21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)062 F
vom 13. Oktober 2025

Schriftliche Stellungnahme

von Ferdinand Gehringer, Konrad-Adenauer-Stiftung e. V., Berlin vom 12. Oktober 2025

Öffentliche Anhörung

Gesetzentwurf der Bundesregierung

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

BT-Drucksache 21/1501

KONRAD ADENAUER STIFTUNG

Deutscher Bundestag
Ausschuss für Inneres
– Sekretariat –
Platz der Republik 1
11011 Berlin

Konrad-Adenauer-Stiftung
Analyse und Beratung
Ferdinand Gehringer

Klingelhöferstr. 23
10785 Berlin

T +49 30 26996 3460
M+49 151 65 26 1391
ferdinand.gehringer@kas.de

10.10.2025

Betreff: Schriftliche Stellungnahme zum Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (BT-Drucksache 21/1501)

Sehr geehrter Herr Vorsitzender,

anbei erhalten Sie als Anlage die erbetene schriftliche Stellungnahme zum Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (BT-Drucksache 21/1501) für den Innenausschuss des Deutschen Bundestages zur Vorlage in der Anhörung am 13. Oktober 2025.

Herzliche Grüße

Ferdinand Gehringer

Schriftliche Stellungnahme

zum

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

(BT-Drucksache 21/1501)

von

Ferdinand Gehringer

Policy Advisor Innere Sicherheit und Cybersicherheit

Konrad-Adenauer-Stiftung e.V.

Inhaltsverzeichnis

Vorbemerkung

Die digitale Resilienz kritischer Infrastrukturen ist in der aktuellen geopolitischen Lage von existentieller Bedeutung. Erst im September 2025 zeigte der Ransomware-Angriff auf Collins Aerospace, einen zentralen IT-Dienstleister für die Luftfahrtbranche, wie verwundbar vernetzte Systeme sind. Auch dieser Vorfall unterstreicht, dass die **Erhöhung der Cybersicherheitsstandards** nicht nur eine **regulatorische Pflicht**, sondern eine **strategische Notwendigkeit** ist, **um die Handlungsfähigkeit des Staates und der Wirtschaft künftig zu sichern**.

Gleichzeitig steht Deutschland unter unmittelbarem Handlungsdruck: Die Europäische Kommission hat bereits, aufgrund der bisher ausgebliebenen Umsetzung der NIS-2-Richtlinie, ein **Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland** eingeleitet. Die damit verbundenen Strafzahlungen – potenziell im zweistelligen Millionenbereich – wären nicht nur eine finanzielle Belastung, sondern würden auch das Vertrauen in die deutsche Cyberresilienz untergraben.

Deshalb ist es von größter Bedeutung, dass die NIS-2-Richtlinie nun sehr schnell umgesetzt wird.

Diese **Stellungnahme konzentriert sich auf die drängendsten Handlungsfelder**, um die Umsetzung der NIS2-Richtlinie in Deutschland zielgerichtet voranzutreiben. Für alle hier nicht explizit aufgeworfenen Punkte besteht aus heutiger Sicht kein akuter Anpassungsbedarf.

Die Empfehlungen zielen darauf ab, die digitale Widerstandsfähigkeit zu stärken, rechtliche Risiken zu minimieren und gleichzeitig die Flexibilität zu wahren, um auf künftige Entwicklungen reagieren zu können.

Zusammenfassung

NIS-2- und CER-Richtlinie harmonisiert und abgestimmt umsetzen
Gesamtstaatliche Resilienz muss ganzheitlich gedacht werden und sowohl digitale als auch physische Gefahren einbeziehen. Wiederkehrende Fälle von Sabotage und Spionage – insbesondere bei Kritischen Infrastrukturen – verdeutlichen dies. Die EU hat mit der NIS-2- und der CER-Richtlinie ein abgestimmtes Vorgehen vorgesehen. Doch die uneinheitliche Umsetzung der Richtlinien in Deutschland schwächt die Resilienz, erhöht den Aufwand für betroffene Einrichtungen und mindert die Akzeptanz staatlicher Maßnahmen. Angesichts der aktuellen hybriden Bedrohungslage ist die weitere Verzögerung eines KRITIS-Dachgesetzes weder nachvollziehbar noch vertretbar.

Information Sharing Portal als Chance der breiten Integration begreifen und aufwerten

Die Plattform sollte zu einem zentralen digitalen Zugangspunkt für sämtliche Informationen, Produkte und Dienstleistungen des BSI weiterentwickelt werden. Dafür gilt es, bestehende Kanäle zu bündeln, wechselseitige Kommunikation zu erleichtern und den Austausch zwischen Teilnehmenden aktiv zu fördern. Ein Cyberlage-Dashboard mit Echtzeitdaten zu Bedrohungen, branchenspezifischen Analysen und praxisorientierten Handlungsempfehlungen würde Transparenz und Reaktionsfähigkeit deutlich verbessern. Ergänzend sollten regionale Unterstützungsangebote und Meldemöglichkeiten integriert werden. Ein modernisiertes Portal kann darüber hinaus freiwillige Meldungen fördern und damit einen wichtigen Beitrag zur Stärkung der gesamtgesellschaftlichen Cybersicherheitskultur leisten.

Gesamte Bundesverwaltung von Regelungen des NIS2UmsG umfassen

Die Ausnahme bei der Bundesverwaltung werden der aktuellen hybriden Bedrohungslage nicht gerecht. Die gesamte Bundesverwaltung sollte denselben Sicherheitsanforderungen unterliegen, um ein einheitlich hohes Schutzniveau zu gewährleisten. Ausnahmen schwächen die Gesamtresilienz und senden ein falsches Signal an die Wirtschaft.

Finanzielle oder organisatorische Einwände greifen zu kurz – Cybersicherheit ist eine dauerhafte staatliche Aufgabe und durch die Ausnahme der Schuldenbremse abgedeckt. Da viele Behörden gemeinsame Strukturen nutzen, ist ein umfassender Schutz notwendig, um Sicherheitslücken und Funktionsausfälle im Krisenfall zu verhindern.

