BDI

INNONATION

STELLUNGNAHME | DIGITALPOLITIK | CYBERSICHERHEIT

Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

Stellungnahme der deutschen Industrie im Rahmen der Verbändebeteiligung

03. Juli 2025

Executive Summary

Die deutsche Industrie begrüßt die Möglichkeit zur Teilnahme an der Verbändebeteiligung zum Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG). Kritisch sieht der BDI die kurze Frist der Beteiligung von Verbänden, die eine intensive Befassung mit dem vorliegenden Gesetzentwurf erheblich erschwert. Angesichts der stetig steigenden Cyberbedrohungslage unterstützt die deutsche Wirtschaft das Bestreben, die Cyberresilienz von Staat und Wirtschaft durch das NIS2UmsuCG nachhaltig zu stärken. Cybersicherheitsanforderungen, die die Breite der deutschen Industrie erfüllen müssen, haben das Potenzial, das Cybersicherheitsniveau der InnoNation, also des Industrie- und Innovationsstandorts Deutschland, zu erhöhen. Sie werden jedoch nur dann dieses Ziel erreichen, wenn sie praxisnah und möglichst unbürokratisch umgesetzt werden. Der BDI fordert daher die Bundesregierung sowie die Abgeordneten des Deutschen Bundestags im laufenden Gesetzgebungsverfahren auf, sicherzustellen, dass

- Unternehmen ihren Melde-, Nachweis- und Registrierungspflichten volldigital nachkommen können und das BSI Information Sharing Portal ein tagesaktuelles Cybersicherheitslagebild auf Basis anonymisierter Informationen aus den Meldungen bietet;
- Kompetenzen zwischen Bundes- und Landesbehörden überlappungsfrei geregelt werden;
- Rechtsunsicherheiten in der Anwendung des NIS2UmsuCG vermieden werden, indem das Bundesamt noch vor Inkrafttreten branchenspezifische Handreichungen veröffentlicht;
- es eine Harmonisierung mit der nationalen Umsetzung der Critical-Entities-Resilience-(CER)-Richtlinie gibt, um Doppelregulierung und Reibungsverluste zu vermeiden.
- das Bundesamt für Sicherheit in der Informationstechnik (BSI) ausreichende personelle und finanzielle Ressourcen hat, um die neuen Anforderungen umsetzen und die Wirtschaft bei der Umsetzung unterstützen zu können;
- die Wirtschaftsverbände bei der Entwicklung von Rechtsverordnungen, die die Wirtschaft betreffen, zwingend angehört werden;
- die Auswirkungen der Änderungen des Begriffs „Kritische Infrastrukturen“ zu „Kritische Anlagen“ BSIG-E als auch in §§ 79, 136, 137, 141, 142 TKG gemeinsam mit der Wirtschaft geklärt wird;
- neben der Gesetzgebung die Sicherheitskultur mit konkreten Maßnahmen, z. B. der Vertrauenswürdigkeitsüberprüfung von Mitarbeitenden gefördert wird und
- die Anforderungen der NIS-2-Richtlinie EU-weit einheitlich und damit ohne zusätzliches nationales Gold-Plating implementiert werden.

Steven Heckler | Stellvertretender Abteilungsleiter Digitalisierung und Innovation | s.heckler@bdi.eu | www.bdi.eu

Angesichts der zahlreichen konkreten Vorschläge, die der BDI sowohl auf EU-Ebene als auch gegenüber der Bundesregierung geäußert hat, bedauern wir, dass diese nahezu alle nicht berücksichtigt worden sind. Rechtssicher und praxisnah formulierte regulatorische Anforderungen sowie unbürokratische und digitale Umsetzungsmaßnahmen sind entscheidend für eine wirksame Erhöhung der Cyberresilienz Deutschlands.

Negative Elemente des Gesetzentwurfs der Bundesregierung

- **Fehlende Harmonisierung mit der nationalen Umsetzung der CER-Richtlinie**: Es fehlt eine Abstimmung mit der geplanten nationalen Umsetzung der CER für die physische Sicherheit kritischer Infrastrukturen. Es besteht die Gefahr paralleler, nicht aufeinander abgestimmter Anforderungen an Unternehmen, die sowohl von NIS2 als auch von der CER-Richtlinie erfasst werden könnten. Zudem führt ein nicht harmonisierter Bestimmungsprozess von KRITIS-Anlagen selbst, ohne gemeinsame Bestimmungsverordnung, zu uneinheitlichen KRITIS-Definitionen und Geltungsbereichen und damit zu einem signifikanten Mehraufwand in den betroffenen Unternehmen. Eine klare Koordinierung innerhalb des federführenden Ressorts erscheint notwendig, um Doppelregulierung und Reibungsverluste zu vermeiden.
- **Fehlende Einbeziehung des Bundesministeriums für Digitales und Staatsmodernisierung:** Unverständlich erscheint, dass bei dem Erlass von Rechtsverordnungen für die Bestimmung „kritischer Anlagen“ durch das Bundesministerium des Innern (BMI) kein Einvernehmen mit dem Bundesministerium für Digitales und Staatsmodernisierung (BMDS) hergestellt werden muss, obwohl das BMDS wegen seiner Zuständigkeit für den TK-Netzausbau regelmäßig sogar in besonderer Weise betroffen sein dürfte. Daher ist das BMDS zwingend in der Aufzählung des § 56 Abs. 4 zu ergänzen.“
- **Definition „wichtige Einrichtungen“ geht über EU-Vorgaben hinaus:** Die Definition wichtiger Einrichtungen muss dringend an die Anforderungen der NIS-2-Richtlinie bzw. an die Empfehlung der EU-Kommission 2003/261 EG angeglichen werden, die vorsieht, dass Unternehmen nur in den Anwendungsbereich fallen, wenn sie mindestens 50 Mitarbeitende beschäftigen und einen Jahresumsatz und / oder eine Jahresbilanzsumme von mindestens zehn Millionen Euro aufweisen.
- **Vernachlässigbare Geschäftsaktivitäten unklar definiert:** Die neue Regelung in § 28 Abs. 3 BSIG, wonach solche Geschäftstätigkeiten unberücksichtigt bleiben können, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind, ist als eine versuchte Vereinfachung zu begrüßen, dennoch führt sie mangels konkreter Definitionen zu erheblichen Unklarheiten. Indirekt führt dies auch zu einer Erweiterung des Scopes, da zunächst alle Dienstleistungen zu betrachten sind, die dann im Rahmen der „Vernachlässigbarkeit“ wieder entfallen. Vor diesem Hintergrund empfehlen wir eine dringende Klarstellung.
- **Fehlende Aufnahme der öffentlichen Verwaltung der Länder und Kommunen in den Anwendungsbereich und fehlende Umsetzungspflicht der Risikomanagementmaßnahmen nach § 30 durch Bundesverwaltung:** Im Sinne der Zeitenwende müssen alle Institutionen aus Wirtschaft, Wissenschaft, Zivilgesellschaft und Staat Maßnahmen zur Stärkung ihrer Resilienz ergreifen. Das NIS2UmsuCG verpflichtet lediglich ausgewählte Behörden der Bundesverwaltung zur Umsetzung der Maßnahmen nach § 30. Da die NIS-2-Richtlinie in den meisten Bundesländern nicht fristgerecht durch landesgesetzliche Regelungen umgesetzt wurde, besteht dringender Nachbesserungsbedarf. Die deutsche Industrie ist auf eine stets funktionierende öffentliche Verwaltung auf allen Ebenen des Staates angewiesen, die nicht durch Cybersicherheitsvorfälle über Monate hinweg lahmgelegt ist. Es sollten alle Behörden des Bundes, der Länder und der Kommunen die Risikomanagementmaßnahmen nach § 30 verpflichtend umsetzen müssen.

- **Geschäftsleitung für Umsetzung der Risikominimierungsmaßnahmen verantwortlich:** Es ist richtig, dass die Geschäftsleitung die Risikominimierungsmaßnahmen genehmigen muss. Regelmäßig wird die Geschäftsleitung jedoch diese nicht direkt umsetzen, sondern hierfür dezidierte Mitarbeitende beschäftigen. Dies muss im NIS2UmsuCG berücksichtigt werden.
- **Weitreichende Ausnahmen von Einrichtungen, die Dienstleistungen für die Verwaltung erbringen:** Die weitreichenden Ausnahmen von Einrichtungen, die Leistungen für die Verwaltung erbringen, sind inakzeptabel. Auch der durch einen Cyberangriff verursachte Ausfall dieser Einrichtungen kann weitreichende negative Folgen für die Industrie sowie die Zivilgesellschaft haben – § 28 Abs. 8 BSIG-E muss zwingend gestrichen werden.
- **Einsatz von Cybersicherheitszertifizierungsschemata:** Da bereits in den CSA-Schemata keinerlei Details zum Anwendungsbereich der Schutzniveaus enthalten sind, sollte der Gesetzgeber § 30 Abs. 6 BSIG-E detaillierter fassen. Die aktuell sehr offene Bestimmung in § 30 Abs. 6 BSIG-E lässt befürchten, dass zukünftig nur noch nach Vertrauensniveau „high“ oder sogar „high+“ zertifizierten Lösungen zum Einsatz kommen dürfen.
- **NIS2UmsuCG sieht keine Vertrauenswürdigkeitsüberprüfung von in sicherheitssensiblen Bereichen tätigen Mitarbeitenden vor:** Damit die weitreichenden Risikomanagementmaßnahmen nicht ins Leere laufen, sollte das NIS2UmsuCG besonders wichtigen Einrichtungen und wichtigen Einrichtungen die Möglichkeit zur Beantragung von Vertrauenswürdigkeitsüberprüfungen von in sicherheitssensiblen Bereichen tätigen Mitarbeitenden einräumen.
- **Drohende Fragmentierung:** Die Umsetzung der NIS-2-Richtlinie in nationales Recht sollte möglichst EU-weit harmonisiert erfolgen, um die Erfüllungsaufwände für international agierende Unternehmen signifikant zu reduzieren, ohne die Cyberresilienz zu schwächen. Mitgliedstaaten sollten auf internationale Standards anstatt auf einen national definierten Stand der Technik o. ä. setzen. Die Bundesregierung sollte in der NIS-2-Richtlinie angelegte Vereinfachungen für bestimmte Branchen, bezüglich Territorialität und Zuständigkeit der deutschen Aufsichtsbehörden für Konzerne mit Hauptsitz in Deutschland zwingend umsetzen.
- **Fehlende Anpassungen bei Kritischen Komponenten:** § 9b BSIG hat sich als unpraktikabel herausgestellt. Es bedarf daher einer gezielten Weiterentwicklung von § 41 BSIG-E hinsichtlich der praktischen Anwendbarkeit des vorgesehenen Verfahrens.
- **Fehlender Bürokratieabbau und fehlende verbindliche Verwaltungsdigitalisierung:** Das NIS2UmsuCG muss zwingend bürokratiearm und unter Ausnutzung der Potenziale des Organisationskontos umgesetzt werden – entsprechende Ansätze fehlen im Gesetzentwurf.
- **Fehlende Anwendbarkeit von Angriffserkennungssystemen in Bezug auf Komponenten und Prozesse:** In § 31 Abs. 2 S. 1 ist der Hinweis auf „Komponenten und Prozessen“ mangels Anschlussmöglichkeit für Angriffserkennungssysteme zu löschen.

Inhaltsverzeichnis

Executive Summary 1

Negative Elemente des Gesetzentwurfs der Bundesregierung 2

Bewertung im Detail 6

Artikel 1 – Änderung des BSI-Gesetzes 7

§ 2 Begriffsbestimmungen 7

§ 3 Aufgaben des Bundesamtes 8

§ 5 Allgemeine Meldestelle für die Sicherheit in der Informationstechnik 9

§ 6 Informationsaustausch 10

§ 11 Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen 11

§ 13 Warnungen 11

§ 14 Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen 12

§ 19a Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden 13

§ 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen 15

§ 29 Einrichtungen der Bundesverwaltung 16

§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen 17

§ 31 Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen 20

§ 32 Meldepflichten 20

§ 33 Registrierungspflicht 22

§ 34 Besondere Registrierungspflicht für bestimmte Einrichtungsarten 24

§ 36 Rückmeldungen des Bundesamts gegenüber meldenden Einrichtungen 24

§ 38 Umsetzung-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen 24

§ 39 Nachweispflichten für Betreiber Kritischer Anlagen 25

§ 41 Untersagung des Einsatzes kritischer Komponenten 25

§ 48 Koordinator für Informationssicherheit 26

§ 52 Zertifizierung 27

§ 53 Konformitätsbewertung und Konformitätserklärung 27

§ 56 Ermächtigung zum Erlass von Rechtsverordnungen 28

§§ 59, 60 Zuständigkeit des Bundesamtes sowie Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten 29

§ 61 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen 30

Anlage 1 30

Artikel 17 – Änderung des Energiewirtschaftsgesetzes 31

§ 5c IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz 31

Artikel 25 – Änderung des Telekommunikationsgesetzes 32

§ 3 Begriffsbestimmungen 32
§ 168 Meldung eines Sicherheitsvorfalls 34

Impressum 36

Bewertung im Detail

Der BDI würde es begrüßen, wenn die neue Bundesregierung die zahlreichen Kommentare zur praxisnahen Ausgestaltung des NIS2UmsuCG, die die Industrie im Folgenden vorlegt, in dieser Legislatur berücksichtigt. Leider ist dies in der vergangenen Legislatur nicht oder zu mindestens nur ungenügend erfolgt. Die deutsche Industrie ist bereit, die Cyberresilienz Deutschlands nachhaltig zu stärken. Hierfür bedarf es jedoch eines praxisnahen Rechtsrahmens sowie einer bürokratiearmen Umsetzung. Der vorliegende Entwurf erfüllt diese Anforderungen weiterhin nicht. Wir würden es begrüßen, wenn die Ressorts sowie die zuständigen Berichterstatter der im Bundestag vertretenden demokratischen Parteien die nachfolgenden Punkte bei der Weiterentwicklung des Gesetzentwurfs berücksichtigen würden.

Das NIS2UmsuCG, das Umsetzungsgesetz der Resilience-of-Critical-Entities-Richtlinie (CER-Umsetzungsgesetz) und kommende Gesetze sollten in Zukunft stärker aufeinander abgestimmt und wesentliche Regelungsinhalte im Sinne des All-Gefahren-Ansatzes besser harmonisiert werden. Der BDI sieht es daher weiterhin kritisch, dass das NIS2UmsuCG nicht zusammen mit dem CER-Umsetzungsgesetz konsultiert wird. Einem ganzheitlichen Sicherheitsansatz folgend, sollten beide Gesetze möglichst kohärent sein, da uneinheitliche Definitionen und Begrifflichkeiten zu Auslegungsproblemen führen können. Beide Gesetze sollten in einem Verfahren beraten und umgesetzt werden, um Doppelungen, Widersprüche und Unklarheiten zu vermeiden. Ein solches integriertes Verfahren würde außerdem späteren Nachbesserungsbedarf an den Gesetzen erheblich verringern. Außerdem sollten in diesem Verfahren bestehende gesetzliche Regelungen zur IT- und Anlagensicherheit mitbetrachtet werden, um auch hier Doppelungen zu vermeiden.

Im Sinne eines ganzheitlichen Schutzkonzepts gegen Cyberkriminalität für den Standort Deutschland sehen wir es weiterhin als notwendig an, dass auch Länder und Kommunen die Anforderungen der NIS-2-Richtlinie entsprechend den Vorgaben des NIS2UmsuCG erfüllen müssen. Wir fordern die Bundesregierung, den Bundestag sowie die 16 Landesregierungen auf, eine einheitliche Cybersicherheitsstrategie zu entwickeln, die ein hohes Niveau bei der Cybersicherheit auf allen Ebenen der Verwaltung ermöglicht.

In Artikel 24 Abs. 1 Satz 2 der NIS-2-Richtlinie (EU) 2022/2555 heißt es: „Darüber hinaus fördern die Mitgliedstaaten, dass wesentliche und wichtige Einrichtungen qualifizierte Vertrauensdienste nutzen.“ Dieser Aspekt findet jedoch im aktuellen Referentenentwurf für ein NIS2UmsuCG keine Berücksichtigung. Wir regen an, diesen Verweis im NIS2UmsuCG aufzunehmen, um durch das Gesetz sicherzustellen, dass Maßnahmen zur breiten Implementierung qualifizierter Vertrauensdienste gefördert werden.

