BDI

INNONATION

STELLUNGNAHME | DIGITALPOLITIK | CYBERSICHERHEIT

Diskussionspapier des BMI zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

BDI begrüßt frühzeitige Einbindung und sieht Anpassungsbedarfe im Detail

20. Oktober 2023

Executive Summary

Die deutsche Industrie begrüßt ausdrücklich, frühzeitig in die Erarbeitung des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) eingebunden zu werden. Mit dem Diskussionspapier beschreitet das Bundesministerium des Innern und für Heimat einen ungewöhnlichen Weg – erlaubt dadurch jedoch eine Einbindung von relevanten Stakeholdern vor der eigentlichen Verbändebeteiligung. Das aktuelle Konsultationsverfahren zum Diskussionspapier darf jedoch keinesfalls die offizielle Verbändeanhörung ersetzen und auch nicht als Argumentation dienen, die Verbändeanhörung erneut mit sehr kurzer Frist – vgl. 27 Stunden beim IT-Sicherheitsgesetz 2.0 – durchzuführen. Die deutsche Industrie erachtet eine mindestens vierwöchige Konsultationsphase zu einem zwischen den Ressorts abgestimmten Entwurf des NIS2UmsuCG als angemessen.

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. Hierfür ist es unabdingbar, dass

- Unternehmen ihren Melde- und Registrierungspflichten volldigital nachkommen können und aus den Meldungen ein tagesaktuelles Cybersicherheitslagebild erstellt wird;
- Kompetenzen zwischen Bundes- und Landesbehörden überlappungsfrei geregelt werden;
- neben der Gesetzgebung auf eine aktive Förderung der Sicherheitskultur mit konkreten Maßnahmen hingearbeitet wird, wie z. B. der Sicherheitsüberprüfung von Mitarbeitenden;
- europaweit agierende Unternehmen nur in einem Mitgliedsstaat gebündelt für die gesamte EU ihren Nachweis-, Melde- und Registrierungspflichten nachkommen müssen und
- die Anforderungen der NIS-2-Richtlinie – insbesondere bezüglich des Anwendungsbereichs und der umzusetzenden Maßnahmen – zeitnah EU-weit möglichst einheitlich implementiert werden.

Positive Elemente des Diskussionspapiers:

- **Streichung Unternehmen im besonderen öffentlichen Interesse:** Die deutsche Industrie begrüßt, dass die Kategorie „Unternehmen im besonderen öffentlichen Interesse“ ersatzlos gestrichen wurde und künftig neben Kritischen Anlagen nur noch wichtige sowie besonders wichtige Einrichtungen existieren. Diese Streichung des deutschen Sonderwegs nach IT-Sicherheitsgesetz 2.0 stärkt die europaweite Harmonisierung der Cybersicherheitsrgeulierung.
- **Nachweis der Umsetzung durch Kritische Anlagen:** Der BDI begrüßt, dass das BSI den Betreibern Kritischer Anlagen eine Frist von mindestens drei Jahren gewährt, bis sie die

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

Erfüllung der Anforderungen nach § 30 Abs. 1 erstmals nachweisen müssen. Diese Frist erhöht signifikant die Umsetzbarkeit der gesetzlichen Anforderungen.

- **Präzisierter Anwendungsbereich:** Die deutsche Industrie begrüßt ausdrücklich die Aufnahme der Anhänge1 und 2 im Diskussionspapier, da sie die Einrichtungskategorien deutlich präziser fassen, als dies bisher in den geleakten Referentenentwürfen erfolgt war. Eine direkte Festlegung der Schwellenwerte für Kritische Anlagen im NIS2UmsuCG wäre wünschenswert.

Negative Elemente des Diskussionspapiers:

- **Fehlende Aufnahme öffentliche Verwaltung der Länder und Kommunen in den Anwendungsbereich:** Das NIS2UmsuCG ordnet nach § 28 Abs. 3 Nr. 5 lediglich Verwaltungseinheiten der Zentralregierung der Kategorie „wichtige Einrichtungen“ zu. Hier bedarf es dringender Nachbesserungen, denn die deutsche Industrie ist auf eine stets funktionierende öffentliche Verwaltung angewiesen, die nicht durch Cybersicherheitsvorfälle über Monate lahmgelegt ist. Neben Bundesbehörden sollten auch Behörden der Länder und Kommunen – insbesondere Genehmigungs- und Überwachungsbehörden, die sensible Daten verarbeiten und für besonders wichtige und wichtige Einrichtungen essenzielle Verwaltungsleistungen erbringen – als besonders wichtige Einrichtungen definiert werden.
- **Einsatz von Cybersicherheitszertifizierungsschemata:** Da bereits in den CSA-Schemes keinerlei Details zum Anwendungsbereich der Schutzniveaus enthalten sind, sollte der Gesetzgeber § 30 Abs. 6 detaillierter fassen. Die aktuell sehr offene Bestimmung in § 30 Abs. 6 lässt befürchten, dass zukünftig nur noch jene nach Vertrauensniveau „high“ oder sogar „high+“ zertifizierten Lösungen zum Einsatz kommen dürfen. Dies würde die digitale Transformation der deutschen Industrie erschweren.
- **NIS2UmsuCG sieht keine Sicherheitsüberprüfung von in sicherheitssensiblen Bereichen tätigen Mitarbeitenden vor:** Damit die weitreichenden Risikomaßnahmen nach § 30 nicht ins Leere laufen, sollten neben technischen Maßnahmen Mitarbeiterinnen und Mitarbeiter, die in sicherheitskritischen Stellen im Unternehmen beispielsweise in für die IT-Sicherheit zuständigen Abteilungen tätig sind, auf ihre Vertrauenswürdigkeit hin überprüft werden. Das NIS2UmsuCG sollte besonders wichtigen Einrichtungen, wichtigen Einrichtungen und Betreibern Kritischer Anlagen diese Möglichkeit kostenfrei einräumen. Da das NIS2UmsuCG als Artikelgesetz angelegt ist, sollte es zwingend auch die Aufnahme von Sicherheitsüberprüfungen von in sicherheitssensiblen Bereichen tätigen Mitarbeitenden enthalten.
- **Drohende Fragmentierung:** Die deutsche Industrie befürwortet die mit der NIS 2 angestrebte EU-weite Harmonisierung. Durch Fragmentierung und unterschiedliche Regelungen innerhalb und außerhalb der Union entstehen für Unternehmen erhebliche Mehraufwände und gegebenenfalls auch ungleiche Standortvoraussetzungen. Die Umsetzung der NIS 2 in nationales Recht sollte daher stets darauf abzielen, dass einzelne Maßnahmen EU-weit einheitlich angewendet werden. Um die Erfüllungsaufwände für international agierende Unternehmen signifikant zu reduzieren, ohne die Cyberresilienz zu schwächen, sollten Mitgliedsstaaten auf internationale Standards setzen und hingegen auf nationale Anforderungen verzichten, die nicht EU-weit anerkannt werden. Die Bundesregierung sollte in der NIS2 angelegte Vereinfachungen für bestimmte Branchen, wie z.B. Cloud-Betrieb (NIS2 Artikel 26), aufgreifen. Die europäische Vereinfachung bezüglich Territorialität und Zuständigkeit der deutschen Aufsichtsbehörden für Konzerne mit Hauptsitz in Deutschland muss zwingend umgesetzt werden.
- **Fehlende Übergangsfristen für wichtige und besonders wichtige Einrichtungen:** Analog zu § 34 Abs. 1 Satz 1 sollte das BSI Nachweise zur Umsetzung und Einhaltung der Anforderungen gemäß § 30, § 31 und § 32 frühestens drei Jahre nach Inkrafttreten des Gesetzes von wichtigen und besonders wichtigen Einrichtungen anfordern dürfen.

Inhaltsverzeichnis

Bewertung im Detail

Auch wenn der BDI die frühzeitige Einbindung im Rahmen des Gesetzgebungsverfahrens noch Veröffentlichung des ressortabgestimmten Referentenentwurfs begrüßt, sehen wir es als kritisch an, dass im vorliegenden Diskussionspapier mehrere Paragrafen nicht enthalten sind. Eine umfängliche und ganzheitliche Beurteilung des NIS2UmsuCG von Seiten der Industrie ist daher nicht möglich. So fehlen die §§41-50 im Papier des BMI und somit zentrale Regelungsinhalte, wie jene zum Einsatzes Kritischer Komponenten. Gleichzeitig fehlt damit auch der Ausblick auf die Verzahnung des NIS2UmsuCG mit dem KRITIS-Dachgesetz.