Untersagung kritischer Komponenten eindeutig, transparent, bürokratiearm und flexibel regeln

Zentrales Anliegen muss die Schaffung eines transparenten, klar strukturierten und risikobasierten Verfahrens auf Grundlage eines einheitlichen Kriterienkatalogs sein, das für alle Sektoren gilt. Abgestufte Maßnahmen, Übergangsfristen und Härtefallregelungen sollen unverhältnismäßige Eingriffe vermeiden. Nur so lassen sich Planungs- und Rechtssicherheit für Staat, Betreiber kritischer Infrastrukturen und Hersteller gewährleisten. Die Umsetzung sollte eng mit der Praxis abgestimmt und EU-weit harmonisiert werden. Die Zuständigkeiten im Vollzug sollten vereinfacht werden – ein Einvernehmen allein mit dem Bundeskanzleramt wäre praktikabler.

Bundes-CISO klare Rolle, Aufgaben, Befugnisse und Rechte zuweisen

Die Einrichtung eines CISO-Bund ist ein wichtiger Schritt zur Stärkung der Informationssicherheit des Bundes. Die aktuelle Regelung bleibt jedoch zu unbestimmt – Zuständigkeiten, Einbindung und Ressourcen müssen klar gesetzlich definiert werden. Der CISO-Bund sollte als zentrale Koordinierungs- und Steuerungsstelle für Informationssicherheit in der Bundesverwaltung agieren, mit klaren Kompetenzen,

ausreichenden Ressourcen und fachlicher Unabhängigkeit. Er koordiniert das operative Informationssicherheitsmanagement, unterstützt die Ressorts und ist in alle relevanten Vorhaben mit IT-Sicherheitsbezug einzubinden.
Eine Ansiedlung beim BSI bietet sich an, um Synergien zu nutzen und die Rolle des BSI als Brücke zwischen BMI und BMDS zu stärken. Damit würde der CISO-Bund zu einem strategischen Bindeglied der staatlichen Cybersicherheitsarchitektur.

Bewertung des NIS2UmsG im Allgemeinen

Ein wesentlicher Kritikpunkt ist, dass die **öffentliche Verwaltung der Länder und Kommunen nicht in den Geltungsbereich des Umsetzungsgesetzes einbezogen** ist. Damit bleiben zentrale Bereiche staatlicher Handlungsfähigkeit – insbesondere in der Daseinsvorsorge und im Verwaltungsvollzug – ohne verbindliche Cybersicherheitsanforderungen. Diese Ebenen sind jedoch entscheidend für die Aufrechterhaltung grundlegender staatlicher Funktionen. Der ENISA Threat Landscape Report 2024/2025 zeigt, dass 38,2 % aller Cyberangriffe in der EU den öffentlichen Sektor treffen, insbesondere staatliche und diplomatische Einrichtungen. Dies verdeutlicht, dass auch Länder- und Kommunalverwaltungen zunehmend Ziel koordinierter, teils staatlich gesteuerter Angriffe sind.
Die Ausklammerung dieser Verwaltungsebenen führt zu Schutzlücken und Bruchstellen in der föderalen Cybersicherheitsarchitektur. Eine Einbeziehung von Ländern und Kommunen in die Regelungsinhalte des NIS2UmsG würde die Resilienz öffentlicher Strukturen stärken und die gesamtstaatliche Cybersicherheitsstrategie deutlich kohärenter und wirksamer gestalten. Es bleibt zu wünschen, dass dies künftig im Einklang mit den Interessen der Bundesländer vorgenommen wird.
Das BSI kann im Hinblick auf seine eigene Funktion und bedeutende Rolle nur darin bestärkt werden, durch weitere Kooperationsvereinbarungen mit den Ländern einen unterstützenden Einfluss zu gewinnen, auch wenn dies nicht kongruent zu einer Zentralstellenfunktion in der staatlichen Cybersicherheitsarchitektur ist.

Für eine umfassende Erhöhung der Sicherheit und Resilienz – nach dem All-Gefahren-Ansatz – wäre es mehr als erforderlich, dass das **NIS2UmsG und** das **KRITIS-Dachgesetz noch viel stärker aufeinander abgestimmt** und die beiden Umsetzungsprozessen weitergehend harmonisiert werden.
Beide Gesetze verfolgen das Ziel, kritische Infrastrukturen zu schützen – eine klare Trennung zwischen physischer Sicherheit und Cybersicherheit ist angesichts hybrider Bedrohungen jedoch kaum möglich. Einheitliche Begriffe sowie kongruente Vorgaben könnten Überschneidungen vermeiden, die Effizienz erhöhen und ein gemeinsames, ganzheitliches Verständnis von Schutzmaßnahmen aufbauen.

Darüber hinaus wäre die **Etablierung gemeinsamer Stresstests** – in Anlehnung an die Regelung des Digital Operational Resilience Act (DORA) – von Behörden, KRITIS-Betreibern und Forschungseinrichtungen im Rahmen der Umsetzung denkbar, um die Wirksamkeit von

Sicherheitsmaßnahmen und Notfallplänen praxisnah zu überprüfen. Solche ressortübergreifenden Übungen ermöglichen es, Schwachstellen in der digitalen Infrastruktur frühzeitig zu identifizieren, Schnittstellenprobleme zwischen staatlichen und privaten Akteuren zu erkennen und die Koordination zu verbessern. Gleichzeitig fördern sie den Wissenstransfer zwischen Verwaltung, Wirtschaft und Wissenschaft und stärken damit die gesamtstaatliche Cybersicherheitsresilienz.

Bewertung des NIS2UmsG im Einzelnen

§ 2 Begriffsbestimmungen

§ 2 Nr. 3 BSIG-E

„‚Bodeninfrastruktur´ den Sektor Weltraum betreffende Einrichtungen, die der Kontrolle des Startes, Fluges oder der eventuellen Landung von Weltraumgegenständen dienen,"

Anmerkungen: Die im Entwurf gewählte Definition der Bodeninfrastruktur ist zu eng gefasst. Sie erfasst nur die Steuerung von Start, Flug und Landung, nicht aber zentrale Komponenten wie Datenverarbeitungszentren, Energieversorgung, Netzwerkinfrastruktur, Sicherheits- und Überwachungssysteme. Eine umfassendere Definition ist für die Cybersicherheit unverzichtbar, da sie alle potenziellen Angriffsvektoren berücksichtigt und so einen ganzheitlichen, resilienten Schutz der gesamten Weltraummission ermöglicht – nicht nur der Steuerungssysteme.