Es ist zu begrüßen, dass die EU einen einheitlichen Rechtsrahmen vorsieht, an dem sich Unternehmen orientieren können. Umso wichtiger ist es, dass in Deutschland kein Gold-Plating betrieben wird. Deutsche Sonderregelungen, die über die EU-Vorgaben hinausgehen, gefährden den Wettbewerb. Deutsche Unternehmen wären gegen die Konkurrenz im EU-Ausland benachteiligt, da etwa eine Komponentenbeschaffung wegen der zusätzlichen Auflagen teurer wäre und zudem das Risiko besteht, dass Lieferanten Kunden aus anderen EU-Ländern wegen niedrigerer Auflagen bevorzugen könnten. Ein Gold-Plating würde daher den Wirtschaftsstandort Deutschland erheblich schwächen und das Wirtschaftswachstum zusätzlich negativ beeinflussen.

Artikel 1 – Änderung des BSI-Gesetzes

§ 2 Begriffsbestimmungen

Damit die Meldepflichten in allen Mitgliedstaaten einheitlich ausfallen – hinsichtlich der zu meldenden Vorfälle sowie deren Auswirkungen – sollten sich die Mitgliedstaaten auf eine einheitliche Auslegungspraxis verständigen. Daher sollte die Bundesregierung im Kontext der Umsetzung von Artikel 23 NIS-2-Richtlinie gemeinsam mit den anderen Mitgliedstaaten dieses gemeinsame Verständnis erarbeiten, anstatt eine nationale Begriffsbestimmung nach § 2 BSIG-E zu entwickeln.

Da das NIS2UmsuCG die Resilienz von Einrichtungen gegenüber digitalen Bedrohungen adressiert, sollte mit der Definition in § 2 Nr. 11 BSIG-E ein erheblicher Cybersicherheitsvorfall und nicht ein erheblicher Sicherheitsvorfall adressiert werden. Diese Unterscheidung würde der zukünftigen Rechtssystematik Rechnung tragen, nach der physische Sicherheitsvorfälle in den Anwendungsbereich des CER-Umsetzungsgesetzes fallen. Die Begriffsbestimmung „finanzielle Verluste“ sollte durch „erheblicher finanzieller Verlust“ ersetzt werden und eindeutig definiert werden, was einen „erheblichen finanziellen Verlust“ kennzeichnet.

Die Definition von „IKT-Produkt“ nach § 2 Nr. 15 BSIG-E sollte zwingend sowohl Hard- als auch Software umfassen. Über den Bezug auf den Cybersecurity Act bestehen diesbezüglich Unsicherheiten, inwiefern Software ebenso mit abgedeckt ist.

Kritische Anlage § 2 Nr. 22 weiterhin als ‚Anlage, die für die Erbringung einer kritischen Dienstleistung erheblich ist; die kritischen Anlagen werden durch Rechtverordnung nach § 56 Abs.4 näher bestimmt. Es fehlt eine Konkretisierung des Begriffes. Begriffsänderung im TKG.

Der Begriff „kritische Infrastrukturen“ wird sowohl im BSIG-E als auch in §§ 79, 136, 137, 141, 142 TKG durch den Begriff „kritische Anlagen“ ersetzt. Die Auswirkungen der Begriffsänderungen sind unklar. Ob hieraus eine Erweiterung des Scopes oder der Verpflichtungen erfolgt ist zu hinterfragen.

Des Weiteren erachten wir die in § 2 Nr. 26 BSIG-E verwendete Definition der „Managed Service Provider“ (MSP) problematisch. Condition Monitoring Services sowie Remote Access sind vielfach Standardfeatures und werden vom Großteil der Hersteller angeboten. Nach der im aktuellen Entwurf vorgenommenen Begriffsbestimmung wäre ein Großteil des deutschen Maschinenbaus sowie die ihn ausrüstenden Komponentenhersteller als besonders wichtige Einrichtungen einzustufen. Hier zeigt sich eine Diskrepanz zwischen dem ursprünglichen Ziel der NIS-2-Richtlinie, den Sektor „Verarbeitendes Gewerbe / Herstellung von Waren“ gem. Punkt 5 in Anlage 2 als „wichtige Einrichtungen“ einzustufen und der bestehenden Regelung. Die Verantwortung für die Sicherheit der beauftragten IT-Dienstleister und die Berücksichtigung entsprechender Features werden außerdem bereits durch die Lieferkettenverantwortung gemäß § 30 Abs. 2 Nr. 4 adressiert. Der Gesetzgeber sollte hier eine klare und kohärente Regelung schaffen, die Doppelbelastungen für die betroffenen Einrichtungen vermeidet. Die Problematik wird durch das weite Begriffsverständnis, welches in der Gesetzesbegründung § 2 Nr. 26 vertreten wird zusätzlich erschwert.

Aktuell besteht aus unserer Sicht die Gefahr einer Überregulierung für Rechenzentrumsbetreiber, da gemäß § 2 Nr. 35 BSIG-E eine weitreichende Einbeziehung aller benötigten Anlagen und Infrastrukturen, insbesondere jene für die Stromverteilung, vorgesehen ist. Diese Regelung geht über die Anforderungen der EU hinaus und könnte zu unnötigen Belastungen führen. Damit werden Rechenzentrumsbetreiber stärker in die Verantwortung genommen als andere Einrichtungen. Die deutsche Industrie fordert eine 1:1-Umsetzung der EU-Vorgaben, um ein Level-Playing-Field zu gewährleisten sowie für EU-weit agierende Unternehmen die Umsetzung möglichst unbürokratisch auszugestalten.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf begrüßen:

§2 11. „erheblicher *Cybers*~~S~~icherheitsvorfall“ ein Sicherheitsvorfall, der

a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder

b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann~~,~~

sofern nach § 58 Absatz 5 keine konkretisierende Begriffsbestimmung erfolgt;

§ 3 Aufgaben des Bundesamtes

Die deutsche Industrie begrüßt, dass das BSI als Deutschlands oberste Cybersicherheitsbehörde weiter gestärkt wird. Es ist jedoch erforderlich, dass der Anwuchs an Kompetenzen sowie Zuständigkeiten, der sich z. B. aus der Betreuung von zukünftig 29.850 Einrichtungen, die in den Anwendungsbereich des NIS2UmsuCG fallen, ergibt, auch durch eine entsprechende Stärkung der personellen und organisatorischen Kapazitäten des BSI unterlegt wird. Es ist daher zwingend erforderlich, dass in den bevorstehenden Haushaltsberatungen das BSI die notwendigen Haushaltsmittel bewilligt bekommt und das Recruiting von neuen Mitarbeitenden rasch initiiert wird. Andernfalls wird das BSI die ihm übertragenen Aufgaben nicht in der notwendigen Qualität sowie Geschwindigkeit umsetzen können. Es muss vermieden werden, dass Unternehmen ihren Meldepflichten gemäß § 32 BSIG-E nachkommen, das BSI jedoch keine personellen Ressourcen vorhalten kann, um die eingehenden Meldungen zu analysieren. Das NIS2UmsuCG darf nicht zu einem bloßen Aufbau von Bürokratie führen, ohne Mehrwerte für die Cyberresilienz Deutschlands zu leisten. Wir fordern die Bundesregierung auf, den im Gesetzentwurf genannten Personalbedarf mit Haushaltsmitteln im Bundeshaushalt für 2025 zu unterlegen.

Der BDI lehnt das Beschreiben und Veröffentlichen eines Stands der Technik durch das BSI ab (vgl. § 3 Abs. 1 Satz 2 Nr. 27 BSIG-E). Der Stand der Technik entwickelt sich stetig weiter, basierend auf Standards und Innovationen sowie am Markt verfügbarer Technologien. Der national definierte Stand der Technik würde daher bereits bei Veröffentlichung veraltet sein. Zudem widerspricht dieses nationale Ansinnen dem Gedanken des Europäischen Binnenmarkts sowie den internationalen Standardisierungsbestrebungen. Die deutsche Industrie befürchtet zudem, dass durch die Definition „Stand der Technik“ bereits eingesetzte Hardware und Technik verboten werden. Hier müssen Ausnahmen unter bestimmten Rahmenbedingungen möglich sein, sofern nicht ein berechtigtes Interesse durch einen bestätigten Sicherheitsmangel oder Vertrauensverlust besteht. Weiter ist sicherzustellen, dass die betroffenen Hersteller und Betreiber vorab über anstehende Verbote informiert werden.

Artikel 24(1) der NIS2 Richtlinie besagt, dass die Mitgliedsstaaten in wesentlichen und wichtigen Einrichtungen die Nutzung qualifizierter Vertrauensdienste fördern. Dies fehlt im vorliegenden Entwurf. Der BDI regt an, dass die Bundesregierung eine entsprechende Formulierung aufnimmt.

Ferner sind die Auswirkungen der zukünftigen geteilten Fachaufsicht über das BSI durch das BMI und das Bundesministerium für Digitales und Staatsmodernisierung noch völlig unklar. Es braucht effiziente Abstimmungen zwischen BMI und BMDS, um die Arbeit des BSI und damit die Cyberresilienz Deutschlands nicht zu schwächen.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf begrüßen:

~~27. einen Stand der Technik von sicherheitstechnischen Anforderungen an IT-Produkte, unter Berücksichtigung bestehender Normen und Standards unter Einbeziehung der betroffenen Wirtschaftsverbände, beschreiben und veröffentlichen;~~

30. Die Förderung des Einsatzes von qualifizierten Vertrauensdiensten bei wesentlichen und wichtigen Einrichtungen durch Erarbeitung von Einsatzempfehlungen.

§ 5 Allgemeine Meldestelle für die Sicherheit in der Informationstechnik

Die deutsche Industrie begrüßt, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) auch zukünftig die zentrale Stelle in Deutschland für die Bearbeitung von Meldungen von Unternehmen sowie im Binnenverhältnis der Behörden des Bundes ist. Im Rahmen der Einführung des in der Nationalen Cyber-Sicherheitsstrategie enthaltenen BSI Information Sharing Portals (BISP) sollten Erkenntnisse aus den Meldungen nach § 32 BSIG-E in anonymisierter Form an alle unter das NIS2UmsuCG fallenden Unternehmen weitergeleitet werden. Das BSI sollte ein tagesaktuelles, kostenfreies Lagebild zu digitalen und physischen Bedrohungen erstellen und täglich mit allen Einrichtungen, die in den Anwendungsbereich des NIS-2-Umsetzungsgesetzes fallen, teilen. Hierfür erachten wir das in der Nationalen Cyber-Sicherheitsstrategie der Bundesregierung angekündigte und in § 6 BSIG-E angelegte BSI Information Sharing Portal als probaten Ansatz.

Die deutsche Industrie fordert, dass die Meldewesen nach § 5 BSIG-E und CER-Umsetzungsgesetz in einem gemeinsamen Meldewesen zusammengefasst werden. So könnte der Zunahme hybrider Bedrohungen und dem All-Gefahren-Ansatz Rechnung getragen werden. Auf Basis der eingegangenen Meldungen könnte so zudem ein ganzheitliches Sicherheitslagebild erstellt werden. Ein gemeinsames Meldewesen würde zudem den bürokratischen Aufwand für Unternehmen signifikant reduzieren, die Kosten für den Betrieb des Meldewesens so weit als möglich minimieren und Effizienzgewinne heben. BSI und das Bundesamt für Bevölkerungs- und Katastrophenschutz (BBK) müssen bei der Erarbeitung des Meldewesens eng zusammenarbeiten.

Im Kontext der Anforderungen des Online-Zugangsgesetzes (OZG) ist es zwingend erforderlich, dass das BSI und das BBK einen Ende-zu-Ende digitalisierten Meldeweg etablieren, der eine sichere Authentifizierung der meldenden Einrichtung ermöglicht. Es ist zu prüfen, inwiefern das auf Elster oder anderen im OZG vorgesehenen Identifizierungsmitteln basierende Organisationskonto hierfür als technische Grundlage fungieren kann, da dies ein Rechte- und Rollenmanagement enthält und zukünftig als zentrale digitale Schnittstelle zwischen Unternehmen und der öffentlichen Verwaltung fungieren soll. Der bundesweite Roll-out des Organisationskontos wäre hierfür eine unverzüglich umzusetzende Voraussetzung. Vom Aufbau von Parallelstrukturen sollte hingegen zwingend Abstand genommen werden.

Damit die Sicherheitsexpertinnen und -experten in den Unternehmen einen zentralen Ort für Informationen zu allen aktuellen Bedrohungen haben, sollte das BSI Information Sharing Portal auch Informationen zu analogen Bedrohungen und Vorfällen (z. B. Sabotage, Naturkatastrophen, Bombenentschärfungen oder durch natürliche Vorfälle bedingte Ausfälle von Strom, Mobilfunk und Glasfaser) enthalten. Des Weiteren ist es für Security-Abteilungen von Unternehmen sehr wichtig, dass die über das Portal bereitgestellten Informationen auch eine hinreichende Detailtiefe aufweisen und umsetzbar sind, diese also auf Basis der Informationen konkrete Maßnahmen zur Stärkung der Resilienz ihrer Systeme ableiten können. Angesichts der Fülle an aktuellen Sicherheitsbedrohungen für Unternehmen ist eine Bündelung entsprechender Informationen in einem zentralem „Sicherheitslagebilds“ von herausgehobener Relevanz. Von zentraler staatlicher Stelle sollten über ein Sicherheitslagebild all diejenigen Informationen in geeignetem Umfang bereitgestellt werden, die aufgrund der verschiedensten Berichtspflichten der Wirtschaft an den Staat gemeldet wurden. Insbesondere die Wahrscheinlichkeit, dass ein gleichgearteter Angriff bei mehreren Unternehmen nacheinander erfolgreich ist, kann so erheblich

verringert werden. Die Zentralisierung derartiger Information setzt zudem Ressourcen zur Bekämpfung von Risiken in den Unternehmen frei, die derzeit auch für mehrfaches, redundantes Reporting eingesetzt werden müssen. Zugleich sollten mit dem Ansteigen der Meldungen auch zusätzliche personelle Strukturen auf staatlicher Seite aufgebaut werden, um die gesammelten Informationen zu sichten, zu filtern, zu verdichten und Warnungen aussprechen zu können.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf begrüßen:

§ 5

(2) Das Bundesamt nimmt zur Wahrnehmung der Aufgaben nach Absatz 1 Informationen zu Schwachstellen, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen sowie zu *Cyber~~S~~*icherheitsvorfällen, Cyberbedrohungen und Beinahevorfällen entgegen. Das Bundesamt richtet hierzu *gemeinsam mit dem Bundesamt für Bevölkerungs- und Katastrophenschutz Ende-zu-Ende digitalisierte* ~~geeignete~~ Meldemöglichkeiten *auf Basis des Organisationskontos* ein. Die Meldungen können anonym erfolgen. Erfolgt die Meldung nicht anonym, kann der Meldende zum Zeitpunkt der Meldung oder später verlangen, dass seine personenbezogenen Daten nur anonymisiert weitergegeben werden dürfen. Dies gilt nicht in den Fällen des § 8 Absatz 6 und 7 Satz 1. Eine Übermittlung der personenbezogenen Daten in den Fällen von § 8 Absatz 6 und 7 Satz 1 hat zu unterbleiben, wenn für das Bundesamt erkennbar ist, dass die schutzwürdigen Interessen des Meldenden das Allgemeininteresse an der Übermittlung überwiegen. Zu berücksichtigen ist dabei auch die Art und Weise, in der der Meldende die Erkenntnisse gewonnen hat. Die Entscheidung nach Satz 6 muss dem oder der behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem oder einer weiteren Bediensteten des Bundesamtes, der oder die die Befähigung zum Richteramt hat, zur vorherigen Prüfung vorgelegt werden.