Artikel 1 – Änderung des BSI-Gesetzes

§ 2 Begriffsbestimmungen

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

Die Definition von IKT-Produkten nach § 2 Abs. 1 Nr. 13 sollte zwingend sowohl Hard- als auch Software umfassen. Über den Bezug auf den Cybersecurity Act bestehen diesbezüglich Unsicherheiten, inwiefern Software ebenso mit abgedeckt ist.

Die Definition „Rechenzentrumsdienst“ nach § 2 Abs. 1 Nr. 30 muss aus Sicht der deutschen Industrie zwingend präzisiert werden. In der jetzigen Formulierung könnten somit neben dem reinen Rechenzentrumsbetrieb (Housing) auch Hosting-Leistungen subsumiert werden, die auch unter „Cloud“ fallen.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Referentenentwurf im Rahmen der Ressortberatungen sowie in den Beratungen in Bundestag und Bundesrat begrüßen:

(1) 9. „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 im-materielle Schäden beeinträchtigt hat oder beeinträchtigen kann~~,~~

soweit nach Absatz 2 keine weitergehende Begriffsbestimmung erfolgt;

(1) 30. „Rechenzentrumsdienst“ ein Dienst, mit dem spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, ~~*die Verbindung und den*~~ *zum* Betrieb von IT- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden.

(2) ~~*Das Bundesministerium des Innern und für Heimat kann durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, bestimmen, wann ein Sicherheitsvorfall im Hinblick auf seine technischen oder organisatorischen Ursachen oder seine Auswirkungen auf die Einrichtung, Staat, Wirtschaft und Gesellschaft oder die Anzahl der von den Auswirkungen Betroffenen als erheblich im Sinne von Absatz 1 Nummer 10 anzusehen ist. Das Bundesministerium kann die Ermächtigung durch*~~

~~*Rechtsverordnung auf das Bundes-amt übertragen.*~~ Für den Fall, dass die Europäische Kommission einen oder mehrere Durchführungsrechtsakte gemäß Artikel 23 Absatz 11 Unterabsatz 2 der NIS-2-Richtlinie erlässt, worin näher bestimmt wird, in welchen Fällen ein Sicherheitsvorfall als erheblich anzusehen ist, geht dieser oder gehen diese der ~~*Rechtsverordnung nach Satz 1 und 2*~~ Definition nach *Absatz 1 Nummer 9* insoweit vor.

§ 5 Allgemeine Meldestelle für die Sicherheit in der Informationstechnik

Obgleich § 5 nicht im Diskussionspapier des BMI enthalten ist, wiederholen wir nachfolgend unsere zentralen Petita zum Meldewesen, da es eines der zentralen Elemente des NIS2UmsuCG ist. 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. Wir sehen es als zwingend erforderlich an, dass aus den an das BSI durch die Wirtschaft übermittelten Informationen zu aktuellen Cybersicherheitsvorfällen ein tagesaktuelles, kostenfreies Lagebild zu digitalen und physischen Bedrohungen erstellt wird und mit den unter das NIS-2-Umsetzungsgesetz fallenden Unternehmen geteilt wird. Hierfür erachten wir das in der Nationalen Cyber-Sicherheitsstrategie der Bundesregierung angekündigte und in § 6 des NIS2UmsuCG angelegte BSI Information Sharing Portal als probaten Ansatz.

Im Kontext der Anforderungen des Online-Zugangsgesetzes (OZG) ist es zwingend erforderlich, dass das BSI einen voll digitalisierten Ende-zu-Ende Meldeweg etabliert, der eine sichere Authentifizierung der meldenden Einrichtung ermöglicht. Es ist zu prüfen, inwiefern das auf Elster- oder anderen im OZG vorgesehenen Identifizierungsmitteln basierende Unternehmenskonto hierfür als technische Grundlage fungieren kann, da dies ein Rechte- und Rollenmanagement enthalten und zukünftig als zentrale digitale Schnittstelle zwischen Unternehmen und der öffentlichen Verwaltung fungieren soll. Der bundesweite Roll-out des Unternehmenskontos wäre hierfür eine bis spätestens März 2024 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 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 „actionable“ 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 von zentraler Bedeutung. Die deutsche Industrie sieht die Notwendigkeit zur Etablierung eines zentralen „Sicherheitslagebilds“. 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 Referentenentwurf im Rahmen der Ressortberatungen sowie in den Beratungen in Bundestag und Bundesrat begrüßen:

(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 Sicherheitsvorfällen, Cyberbedrohungen und Beinahevorfällen entgegen. Das Bundesamt richtet hierzu *Ende-zu-Ende digitalisierte* ~~geeignete~~ Meldemöglichkeit~~e~~ *auf Basis des Unternehmenskontos* ein. Die Meldungen können anonym erfolgen. Soweit die Meldung nicht anonym erfolgt, 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, mittels derer 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. Betreiber Kritischer Anlagen, besonders wichtiger Einrichtungen und wichtiger Einrichtungen gemäß § 38 Absatz 2 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 einen Informationsaustausch zu Cybersicherheitsvorfällen, Beinahevorfällen, Schwachstellen, Techniken und Verfahren, Kompromittierungsindikatoren, gegnerischen Taktiken, bedrohungsspezifischen Informationen, Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten sowie zur Aufdeckung von Cyberangriffen etablieren 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.

Neben dem Informationsaustausch in digitaler Form sollte jedoch auch weiterhin der Umsetzungsplan KRITIS fortgeführt werden, um den persönlichen und vertrauensvollen Austausch zwischen den Akteuren zu ermöglichen.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Referentenentwurf im Rahmen der Ressortberatungen sowie in den Beratungen in Bundestag und Bundesrat begrüßen:

(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 zwingend das Einverständnis des Ersuchenden eingeholt werden. Dies gilt umso mehr, als dass der Ersuchende die Kosten für den Einsatz Dritter übernehmen muss.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Referentenentwurf im Rahmen der Ressortberatungen sowie in den Beratungen in Bundestag und Bundesrat begrüßen:

(5) Das Bundesamt kann sich bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden der Hilfe qualifizierter Dritter bedienen, wenn dies zur rechtzeitigen oder vollständigen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich ist. Die hierdurch entstehenden Kosten hat der Ersuchende zu tragen. *Vor Beauftragung eines Dritten muss das Bundesamt das Einverständnis des Ersuchenden einholen.* Das Bundesamt kann den Ersuchenden auch auf qualifizierte Dritte verweisen. D*urch d*as Bundesamt und vom Ersuchenden oder vom Bundesamt nach Satz 1 beauftragte Dritte können einander bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden Daten übermitteln. Hierfür gilt Absatz 3 entsprechend.

§ 19a Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden

Die deutsche Industrie fordert, dass Betreiber Kritischer Anlagen, besonders wichtiger Einrichtungen und wichtiger Einrichtungen geeignete Prozesse vorsehen können, um die Vertrauenswürdigkeit der Beschäftigten zu überprüfen. Dies ist von herausgehobener Bedeutung. Neben technischen Maßnahmen ist es sinnvoll, Mitarbeiterinnen und Mitarbeitern, die in sicherheitskritischen Stellen im Unternehmen, beispielsweise in für die IT-Sicherheit zuständigen Abteilungen tätig sind, auf ihre Vertrauenswürdigkeit hin zu untersuchen. Dies würde die Bestrebungen der Unternehmen, ihre Cyberresilienz ganzheitlich zu stärken, unterstützen. Staatliche Stellen müssen diese Möglichkeit unterstützen, beispielsweise indem Anträge auf Führungszeugnisse rasch bearbeitet werden und Unternehmen eine Sicherheitsüberprüfung von entsprechenden Mitarbeiterinnen und Mitarbeiter beantragen können. Hierfür müssen die notwendigen personellen Ressourcen vorgehalten werden. Eine entsprechende personelle Aufstockung der zuständigen Stellen ist unbedingt angezeigt. Um den Aufwand bei den für Sicherheitsüberprüfungen zuständigen Überwachungsbehörden zu reduzieren und die Prozesse möglichst effizient auszugestalten, wäre eine Anerkennungsklausel für Sicherheitsüberprüfungen aus anderen Bereichen bei inhaltlich ähnlichen Abfragedaten zielführend. Darüber hinaus sind die Prozesse auch für ausländische Arbeitnehmerinnen und -arbeitnehmer praxisgerecht zu gestalten.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Referentenentwurf im Rahmen der Ressortberatungen sowie in den Beratungen in Bundestag und Bundesrat 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 in Zusammenarbeit mit dem Bundeskriminalamt, dem Bundesamt für Verfassungsschutz, den Polizeibehörden sowie dem Bundesministerium für Wirtschaft und Klimaschutz eine Überprüfung nach SÜG von in besonders sicherheitskritischen Bereichen tätigen oder zukünftig tätigen Personen durch.