Empfehlung 1: *„‚Bodeninfrastruktur´ den Sektor Weltraum betreffende Einrichtungen, alle irdischen Einrichtungen und Systeme, die für den Betrieb, die Kontrolle, die Überwachung und die Unterstützung von Weltraumaktivitäten notwendig sind."*

Empfehlung 2: Für einen umfassenden Schutz sollten auch die Weltraumsysteme selbst in die Regulierung aufgenommen werden.

§ 2 Nr. 10 BSIG-E (neu)

Anmerkungen: An zahlreichen Stellen – so beispielsweise in §§ 4, 5, 6, 8, 9, 10, 15 BSIG-E – wird bereits auf „Einrichtungen der Bundesverwaltung" abgestellt, ohne diese begrifflich darzulegen und einzugrenzen. Im Sinne einer konsistenten Regelungssystematik bietet es sich an § 29 Abs. 1 BSIG-E als neue § 2 Nr. 10 BSIG-E in die Allgemeinen Vorschriften zu verlagern.

Empfehlung: *„Einrichtungen der Bundesverwaltung im Sinne dieses Gesetzes sind, mit Ausnahme der Institutionen der Sozialen Sicherung und der Deutschen Bundesbank,*
1. Bundesbehörden,

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

§ 2 Nr. 10 BSIG-E

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

Anmerkungen: Immaterielle Schäden und die Erheblichkeit der Beeinträchtigung sind zu unbestimmt. Sie bedürfen einer Konkretisierung durch zumindest beispielhafte Aufzählungen, welche Vorstellungen der Gesetzgeber im Rahmen der Erheblichkeit eines immateriellen Schadens hat, um eine hinreichende Rechtssicherheit gewährleisten zu können und um eine Überkompensation des Meldewesens zu vermeiden. Zugleich sollte eine Erheblichkeitsschwelle formuliert werden.

Empfehlung: *„‚erhebliche Cyberbedrohung´ eine Cyberbedrohung, die das Potenzial besitzt, die informationstechnischen Systeme, Komponenten und Prozesse aufgrund der besonderen technischen Merkmale der Cyberbedrohung erheblich zu beeinträchtigen; eine Beeinträchtigung ist erheblich, wenn sie erheblichen materiellen oder immateriellen Schaden verursachen kann. Hierzu gehören auch inner- und außerbetriebliche Vertrauens- und Reputationsverluste, Wettbewerbsnachteile, beeinträchtigte Geschäftsbeziehungen;“*

§ 2 Nr. 11 lit. b BSIG-E

„‚erheblicher Sicherheitsvorfall´ ein Sicherheitsvorfall, der andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann, sofern durch die Rechtsverordnung nach § 56 Absatz 5 keine konkretisierende Begriffsbestimmung erfolgt;“

Anmerkungen: Hier wird hinsichtlich der Unbestimmtheit von „erheblichen immateriellen Schaden“ auf die Ausführung zu § 2 Nr. 10 BSIG-E verwiesen.

§ 2 Nr. 17 BSIG-E

„‚Informationssicherheit´ der angemessene Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen;“

Anmerkungen: „Informationssicherheit“ ist nicht ausreichend definiert. Es fehlt das Schutzziel der Authentizität und sollte ergänzt werden.

Empfehlung: *„‚Informationssicherheit´ der angemessene Schutz der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Informationen;“*

§ 2 Nr. 23 lit. b BSIG-E

„‚kritische Komponenten´ IKT-Produkte, […] bei denen Störungen der Verfügbarkeit, Integrität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit kritischer Anlagen oder zu Gefährdungen für die öffentliche Sicherheit führen können und […];“

Anmerkungen: Die Regelung ist zu weit gefasst. Die Verletzung bereits eines der Schutzziele kann ausreichend sein, um den Ausfall oder die erhebliche Beeinträchtigung herbeizuführen. Zudem wird auf das fehlende Schutzziel der Authentizität verwiesen.

Empfehlung: *„‚kritische Komponenten´ IKT-Produkte, […] bei denen Störungen der Verfügbarkeit, Integrität oder Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit kritischer Anlagen oder zu Gefährdungen für die öffentliche Sicherheit führen können und […];“*

§ 2 Nr. 41 BSIG-E

„‚weltraumgestützte Dienste´ Dienste, […] die auf Daten und Informationen beruhen, die entweder von Weltraumgegenständen erzeugt oder über diese weitergegeben werden und […];“

Anmerkungen: Die Regelung ist unvollständig. „Signale“ fehlen in der Begriffsdefinition im Rahmen der weltrumgestützten Dienste und sollten ergänzt werden, um den Schutzzweck zu erreichen. Weltraumgegengestände erzeugen, übertragen oder verarbeiten auch reine Signale (Timing-Signale). Zudem geht es nicht nur um die Erzeugung oder Weitergabe, sondern auch um die „Verarbeitung“ von Daten, Informationen oder Signalen.

Empfehlung: *„‚Weltraumgestützte Dienste´ sind Dienste, […] die auf Daten, Informationen oder Signalen beruhen, die von Weltraumgegenständen erzeugt, verarbeitet oder über diese weitergegeben werden und […];“*

§ 3 Aufgaben des Bundesamts

§ 3 Abs. 1 Nr. 18 BSIG-E

Anmerkungen: Die zusätzlichen Verantwortlichkeiten und Anforderungen an die Fachlichkeit und Unabhängigkeit des BIS werden in § 3 BSIG-E nicht ausreichend dargestellt und von anderen Behörden abgegrenzt. Die Art, Ziele und Grenzen der Unterstützung des BSI für Polizei, Strafverfolgungs- und Nachrichtendienstbehörden sind zu unklar. Das BSI soll immer mehr als (die) zentrale Stelle für Informationssicherheit in Deutschland fungieren.

