehnt den Vorschlag ab. Das BSI hat mit der Modernisierung und Fortentwicklung des IT-Grundschutzes („Grundschutz++“) bereits begonnen und deutliche Fortschritte erreicht. Die Anforderungen des Grundschutz++ sind vollständig aus dem alten IT-Grundschutz überführt und sollen noch 2025 veröffentlicht werden. Auch die Entwicklung der Methodik des Grundschutz++ wird im BSI mit sehr großer Priorität vorangetrieben und erste Ergebnisse wurden bereits präsentiert. Anforderungen und Methodik zu Grundschutz++, aber auch die BSI-Mindeststandards, werden in agiler Arbeitsweise auch nach dem 1. Oktober 2026 sukzessive gepflegt und weiterentwickelt.

Zu Nummer 15. [Zu Artikel 1 (§ 49 Absatz 3 Satz 3 – neu – BSIG), Artikel 30 (Inkrafttreten)]

Die Bundesregierung lehnt den Vorschlag ab. Im Übrigen wird auf die Gegenäußerung der Bundesregierung zu Nummer 1 verwiesen.

Zu Nummer 16. [Zu Artikel 1 (§ 55 BSIG)]

Die Bundesregierung lehnt den Vorschlag ab.

Die Bundesregierung teilt grundsätzlich das Anliegen des Bundesrates, die Transparenz der Sicherheitseigenschaften von verbrauchernahen Produkten mit digitalen Elementen zu erhöhen. In dieser Sache wurden bereits wesentliche Fortschritte erzielt, insbesondere durch die Verabschiedung der Verordnung (EU) 2024/2847 (Cyber Resilience Act – CRA). Der CRA bestimmt erstmals allgemeine Mindestanforderungen an die Cybersicherheit von vernetzten Produkten und ergänzt das CE-Kennzeichen um den Aspekt der Cybersicherheit. Das bedeutet, dass Verbraucherinnen und Verbraucher ab Dezember 2027 bei Kauf eines vernetzen Produktes mit einem Blick erkennen können, dass das Produkt auch unter Cybersicherheitsgesichtspunkten geprüft wurde.

Zu a)

Der Vorschlag einer Berücksichtigung von Fragen des Datenschutzes bei der Vergabe des IT-Sicherheitskennzeichens wird seitens der Bundesregierung als nicht zielführend bewertet. Das IT-Sicherheitskennzeichen wurde bewusst mit dem Fokus auf IT-Sicherheit entwickelt. Das IT-Sicherheitskennzeichen soll den Herstellern eine Hilfestellung bei der Erfüllung der Schutzziele des CRA bieten. Eine Aufnahme des Datenschutzes entspricht nicht dieser Zielsetzung.

Zu b)

Das BSI arbeitet stetig an der Ausweitung des Produktkatalogs. Für die Aufnahme von neuen Produkt- und Dienstleistungskategorien bedarf es aber der Verfügbarkeit von angemessenen IT-Sicherheitsanforderungen sowie korrespondierender Prüfspezifikationen. Die Entwicklung dieser Anforderungen und Spezifikationen ist zeitintensiv, so dass eine Ausweitung nur sukzessive und nicht sogleich für alle verbrauchernahen Produkte erfolgen kann.

Zu c)

Der Evaluierungsbericht zum IT-Sicherheitskennzeichen spricht sich bereits für eine Mehrstufigkeit des IT-Sicherheitskennzeichens, etwa in Form einer Skala, aus. Einer gesetzlichen Änderung bedarf es nicht, um diese einzuführen. Bei den weiteren Prüfungen wird abzuwägen sein, ob der mögliche Mehrwert in einem angemessenen Verhältnis zum erwartbaren Aufwand steht. Zudem muss eine Überfrachtung des IT-Sicherheitskennzeichens vermieden werden, um dessen Aussagekraft für die Verbraucherinnen und Verbraucher zu wahren.

Zu Nummer 17. [Zu Artikel 1 (§ 56 Absatz 4 BSIG)]

Die Bundesregierung lehnt den Vorschlag ab. Eine sachgerechte Einbindung der Länder ist bereits durch andere Regelungen im BSIG-E sichergestellt.

Zu Nummer 18. [Zu Artikel 1 (§ 62 BSIG)]

Die Bundesregierung begrüßt die Ausführung zu a) und lehnt den Vorschlag zu b) ab.

Wie in Artikel 33 der NIS-2-Richtlinie vorgesehen, gilt für wichtige Einrichtungen eine ex post-Aufsicht. So kann das BSI bei einer wichtigen Einrichtung z.B. im Fall des Auftretens eines IT-Sicherheitsvorfalls die Einhaltung der gesetzlichen Verpflichtungen überprüfen und Maßnahmen nach § 61 BSIG-E ergreifen, vgl. § 62 BSIG-E. Eine ex ante-Aufsicht – wie bei besonders wichtigen Einrichtungen – oder gar eine allgemeine Nachweispflicht – wie bei Betreibern kritischer Anlagen – ist gerade nicht vorgesehen. Da hierdurch die Verhältnismäßigkeit der Aufsichtsmaßnahmen bereits ausreichend sichergestellt ist, wird der Änderungsbedarf im Sinne des Vorschlags nicht geteilt.

Zu Nummer 19. [Zu Artikel 1 (Anlage 1 Nummer 5.2.1 Spalte D BSIG)]

Die Bundesregierung wird den Antrag prüfen.

Zu Nummer 20. [Zu Artikel 17 Nummer 2 (§ 5c Absatz 3 Satz 3 Nummer 2a – neu – EnWG)]

Die Bundesregierung lehnt den Vorschlag ab. Das System der IT-Sicherheitskataloge besteht bereits seit der ersten NIS-Regulierung und hat seither nicht zu einer Überregulierung durch die praktische Anwendung durch die Bundesnetzagentur (BNetzA) geführt. Aus Sicht der Bundesregierung besteht auch nicht die Gefahr einer Überregulierung, da die BNetzA ohnehin die neuerlich eingeführten Kategorien der Einrichtungen als maßgeblich für die IT-Sicherheitskataloge heranziehen wird.

Zu Nummer 21. [Zu Artikel 30 (Inkrafttreten)]

Die Bundesregierung lehnt den Vorschlag ab. Die vorgeschlagene Änderung stellt keine richtlinienkonforme Umsetzung der NIS-2-Richtlinie dar.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333