(3)

1. Dritte *im Rahmen eines tagesaktuellen Lageberichts oder über das BSI Information Sharing Portal* bekannt gewordene Schwachstellen, Schadprogramme, erfolgte oder versuchte Angriffe auf die Sicherheit in der Informationstechnik zu informieren, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,

4. besonders wichtige Einrichtungen und wichtige Einrichtungen gemäß § 40 Absatz 3 Nummer 4 Buchstabe a über die sie betreffenden Informationen *im Rahmen eines tagesaktuellen Lageberichts oder über das BSI Information Sharing Portal tagesaktuell* zu unterrichten.

§ 6 Informationsaustausch

Die deutsche Industrie begrüßt, dass das BSI eine Online-Plattform zum Informationsaustausch mit wichtigen Einrichtungen, besonders wichtigen Einrichtungen und Einrichtungen der Bundesverwaltung betreiben wird. In diesem Kontext erachten wir den Aufbau des BSI Information Sharing Portals als richtigen und zwingend notwendigen Ansatz, um für die Breite der Organisationen, die in den Anwendungsbereich des NIS2UmsuCG fallen, einen effizienten Informationsaustausch zu ermöglichen. BMI und BSI sollten rasch in einer Beta-Fassung einen ersten Entwurf des BSI Information Sharing Portals vorlegen und diesen gemeinsam mit der Wirtschaft entlang deren Bedarfe weiterentwickeln. In jedem Fall sollte das Portal zielgruppengerechte, hilfreiche Lageinformationen für Unternehmen bereitstellen. Um den Anforderungen des Onlinezugangsgesetzes gerecht zu werden, sollte das BMI über das Organisationskonto ein praktikables Zugangsmanagement ermöglichen. Ferner müssen sensible Unternehmensdaten im BSI Sharing Portal geschützt sein.

Neben dem Informationsaustausch in digitaler Form sollte jedoch auch weiterhin der Umsetzungsplan KRITIS (UP KRITIS) fortgeführt werden, um den persönlichen und vertrauensvollen Austausch zwischen den Akteuren zu ermöglichen. In den UP KRITIS sollten die neu in den Anwendungsbereich fallenden KRITIS-Unternehmen aufgenommen werden. Ferner muss geklärt werden, wie der Informationsaustausch zwischen Behörden und wichtigen Einrichtungen ebenso vertieft werden kann.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf begrüßen:

§ 6

(3) Das Bundesamt stellt den Betreibern Kritischer Anlagen, besonders wichtigen Einrichtungen, wichtigen Einrichtungen, Einrichtungen der Bundesverwaltung sowie deren jeweiligen Lieferanten oder Dienstleistern bis spätestens [drei Monate nach Inkrafttreten] eine Beta-Version einer volldigitalen Plattform zum Informationsaustausch bereit und entwickelt diese auf Basis einer öffentlichen Konsultation weiter.

§ 11 Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

Die deutsche Industrie begrüßt, dass das BSI in herausgehobenen Cybersicherheitsvorfällen auf Ersuchen eines Betreibers Kritischer Anlagen, einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen IT-Systems unterstützen wird. Angesichts der weitreichenden Expertise des BSI sowie der zunehmenden Schwere von Cybersicherheitsvorfällen ist jede Form der verstärkten Kooperation von Staat und Wirtschaft im Bereich Cybersecurity ein begrüßenswerter Schritt.

Sofern das Bundesamt zur Behebung eines herausgehobenen Falles einer Kompromittierung der informationstechnischen Systeme einen Dritten hinzuzieht, muss die in Absatz 5 angelegte Pflicht zum Einholen des Einverständnisses zwingend erfolgen. Dies gilt umso mehr, als dass der Ersuchende die Kosten für den Einsatz Dritter übernehmen muss.

§ 13 Warnungen

Die deutsche Industrie begrüßt, dass Hersteller von betroffenen Produkten vor der Veröffentlichung einer Warnung durch das BSI informiert werden sollen. Der BDI spricht sich dafür aus, dass Warnungen durch das BSI über Sicherheitslücken in Produkten (§ 13 Abs. 1 BSIG-E) grundsätzlich mit dem Produkthersteller kooperativ durchgeführt werden sollten (siehe Coordinated Vulnerability Disclosure z. B. ISO/IEC 29147:2018 Information technology – Security techniques – Vulnerability disclosure). Hersteller, respektive ihre europäischen Inverkehrbringer, müssen grundsätzlich in einem angemessenen Zeitraum vor Veröffentlichung einer Warnung durch das BSI informiert werden, um entsprechende Lösungen zur Behebung der Sicherheitslücken in Produkten für Kunden anbieten zu können.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf begrüßen:

§ 13

(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 20 und 21 kann das Bundesamt *gemeinsam mit dem Produkthersteller entsprechend dem Coordinated Vulnerability Disclosure-Prinzip in einem angemessenen Zeitraum entsprechende Lösungen zur Behebung der Sicherheitslücken anbieten.*

(2) Die Hersteller betroffener Produkte *respektive ihre europäischen Inverkehrbringer* sind rechtzeitig vor Veröffentlichung der Warnungen zu informieren.

§ 14 Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen

Zur Stärkung der Cyberresilienz Europas sind sichere informationstechnische Produkte und Systeme unerlässlich. Der BDI begrüßt daher ausdrücklich, dass mit dem Cyber Resilience Act (CRA) ein EU-weit geltender Rechtsrahmen zur Stärkung des Cybersicherheitsniveaus von allen auf dem Binnenmarkt verfügbaren Produkten mit digitalen Elementen geschaffen wurde. Die deutsche Industrie wird im Rahmen von Konsultationsverfahren und Standardisierungsgremien die Umsetzung des CRA engagiert unterstützen. Bis zum Inkrafttreten des CRA ist das in § 14 BSIG-E vorgesehene Vorgehen eine probate Übergangslösung. Ab dem Inkrafttreten des CRA muss zwingend sichergestellt werden, dass es keine parallelen Formen der Marktaufsicht gibt.

Aus dem Gesetzentwurf sowie aus dessen Begründung geht nicht hervor, inwieweit der Gesetzgeber im Kontext des Auskunftsverlangens des BSI gegenüber Herstellern informationstechnischer Produkte eine sachgerechte Abwägung der Interessen der Allgemeinheit an der Sachverhaltsaufklärung sowie dem Interesse des in Anspruch genommenen Betroffenen an der Geheimhaltung von produkt- bzw. servicebezogenen Informationen vorgenommen hat. Insbesondere ist das Verhältnis der entsprechenden Auskunftsrechte zum GeschGehG gänzlich unklar. Mit Blick auf „Auskünfte, insbesondere auch zu technischen Details“ (§ 14 Abs. 2 BSIG-E), muss der Gesetzgeber sicherstellen, dass das BSI ein Verfahren etabliert, welches, soweit technisch und prozedural möglich, den Schutz von Betriebs- und Geschäftsgeheimnissen gewährleistet und die Gefahr von Industriespionage minimiert.

Wenn Schwachstellen gemeldet werden, für die ein Patch zeitnah nicht verfügbar ist, darf eine externe Kommunikation nur in Absprache mit den Herstellern erfolgen, um Schäden für Kunden und Betreiber durch die Veröffentlichung von Angriffsmöglichkeiten zu vermeiden. Das BSI muss verpflichtet sein, dem Hersteller unverzüglich den Eingang der Meldung über die Beschreibung der Angriffsmöglichkeit sowie den Inhalt der vom BSI geplanten externen Kommunikation rechtzeitig vor deren Veröffentlichung mitzuteilen. Dem Hersteller muss angemessene Zeit eingeräumt werden, den Punkt zu beheben, bevor eine Veröffentlichung erfolgt.

Damit auch diejenigen Hersteller, die ihre Produkte von außerhalb der EU auf dem Europäischen Binnenmarkt platzieren, durch die Informationen des BSI erreicht werden, sollte an jeder Stelle in § 14 BSIG-E, der bisher ausschließlich „Hersteller“ nennt, zugleich auf Inverkehrbringer verwiesen werden. Nur so wird sichergestellt, dass auch außereuropäische Hersteller erreicht werden, deren Waren durch Marktplätze sowie den Einzelhandel in Deutschland in Verkehr gebracht werden.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf begrüßen:

§ 14

(6) Um den Schutz von Geschäfts- und Betriebsgeheimnissen des Herstellers nach Satz 1 zu wahren, nutzt das Bundesamt ein sicheres Verfahren zu Übermittlung von Daten. Ist dem Hersteller nach Satz 1 eine sichere Übermittlung auf elektronischem Wege nicht möglich, so gewährt dieser Einsicht an einem Ort, der sich unter der Kontrolle des Herstellers befindet und an dem der Hersteller die Sicherheitsbestimmungen festlegt.

§ 19a Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden

Der Schutz von Unternehmen vor Spionage, Sabotage, Wirtschafts- sowie Cyberkriminalität setzt ein ganzheitliches Schutzkonzept voraus. Neben organisatorischen und technischen Maßnahmen müssen auch die Mitarbeitenden integraler Bestandteil ganzheitlicher Sicherheitsansätze sein. Stetige Schulungs- und Sensibilisierungsmaßnahmen sind hier die zentralen Bausteine. Daneben kann die Überprüfung der Vertrauenswürdigkeit von aktuellen und künftigen Mitarbeitenden, die in sicherheitsrelevanten Unternehmensbereichen tätig sind, im Sinne des vorbeugenden personellen Sabotageschutzes einen Beitrag zur Resilienz von Unternehmen leisten. Bislang fehlt eine gesetzliche Grundlage, die definiert, wie Unternehmen rechtssicher überprüfen lassen können, ob Bewerbende, Mitarbeitende sowie Dienstleistende, die für die Entwicklung und Umsetzung von physischen und digitalen Schutzkonzepten im Rahmen des NIS2UmsuCG sowie des CER-Umsetzungsgesetzes zuständig sind, zuverlässig und vertrauenswürdig sind.

Die deutsche Industrie fordert die Bundesregierung im Rahmen der Gesetzgebungsverfahren zum NIS2UmsuCG sowie CER-Umsetzungsgesetz auf, die in Artikel 14 der Resilience-of-Critical-Entities-Richtlinie ((EU) 2022/2557) angelegte Möglichkeit zur Schaffung einer freiwilligen Zuverlässigkeits- / Vertrauenswürdigkeitsüberprüfung von Mitarbeitenden bei der Umsetzung der europarechtlichen Anforderungen in Deutschland zu implementieren. Die freiwillige Vertrauenswürdigkeitsüberprüfung sollte – analog zur Sicherheitsüberprüfung und zur Zuverlässigkeitsüberprüfung – durch staatliche Stellen erfolgen. Ein geeigneter rechtlicher Rahmen ist hierfür zu schaffen. Von der Vertrauenswürdigkeitsüberprüfung (VWÜ) soll explizit die Luftverkehrswirtschaft, für die bereits die Zuverlässigkeitsüberprüfung (ZÜP) nach § 7 Luftfahrtsicherheitsgesetz (LuftSiG) geschaffen wurde, ausgenommen werden, um Doppelprüfungen auszuschließen. Gleiches gilt für die bestehenden verpflichtenden Zuverlässigkeitsüberprüfungen für das Sicherheitsgewerbe gemäß dem Bewacherregister (zukünftig: Sicherheitsgewerberegister). Die VWÜ ist ferner in Ergänzung zur bestehenden staatlichen Sicherheitsüberprüfung im Geheim- und vorbeugendem personellen Sabotageschutz angelegt. Außerdem muss gewährleistet werden, dass sich die VWÜ in das Zusammenspiel mit bestehenden Überprüfungsmöglichkeiten einfügt, ohne diese zu beeinträchtigen.

Die VWÜ sollte auf drei Prämissen fußen:

1. **Freiwilligkeit:** Unternehmen, die dem NIS2UmsuCG und / oder dem CER-Umsetzungsgesetz unterliegen, sollten die Möglichkeit erhalten, für einen eng umrissenen Personenkreis bei staatlichen Stellen eine Vertrauenswürdigkeitsüberprüfung beantragen zu können, wenn sie dies im Rahmen ganzheitlicher Schutzkonzepte für angezeigt erachten.

2. **Enger Personenkreis:** Unternehmen sollten ausschließlich für Mitarbeitende, Bewerbende sowie Dienstleistende, die gemäß CER-Umsetzungsgesetz und NIS2UmsuCG Risikominimierungsmaßnahmen entwickeln, umsetzen und überprüfen, eine Vertrauenswürdigkeitsüberprüfung beantragen können. Hierbei handelt es sich üblicherweise um Mitarbeitende, Bewerbende und Dienstleistende in den Bereichen der Konzernsicherheit, IT-Administration und Informationssicherheit eines Unternehmens.

3. **Prinzipien und Verfahrensweisen der Sicherheitsüberprüfung:** Die Vertrauenswürdigkeitsüberprüfung sollte auf den Prinzipien und Verfahrensweisen der Sicherheitsüberprüfung nach Sicherheitsüberprüfungsgesetz aufbauen und diese an die aktuellen Gegebenheiten – wie die zunehmende Relevanz von Anbahnungen über Social Media – anpassen.

Um ganzheitliche Schutzkonzepte implementieren zu können, fordert die deutsche Industrie, dass im NIS2UmsuCG sowie im CER-Umsetzungsgesetz für Unternehmen die Möglichkeit geschaffen wird, für Personen, die die in diesen Gesetzen genannten Risikominimierungsmaßnahmen in einem

Unternehmen entwickeln und umsetzen, bei den Sicherheitsbehörden respektive dem Landes- / Bundeswirtschaftsministerium Vertrauenswürdigkeitsüberprüfungen (VWÜ) beantragen zu können. Angesichts der derzeit angespannten Haushalts- und Personallage in der öffentlichen Verwaltung, wäre die deutsche Industrie bereit, die mit einer solchen VWÜ verbundenen Verwaltungskosten mindestens anteilig zu tragen. Diese Bereitschaft gilt unter folgenden Voraussetzungen:

- **Prüftiefenbezogene Gebührenhöhe:** Die für eine Vertrauenswürdigkeitsüberprüfung erhobene Gebühr sollte maximal die tatsächlich anfallenden Kosten decken und je nach Prüftiefe gestaffelt sein.
- **Feste Höchstdauer:** Die Überprüfung sollte – je nach Prüftiefe – innerhalb von maximal zwei Monaten abgeschlossen sein.
- **Bedarfsgerechte Prüftiefe:** Unternehmen müssen die Prüftiefe abhängig von ihren Bedarfen aus zwei Kategorien frei wählen können.
- **Volldigitaler Antrags- und Bearbeitungsprozess:** Der Antrags- und Bearbeitungsprozess muss Ende-zu-Ende digital erfolgen können, die Möglichkeit zur digitalen Signatur muss geschaffen werden.
- **Zusätzliches Personal:** Der Staat muss das durch die Gebühren eingenommene Geld zweckgebunden in zusätzliche personelle und organisatorische Ressourcen in den zuständigen staatlichen Stellen direkt reinvestieren, um so die zügige Durchführung von Vertrauenswürdigkeitsüberprüfungen zu gewährleisten. Bisherige Überprüfungen sollten keinesfalls zukünftig länger dauern als bisher. Um einen Nachfrage-orientierten Kapazitätsaufbau zu gewährleisten, könnte daher neben der stufenweisen Einführung der VWÜ eine vorgelagerte Bedarfsprüfung notwendig sein.
- **Äquivalenz und keine Doppelüberprüfungen:** Um den Aufwand sowohl für Unternehmen als auch für die öffentliche Verwaltung zu begrenzen, ist es zwingend geboten, dass eine sachgemäße Äquivalenz zwischen unterschiedlichen Kategorien der VWÜ, der Sicherheitsüberprüfungen sowie der Zuverlässigkeitsüberprüfung hergestellt wird. Unternehmen sollten für ein und dieselbe Person nicht zur Durchführung mehrerer ähnlich gelagerter Überprüfungen aufgefordert werden. Eine EU-weite Anerkennung sollte geschaffen werden.
- **Staatliche Durchführung:** Auf Antrag durch Unternehmen beim Bundeswirtschaftsministerium (oder einem Landeswirtschaftsministerium) sollte die Sicherheitsüberprüfung durch das Bundesamt für Verfassungsschutz durchgeführt werden.