Empfehlung: Vor allem § 3 Abs. 1 Nr. 18 lit. a und lit. c BSIG-E (Wahrnehmung seiner gesetzlichen Aufgaben) sollten weiter konkretisiert werden, um nicht nur eine entsprechende einheitliche Konkretisierung in Anlehnung an § 3 Abs. 1 Nr. 18 lit. b gewährleisten zu können, sondern auch um im Hinblick auf die Gefahrenabwehrfunktion des BSI nach § 3 Abs. 1 Nr. 1 BSIG-E hinreichende Rechtssicherheit und Abgrenzung zu polizeilichen Aufgaben und strafverfolgungsbehördlichen Kompetenzen sicherzustellen.

§ 3 Abs. 1 Nr. 20 BSIG-E

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

Anmerkungen: Es ist nicht ersichtlich, wieso hier Einrichtungen der Bundesverwaltung explizit aufgeführt werden. Im Sinne einer weitreichenden Sicherheit in der Informationstechnik sollte nicht nur die Bundesverwaltung umfasst sein, sondern neben Einrichtungen der Landesverwaltung, kommunalen Einrichtungen sollten Bundestag, Landtage, politische Parteien und Stiftung ebenfalls vom BSI beraten, informiert und gewarnt werden. Zur Klarstellung des Aufgabenbereiches sollte eine enumerative Aufzählung der Einrichtungen erfolgen. Wenn es im Rahmen dieser Umsetzung bereits nicht gelingt, die Landes- und kommunale Ebene in den Anwendungsbereich aufzunehmen, sollte zumindest das BSI die Möglichkeit erhalten diesen Einrichtungen beratende und informierende Unterstützung anzubieten.

Empfehlung: *„Einrichtungen der Bundes-, Landesverwaltung und Kommunalverwaltung, Bundestag, Landesparlamente, politische Parteien, politische Stiftungen sowie Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, […];“*

§ 5 Allgemeine Meldestelle für die Sicherheit in der Informationstechnik

§ 5 Abs. 3 BSIG-E

„Das Bundesamt soll die gemäß Absatz 2 gemeldeten Informationen nutzen, um […]“

Anmerkungen: Die Regelungen des § 5 BSIG-E enthalten eine teilweise für die Meldung von Informationen im Sinne des § 5 Absatz 1 und Abs. 2 BSIG-E erforderliche Vertrauensbasis für Meldende nicht. Das BSI ist im Geschäftsbereich des BMI nicht unabhängig. Daher sollte in die „Soll-Regel“ des Abs. 3 die grundsätzliche Nutzung der Informationen zur Verbesserung der Informationssicherheit ergänzt werden. Im besonders begründeten und dokumentierten Ausnahmefall kann hiervon abgewichen.

Empfehlung: *„Das Bundesamt soll die gemäß Absatz 2 gemeldeten Informationen zur Verbesserung der Informationssicherheit nutzen, um […]“*

§ 6 Informationsaustausch

§ 6 Abs. 1 BSIG-E

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

Anmerkungen: Die Plattform (oder auch das Information Sharing Portal) fehlt in der dargestellten Form seine Wirkungspotenziale. Sie sollte zu einem zentralen digitalen Zugangspunkt für alle relevanten Informationen, Produkte und Dienstleistungen des BSI weiterentwickelt werden. Dafür gilt es, bestehende Kanäle zu bündeln, die bidirektionale Kommunikation zu erleichtern und auch den Austausch der Teilnehmenden untereinander zu ermöglichen. Neben Echtzeitinformationen über aktuelle Angriffsvektoren und Schwachstellen sollten gemeldete Vorfälle nach Branchen und Unternehmensgrößen ausgewertet sowie zielgruppengerechte Handlungsempfehlungen – insbesondere für kleine und mittlere Unternehmen – bereitgestellt werden.
Ein tägliches Cyberlage-Dashboard könnte sowohl die aktuelle Bedrohungslage abbilden als auch die Meldung von Vorfällen ermöglichen, die mit regionalspezifischen Unterstützungsangeboten (Informationen über schnelle Vor-Ort-Unterstützung, Kontaktdaten von Meldebehörden, Polizei, CERTS) und Erste-Hilfe-Maßnahmen verknüpft werden. Um Effizienz und Praxistauglichkeit sicherzustellen, sollten Verbände und Wirtschaftsakteure frühzeitig in den Entwicklungsprozess einbezogen werden. Entscheidend ist hierbei auch, dass das Cyberlagebild einen wesentlichen Teil umfasst, der der Öffentlichkeit zugänglich gemacht werden kann. Die Integration von Inhalten der Allianz für Cybersicherheit und deren Anbindung an die Plattform ist hierbei sinnvoll.
Durch das aufgewertete Portal kann auch ein Anreiz für Einrichtungen geschaffen werden, die nicht von diesem Gesetz umfasst sind und grundsätzlich keiner Meldepflicht nach diesem Gesetz unterliegen. Wenn Einrichtungen für „freiwillige Meldungen“ Informationen und Hinweise über das Portal erlangen, kann dies die Bereitschaft zur Zusammenarbeit erhöhen.

Empfehlung: *„[…]. Es kann weitere Stellen, insbesondere Hersteller, Lieferanten oder Dienstleister, einbeziehen. Die Plattform ist als zentraler digitaler Zugang zu den Informationen, Produkten und Dienstleistungen des Bundesamtes auszugestalten und hat den Austausch der Teilnehmer in Echtzeit zu ermöglichen. Über die Plattform sind anonymisierte Informationen zu Angriffsvektoren und Schwachstellen, ausgewertete Cybersicherheitsvorfälle sowie zielgruppengerechte Handlungsempfehlungen, insbesondere für kleine und mittlere*

Unternehmen, bereitzustellen. Das Bundesamt richtet hierzu ein Dashboard zur aktuellen Cyberlage ein, das die Meldung von Vorfällen sowie deren Verknüpfung mit regionalspezifischen Unterstützungsangeboten ermöglicht. Bei der Ausgestaltung der Plattform sind betroffene Verbände und Wirtschaftsakteure einzubeziehen."