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

(3) Die Überprüfung nach Absatz 1 erfolgt kostenfrei.

§ 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.

Wir begrüßen, dass das Diskussionspapier – anders als die zuvor bekanntgewordenen Referentenentwürfe – eine eindeutige Nennung der Sektoren inklusive Subsektoren enthält. Es ist jedoch weiterhin unerlässlich, dass die drei Kategorien – und insbesondere die „Kritischen Anlagen“ – identisch im KRITIS-Dachgesetz und im NIS2UmsuCG definiert werden.

Im Falle der Qualifizierung als „besonders wichtige Einrichtung“ ausschließlich aufgrund des Betriebs einer „Kritischen Anlage“ gemäß § 28 Abs. 1 Nr. 4 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.

Das NIS2UmsuCG ordnet nach § 28 Abs. 1 Nr. 5 lediglich Verwaltungseinheiten der Zentralregierung der Kategorie „wichtige Einrichtungen“ zu. Hier bedarf es dringender Nachbesserungen, denn die deutsche Industrie ist auf eine stets funktionierende öffentliche Verwaltung auf allen Ebenen des Föderalstaats angewiesen, die nicht durch Cybersicherheitsvorfälle über Monate lahmgelegt ist. 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 und den Bundesrat auf, die öffentliche Verwaltung aller Ebenen des Föderalstaats in den Anwendungsbereich des NIS2UmsuCG

aufzunehmen, damit alle Behörden risikoadäquate Cybersicherheitsmaßnahmen implementieren und so sensible Daten besser vor Cyberkriminellen zu schützen. Nur so kann die Integrität und Verfügbarkeit wichtiger Verwaltungsverfahren angesichts stetig steigender Cyberbedrohungen sichergestellt werden.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Referentenentwurf im Rahmen der Ressortberatungen sowie in den Beratungen in Bundestag und Bundesrat begrüßen:

Absatz 1

5. eine Einrichtung, die ~~gemäß Anlage 3 dem Teilsektor Zentralregierung~~ de*m*~~s~~ Sektor~~s~~ öffentliche Verwaltung *auf Bundes-, Landes- und Kommunalebene* angehört.

§ 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 aufgenommen hat. Da der Anwendungsbereich des NIS2UmsuCG sehr weit ist, wäre ein One-size-fits-all Ansatz für den risikoadäquaten Schutz nicht zielführend.

Zu Absatz 2: Die entsprechenden Anforderungen sollten der NIS 2 entsprechen, wobei folgende Formulierung in Absatz 2 von der NIS 2 abweicht: „Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten […]“. Es sollte klargestellt werden, dass dies im Einklang mit der NIS 2 so zu verstehen ist, dass der Stand der Technik wie alle anderen in § 30 festgelegten Kriterien im Rahmen des Risikomanagements zu berücksichtigen sind. Der Stand der Technik gibt dabei vor, was überhaupt technisch möglich ist und somit im Rahmen des Riskmanagements erwogen werden kann. Eine Grundregel, dass allein das technisch Mögliche in aller Regel auch umzusetzen sei, wäre unverhältnismäßig. Um einen möglichst hohen Grad an EU-weiter Harmonisierung zu erreichen und damit die Erfüllungsaufwände für die Industrie in einem überschaubaren und praktibalen Rahmen zu halten, sollte der deutsche Gesetzestext entsprechend der Formulierung in der NIS 2 angepasst werden, sodass der Stand der Technik für das Risikomanagement zu berücksichtigen ist. 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 Verordnung die Anwendung bestimmter Cybersicherheitszertifizierungsschemata nach EU Cybersecurity Act für besonders wichtige 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 Abs. 6. 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 Cloud-Anbietern und den Anwenderindustrien. Der BDI bietet an, hierfür ein Format unter

Einbeziehung der zuständigen Ressorts durchzuführen. Ferner ist im Rahmen der NIS-2-Umsetzung auf eine europaweit einheitliche Implementierungspraxis des EUCS – sowie zukünftiger Schemata – 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 von Cybersecurity bereits enthalten (z. B. MDR / IVDR) und die von der Europäischen Kommission als ausreichend angesehen werden (vergleiche Erwägungsgrund 12 zu MDR / IVDR 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 die ineinandergreifenden Anforderungen aus dem CRA Berücksichtigung finden.