Details zum Vorschlag des BDI zur Einführung einer Vertrauenswürdigkeitsüberprüfung hat der BDI in einem separaten Positionspapier verfasst: https://bdi.eu/media/publikationen#/publikation/news/vertrauenswuerdigkeitsueberpruefung

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf begrüßen:

§ 19a Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden

(1) Auf Bitte einer besonders wichtigen Einrichtung, einer wichtigen Einrichtung oder eines Betreibers einer Kritischen Anlage führt das Bundesamt für Verfassungsschutz in Zusammenarbeit mit dem Bundeskriminalamt, dem Bundesamt für Sicherheit in der Informationstechnik, den Polizeibehörden des Bundes und der Länder sowie dem Bundesministerium für Wirtschaft und Klimaschutz eine Überprüfung von in besonders sicherheitskritischen Bereichen tätigen oder zukünftig tätigen Personen durch.

(2) Das Bundesamt für Verfassungsschutz teilt der besonders wichtigen Einrichtung, der wichtigen Einrichtung oder dem Betreiber einer Kritischen Anlage das Ergebnis der Überprüfung nach Absatz 1 binnen zwei Monaten mit.

(3) Die in Absatz 1 Satz 1 genannten Einrichtungen können für in sicherheitskritischen Bereichen tätige Mitarbeitende eine einfache sowie eine erweiterte Vertrauenswürdigkeitsüberprüfung beantragen. Die Kosten für eine einfache Vertrauenswürdigkeitsüberprüfung belaufen sich auf maximal 225 Euro, für eine erweiterte auf maximal 600 Euro.

§ 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen

Die deutsche Industrie begrüßt, dass die Unternehmen im besonderen öffentlichen Interesse (UBI) als gesonderte Unternehmenskategorie gestrichen wurden. Einheitliche europäische Anforderungen sind insbesondere für europaweit agierende Unternehmen von zentraler Bedeutung.

Gemäß Art. 2 Abs. 1 NIS-2-Richtlinie gilt diese für öffentliche oder private Einrichtungen der in den Anhängen I oder II genannten Art, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 jenes Artikels überschreiten. Mittlere Unternehmen sind jene, die 50 bis 249 Personen beschäftigen **und** die einen Jahresumsatz von höchstens 50 Millionen Euro erzielen und deren Jahresbilanzsumme sich auf höchstens 43 Millionen Euro beläuft. Es müssen demnach beide Kriterien – die Zahl der Mitarbeitenden und der Jahresumsatz und / oder die Jahresbilanzsumme – gegeben sein, um ein Unternehmen in den Anwendungsbereich der Richtlinie zu bringen. Der Entwurf des deutschen Umsetzungsgesetzes geht indes darüber hinaus, indem er mit § 28 Abs. 2 Nr. 3 lit. a und b „wichtige Einrichtungen“ als im Anhang 1 und 2 aufgeführte Unternehmen umfasst, die mindestens 50 Mitarbeitende beschäftigen **oder** einen Jahresumsatz und / oder eine Jahresbilanzsumme von jeweils über zehn Millionen Euro aufweisen. Durch die Ersetzung des „und“ durch ein „oder“ wird der Anwendungsbereich im Vergleich zur Richtlinie deutlich ausgeweitet. Die deutsche Industrie fordert die Mitglieder des Deutschen Bundestags auf, den Anwendungsbereich des deutschen Gesetzes an die Vorgaben der NIS-2-Richtlinie anzugleichen, um eine übermäßige Belastung für Unternehmen in Deutschland zu vermeiden und die Verhältnismäßigkeit zu gewährleisten. Das deutsche Umsetzungsgesetz sollte die europarechtlich definierten Schwellenwerte 1:1 umsetzen.

Im Falle der Qualifizierung als „besonders wichtige Einrichtung“ ausschließlich aufgrund des Betriebs einer „kritischen Anlage“ gemäß § 28 Abs. 1 Nr. 41 BSIG-E sollte auch nur der diese „kritische Anlage“ betreffende Unternehmensteil den speziellen Anforderungen an „kritische Anlagen“ unterliegen. Dies zudem unter der Voraussetzung, dass Beschaffenheit und Betrieb der informationstechnischen Systeme, Komponenten und Prozesse, die das Unternehmen für die Erbringung der Dienste der Kritischen Anlage nutzt, sich nachvollziehbar innerhalb des Gesamtbetriebs abgrenzen lassen. Ansonsten wären die betroffenen Unternehmen gezwungen, Unternehmensteile, die Betreiber der Kritischen Anlage sind, unternehmensrechtlich in ein verbundenes Unternehmen auszugliedern, einzig um eine Betroffenheit des Gesamtunternehmens zu verhindern.

Wir fordern die Bundesregierung auf, in § 28 BSIG-E klarzustellen, welche Anforderungen bei Unternehmen, die sowohl Kritische Anlagen betreiben sowie Konzernteile, die aufgrund anderer Geschäftsaktivitäten als besonders wichtige Einrichtungen beziehungsweise wichtige Einrichtung einzustufen wären, einschlägig sind. Es muss zwingend sichergestellt sein, dass wichtigen Einrichtungen durch den Betrieb einer Kritischen Anlage regelmäßig kein unverhältnismäßiger Mehraufwand entsteht. Diese Klarstellung ist auch im Hinblick auf die Bußgeldvorschriften nach § 65 BSIG-E notwendig. Grundsätzlich sollte die sich nach Umsatz und Zahl der Mitarbeitenden ergebende Haupttätigkeit bei doppelter Betroffenheit Vorrang haben.

Die neue Regelung in § 28 Abs. 3 BSIG-E, wonach solche Geschäftstätigkeiten unberücksichtigt bleiben können, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind, ist als eine versuchte Vereinfachung zu begrüßen, dennoch führt sie mangels konkreter Definitionen zu erheblichen Unklarheiten. Indirekt führt dies auch zu einer Erweiterung des Scopes, da zunächst alle Dienstleistungen zu betrachten sind, die dann im Rahmen der „Vernachlässigbarkeit“ wieder entfallen. Vor diesem Hintergrund empfehlen wir eine dringende Klarstellung.

Die weitreichenden Ausnahmen von Einrichtungen, die Leistungen für die Verwaltung erbringen, sind inakzeptabel. Auch der durch einen Cyberangriff verursachte Ausfall dieser Einrichtungen kann weitreichende negative Folgen für die Industrie sowie die Zivilgesellschaft haben – § 28 Abs. 8 BSIG-E muss zwingend gestrichen werden, da sonst die Cyberresilienz Deutschlands erheblich beeinträchtigt wird. Unternehmen sowie Bürgerinnen und Bürger sind auf eine stets funktionierende Verwaltung angewiesen. Cyberangriffe auf Kommunen, Länder sowie deren Dienstleister, die zu langwierigen Stillständen in den Verwaltungen führen, verzögern die digitale und grüne Transformation. Zugleich senken sie das öffentliche Vertrauen in die Wehrhaftigkeit und Funktionsfähigkeit des Staates. Dies hätte mittelfristig negative Auswirkungen auf unsere Demokratie.

Die deutsche Industrie erachtet die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf als dringend angezeigt, um die europarechtlichen Vorgaben verhältnismäßig zu implementieren und die Cyberresilienz Deutschlands bestmöglich zu stärken:

(2)

3. natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet, die einer der in Anlagen 1 und 2 bestimmten Einrichtungsarten zuzuordnen sind und die

   a) mindestens 50 Mitarbeiter beschäftigen ~~*oder*~~ *und*

   b) einen Jahresumsatz und */ oder* eine Jahresbilanzsumme von jeweils über zehn Millionen Euro aufweisen.

~~*(8) Dieses Gesetz findet keine Anwendung auf rechtlich unselbstständige Organisationseinheiten von Gebietskörperschaften und auf juristische Personen, an denen ausschließlich Gebietskörperschaften, ausgenommen der Bund, beteiligt sind, wenn sie*~~

~~*1. zu dem Zweck errichtet wurden, im öffentlichen Auftrag Leistungen für Verwaltungen zu erbringen, und*~~

~~*2. durch vergleichbare landesrechtliche Vorschriften unter Bezugnahme auf diesen Absatz reguliert werden.*~~

§ 29 Einrichtungen der Bundesverwaltung

Die deutsche Industrie erachtet es als dem Ziel der NIS-2-Richtlinie nicht angemessen, dass in Deutschland lediglich bestimmte Einrichtungen der Bundesverwaltung in den Anwendungsbereich des NIS2UmsuCG fallen. Hier bedarf es dringender Nachbesserungen, denn die deutsche Industrie ist auf eine stets funktionierende öffentliche Verwaltung auf allen Ebenen des Föderalstaats angewiesen. Damit Cybersicherheitsvorfälle Behörden nicht über Monate lahmlegen, müssen Behörden in ihre Cyberresilienz investieren und hierfür alle in § 30 genannten Risikomanagementmaßnahmen konsequent implementieren. Anhalt-Bitterfeld, Schwerin, Potsdam – zahlreiche Städte und Landkreise sind in den

letzten Jahren Opfer von weitreichenden Cybersicherheitsvorfällen geworden. Bürgerinnen und Bürgern sowie Unternehmen standen infolgedessen – teils über Monate – wichtige Verwaltungsdienstleistungen nicht zur Verfügung. Die deutsche Industrie ist auf eine stets gut funktionierende öffentliche Verwaltung, beispielsweise bei Planungs- und Genehmigungsverfahren, angewiesen. Angesichts der weitreichenden Ausweitung des Anwendungsbereichs auch auf mittlere Unternehmen mit mehr als 50 Mitarbeiterinnen und Mitarbeitern, respektive einem Jahresumsatz größer zehn Millionen Euro, müssen auch Kommunen, Landkreise und Städte zur Umsetzung von risikoadäquaten Cybersicherheitsmaßnahmen verpflichtet werden.

Wir fordern die Bundesregierung, den Bundestag, den Bundesrat und alle 16 Landesregierungen auf, die öffentliche Verwaltung aller Ebenen des Föderalstaats in den Anwendungsbereich des NIS2UmsuCG respektive Umsetzungsgesetze auf Landesebene aufzunehmen, damit alle Behörden risikoadäquate Cybersicherheitsmaßnahmen implementieren und so sensible Daten besser vor Cyberkriminellen schützen. Es ist zwingend sicherzustellen, dass bei Umsetzung in Landesrecht die Anforderungen gleichwertig umgesetzt werden. Nur so kann die Integrität und Verfügbarkeit wichtiger Verwaltungsverfahren angesichts stetig steigender Cyberbedrohungen sichergestellt werden. Bund, Länder und Kommunen müssen zwingend sicherstellen, dass Verwaltungseinheiten auf allen Ebenen des Föderalstaats die an besonders wichtige Einrichtungen gestellten Anforderungen konsequent umsetzen. Andernfalls werden insbesondere Kommunen auch zukünftig vielfach durch Cyberangriffe lahmgelegt. Dadurch würden die digitale und ökologische Transformation ausgebremst und das Vertrauen in die Wehrhaftigkeit des Staates massiv beschädigt. Die deutsche Industrie sieht es ferner zur Wahrung der Wehrhaftigkeit und Funktionsfähigkeit der Bundesverwaltung es als zwingend notwendig an, dass die Bundesbehörden konsequent die in Artikel 1 § 30 genannten Risikomanagementmaßnahmen umsetzen.

Die deutsche Industrie erachtet die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf als dringend angezeigt, um die Wehrhaftigkeit und Funktionsfähigkeit der Bundesverwaltung sicherzustellen:

(2) 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 an-zuwenden.]*~~

§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Die Implementierung von verhältnismäßigen und wirksamen technischen sowie organisatorischen Risikomanagementmaßnahmen ist von herausgehobener Bedeutung, um die Resilienz gegenüber Cyberkriminalität zu erhöhen. Die deutsche Industrie begrüßt, dass die Bundesregierung den Grundsatz der Verhältnismäßigkeit direkt in § 30 Abs. 1 Satz 1 BSIG-E aufgenommen hat. Da der Anwendungsbereich des NIS2UmsuCG sehr weit ist, wäre ein One-Size-Fits-All-Ansatz für den risikoadäquaten Schutz nicht zielführend. Im Sinne des risikobasierten Ansatzes sollte außerdem die Umsetzung und Auswahl von verhältnismäßigen und wirksamen Risikomanagementmaßnahmen dadurch verbessert werden, dass eine noch stärkere Orientierung an den Anforderungen der NIS-2-Richtlinie erfolgt. In Art. 21 Abs. 1 der NIS-2-Richtlinie liegt der Fokus auf der Beherrschung der Risiken für den Betrieb und der Verringerung der Auswirkungen auf die Empfänger der Dienste, während im derzeitigen Entwurf des NIS2umsCG auf die Vermeidung von Störungen (und die Verringerung von Auswirkungen) referenziert wird. Dies sollte im Sinne der Rechtsklarheit und der europäischen Harmonisierung in § 30 Abs. 1 BSIG-E angepasst werden.

Da die NIS-2-Richtlinie keine Umsetzungsfrist für die Betroffenen vorsieht und Unternehmen somit zur Umsetzung der Maßnahmen nach § 30 BSIG-E keinerlei Umsetzungsfrist zugestanden wird, muss der Bundestag klarstellen, was passiert, wenn Unternehmen am Tag nach Inkrafttreten des Gesetzes einen erheblichen Cybersicherheitsvorfall erleiden, jedoch noch nicht die Maßnahmen nach § 30 BSIG-E umgesetzt haben. In solchen Fällen muss es zwingend ausreichen, wenn Einrichtungen einen Projektplan mit klaren Meilensteinen zur Umsetzung der Anforderungen vorweisen können. Die deutsche Industrie fordert die Bundesregierung und den Bundestag auf, Unternehmen mindestens bis zur nächsten Nachweispflicht bei Kritischen Infrastrukturen für die Umsetzung der Risikomanagementmaßnahmen zu gewähren.

Zu Absatz 1: Handlungsbedarf in § 30 besteht in den unzureichenden Formulierungen im Gesetzestext beziehungsweise in den Erläuterungen zum Verständnis des Begriffs „Erbringung ihrer Dienste", wodurch die konkrete Reichweite der Pflichten nach § 30 Abs. 1 unklar bleibt. Ausweislich der Begründung soll der Begriff Erbringung ihrer Dienste weit verstanden werden und sich auf „sämtliche Aktivitäten der Einrichtung (beziehen), für die IT-Systeme eingesetzt werden, dies beinhaltet beispielsweise auch Büro-IT oder andere IT-Systeme, die durch die Einrichtung betrieben werden". Die NIS-2-Richtlinie (EU) 2022/2555 selbst enthält aber keine vergleichbare Konkretisierung beziehungsweise Aussage. Unterstellt man ein derart weites Begriffsverständnis bei § 30 Abs. 1, führt das dazu, dass Unternehmen, die in verschiedenen Geschäftsbereichen tätig sind, dabei aber nur teilweise Dienste erbringen, die unter die in Anlage 1 und Anlage 2 genannten Kategorien zu fassen sind (sektorbezogene Teilbereiche), wohl ihre gesamte IT-Landschaft an den Vorgaben des § 30 Abs. 1 ausrichten müssten. Auch in großen Konzernstrukturen, die sowohl wichtige als auch besonders wichtige Anlagen umfassen, besteht Unklarheit darüber, inwieweit die jeweiligen Verpflichtungen der Bereiche voneinander abgegrenzt werden können. Für Dienste nach § 30, die in verschiedenen Geschäftsbereichen erbracht werden, empfehlen wir, die Definition auf IT-Systeme und IT-Komponenten zu beschränken, die für die Erbringung der Dienste in der jeweils einschlägigen Einrichtungsart nach Anlage 1 oder 2 eingesetzt werden.