§ 7 Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte

Anmerkungen: Das Bundesamt sollte die Kommunikationstechnik des Bundes umfänglich kontrollieren. Es wird nicht ersichtlich, wer alternativ die technische Kontrolle fachlich und sachlich angemessen durchführt. Im Sinne einer einheitlichen Gewährung der Informationssicherheit sollten daher die Ausnahmetatbestände in § 7 Abs. 6 und Abs. 7 BSIG-E gestrichen werden.

§ 28 Besonders wichtige und wichtige Einrichtungen

Anmerkungen: Für eine bessere Eingliederung in den europäischen Rechtsrahmen und gerade auch für die einfachere Rechtshandhabe für Unternehmen, die innerhalb der Europäischen Union und in Deutschland tätig sind, sollte auf die Begriffe „wesentliche" und „wichtigen" Einrichtungen" zurückgegriffen und keine neuen eingeführt werden.

§ 28 Abs. 3 BSIG-E

Anmerkungen: Die Regelung in § 28 Absatz 3 BSIG-E ist im Grundsatz sinnvoll, jedoch zu unbestimmt. Sie soll verhindern, dass eine nur geringfügige Nebentätigkeit zur Einstufung eines Unternehmens als „wichtige" oder „besonders wichtige Einrichtung" führt. Sie bedarf einer konkreteren Ausgestaltung, um Rechtsunsicherheit zu vermeiden und eine einheitliche Anwendung zu gewährleisten.
Um dies zu erreichen, sollte der Gesetzgeber klare Anhaltspunkte – wie beispielsweise die Ausrichtung in Gründungsdokumenten, die Anzahl der Mitarbeiter, die Anzahl an Sachmitteln, der Anteil des Umsatzes oder die Bilanzsumme des betreffenden Bereichs – festlegen. Quantitative Vorgaben könnten transparente und nachvollziehbare Kriterien für die Praxis darstellen.
Zudem wäre es hilfreich, den Begriff des „Gesamtbilds" durch eine präzisere Abwägungsregel zu ersetzen. Statt einer generellen Betrachtung aller Umstände sollte festgelegt werden, welche Mindestanzahl von Indizien – etwa zwei von drei Kriterien – erfüllt sein müssen, um eine Tätigkeit als nicht vernachlässigbar einzustufen. Ergänzend könnte ein nicht abschließender Beispielkatalog typischer Konstellationen in den Gesetzestext aufgenommen werden, um die Anwendung zu erleichtern. Dies würde Unternehmen und Behörden eine bessere Orientierung bieten. Schließlich könnte eine Dokumentationspflicht für die Selbsteinstufung eingeführt werden. Unternehmen müssten dann kurz darlegen, warum sie eine bestimmte Tätigkeit als vernachlässigbar einordnen.

Zugleich wird in diesem Zusammenhang auf eine mögliche Europarechtswidrigkeit verwiesen. Durch die Regelung könnte der Anwendungsbereich der NIS-2-Richtlinie unzulässig verkleinert werden und damit gegen das Prinzip der Mindestharmonisierung verstoßen, was wiederum im Hinblick auf das laufende Vertragsverletzungsverfahren nachteilig wirken kann.

§ 29 Einrichtungen der Bundesverwaltung

§ 29 Abs. 2 BSIG-E

„Für Einrichtungen der Bundesverwaltung sind die Regelungen für besonders wichtige Einrichtungen anzuwenden, nicht jedoch die Regelungen der §§ 38, 40 Absatz 3 und der §§ 61 und 65. Für Einrichtungen der Bundesverwaltung, ausgenommen das Bundeskanzleramt und die Bundesministerien, sind zusätzlich die Regelungen des § 30 nicht anzuwenden."

Anmerkungen: Mit Verweis auf die Ausführungen zu § 2 BSIG-E sollte § 29 Abs. 1 BSI-E als § 2 Nr. 10 BSIG-E eingefügt werden. Die übrigen Absätze 2 und 3 sollten als § 29 Abs. 1 und § 29 Abs. 2 BSIG-E erhalten bleiben. Zudem wird zur Klarstellung der Regelungssystematik angeregt, einen Satz mit Verweis auf die §§ 43 ff. BSIG-E zu ergänzen.

Außerdem wird § 29 Abs. 2 S. 2 BSIG-E weder der allgemeinen hybriden Bedrohungslage noch den Gefährdungspotenzialen in Deutschland im Besonderen gerecht. Es ist nicht ersichtlich, wieso sich Teile der staatlichen Einrichtungen einem allgemein angestrebten hohen Cybersicherheitsniveau entziehen. Weitergehend wäre dies ein fatales Zeichen gegenüber den wirtschaftlichen Unternehmen, die neue höhere Anforderungen erfüllen müssen. Die gesamte Bundesverwaltung, inklusive aller nachgeordneten Behörden sollten von den Anforderungen dieses Gesetzes umfasst sein. Einwände wie die finanzielle Mehrbelastung oder erschwerte Meldewege für die behördliche Einrichtungen können hierbei bei hinreichend gewichtet werden. Ein finanzieller Aufwand zur Erreichung eines hohen Cybersicherheitsniveau wird auch künftig durch verschleppte Maßnahmen nicht verringert. Mehrausgaben für den Schutz der informationstechnischen Systeme sind ausdrücklich von der Bereichsausnahme Verteidigung der Schuldenbremse umfasst (Art. 109 Abs. 3 Satz 5 GG). Da Bundeseinrichtungen teilweise gemeinsame Netz- und Lieferstrukturen nutzen, ist ein einheitlicher Schutz der gesamten Bundesverwaltung erforderlich, um Schwachstellen und potenzielle Einfallstore zu vermeiden. Zudem ist ein hohes Cybersicherheitsniveau und eine dazugehörige Resilienz der gesamten Bundesverwaltung im Rahmen der zivilen Verteidigung zwingende Voraussetzung für das Aufrechterhalten der Staats- und Regierungsfunktionen. Demnach sollten die Verweise auf die §§ 40 Abs. 3 und 61 BSIG-E ebenso gestrichen werden, wie § 29 Abs. 2 S. 2 BSIG-E.