Zu Absatz 2: Die entsprechenden Anforderungen sollten der NIS-2-Richtlinie entsprechen, wobei folgende Formulierung in Absatz 2 von der NIS-2-Richtlinie abweicht: „Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten […]". Um einen möglichst hohen Grad an EU-weiter Harmonisierung zu erreichen und damit die Erfüllungsaufwände für die Industrie in einem überschaubaren und praktikablen Rahmen zu halten, sollte der deutsche Gesetzestext entsprechend der Formulierung in der NIS-2-Richtlinie angepasst werden, sodass der Stand der Technik für das Risikomanagement zu berücksichtigen – nicht zwingend einzuhalten – ist. Der Stand der Technik gibt dabei vor, was überhaupt technisch möglich ist und somit im Rahmen des Riskmanagements maximal erwogen werden kann. Eine Grundregel, dass immer das technisch maximal Mögliche in aller Regel auch umzusetzen sei, wäre unverhältnismäßig. Um eine möglichst hohe Planungssicherheit zu gewährleisten, sollte sich diese Anforderung auch auf Systeme und Komponenten beziehen.

Ferner sollte Punkt 9 in der Aufzählung der umzusetzenden Maßnahmen in Absatz 2 nicht auf das „Management von Anlagen", sondern das „Asset Management" rekurrieren, da der englische Begriff im Kontext der Wahrung der Cybersecurity präziser ist.

Zu Absatz 6: Viele Anwenderunternehmen der deutschen Industrie sehen weiterhin kritisch, dass der Gesetzgeber per Rechtsverordnung die Anwendung bestimmter Cybersicherheitszertifizierungsschemata nach EU Cybersecurity Act für besonders wichtige Einrichtungen und wichtige Einrichtungen verpflichtend vorschreiben kann. Insbesondere da weiterhin völlig unklar ist, welche technischen Anforderungen mit den Leveln „basic", „substantial" und „high" verbunden werden, bedarf es hier einer risikoadäquaten Anwendung von § 30 Abs. 6. BSIG-E. Im Rahmen eines risikobasierten Ansatzes sollten – unter Berücksichtigung des bestimmungsgemäßen Gebrauchs – insbesondere der konkrete

Verwendungszweck und die Integrationstiefe des betreffenden IKT-Produkts oder -Prozesses berücksichtigt werden. Um praxisnahe Lösungen zu finden, bedarf es dringend eines strukturierten Dialogs zwischen den Bundesministerien sowie Anbieter- und Anwenderindustrien. Der BDI bietet an, hierfür ein Format unter Einbeziehung der zuständigen Ressorts durchzuführen. Ferner ist im Rahmen der Umsetzung der NIS-2-Richtlinie auf eine europaweit einheitliche Implementierungspraxis der Schemata, z. B. des EUCS, hinzuwirken, um den digitalen Binnenmarkt nicht zu zersplittern.

Sofern sektorale Gesetze (z. B. Medizinprodukteverordnung (MDR) / Verordnung (EU) 2017/745 sowie die Verordnung über In-vitro-Diagnostika (IVDR) / Verordnung (EU) 2017/746) Anwendung finden, die Anforderungen an die Cybersecurity bereits enthalten (z. B. MDR / IVDR) und die von der Europäischen Kommission als ausreichend angesehen werden (vergleiche Erwägungsgründe 12 zu MDR / IVDR und 27 zur Typgenehmigung von Fahrzeugen, ihren Systemen und Komponenten nach (EU) 2019/2144 und entsprechend Luftfahrt-Grundverordnung, EU 2018/1139, zertifizierten Produkten aus dem Verordnungsvorschlag zum „Cyber Resilience Act“), sollte auf eine zusätzliche Zertifizierung über Cybersicherheitszertifizierungsschemata nach EU Cybersecurity Act verzichtet werden. Auch sollten nach Abschluss des Gesetzgebungsverfahrens zum Cyber Resilience Act (CRA) die ineinandergreifenden Anforderungen von CSA und CRA Berücksichtigung finden.

Es ist sehr zu begrüßen, dass der Gesetzgeber die die im Erwägungsgrund 29 der NIS-2-Richtlinie genannte Möglichkeit zur Harmonisierung bestehender Cybersicherheitsverpflichtungen bei Luftverkehrseinrichtungen in der Gesetzesbegründung § 39 (Nachweispflichten für Betreiber kritischer Anlagen in) aufgriffen hat. Im Anwendungsbereich der NIS-2-Richtlinie liegende Unternehmen in der Luftverkehrswirtschaft (u. a. Luftfahrtunternehmen) müssen bereits vergleichbare Anforderungen (siehe Cybersicherheitsmaßnahmen nach der DVO (EU) 2019/1583) erfüllen, unabhängig davon, ob sie bisher in den Wirkungsbereich der geltenden BSI-Kritis-Verordnung fallen. Es ist daher sinnvoll, dass das BSI prüfen können sollte, ob diese Anforderungen und die darin enthaltenen Vorgaben gleichwertig zu denen des NIS2UmsuCG sind. So können Doppelstrukturen und -anforderungen vermieden werden. Auch hinsichtlich der Meldepflichten bzgl. Cybersicherheitsvorfällen, die sich aus der NIS-2 und den oben genannten Regulierungen ergäben, wäre eine weitere Harmonisierung und Zentralisierung der Meldestellen wünschenswert (s.u.).

Das Sicherheitsziel “Authentizität” findet sich nicht in § 30 Abs. 1, da davon ausgegangen wird, dass dieses bereits im Ziel „Integrität“ enthalten ist. Dies entspricht nicht der Regelung im TKG-E. § 3 TKG-E wird wie folgt geändert: „53. „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigt;“

Entgegen der Gesetzesbegründung sollte „Erbringung ihrer Dienste“ auf das Erbringen kritischer Versorgungsleistungen respektive der Produktion zentraler Güter verstanden werden.

Die deutsche Industrie würde die Umsetzung folgender Änderung am vorliegenden Gesetzentwurf begrüßen:

§ 30

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik *berücksichtigen* ~~*einhalten*~~, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

§ 31 Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

Angriffssysteme können nur an Systemen angeschlossen werden und nicht an Prozessen oder Komponenten. Daher muss Abs. 2 geändert werden.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf begrüßen:

(2) Betreiber kritischer Anlagen sind verpflichtet, für die informationstechnischen Systeme~~, Komponenten und Prozesse~~, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Dabei soll der Stand der Technik eingehalten werden. Der hierfür erforderliche Aufwand soll nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen.

§ 32 Meldepflichten

Die NIS-2-Richtlinie sieht die Einführung eines sehr bürokratischen Meldewesens vor. Dieses soll mit dem NIS2UmsuCG sowohl in § 32 BSIG-E als auch in § 168 TKG-E implementiert werden, wobei im letzteren Fall eine überflüssige doppelte Meldepflicht zum BSI und zur Bundesnetzagentur (BNetzA) beibehalten werden soll (siehe hierzu unten). Im Sinne des dringend notwendigen Bürokratieabbaus fordert die deutsche Industrie die Bundesregierung sowie die nachgeordneten Bundesbehörden auf, die europäische Anforderungen so bürokratiearm und digital wie möglich umzusetzen. Zahlreiche deutsche Industrieunternehmen haben Standorte in mehreren EU-Mitgliedstaaten. Vielfach erfolgt die unternehmensweite Steuerung der Cybersicherheit jedoch von einem zentralen Standort aus. Vor diesem Hintergrund wäre es wünschenswert und im Sinne eines digitalen Binnenmarkts dringend angezeigt, dass Unternehmen, die in mehr als einem EU-Mitgliedstaat tätig sind, ihren Nachweis-, Registrierungs- und Meldepflichten nur in einem Mitgliedstaat nachkommen müssen, um den Erfüllungsaufwand in einem akzeptablen Rahmen zu belassen.

Besonderes Augenmerk sollte auf ein überlappungs- und dopplungsfreies Meldewesen im Zusammenhang mit den Anforderungen aus Artikel 14 des Cyber Resilience Act (CRA) gelegt werden. Gemäß Artikel 14 des CRA müssen Hersteller von Produkten mit digitalen Elementen aktiv ausgenutzte Schwachstellen und jeden schwerwiegenden Sicherheitsvorfall innerhalb von 24 Stunden an eine einheitliche Meldeplattform zwischen BSI und ENISA melden, was sich mit den Vorgaben aus § 32 des BSIG-E überschneidet. Das BSI empfängt als CSIRT in Deutschland zunächst alle diesbezüglichen Meldungen unter dem CRA und leitet sie dann an die ENISA weiter. Hierbei ist darauf zu achten, dass Hersteller unter beiden Melderegimen – also unter CRA und BSIG – nur an eine zentrale Stelle in Deutschland melden müssen.

Vor dem Hintergrund der parallel umzusetzenden EU-Richtlinie über die Resilienz kritischer Einrichtungen und den darin enthaltenen Meldepflichten begrüßt die deutsche Industrie, dass das Meldewesen nach NIS2UmsuCG durch das BSI im Einvernehmen mit dem Bundesamt für Bevölkerungs- und Katastrophenschutz aufgebaut werden soll.

Zur konkreten Umsetzung der Anforderungen nach § 32 BSIG-E bestehen grundlegende Unklarheiten, die der Gesetzgeber durch Klarstellungen im Gesetzestext sowie durch verbindliche Handreichungen lösen sollte. Gemäß § 2 Abs. 1 Nr. 10. BSIG-E des Referentenentwurfs ist ein „erheblicher Sicherheitsvorfall“ „ein Sicherheitsvorfall, der a) schwerwiegende Betriebsstörungen der Dienste oder

finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann; oder b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann“. Da Unternehmen zunächst prüfen müssen, ob ein Sicherheitsvorfall die Erheblichkeitsschwelle reißt, muss zwingend klargestellt werden, dass die 24-stündige Frist zur Abgabe einer Erstmeldung erst nach Abschluss der Prüfung, ob ein Cybersicherheitsvorfall erheblich ist, beginnt. Die in § 32 Abs. 1 Nr. 1 BSIG-E gewählte Formulierung könnte indes dahingehend interpretiert werden, dass die 24-Stunden-Frist ab dem Zeitpunkt beginnt, an dem die betroffene Einrichtung von einem Sicherheitsvorfall erfährt.

Angesichts der massiven Ausweitung der Meldepflichten pro erheblichem Sicherheitsvorfall (von einer Meldung pro Vorfall nach IT-Sicherheitsgesetz 2.0 zu bis zu fünf Meldungen nach NIS2UmsuCG), ist es zwingend erforderlich, dass das BSI gemeinsam mit der Europäischen Kommission und der ENISA – sowie unter Einbeziehung des Bundesamts für Bevölkerungs- und Katastrophenschutz – zusammenarbeitet, um im Wege eines Durchführungsrechtsaktes ein effizientes, volldigitalisiertes Meldeportal zu etablieren. Dies dient dazu, dass die ohnehin kurzen Meldefristen durch Mehrfachmeldungen und unterschiedliche Formerfordernisse in der Umsetzung nicht zusätzlich verkürzt werden. Pro erheblichen Cybersicherheitsvorfall sollten Unternehmen ein Formular sukzessive befüllen, statt immer wieder ihre Meldungen neu beginnen zu müssen oder eine Meldung in einem EU-weit standardisierten Datenformat hochladen können.

Angesichts des erheblichen Erfüllungsaufwands, der mit jeder Meldung verbunden ist, sollte das BSI in der überwiegenden Mehrzahl der Fälle von einer Zwischenmeldung nach § 32 Abs. 1 Nr. 3 BSIG-E absehen. Insbesondere mittlere Unternehmen werden während der Bearbeitung eines erheblichen Cybersicherheitsvorfalls ihre gesamten personellen und finanziellen IT-Security-Ressourcen in die Vorfallsbearbeitung investieren müssen, sodass jede zusätzliche und nicht zwingend notwendige Meldung vermieden werden muss. Stattdessen muss das Beratungsangebot nach § 36 Abs. 1 BSIG-E gestärkt werden.

Der BDI würde es begrüßen, wenn das im Rahmen der Umsetzung des Onlinezugangsgesetzes entwickelte Organisationskonto als Portallösung für die Meldung genutzt würde. Dies würde bürokratischen Mehraufwand in den Unternehmen deutlich reduzieren, da das Organisationskonto als zentrale Kommunikationsoberfläche zwischen Staat und Industrie fungieren würde. Zugleich würde eine einheitliche Schnittstelle zwischen Staat und Industrie auch für den Staat die Umsetzungskosten erheblich reduzieren, da nur ein und nicht mehrere Systeme gepflegt und weiterentwickelt werden müssten. Die Nutzung des Organisationskontos würde zudem dem Once-Only-Prinzip Rechnung tragen. Da Meldungen nach § 32 BSIG-E auf hochgradig sensiblen Daten beruhen, muss das Modul 6 des Organisationskontos vollständig implementiert sein, da es ein Rechte- und Rollenmanagement ermöglicht.

Da das NIS2UmsuCG den Schutz von besonders wichtigen Einrichtungen sowie wichtigen Einrichtungen vor erheblichen Cybersicherheitsvorfällen in den Fokus nimmt, sollte § 32 BSIG-E durchgehend Bezug auf erhebliche Cybersicherheitsvorfälle und nicht erhebliche Sicherheitsvorfälle nehmen. Andernfalls müssten Unternehmen auch physische Angriffe melden, die die betroffenen Einrichtungen bereits im Zuge der Umsetzung des CER-Umsetzungsgesetzes werden melden müssen.

Für international tätige Unternehmen, deren Cybersecurity-Teams vielfach englischsprachig sind, sollte die Möglichkeit angeboten werden, dass diese die Meldung auch in englischer Sprache an das Bundesamt absetzen können. Da viele Meldungen weitergabepflichtig sind – auch an internationale Partner – würde dies zudem die Arbeit des Bundesamts erleichtern.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf begrüßen:

§ 32

(1)

1. unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen *Cybers~~S~~*icherheitsvorfall, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche *Cybers~~S~~*icherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte,

2. unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen *Cybers~~S~~*icherheitsvorfall, eine Meldung über den *Cybers~~S~~*icherheitsvorfall, in der die in Nummer 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen *Cybers~~S~~*icherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;

(3 a) Unternehmen können die Meldungen nach Absatz 2 und 3 in deutscher oder englischer Sprache an das Bundesamt übermitteln.

(3 b) Im Sinne des Bürokratieabbaus und der Umsetzung des Once-Only-Prinzips richtet das Bundesamt binnen drei Monaten nach Inkrafttreten eine Schnittstelle zwischen dem Meldewesen nach diesem Paragrafen und dem Organisationskonto ein, damit Unternehmen über das Organisationkonto auf das Meldewesen zugreifen können.

§ 33 Registrierungspflicht

Die deutsche Industrie fordert die Bundesregierung auf, ein volldigitales, sicheres Registrierungswesen aufzusetzen, über das Unternehmen ihren Registrierungspflichten nach NIS2UmsuCG und CER-Umsetzungsgesetz nachkommen können. Im Sinne der durchgängigen Implementierung des Once-Only-Prinzips muss sichergestellt sein, dass Unternehmen sich nicht beim BSI und zusätzlich per separatem Formular beim Bundesamt für Bevölkerungs- und Katastrophenschutz registrieren müssen. Vielmehr sollten diese Registrierungspflichten im Sinne einer nutzendenorientierten öffentlichen Verwaltung in einem effizienten und volldigitalisierten Prozess zusammengeführt werden. Auf die so gemeldeten Registrierungsdaten sollten die zuständigen staatlichen Stellen nach dem Need-to-know-Prinzip zugreifen können. Dies würde die Erfüllungsaufwände für Unternehmen reduzieren und Kapazitäten in der Wirtschaft schaffen, die in den Schutz vor Bedrohungen investiert werden könnten. Um die Registrierung möglichst unbürokratisch auszugestalten, sollte das BSI eine Möglichkeit schaffen, dass Einrichtungen ihrer Registrierungspflicht direkt über das Organisationskonto nachkommen können, da dort bereits wesentliche Informationen über ein Unternehmen hinterlegt sind. Im Sinne eines möglichst EU-weit einheitlichen Verfahrens sollte auf die Nennung der Handelsregisternummer verzichtet werden.

Insbesondere aus Perspektive von Anbietern von Telekommunikationsdiensten (z. B. 4G / 5G) ist die Formulierung „Auflistung der Mitgliedstaaten der Europäischen Union, in denen die Einrichtung Dienste der in Anlage 1 oder 2 genannten Einrichtungsarten erbringen“ unpräzise, da der Anbieter bei der Registrierung nicht zweifelsfrei weiß, wo seine Kundinnen und Kunden den Dienst nutzen werden (Stichwort Roaming). Ferner kann sich die Auflistung täglich ändern, da in einem Konzern täglich neue Kundinnen und Kunden aus der EU hinzukommen und die Registrierung müsste somit regelmäßig

überprüft werden. Andernfalls käme nur eine Auflistung aller Mitgliedstaaten in Betracht, um im Zweifel keinen Fehler zu machen.

Da die deutsche Industrie aktuell eine Vielzahl neuer Melde- und Registrierungspflichten umsetzen muss, sehen wir es im Sinne der Verhältnismäßigkeit als notwendig an, dass die erstmalige Pflicht zur Registrierung nach Inkrafttreten des NIS2UmsuCG auf sechs Monate verlängert wird.

Unternehmen, die sich registrieren, obgleich sie nicht in den Anwendungsbereich des NIS2UmsuCG fallen, sollten auch nicht den Meldepflichten nach § 32 nachkommen müssen.

Sollten Unternehmen widerrechtlich den Registrierungspflichten nicht nachkommen, ist die in § 33 Abs. 3 BSIG-E enthaltene Möglichkeit zur Registrierung durch das BSI folgerichtig. Allerdings sollte das Bundesamt Einrichtungen vor einer Registrierung durch das BSI anhören. Nach einer durch das Bundesamt erfolgten Registrierung muss dieses die Einrichtung zwingend binnen angemessener Frist informieren und zudem auf die sich daraus ergebenen Pflichten hinweisen.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf begrüßen:

§ 33

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sowie Domain-Name-Registry-Diensteanbieter sind verpflichtet, spätestens drei Monate, nachdem sie erstmals oder erneut als eine der vorgenannten Einrichtungen gelten oder Domain-Name-Registry-Dienste anbieten, dem Bundesamt über eine gemeinsam vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit folgenden Angaben zu übermitteln:

1. Name der Einrichtung~~,~~ einschließlich der Rechtsform ~~*und falls einschlägig der Handelsregisternummer*~~;

Abweichend von Satz 1 hat die Erstregistrierung nach Inkrafttreten dieses Gesetzes spätestens sechs Monate nach Inkrafttreten des Gesetzes zu erfolgen.

(3) Die Registrierung von besonders wichtigen Einrichtungen und wichtigen Einrichtungen und Domain-Name-Registry-Diensteanbieter kann das Bundesamt im Einvernehmen mit den jeweils zuständigen Aufsichtsbehörden auch selbst vornehmen, wenn ihre Pflicht zur Registrierung nicht erfüllt wird. *Das BSI wird die Unternehmen vor einer Registrierung anhören und nach einer Registrierung über die begründete Einordnung innerhalb eines angemessenen Zeitraums unterrichten. Das Unternehmen kann auf dem Verwaltungsweg gegen die Einordnung in eine der beiden Kategorien vorgehen.*

(6) Das Bundesamt legt die Einzelheiten zur Ausgestaltung des Registrierungsverfahrens im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe fest. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamts. *Das Bundesamt stellt eine Schnittstelle zum Organisationskonto nach Onlinezugangsgesetz sicher, um das Once-Only-Prinzip umzusetzen.*

(7) Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundesamt für Bevölkerungs- und Katastrophenschutz stellen spätestens am 15. Tag nach Inkrafttreten dieses Gesetzes ein gemeinsames, voll digitales Registrierungswesen auf Basis des Organisationskontos zur Verfügung, über welches die besonders wichtigen Einrichtungen und wichtigen Einrichtungen sowie Domain-Name-Registry-Diensteanbieter ihren sich aus diesem Gesetz sowie dem [CER-Umsetzungsgesetz] ergebenden Registrierungspflichten nachkommen können.

§ 34 Besondere Registrierungspflicht für bestimmte Einrichtungsarten

Für deutsche Industrieunternehmen mit Standorten in mehreren Mitgliedstaaten ist es essenziell, dass die Bundesregierung in Abstimmung mit ihren europäischen Partnern sicherstellt, dass Nachweispflichten jeweils nur in dem Land erfolgen müssen, in dem eine Einrichtung ihren Hauptsitz hat, da von diesem zumeist die Cybersicherheitsgovernance erfolgt. Zu berücksichtigen ist hierbei, dass die Definition der Hauptniederlassung und die Auswirkung auf die Tochtergesellschaften in einem Konzernkonstrukt nach wie vor unklar ist. Es ist ferner zu klären, welche Geschäftsleitung innerhalb eines Konzernkonstrukts haftet. Ferner muss geklärt werden, welcher – im Zweifel national definierte – Stand der Technik in einem Konzernkonstrukt umzusetzen ist, jener der Hauptniederlassung oder jener des Landes, in dem eine Tochtergesellschaft tätig ist.

Eine europäisch einheitliche Lösung ist grundsätzlich vorzugswürdig. National abweichende Regelungen, welche über die Anforderungen der NIS-2-Richtlinie hinausgehen, führen zu einer zusätzlichen Belastung für die betroffenen Einrichtungen.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf begrüßen:

§ 34

(3a) Eine Einrichtung im Sinne des Satzes 1, die ihren Hauptsitz in Deutschland hat und für die aus Deutschland heraus die Cybersicherheitsgovernance erfolgt, muss den Nachweispflichten nur in Deutschland nachkommen.

(3b) Eine Einrichtung im Sinne des Satzes 1, deren Hauptsitz in einem anderen EU-Mitgliedstaat liegt, muss dem Bundesamt einmalig bei der Registrierung eine Bescheinigung der nationalen zuständigen Behörde vorlegen, in der ihr Hauptsitz ist und aus der hervorgeht, dass sie ihren Pflichten nach § 30, § 32 und § 34 dort nachkommt. Das Bundesamt kann das Unternehmen alle fünf Jahre auffordern, eine neuerliche Bescheinigung gemäß Satz 1 vorzulegen.

§ 36 Rückmeldungen des Bundesamts gegenüber meldenden Einrichtungen

Der BDI begrüßt ausdrücklich, dass das BSI auf Ersuchen der meldenden Einrichtung, ihr zusätzliche technische Unterstützung zukommen lassen soll. Dies wird insbesondere für mittlere Unternehmen von herausgehobener Bedeutung zur effizienten Vorfallsbearbeitung sein.

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

Der europäische Gesetzgeber hat die „Managerhaftung“ in der NIS-2-Richtlinie in Art. 20 Abs. 1 allgemein und in Art. 32 Abs. 6 BSIG-E zusätzlich für besonders wichtige Einrichtungen definiert. Diese Differenzierung fehlt in § 38 BSIG-E. Die deutsche Industrie fordert den Gesetzgeber auf, diese Differenzierung ins nationale Umsetzungsgesetz aufzunehmen und keine über den europäischen Rechtsrahmen hinausgehenden Anforderungen im NIS2UmsuCG festzuschreiben. Zugleich erachten wir es als sehr problematisch, dass die Behördenleitung in der öffentlichen Verwaltung keine einer Geschäftsleitung eines Unternehmens gleichgelagerten Verpflichtungen auferlegt wird. Hier müsste die öffentliche Verwaltung auf Bundesebene eine Vorbildfunktion einnehmen.

Die Industrie begrüßt es grundsätzlich, dass der Geschäftsleitung eine Mitverantwortlichkeit für die Umsetzung von Cyberrisikominimierungsmaßnahmen zugeschrieben wird. Dadurch wird sichergestellt, dass Einrichtungen hinreichendes Budget für die Umsetzung entsprechender Maßnahmen

vorsehen. Gleichwohl bedarf es aus unserer Sicht einer Klarstellung bezüglich der Möglichkeit zur Delegation der Umsetzung. Insbesondere aus der Perspektive einer Konzernstruktur ist unklar, in welchem Umfang die Delegation von Verantwortlichkeiten auf Konzern- / Unternehmensangehörige im Zusammenhang mit der Einhaltung der Risikomanagementvorgaben zur IT-Sicherheit noch möglich ist. Üblicherweise erfolgt die Verteilung von Aufgaben im Zusammenhang mit der IT-Sicherheit auf einzelne Unternehmensabteilungen und damit korrespondierende Führungsfunktionen (auch unternehmensübergreifend innerhalb eines Konzerns; CISO o. ä.). Es bedarf einer ausdrücklichen Klarstellung, wonach die Umsetzung von Cybersicherheitsmaßnahmen durch Dritte weiterhin möglich ist. Dies würde Rechtssicherheit schaffen. Ferner bedarf es einer raschen Klärung hinsichtlich der inhaltlichen Ausgestaltung der zu belegenden Schulungen.

Da Geschäftsführer regelmäßig die Maßnahmen nach § 30 nicht selbst umsetzen werden, sondern dezidierte Mitarbeitende, z. B. den Chief Information Security Officer, haben, ist die Formulierung von § 38 Abs. 1 realitätsfern. Diese sollte auf die Formulierung des dritten Referentenentwurfs zurückgeändert werden.

Die deutsche Industrie empfiehlt die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf:

(1) Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen *im Bereich der Cybersicherheit zu billigen* ~~*umzusetzen*~~ und ihre Umsetzung zu überwachen.

§ 39 Nachweispflichten für Betreiber Kritischer Anlagen

Der BDI begrüßt, dass das BSI den Betreibern Kritischer Anlagen eine Frist von mindestens drei Jahren gewähren kann, bis sie die Anforderungen nach § 30 Abs. 1 BSIG-E und § 32 BSIG-E erstmals nachweisen müssen. Diese Frist erhöht signifikant die Umsetzbarkeit der gesetzlichen Anforderungen.

Die Nachweispflichten für Betreiber Kritischer Anlagen sind in § 39 BSIG-E nicht hinreichend trennscharf formuliert, sodass nicht nur zum Betrieb Kritischer Anlagen genutzte Systeme, Komponenten und Prozesse umfasst wären. Betreiber Kritischer Anlagen haben laut Referentenentwurf die Erfüllung der Anforderungen nach § 30 Abs. 1 BSIG-E und § 32 BSIG-E dem BSI auf geeignete Weise nachzuweisen. Damit soll der bisherige § 8a BSIG fortgeführt werden. Dieser sieht jedoch unter Verweis auf § 8a Abs. 1 Satz 1 BSIG vor, dass das Schutzziel der Maßnahmen auf die „Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen“ abzielt. Die unter § 30 BSIG-E gelisteten Risikomanagementmaßnahmen stehen jedoch unspezifisch in Bezug zu den informationstechnischen Systemen, Komponenten und Prozessen, die sie für die „Erbringung ihrer Dienste“ nutzen. Diese Diskrepanz wird zu Unklarheiten bei der Umsetzung führen. Es bedarf einer genaueren Definition, was unter diesen Diensten zu verstehen ist. Unserem Verständnis nach können darunter nur die Dienste verstanden werden, die von der Kritischen Anlage erbracht werden. Im Falle der Qualifizierung eines Unternehmens als „besonders wichtige Einrichtung“ ausschließlich aufgrund des Betriebs einer „kritischen Anlage“ gem. § 28 Abs. 1 Nr. 4 BSIG-E sollte daher auch nur der diese „kritische Anlage“ betreffende Unternehmensteil den speziellen Anforderungen an „besonders wichtige Einrichtungen“ unterliegen. Dies ist insbesondere vor dem Hintergrund sinnvoll, wenn die von der Kritischen Anlage erbrachte Dienstleistung in keinem Zusammenhang mit den im sonstigen Kerngeschäft erbrachten Dienstleistungen der betroffenen Einrichtung steht.

§ 41 Untersagung des Einsatzes kritischer Komponenten

Der bisherige § 9b BSIG (zukünftig § 41 BSIG) hat in der Anwendungspraxis zu einem Höchstmaß an Bürokratie sowie Investitions- und Rechtsunsicherheit geführt. Die Resilienz Kritischer Infrastrukturen stellt einen entscheidenden Standortfaktor für die deutsche Industrie dar. Der BDI unterstützt weiterhin

uneingeschränkt das Ansinnen des Gesetzgebers, Kritische Infrastrukturen, soweit technisch und personell nur möglich und sinnvoll, wirksam zu schützen. Der erfolgreiche Abschluss des Öffentlich-Rechtlichen-Vertrags der Bundesregierung mit der TK-Industrie und das demnächst stattfindende Forum, in welchem Lösungen gemeinsam durch die Bundesregierung mit den Betreibern von 5G-Mobilfunknetzen sowie Industriepartnern und Herstellern für die Umsetzung und Förderung der in den Verträgen vereinbarten Ziele erarbeitet werden sollen, sind ein guter Ansatz, um die Resilienz Kritischer Infrastrukturen zu stärken. Dieser Ansatz könnte auch für andere Sektoren als Vorbild dienen. Es braucht anbieterunabhängige Regelungen, die zwingend technische, geo- und sicherheitspolitische Belange gleichermaßen berücksichtigen. Die unreflektierte nahezu wortgleiche Übernahme dieser Vorschrift in das NIS2UmsuCG ohne wesentliche Überarbeitung der Anwendungspraxis ist aus Sicht der deutschen Industrie nicht sachgerecht. Zudem sollte die Bundesregierung erläutern, was mit der neuen Formulierung „kritische Anlagen“, die die Formulierung „kritische Funktionen“ ersetzen soll, für eine inhaltliche Änderung bezweckt wird.

Offen bleiben ferner grundlegende Fragen, wie sich die Kostenträgerschaft im Falle des Rückbaus bereits verbauter Technologie gestaltet und wie sich die Anwendung von § 41 mit der zwingend vorgegebenen Durchführung von Vergabeverfahren für öffentliche Unternehmen in Einklang bringen lässt.

Insbesondere auch vor dem Hintergrund der geplanten Ausweitung der Anforderungen von § 41 auf weitere Sektoren, die zu einem Anwuchs an Anzeigen führen wird, ist es notwendig, ein vereinfachtes und beschleunigtes Verfahren umzusetzen. Dieses könnte auch eine Positiv- und Negativliste von betroffenen Komponenten enthalten. Weiter sollte auch überprüft werden, wie in Fällen verfahren wird, in denen der Einsatz von Kritischen Komponenten aus Mangel an Alternativen notwendig ist, damit eine Anlage überhaupt errichtet oder betrieben werden kann. Die Gesetzgebung sollte nicht dazu führen, dass Anlagen wegen potenzieller Risiken konkret nicht realisiert werden. Daher sollte die Regelung in § 41 Abs. 3 dahingehend angepasst werden, dass Betreiber von Kritischen Anlagen die Möglichkeit erhalten, Kritische Komponenten unabhängig vom Hersteller selbst von einer unabhängigen Stelle überprüfen und gegebenenfalls zertifizieren zu lassen. Dies würde die Anlagensicherheit stärken und gleichzeitig den Druck auf die Lieferkette verringern. Das BMI hatte angekündigt, dass die ausgesetzte Pflicht zur Abgabe von Garantieerklärungen der Hersteller zukünftig entfallen soll. Der Entwurf sieht jedoch in Absatz 3 diese Verpflichtung unverändert vor. Der BDI hält eine solche Verpflichtung für wenig sachdienlich, da die Richtigkeit der Inhalte der Garantieerklärung durch den Betreiber der kritischen Anlage als Erklärungsempfänger und Verpflichteter nicht überprüfbar sind und dementsprechend keine vertraglichen Rechte gegenüber den Herstellern geltend gemacht werden können. Mit der Einholung einer solchen Erklärung wird eine Scheinsicherheit erzeugt, die für den Standort Deutschland kontraproduktiv ist.

§ 44 Vorgaben des Bundesamtes

Das Bundesamt wird nach Abs. 1 den IT-Grundschutz bis zum 1. Januar 2026 modernisieren und fortentwickeln. Abweichungen vom Mindeststandard, die unter sachlich gerechtfertigten Fällen zulässig sind, ist wieder einzufügen. Ferner ergibt sich aus den kurzfristig geplanten Änderungen im IT-Grundschutz eine weitere Umsetzungsverpflichtung je nach Regelungsgehalt für entsprechende Dienstleister.