Empfehlung: *„Für Einrichtungen der Bundesverwaltung sind die Regelungen für besonders wichtige Einrichtungen anzuwenden. Näheres regeln die §§ 43 ff. BSIG-E. Nicht anwendbar sind jedoch die Regelungen der §§ 38 und 65."*

§ 29 Abs. 3 BSIG-E

„[…] Das Auswärtige Amt erlässt im Einvernehmen mit dem Bundesministerium für Digitales und Staatsmodernisierung eine allgemeine Verwaltungsvorschrift, um die Ziele der NIS-2-Richtlinie im Geschäftsbereich des Auswärtigen Amtes durch ergebnisäquivalente Maßnahmen umzusetzen."

Anmerkungen: Es sollte keine Sonderregelungen für Teile der Bundesverwaltung geben, die nicht ausdrücklich vorsehen, dass das Mindestmaß an Cybersicherheit der NIS-2-Richtlinie und deren Ziele umfasst, selbst wenn dies nur deklaratorisch sein sollte.

Empfehlung: *„[…] Das Auswärtige Amt, das Bundesministerium der Verteidigung, der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz erlassen im Einvernehmen mit dem Bundesministerium für Digitales und Staatsmodernisierung eine allgemeine Verwaltungsvorschrift, um die Ziele und das Mindestmaß an Cybersicherheit der NIS-2-Richtlinie oder höher in ihren Geschäftsbereichen durch ergebnisäquivalente Maßnahmen umzusetzen."*

§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

§ 30 Abs. 2 BSIG-E

„Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. […]"

Anmerkungen: Um branchenspezifische Maßnahmen und Standards zu implementieren, sollte § 30 Abs. 2 um einen Satz 3 ergänzt werden.

Empfehlung: *„Das Bundesamt kann in Abstimmung mit Branchenverbänden bereichsspezifischer Standards für die Informationssicherheit erarbeiten, um die Maßnahmen aus § 30 Abs. 2 S. 2 BSIG-E zu konkretisieren."*

§ 32 Meldepflichten

Anmerkungen: Das eingeführte Meldewesen ist richtig. Entscheidend ist jedoch, dass das Verfahren praxisnah, effizient und unbürokratisch ausgestaltet wird, um Mehrfachmeldungen und unnötige Doppelstrukturen zu vermeiden. Eine enge und verbindliche Harmonisierung mit dem noch umzusetzenden KRITIS-Dachgesetz ist hierfür unerlässlich, um ein kohärentes und leistungsfähiges Meldewesen sicherzustellen.
Da neben dem BSI auch BNetzA, BaFin und die Datenschutzaufsichtsbehörden beteiligt sind, sollte die Zentralisierung der Meldeverfahren konsequent ausgebaut werden. Ziel ist ein

einheitlicher Meldekanal, über den Meldungen automatisiert und datenschutzkonform an alle zuständigen Stellen weitergeleitet werden. Dies erhöht die Akzeptanz und Rechtssicherheit, verringert den bürokratischen Aufwand und stärkt zugleich das gesamte Informationssicherheitsniveau.
Darüber hinaus sollte die nationale Umsetzung in enger europäischer Abstimmung erfolgen, um insbesondere multinational tätigen Unternehmen einheitliche und vereinfachte Meldewege zu ermöglichen.

§ 33 Registrierungspflicht

Anmerkungen: Die Regelung ist nicht praxinah. Sie trägt einer verbreiteten Verunsicherung zahlreicher Unternehmen hinsichtlich ihrer Betroffenheit, der Berechnung der Anzahl der Mitarbeitenden oder Abgrenzungsfragen sowie einer Registrierungspflicht nicht Rechnung. Es bietet sich an, die Registrierungsmöglichkeit in der Plattform (bzw. Information Sharing Portal – siehe § 6 BSIG-E) zu integrieren und zugleich dem Bundesamt die Möglichkeit einzuräumen, den Unternehmen bei juristischer Fehlbewertung eine sofortige Mitteilung zu übermitteln. Zugleich sollte es aber diesen Unternehmen ermöglicht werden, weiterhin über die Plattform – trotz fehlender Pflicht – Informationen zu erlangen und somit auch einen Anreiz für eigene Meldungen zu schaffen.

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

§ 38 Abs. 3 BSIG-E

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

Anmerkungen: Diese Regelung ist zu unbestimmt und nicht ergebnis- bzw. erkenntnisorientiert. Es werden keine inhaltlichen und zeitlichen Standards für die Schulungen formuliert. Auch die formelle und inhaltliche Nachweisbarkeit bleibt unklar für Geschäftsleitungen. Demnach sollte der § 38 Abs. 3 ergänzt und konkretisiert werden.

Empfehlung: *„[…] sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können. Der regelmäßige Nachweis für erfolgreich durchgeführte Schulungen soll durch eine ausgestellte Bescheinigung erfolgen, jedoch nicht später als [18] Monate nach letztmaligem Nachweis. Das Bundesamt veröffentlicht eine Liste mit entsprechend qualifizierten Schulungsangeboten.“*

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

Anmerkungen: Die Regelung ist noch nicht hinreichend vereinfacht. Sie sieht noch zwei Meldungen vor. Meldungen können jedoch zentral gebündelt werden. Ziel ist es, dass meldepflichtige Einrichtungen mit einer einzigen Meldung sowohl ihrer Verpflichtung nach der NIS-2-Richtlinie als auch nach Art. 33 DSGVO nachkommen können. Der Bundesrat hatte das BSI als zentrale Anlaufstelle für solche gebündelten Meldungen vorgesehen. Die Meldung sollte dann an die zuständigen Datenschutzbehörden weitergeleitet werden. Die Bundesregierung lehnt dies jedoch ab, da Art. 33 DSGVO keine Meldung an andere Stellen als die Datenschutzaufsichtsbehörden erlaubt (keine Öffnungsklausel) und zugleich auch das Verbot der Mischverwaltung gilt.