§ 48 Koordinator für Informationssicherheit

Die deutsche Industrie begrüßt grundsätzlich das Ziel, Informationssicherheit zentral über Ressortgrenzen hinweg zu koordinieren. Wir regen an, dass das Amt des Koordinators / der Koordinatorin für Informationssicherheit entweder durch die Präsidentin / den Präsidenten des BSI oder den / die für Cybersicherheit im Bundesinnenministerium zuständige(n) Staatssekretär(in) in Personalunion

ausgeführt wird. Die Zersplitterung inhaltlich eng zusammengehöriger Aufgaben auf drei Personen würde zu massiven Ineffizienzen führen.

§ 52 Zertifizierung

Potenzielle Entscheidungen nach § 52 Abs 5 BSIG-E müssen frühzeitig und öffentlich durch das Bundesministerium des Innern gegenüber der Industrie angezeigt werden, um Planungs- und Investitionssicherheit zu schaffen.

§ 53 Konformitätsbewertung und Konformitätserklärung

Das in § 53 BSIG-E angelegte Verfahren ist nach unserer Lesart der NIS-2-Richtlinie ein nationaler Alleingang, bei dem nicht ersichtlich ist, wo dieser in der NIS-2-Richtlinie angelegt sein soll. Wir sprechen uns daher für eine Streichung aus, zumindest aber für eine Konformitätserklärung mit europäischen und internationalen Standards, um weitere nationale Alleingänge zu vermeiden.

§ 53 BSIG-E sorgt für erhebliche Unsicherheiten bei den Unternehmen. Deutsche Hersteller stehen bereits heute angesichts umfassender und tiefgreifender digitalpolitischer Regulierungen vor großen Herausforderungen. Mit dem Cyber Resilience Act (CRA) steht ein EU-Rechtsakt kurz vor dem Abschluss, der mit einem horizontalen Regulierungsansatz neue Cybersicherheitsanforderungen für Produkte mit digitalen Elementen vorschreibt. Die deutsche Industrie unterstützt den CRA und sieht ihn als zentralen Mechanismus zur Stärkung der Cyberresilienz von Produkten auf dem europäischen Binnenmarkt. Wir fordern alle EU-Mitgliedstaaten nachdrücklich auf, von nationalen Alleingängen abzusehen, da sie die regulatorische Komplexität erhöhen, ohne einen Mehrwert für Europas Cyberresilienz zu leisten. Die Anpassungen der Entwicklungs- und Produktionsprozesse an den CRA erfordern beträchtliche Ressourcen und haben bereits heute Auswirkungen auf die betriebliche Effizienz sowie die finanzielle Leistungsfähigkeit der Unternehmen.

Gleichzeitig wurde 2019 mit dem Cybersecurity Act (CSA) ein einheitlicher europäischer Zertifizierungsrahmen für IKT-Produkte, -Dienstleistungen und -Prozesse auf den Weg gebracht, der die Notwendigkeit eines zusätzlichen nationalen Zertifizierungssystems infrage stellt. Die deutsche Industrie fordert, dass die Bundesregierung konsistente und EU-weit einheitliche Regelungen priorisiert. Die in § 53 BSIG-E aufgeführten nationalen Zertifizierungen, deren internationale Gültigkeit zudem ungeklärt ist, stehen im Widerspruch dazu und sollten aus dem Gesetzestext entfernt werden.

Der Entwurf des NIS2UmsuCG sieht vor, dass das BSI technische Richtlinien erstellt, die Anforderungen definieren. Der CRA verweist dagegen ausdrücklich auf europäische harmonisierte Normen (hEN), die rechtlich bindend sind und durch CEN, CENELEC und ETSI auf Basis eines Standardisation Requests entwickelt werden. Nationale technische Richtlinien dürfen europäischen harmonisierten Normen nicht entgegenstehen. Eine Herstellerselbsterklärung für wichtige Produkte - darunter fallen teilweise IKT-Produkte - ist nur dann möglich, wenn der Hersteller eine im Amtsblatt der EU gelistete harmonisierte Norm vollständig anwendet. Technische Richtlinien des BSI können diese Funktion nicht übernehmen, da sie keine harmonisierten Normen darstellen. Somit entfällt auch die mit der vollständigen Anwendung harmonisierter Normen verbundene Konformitätsvermutung bei Anwendung technischer Richtlinien des BSI. Daher eignen sich technische Richtlinien nicht für CRA-relevante IKT-Produkte und IKT-Dienstleistungen.

Der CRA schreibt für Produkte die CE-Kennzeichnung sowie klare EU-weite Marktüberwachungsmechanismen vor. § 53 hingegen sieht eine eigene nationale Kennzeichnung vor, was zu doppelter Regulierung und Verwirrung führen kann. Zudem entsteht ein potenzieller Interessenkonflikt im BSI, da es gleichzeitig als Marktüberwachungsbehörde, Ersteller technischer Richtlinien, Benannte Stelle (Notified Body) und Zertifizierungsstelle (Conformity Assessment Body) auftreten soll. Ein solcher Interessenkonflikt sollte vermieden werden, indem das BSI beispielsweise keine Produktzertifizierungen für

Produkte mit digitalen Elementen mehr durchführt und die freiwerdenden Ressourcen stattdessen für eine effektive Marktüberwachung nutzt.

Der § 53 NIS2UmsuCG ist in seiner jetzigen Form nicht mit den Anforderungen des Cyber Resilience Acts (EU 2024/2847) und des Delegierten Rechtsakts der Funkanlagenrichtlinie (EU 2022/30) vereinbar. Die Möglichkeit der Selbstbewertung ohne Unterscheidung der Produktkategorien sowie die parallele Existenz nationaler technischer Richtlinien und Kennzeichnungen stehen im klaren Widerspruch zu den Vorgaben des CRA. Dies könnte Konflikte und Unsicherheiten für Hersteller erzeugen, die ihre Produkte EU-weit vertreiben möchten. Eine Streichung des § 53 schafft Rechtssicherheit und vermeidet unnötige regulatorische Doppelungen.

Die deutsche Industrie empfiehlt folgende Änderungen am vorliegenden Gesetzentwurf:

Komplette Streichung von § 53 BSIG-E

§ 56 Ermächtigung zum Erlass von Rechtsverordnungen

Die deutsche Industrie sieht es kritisch, dass erst per Rechtsverordnung nach § 56 Abs. 4 BSIG-E sowie einer dem CER-Umsetzungsgesetz nachgelagerten Rechtsverordnung die Schwellenwerte für Kritische Anlagen definiert werden. Vorzugswürdig wäre, dass die Schwellenwerte direkt im Gesetzgebungsverfahren für das NIS2UmsuCG und das CER-Umsetzungsgesetz gleichlautend bestimmt werden. Eine direkte Bestimmung im Rahmen der Gesetzgebungsverfahren würde schnellere Rechtssicherheit für die Betroffenen bedeuten und zudem die Umsetzung der Vorgaben beschleunigen. Heute bereits in der BSI-Kritisverordnung bestehende sektorspezifische Schwellenwerte sollten beibehalten werden und nicht weiter abgesenkt werden. Einrichtungen, die unter den Schwellenwerten liegen, sollten als besonderes wichtige Einrichtungen respektive wichtige Einrichtungen gewertet werden.

Ferner erachten wir es als zwingend erforderlich, dass die Wirtschaftsverbände bei der Entwicklung von Rechtsverordnungen, die die Wirtschaft betreffen, angehört werden. Die Anhörung der Wirtschaftsverbände war im Bereich des IT-Sicherheitsrechts bisher gelebte Praxis und sollte zwingend fortgesetzt werden und hat erheblich dazu beigetragen, dass rechtliche Vorgaben möglichst praxistauglich ausgestaltet sind. Die Streichung der entsprechenden Textstellen sollte zurückgenommen werden. Der vom Bundesministerium des Innern und für Heimat im Gesetzgebungsverfahren mehrfach vorgetragene Verweis auf die Geschäftsordnung der Bundesregierung, nach der Anhörungen von Verbänden grundsätzlich vorgesehen sind, erachten wir als nicht ausreichend. Die Durchführung von Anhörungen von Verbänden sollten direkt in den einschlägigen Fachgesetzen verpflichtend verankert werden.

Das neue Bundesministerium für Digitales und Staatsmodernisierung muss als zu beteiligendes Ministerium zwingend in die Aufzählungen mit aufgenommen werden.

Die deutsche Industrie empfiehlt folgende Änderungen am vorliegenden Gesetzentwurf:

(3) Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, *nach Anhörung der betroffenen Wirtschaftsverbände sowie Vertretern der Wissenschaft* im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, *dem Bundesministerium für Digitales und Staatsmodernisierung,* dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Landwirtschaft, Ernährung und Heimat, dem Bundesministerium für Gesundheit, dem Bundesministerium für Ver-kehr, dem Bundesministerium für Forschung, Technologie und Raumfahrt und dem Bundesministerium für Umwelt,

Klimaschutz, Naturschutz und nukleare Sicherheit, welche durch eine besonders wichtige Einrichtung oder eine wichtige Einrichtung eingesetzten Produkte, Dienste oder Prozesse gemäß § 30 Absatz 6 über eine Cybersicherheitszertifizierung verfügen müssen, da sie für die Erbringung der Dienste der Einrichtung maßgeblich sind und Art und Ausmaß der Risikoexposition der Einrichtung einen verpflichtenden Einsatz von zertifizierten Produkten, Diensten oder Prozessen in diesem Bereich erforderlich machen.

(4) Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, *nach Anhörung der betroffenen Wirtschaftsverbände sowie Vertretern der Wissenschaft* im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, *dem Bundesministerium für Digitales und Staatsmodernisierung,* dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Landwirtschaft, Ernährung und Heimat, dem Bundesministerium für Gesundheit, dem Bundesministerium für Ver-kehr und dem Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit unter Festlegung der in § 2 Nummer 24 genannten Sektoren wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Anlagen als kritische Anlagen im Sinne dieses Gesetzes gelten. Der als bedeutend anzusehende Versorgungsgrad ist anhand branchenspezifischer Schwellenwerte für jede als kritisch anzusehende Dienstleistung zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.

(5) Das Bundesministerium des Innern kann *nach Anhörung der betroffenen Wirtschaftsverbände sowie Vertretern der Wissenschaft* im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie und im Benehmen mit dem Bundesministerium der Justiz und für Verbraucherschutz, *dem Bundesministerium für Digitales und Staatsmodernisierung,* dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Landwirtschaft, Ernährung und Heimat, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, bestimmen, wann ein Sicherheitsvorfall im Hinblick auf seine technischen oder organisatorischen Ursachen oder im Hinblick auf seine Auswirkungen auf die Einrichtung, den Staat, die Wirtschaft oder die Anzahl der von den Auswirkungen Betroffenen als erheblich im Sinne von § 2 Nummer 11 anzusehen ist. Das Bundesministerium kann diese Ermächtigung durch Rechtsverordnung auf das Bundesamt übertragen. Etwaige Durchführungsrechtsakte der Europäischen Kommission gemäß Artikel 23 Absatz 11 Unterabsatz 2 der NIS-2-Richtlinie, die die Voraussetzungen eines erheblichen Sicherheits-vorfalls bestimmen, gehen der Rechtsverordnung nach den Sätzen 1 und 2 insoweit vor. - 64 - Bearbeitungsstand: 23.06.2025 17:12

§§ 59, 60 Zuständigkeit des Bundesamtes sowie Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten

§ 59 legt die Zuständigkeit des Bundesamtes für die Einhaltung der Vorschriften aus Teil 3 (§§ 28-50) für wichtige Einrichtungen und besonders wichtige Einrichtungen, aber auch für Kritische Anlagen in Deutschland fest. Mit § 60 wird diese Zuständigkeit – hierzu gehört auch die Zuständigkeit für Kritische Anlagen – bei IT-Dienstleistungen auf Unternehmensteile oder Beteiligungen in EU-Mitgliedstaaten erweitert, wenn der Hauptsitz des Unternehmens / Konzerns in Deutschland liegt. Das hätte in der jetzigen Formulierung die Konsequenz, dass das deutsche rechtliche Konzept der „Kritischen Anlagen“ auch im europäischen Ausland gelten würde, wenn der Hauptsitz des Betreibers in Deutschland liegt. Diesen „Export“ der erhöhten deutschen KRITIS-Anforderungen in das europäische Ausland gilt es zu vermeiden, weil es über die eigentlichen Anforderungen der NIS-2-Richtlinie hinausgeht und in anderen EU-Mitgliedstaaten nicht umsetzbar wäre.

§ 61 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

Die Untersagung der Ausübung leitender Funktionen auf der Ebene der Geschäftsführung, des Vorstands oder als gesetzlicher Vertreter stellt einen erheblichen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb und damit in die geschützte Unternehmensorganisation dar. Dieser Eingriff berührt ferner das Grundrecht der Berufsfreiheit natürlicher Personen gemäß Art. 12 Abs. 1 GG und hat weitreichende Folgen für die Funktionsfähigkeit des Unternehmens. Die Leitungsfunktion ist für die ordnungsgemäße Führung und den Fortbestand des Unternehmens von zentraler Bedeutung. Sofern eine Untersagungsanordnung nach § 61 Abs. 9 Nr. 2 BSIG-E erlassen wird, ist das Bundesamt bei Konzerngesellschaften gehalten, die Untersagungsverfügung nur auf das Leitungsorgan zu erstrecken, das nach der Geschäftsordnung des Leitungsorgans (z. B. Geschäftsordnung des Vorstands) für den für die Einstufung als besonders wichtige Einrichtung relevanten Geschäftsbereich zuständig ist.

Gemäß Art. 35 Abs. 2 NIS-2-Richtlinie besteht eine Sperrwirkung für das Bundesamt zur Verhängung eines Bußgeldes. Diese Sperrwirkung greift, wenn die Datenschutzaufsichtsbehörden bereits ihrerseits ein Bußgeld verhängt haben, nachdem sie eine Meldung über das Bundesamt gemäß § 61 Abs. 11 NIS2UmsuCG erhalten haben. Allerdings ist umgekehrt keine solche Sperrwirkung vorgesehen. Das bedeutet, dass, wenn das Bundesamt ein Bußgeld verhängt, dies nicht automatisch verhindert, dass die Datenschutzaufsichtsbehörden ebenfalls ein Bußgeld verhängen können. Diese asymmetrische Regelung wirft die Frage auf, ob dadurch das Doppelbestrafungsverbot („ne bis in idem“) verletzt wird. Die fehlende wechselseitige Sperrwirkung könnte daher zu einer Situation führen, in der dieselbe Tat sowohl vom Bundesamt als auch von den Datenschutzaufsichtsbehörden sanktioniert wird, was eine Doppelbestrafung darstellen würde. Wir fordern das Bundesministerium des Innern auf, das Doppelbestrafungsverbot auch im NIS2UmsuCG vollumfänglich umzusetzen.

Anlage 1

Bei den Einträgen 6.1.10 und 6.1.11 sollte in Analogie zum Passus 2.1.1 der Anlage 2 der Zusatz „ausgenommen Unternehmen, für die der Managed Service / Managed Security Service nicht ihre Hauptwirtschaftstätigkeit ist“ ergänzt werden. In mittelständischen / großen Einrichtungen ist es durchaus üblich, einen internen, zentralisierten Managed-Service-Provider / Managed Security Services-Provider für IT- und / oder Security-Dienstleistungen zu haben.

Ohne den geforderten Zusatz würde die Einrichtung (i. d .R. der Konzern) ansonsten gem. §28 (1) 4 als besonders wichtige Einrichtung eingestuft.

Nach dem aktuellen Entwurf würden auch rein konzerninterne Rechenzentrumsbetreiber als 'besonders wichtige Einrichtungen' klassifiziert, obwohl sie ausschließlich Dienste innerhalb des Konzerns erbringen und nicht für externe Kunden tätig sind. Wir fordern daher die Ergänzung einer Ausnahmeregelung in § 28 BSIG-E sowie bei den Einträgen 6.1.10 und 6.1.11 der Anlage 1 analog zum Passus 2.1.1 der Anlage 2: 'ausgenommen Unternehmen, für die der Betrieb von Rechenzentren bzw. der Managed Service / Managed Security Service nicht ihre Hauptwirtschaftstätigkeit ist oder die diese Dienste ausschließlich innerhalb ihres eigenen Konzernverbunds erbringen'. Diese Anpassung ist notwendig, um eine unverhältnismäßige Regulierungslast zu vermeiden und die tatsächliche Risikolage adäquat abzubilden. Konzerninterne IT-Dienstleistungen sollten regulatorisch im Kontext des Gesamtkonzerns betrachtet werden.

Die deutsche Industrie empfiehlt folgende Änderungen am vorliegenden Gesetzentwurf:

6.1.10			Managed Services Provider*, ausgenommen Unternehmen, für die der Managed*

			Service nicht ihre Hauptwirtschaftstätigkeit ist
6.1.11			Managed Security Services Provider*, ausgenommen Unternehmen, für die der Managed Security Service nicht ihre Hauptwirtschaftstätigkeit ist*

Artikel 17 – Änderung des Energiewirtschaftsgesetzes

§ 5c IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz

Die Versorgung der deutschen Industrie mit Energie ist für das Wirtschaften von herausgehobener Relevanz. Die Industrie begrüßt folglich, dass die IT-Sicherheit im Anlagen- und Netzbetrieb in § 5c des Energiewirtschaftsgesetzes (EnWG) vollumfänglich adressiert wird. Allerdings muss zwingend sichergestellt sein, dass die Formulierungen in § 5c EnWG-E identisch mit jenen in § 30 BSIG-E sind, um rechtliche Unsicherheiten zu vermeiden. So werden viele Begriffe aus dem BSIG-E verwendet, ohne diese jedoch im EnWG-E zu definieren. Es wird empfohlen, bei der Einführung jedes Begriffs auf die entsprechende Definition im BSIG-E zu verweisen, um Rechtsunsicherheiten zu vermeiden.

Die in Absatz 1 gewählte Formulierung „haben einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für den sicheren Netzbetrieb notwendig sind, zu gewährleisten“, entspricht nicht dem im BSIG gewählten allgemeinen Schutzziel. Wir sehen es als angezeigt, dass die Formulierung zu „der informationstechnischen Systeme, Komponenten und Prozesse, die für den sicheren Netzbetrieb notwendig sind“ angeglichen wird. Die Formulierung „angemessener Schutz“ lässt deutlich mehr Interpretationsspielraum als die Formulierung in § 30 BSIG-E und sollte ebenfalls angeglichen werden, um die notwendige Rechtssicherheit zu schaffen.

Unsere Stellungnahme zu § 41 BSIG-E gilt entsprechend für § 5c Absatz 9 EnWG-E. Es wird empfohlen Absatz 9 zu streichen.

§ 5c Absatz 4 Nr. 11 EnWG-E erfordert Systeme zur Angriffserkennung nicht nur für Kritische Anlagen, sondern für alle wichtigen und besonders wichtigen Einrichtungen. Dies geht deutlich über die Regelungen im BSIG-Entwurf hinaus und ist zudem keine Anforderung der NIS-2-Richtlinie. § 5c Abs. 4 Nr. 11 EnWG-E ist daher unverhältnismäßig und sollte komplett gestrichen werden. Gegebenenfalls sollte ein separater Absatz für Betreiber Kritischer Anlagen aufgenommen werden.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Gesetzentwurf begrüßen:

§ 5c

(1) Der Betreiber eines Energieversorgungsnetzes hat *geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die für den sicheren Netzbetrieb notwendig sind, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.* ~~*einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungs-systeme, die für den sicheren Netzbetrieb notwendig sind, zu gewährleisten*~~. Die *geeigneten, verhältnismäßigen und wirksamen technischen und organisatorischen Maßnahmen* ~~*er angemessene Schutz*~~ nach Satz 1 sind ~~*ist*~~ auch durch Berücksichtigung erforderlicher

Anforderungen bei der Beschaffung von Anlagengütern und Dienstleistungen sicherzustellen. Die Bundesnetzagentur bestimmt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 in einem Katalog von Sicherheitsanforderungen (IT-Sicherheitskatalog) die *geeigneten, verhältnismäßigen und wirksamen technischen und organisatorischen Maßnahmen.* ~~*Anforderungen an den angemessenen Schutz*~~. Dabei beteiligt die Bundesnetzagentur die Betreiber von Energieversorgungsnetzen und deren Branchenverbände. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf. *Die geeigneten, verhältnismäßigen und wirksamen technischen und organisatorischen Maßnahmen sind umgesetzt,* ~~*Ein angemessener Schutz nach Satz 1 liegt vor,*~~ wenn der IT-Sicherheitskatalog eingehalten und dies vom Betreiber dokumentiert worden ist.

(3)

5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von ~~*Netz- und Informationssystemen*~~ *informationstechnischen Systemen, Komponenten und Prozessen*, einschließlich Management und Offenlegung von Schwachstellen,

11. Einsatz von Systemen zur Angriffserkennung nach § 2 Absatz 1 Nummer 40 des BSI-Gesetzes. *Nummer 11 gilt ausschließlich für Kritische Anlagen.*

~~*(12) Die Bundesnetzagentur legt bis zum Ablauf des … [einsetzen: Datum desjenigen Tages des ersten auf den Monat des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 folgenden Kalendermonats, dessen Zahl mit der des Tages des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 übereinstimmt, oder, wenn es einen solchen Kalendertag nicht gibt, Datum des ersten Tages des darauffolgenden Kalendermonats] im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Allgemeinverfügung im Wege einer Festlegung nach § 29 Absatz 1 in einem Katalog von Sicherheitsanforderungen für das Betreiben von Energieversorgungsnetzen und Energieanlagen fest,*~~

~~*1. welche Komponenten kritische Komponenten nach § 2 Nummer 23 Buchstabe c Doppelbuchstabe aa des BSI-Gesetzes sind oder*~~

~~*2. welche Funktionen kritisch bestimmte Funktionen nach §2 Nummer 23 Buchstabe c Doppelbuchstabe bb des BSI-Gesetzes sind.*~~

~~*Der Betreiber eines Energieversorgungsnetzes, das eine kritische Anlage nach § 2 Nummer 22 des BSI-Gesetzes ist, oder der Betreiber einer Energieanlage, die eine kritische Anlage nach § 2 Nummer 22 des BSI-Gesetzes ist, hat die Vorgaben des Katalogs spätestens sechs Monate nach dessen in der Allgemeinverfügung bestimmten Inkrafttreten zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden. Der Katalog wird mit den IT-Sicherheitskatalogen nach den Absätzen 1 und 2 verbunden.*~~

Artikel 25 – Änderung des Telekommunikationsgesetzes

§ 3 Begriffsbestimmungen

Es gibt Fälle, in denen Immobilienunternehmen Wegerechte nach TKG beantragen, um über eine Straße oder andere öffentliche Flächen eine entsprechende Telekommunikations-Infrastruktur (Glasfaser) zu verlegen. Dies geschieht oft im Zuge der Quartiersentwicklung und dem zugehörigen Aufbau eines Campusnetzes für die digitale Breitbandversorgung der Nutzer. Gegebenenfalls werden diese Unternehmen dann als Betreiber öffentlicher Telekommunikationsnetze bei der BNetzA registriert, was sie laut Gesetzentwurf (BSIG-E) zu einer (besonders) wichtigen Einrichtung macht, obwohl es letztlich nur zur Verpachtung von passiver Netzinfrastruktur kommt.

Aufgrund des fehlenden gewerblichen Betriebs des Netzes sollte eine Ausnahme für die Verpachtung geschaffen werden. Dies sollte über die Begriffsdefinition im TKG erfolgen, die auch in Übereinstimmung mit der bisherigen Entscheidungspraxis der BNetzA steht.

Die deutsche Industrie empfiehlt folgende Änderungen am vorliegenden Gesetzentwurf:

§ 3

(7) „Betreiber“ ein Unternehmen, das ein öffentliches Telekommunikationsnetz oder eine zugehörige Einrichtung bereitstellt oder zur Bereitstellung hiervon befugt ist; *die Verpachtung von Telekommunikationslinien und Verkabelungen ohne aktive Netzbestandteile ist kein Betrieb eines öffentlichen Telekommunikationsnetzes.*

§ 165 Technische und organisatorische Schutzmaßnahmen

In Bezug auf die Neugestaltung des § 165 Abs. 2 inklusive der Ergänzung (2a) mit der Ausweisung der Mindestanforderungen für Risikomanagementmaßnahmen im Bereich der Cybersicherheit ist ein Abgleich mit dem Sicherheitskatalog der BNetzA erforderlich bzw. zu erwarten, dass die BNetzA aufgrund der dort niedergelegten Anforderungen den Sicherheitskatalog überarbeiten wird. Diesbezüglich sind folgende Überlegungen zu den dort aufgeführten Maßnahmen zu berücksichtigen:

§ 165 Abs. 2 Satz 3 (neu): In der Altfassung waren der Stand der Technik maßgeblich. Nun sind neue Abwägungskriterien für die Angemessenheit der technischen und organisatorischen Vorkehrungen und sonstigen Maßnahmen hinzugekommen. Eine Spezifikation des Ausmaßes der Risikoexplosion, der Größe des Betreibers sowie der Eintrittswahrscheinlichkeit, der Schwere des Vorfalls sowie der gesellschaftspolitischen und wirtschaftlichen Auswirkungen ist zu erwarten.

§ 165 Abs. 2a: Der ‚gefahrenübergreifende Ansatz“ war bislang nicht gesetzlich vorgeschrieben. Der Schutz gegen Störungen durch äußere Angriffe und Katastrophen sowie die Beherrschung von Risiken für die Sicherheit von TK-Netzen und Diensten war bereits in § 165 Abs. 2 enthalten und es ist zu hinterfragen, ob sich aus der Formulierung neue Verpflichtungen ergeben. Alle weiteren aufgenommenen Punkte sind den Implementing Regulations (Annex) der EU zu entnehmen. Die Punkte machen einen Abgleich mit dem Sicherheitskatalog der BNetzA erforderlich bzw. es ist zu erwarten, dass die BNetzA den Sicherheitskatalog überarbeiten wird.

Besonders hervorzuheben ist die Regelung des § 165 Abs. 2a Nr. 4: In Bezug auf die Harmonisierung der Neuregelungen sollte ein Abgleich mit § 30 Abs.2 Nr.4 erfolgen unter Streichung ‚zwischen den einzelnen Einrichtungen‘ in Bezug auf die Lieferkette unter Verbleib der Regelung ‚zu unmittelbaren Anbietern oder Diensteanbietern‘.

§ 165 Abs. 2 (2b) Die Geschäftsleitungen von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, sind verpflichtet, die von diesen Einrichtungen nach Absatz 2 zu ergreifenden Maßnahmen umzusetzen und ihre Umsetzung zu überwachen. Die Umsetzung solcher Maßnahmen erfordert spezifische Fachkenntnisse im Bereich der Informationssicherheit, über die die Geschäftsleitung in der Regel nicht verfügt. Diese Aufgaben liegen sachlogisch bei den entsprechend qualifizierten Fachabteilungen innerhalb der Organisation. Es wäre daher konsequent, zur ursprünglichen Formulierung „zu genehmigen“ zurückzukehren, die der Rolle der Geschäftsführung als verantwortliche Instanz ohne operative Überforderung gerecht wird. Ergänzend sollte gesetzlich klargestellt werden, dass die Geschäftsleitung zur Erfüllung ihrer Pflichten geeignete

Dritte beauftragen kann – ähnlich wie bei § 38 Abs. 1 BSIG-E. Die Letztverantwortung verbleibt dabei weiterhin bei der Geschäftsleitung.

§ 168 Meldung eines Sicherheitsvorfalls

Mit der NIS-2-Richtlinie beabsichtigt der EU-Gesetzgeber eine EU-weite Harmonisierung der Cybersicherheitsanforderungen für die in den Anwendungsbereich fallenden Unternehmen. Leider kann das erklärte Harmonisierungsziel mit dem vorgelegten Entwurf nicht erreicht werden. Zum einen entfernt sich der deutsche Gesetzgeber bei der Umsetzung von der Struktur der NIS-2-Richtlinie, was die Anwendung für grenzüberschreitend tätige Unternehmen unnötig komplex macht. Zum anderen hat der deutsche Gesetzgeber über die Anforderungen der EU hinausgehende Verpflichtungen aufgenommen, die zu einem erheblichen Aufwand und zu Doppelregulierungen führen. So bleibt es für Telekommunikationsunternehmen bei einer nicht nachvollziehbaren doppelten Meldepflicht von Vorfällen sowohl an das BSI als auch an die Bundesnetzagentur (BNetzA) (vgl. Artikel 23 § 168 Abs. 1 TKG). Die deutsche Industrie fordert daher die Streichung der gesonderten Meldepflicht nach Artikel 26 § 168 Abs. 1 TKG-E.

Die deutsche Industrie empfiehlt folgende Änderungen am vorliegenden Gesetzentwurf:

~~*(1) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, übermittelt der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik:*~~

1. ~~*unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;*~~

2. ~~*unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Meldung über den Sicherheitsvorfall, in der die in Nummer 1 genannten Informationen bestätigt o-der aktualisiert werden und eine erste Bewertung des erheblichen Sicherheits-vorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;*~~

3. ~~*auf Ersuchen der Bundesnetzagentur oder dem Bundesamt für Sicherheit in der Informationstechnik eine Zwischenmeldung über relevante Statusaktualisierungen;*~~

4. ~~*spätestens einen Monat nach Übermittlung der Meldung des erheblichen Sicherheitsvorfalls gemäß Nummer 2, vorbehaltlich Absatz 2, eine Abschluss-meldung, die Folgendes enthält: a) eine ausführliche Beschreibung des erheblichen Sicherheitsvorfalls, ein-schließlich seines Schwergrads und seiner Auswirkungen;*~~

    a. ~~*eine ausführliche Beschreibung des erheblichen Sicherheitsvorfalls, einschließlich seines Schwergrads und seiner Auswirkungen;*~~

    b. ~~*Angaben zur Art der Bedrohung beziehungsweise zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;*~~

    c. ~~*Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;*~~

    d. ~~*Gegebenenfalls die grenzüberschreitenden Auswirkungen des erheblichen Sicherheitsvorfalls.*~~

~~*(2) Dauert der erhebliche Sicherheitsvorfall im Zeitpunkt des Absatz 1 Nummer 4 noch an, legt der Betroffene statt einer Abschlussmeldung zu diesem Zeit-punkt eine Fortschrittsmeldung und eine Abschlussmeldung innerhalb eines Monats nach Abschluss der Bearbeitung des erheblichen Sicherheitsvorfalls vor.*~~

~~*(3) Ein Sicherheitsvorfall gilt als erheblich, wenn*~~

~~*1. er schwerwiegende Betriebsstörungen oder finanzielle Verluste für den betreffenden Betreiber öffentlicher Telekommunikationsnetze oder Anbieter öffentlich zugänglicher Telekommunikationsdienste verursacht hat oder verursachen kann, oder*~~

~~*2. er andere natürliche oder juristische Personen durch erhebliche materielle o der immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.*~~

(1) Das Bundesamt für Sicherheit in der Informationstechnik leitet die gemäß § 32 BSIG von Betreibern eines öffentlichen Telekommunikationsnetzes oder öffentlich zugänglicher Telekommunikationsdienste übermittelten Meldungen erheblicher Cybersicherheitsvorfälle an die Bundesnetzagentur weiter. Eine separate Meldung ist nicht notwendig, sofern Betreiber eines öffentlichen Telekommunikationsnetzes oder öffentlich zugänglicher Telekommunikationsdienste gegenüber dem BSI ihr Einverständnis zur Weiterleitung der gemeldeten Informationen an die Bundesnetzagentur erteilt haben.

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29
10178 Berlin
www.bdi.eu
T: +49 30 2028-0

EU-Transparenzregister: 1771817758-48

Lobbyregister: R000534

Autor
Steven Heckler
Stellvertretender Abteilungsleiter Digitalisierung und Innovation
T: +49 30 2028-1523
s.heckler@bdi.eu

BDI-Dokumentennummer: D 2102