Um dennoch das Verfahren zu vereinfachen, sollte das BSI ein elektronisches Verfahren bereitstellen, das es den Einrichtungen ermöglicht, aus einer NIS-2-Meldung heraus auch die DSGVO-Meldung vorzubereiten. Die Meldung selbst würde weiterhin durch die Einrichtung direkt an die Datenschutzbehörde erfolgen. Diese Lösung wahrt die rechtlichen Vorgaben und vermeidet Probleme mit der Mischverwaltung zwischen Bundes- und Landesbehörden.

§ 41 Untersagung des Einsatzes kritischer Komponenten

Anmerkungen: Eine Regelung zur Untersagung kritischer Komponenten ist grundsätzlich sinnvoll. Sie dient der Erfüllung einer staatlichen Schutzpflicht aus dem IT-System Grundrecht (Art. Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) und soll den Einsatz unsicherer Komponenten in kritischen Infrastrukturen verhindern und die Cybersicherheit stärken.

Um den geopolitischen Entwicklungen, der Bedeutung kritischer Infrastrukturen im Allgemeinen sowie der Bedeutung kritischer Komponenten im Speziellen für die nationale Sicherheit als auch der Handlungsfähigkeit und Wettbewerbsfähigkeit deutscher KRITIS-Unternehmen hinreichend Rechnung zu tragen, sollte § 41 BSIG-E transparenter, praxistauglicher und flexibler ausgestaltet werden. Nur ein risikobasiertes, dynamisches Verfahren, das sich an die rasante digitale Entwicklung anpasst, kann die notwendige Sicherheit schaffen, ohne unverhältnismäßige Bürokratie, Eingriffe oder Planungsunsicherheit zu verursachen.
Die Regelung sollte der ermächtigten Behörde einen hinreichenden Entscheidungsspielraum für sicherheitspolitische Entwicklungen einräumen, zugleich den Betreibern und Herstellern kritischer Komponenten Planungs- und Rechtssicherheit einräumen. Der Eingriff der ermächtigten Behörde in privatwirtschaftliche Prozesse muss dabei ausreichend gerechtfertigt und begrenzt werden.
Außerdem sollte diese Regelung der gegenseitigen Vertrauensbildung zwischen ermächtigter Behörde, Betreiber und Hersteller dienen.

Dazu bedarf es klarer, objektiver Kriterien für die Einstufung als „kritische Komponente“. Die Kriterien für die Zulassung oder Untersagung müssen technische, rechtliche, organisatorische und geopolitische Anforderungen umfassen, insbesondere gültige

Zertifizierungen, bekannte Sicherheitslücken, Kill-Switch-Funktionen, Hersteller-Support, Anforderungen an Wartbarkeit, Auditierbarkeit, Dokumentation, Datenschutz- und Sicherheitsvorgaben sowie Herkunfts- und Abhängigkeitsanalysen.
Eine dynamische Positivliste sicherer Komponenten würde Unternehmen zunächst Planungssicherheit bieten.
Gleichzeitig sollten abgestufte Maßnahmen möglich sein – von Nachbesserungsauflagen über (befristete) Nutzungsgenehmigungen bis hin zur Untersagung als letztes Mittel. Übergangsfristen und Härtefallregelungen sind notwendig, um betroffene Unternehmen nicht zu überfordern.

Die vorgesehene Anzeigepflicht und das bisherige Moratorium von zwei Monaten erschweren die Planungssicherheit der Betreiber und könnten hierbei abgeschafft werden. Kritische Komponenten könnten einmalig registriert und erfasst werden.
Um die Vollzugsfähigkeit zu verbessern, sollte das derzeitige Einvernehmenserfordernis mit den Bundesressorts aus § 41 Abs. 4 BSIG-E vereinfacht werden, etwa durch eine Beschränkung auf das Bundeskanzleramt.

Regelmäßiger Austausch mit Branchenverbänden und eine Orientierung an EU-weit harmonisierten Standards sind ebenso notwendig wie transparente Risikoeinstufungen durch das BSI.

Eine solche Regelung könnte auch im Rahmen des Cyber-Resilience-Act (CRA) getroffen werden. Zumal die auf europäischer Ebene angekündigte „ICT-Supply Chain Toolbox“ zu einem späteren Zeitpunkt berücksichtigt werden könnten.

§ 43 Informationssicherheitsmanagement

§ 43 Abs. 2 BSIG-E

„[…] sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.“

Anmerkungen: Es wird auf die Ausführungen zu § 38 Abs. 3 BSIG-E verwiesen. Um hinreichende Anforderungen an die formelle und inhaltliche Nachweisbarkeit zu schaffen, wird eine Konkretisierung angeregt.

Empfehlung: *„[…] sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können. Der regelmäßige Nachweis für erfolgreich durchgeführte Schulungen soll durch eine ausgestellte Bescheinigung erfolgen, jedoch nicht später als 18 Monate nach letztmaligem Nachweis. Das Bundesamt veröffentlicht eine Liste mit entsprechend qualifizierten Schulungsangeboten.“*

§ 44 Vorgaben des Bundesamtes

Anmerkungen: Es sollten einheitliche Standards für alle Einrichtungen der Bundesverwaltung gelten. Sonderregelungen für Teilbereiche erschließen nicht. § 44 Abs. 1 BSIG-E sollte neu gefasst und § 44 Abs. 2 BSIG-E gestrichen werden. Die Empfehlungsregelung *(„Für die in § 2 Nummer 21 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach Satz 1 empfehlenden Charakter.“*) und die Ausnahmetatbestände *(„Für die Verpflichtung nach Satz 1 gelten die Ausnahmen nach § 7 Absatz 6 und 7 entsprechend.“*) sollten gestrichen werden, um hohe IT-Sicherheitsstandards auch in den sensiblen Bereichen der Justiz, im Auswärtigen Dienst und bei den Streitkräften zu gewährleisten.

Empfehlung**:** *„Die Einrichtungen der Bundesverwaltung müssen die Mindeststandards für die Sicherheit in der Informationstechnik des Bundes (Mindeststandards), BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) in den jeweils geltenden Fassungen als Mindestanforderungen zum Schutz der in der Bundesverwaltung verarbeiteten Informationen erfüllen. Die Mindeststandards werden vom Bundesamt im Benehmen mit den Ressorts und weiteren obersten Bundesbehörden festgelegt und auf der Internetseite des Bundesamtes veröffentlicht. Die jeweils geltenden Fassungen werden auf der Internetseite des Bundesamtes veröffentlicht. Der IT-Grundschutz wird durch das Bundesamt regelmäßig evaluiert und entsprechend dem Stand der Technik sowie unter Berücksichtigung der Erfahrungen aus der Praxis und aus der Beratung und Unterstützung nach Absatz 4 fortentwickelt; dabei wird der Umsetzungsaufwand soweit möglich minimiert. Das Bundesamt wird den IT-Grundschutz bis zum 1. Januar 2026 modernisieren und fortentwickeln.*
Abweichungen von den Mindeststandards sind nur in sachlich gerechtfertigten Fällen zulässig, sie sind zu dokumentieren und zu begründen.“

§ 48 Amt des Koordinators für Informationssicherheit

Anmerkungen: Grundsätzlich ist die Bestellung sinnvoll. Jedoch ist die Regelung zu unbestimmt. Weder organisatorische Einbindung noch Zuständigkeiten oder Ressourcenausstattung sind bisher gesetzlich geregelt, sondern einem späteren Kabinettsbeschluss vorbehalten.
Die oder der Chief Information Security Officer (CISO) des Bundes soll als zentrale Anlaufstelle für Maßnahmen der Informationssicherheit in der Bundesverwaltung fungieren und die Ressorts bei der Umsetzung unterstützen.
Das Amt bedarf klarer Kompetenzen, Abgrenzungen zu Aufgaben anderer und Durchsetzungsmöglichkeiten, die ausformuliert werden sollten. Zugleich ist die Ausgestaltung des Amtes auch von der Rolle und dem Grad der Unabhängigkeit des BSI abhängig. Demnach sollte die Regelung zwingend konkretisiert ausgestaltet werden.
Der CISO-Bund sollte die nötige fachliche und sachliche Qualifikation und Erfahrung mitbringen, die für die Informationssicherheit des Bundes erforderlich ist. Er koordiniert das operative Informationssicherheitsmanagement des Bundes.

Im Benehmen mit den obersten Bundesbehörden entwickelt der CISO-Bund die Stärkung der Informationssicherheit innerhalb der Bundesverwaltung kontiniuierlich fort. Zudem sollte der CISO-Bund bei allen Regulierungsvorhaben mit einem Bezug zur Informationssicherheit eingebunden werden.
Der CISO-Bund sollte mit ausreichenden Ressourcen, Koordinierungs- und Prüfkompetenzen, einem Vortragsrecht gegenüber dem zuständigen Minister und Berichtspflichten gegenüber dem Bundesrechnungshof und dem Deutschen Bundestag ausgestattet werden. Zugleich sollte er fachlich unabhängig agieren, um Interessenkonflikte bei sicherheitsrelevanten Bewertungen zu vermeiden.
Denkbar wäre eine Verortung im BMDS, um die Verzahnung mit dem CIO des Bundes zu ermöglichen.
Eine Aufhängung beim BSI erscheint jedoch angesichts der fachlichen Nähe passerender. Durch die geteilte Fachaufsicht von BMI und BMDS übernimmt das BSI bereits eine Brückenfunktion zwischen den Ministerien. Diese könnte durch den CISO-Bund beim BSI gestärkt werden. Zumal der CISO-Bund die Aufsichtsbefugnisse des BSI nutzen könnte. Durch die Berichtspflichten würden die Bedeutung und Integration des BSI für Cybersicherheitsaufgaben in der gesamtstaatlichen Sicherheitsarchitektur gestärkt werden. Zugleich verhindert sie eine Bündelung beim Präsidenten.

§ 55 Freiwilliges IT-Sicherheitskennzeichen

Anmerkungen: Angesichts des Regelungsgehaltes des Cyber-Resilience-Acts (CRA) sollte diese Regelung gestrichen werden.

Schlussbemerkungen

Das NIS2-UmsG bietet die Chance, digitale Sicherheit in Deutschland auf ein neues Niveau zu heben. Es schafft vertrauensvolle Rahmenbedingungen. Wer in Cybersicherheit investiert, investiert zugleich in Vertrauen. Damit dieser Anspruch nicht nur auf dem Papier besteht, sondern auch in der Praxis Wirkung entfaltet, braucht es einen echten Schulterschluss von Staat, Wirtschaft und Gesellschaft. Starke Public-Private-Partnerships, klare Zuständigkeiten und eine praxisnahe Umsetzung sind dabei zentrale Erfolgsfaktoren. Die Cybersicherheitsarchitektur Deutschlands muss föderal abgestimmt, aber zugleich kohärent und handlungsfähig sein. Das BSI sollte seine Rolle als zentrale Fachbehörde weiter ausbauen – auch ohne Grundgesetzänderung. Es kann und sollte als Impulsgeber für ein modernes, föderal abgestimmtes Cybersicherheitsmanagement wirken und dabei insbesondere die Schnittstellen zu Ländern, Kommunen und privaten Akteuren stärken.
Die Umsetzung der NIS2-Richtlinie darf nicht als isoliertes Projekt verstanden werden, sondern muss nun eingebettet sein in die neue nationale Cybersicherheitsstrategie.
Nur wenn alle relevanten Akteure gemeinsam Verantwortung übernehmen, kann die digitale Resilienz Deutschlands nachhaltig gestärkt werden.

Der Ersteller bedankt sich bei den Expertinnen und Experten aus Ministerien, Verwaltung, Wirtschaft, Wissenschaft und Zivilgesellschaft für die immerzu bereichernden Diskussionen und den Austausch, die Grundlage für diese Stellungnahme sind.