Das NIS2UmsuCG sollte die im Erwägungsgrund 29 der NIS-2-Richtlinie genannte Möglichkeit zur Harmonisierung bestehender Cybersicherheitsverpflichtungen bei Luftverkehrseinrichtungen aufgreifen. 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-Kritisverordnung fallen. Das BSI sollte prüfen können, ob diese Anforderungen und die darin enthaltenen Vorgaben gleichwertig zu denen des NIS2UmsuCG sind. Sollte dies der Fall sein, sind Doppelstrukturen und -anforderungen zu vermeiden. Eine derartige Regelung könnte vergleichbar zu jener die branchenspezifischen Sicherheitsstandards betreffend unter Absatz 12 geschaffen werden.

Absatz 2:

(9) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und *Asset* Management ~~*von Anlagen*~~,

§ 32 Meldepflichten

Zahlreiche deutsche Industrieunternehmen haben Standorte in mehreren EU-Mitgliedsstaaten. Vielfach erfolgt die unternehmensweite Steuerung der Cybersicherheit jedoch von einem zentralen Standort aus. Vor diesem Hintergrund ist es zwingend erforderlich, dass Unternehmen, die in mehr als einem EU-Mitgliedsstaat tätig sind, ihren Nachweis-, Registrierungs- und Meldepflichten nur in einem Mitgliedsstaat nachkommen müssen, um den Erfüllungsaufwand in einem akzeptablen Rahmen zu belassen.

Vor dem Hintergrund der parallel umzusetzenden Resilience of Critical Entities Directive 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.

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 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 Cybersicherheitsvorfall sollten Unternehmen ein Formular sukzessive befüllen, statt immer wieder ihre Meldungen neu beginnen zu müssen oder eine Meldung in einem mindestens europäisch 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 absehen. Insbesondere mittlere Unternehmen werden während der Bearbeitung eines erheblichen Sicherheitsvorfalls 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 gestärkt und alle Sicherheitsbehörden zur Einbeziehung wichtiger Einrichtungen verpflichtet werden.

Da das NIS2UmsuCG den Schutz von besonders wichtigen sowie wichtigen Einrichtungen vor Cybersicherheitsvorfällen in den Fokus nimmt, sollte § 32 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 KRITIS-Dachgesetzes 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 Referentenentwurf im Rahmen der Ressortberatungen sowie in den Beratungen in Bundestag und Bundesrat begrüßen:

(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.

(6) Wichtige Einrichtungen haben die Erfüllung der Anforderungen nach Absatz 1 bis 5 spätestens zu einem vom Bundesamt bei der Registrierung festgelegten Zeitpunkt umzusetzen. Der in Satz 1 genannte Zeitpunkt ist durch das Bundesamt auf einen Zeitpunkt spätestens vier Jahre nach Inkrafttreten dieses Gesetzes festzulegen.

§ 33 Registrierungspflicht

Die deutsche Industrie fordert die Bundesregierung auf, ein volldigitales, sicheres Registrierungswesen aufzusetzen, über das Unternehmen ihren Registrierungspflichten nach NIS2UmsuCG und KRITIS-Dachgesetz 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.

Insbesondere aus Perspektive von Anbieter 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 Mitgliedsstaaten in Betracht, um im Zweifel keinen Fehler zu machen.

Sollten Unternehmen widerrechtlich den Registrierungspflichten nicht nachkommen, ist die in § 33 Abs. 3 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 vorgesehene dreimonatige Frist zur Registrierung ist sehr eng bemessen. Die deutsche Industrie plädiert für eine sechsmonatige Frist zur Erstregistrierung.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Referentenentwurf im Rahmen der Ressortberatungen sowie in den Beratungen in Bundestag und Bundesrat begrüßen:

(3) Die Registrierung von besonders wichtigen Einrichtungen und wichtigen Einrichtungen und Domain-Name-Registry-Diensteanbieter kann das Bundesamt auch selbst vornehmen, wenn ihre Pflicht zur Registrierung nicht erfüllt wird. *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.*

(8) 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 Registrierungsformular zur Verfügung, über welches die besonders wichtigen Einrichtungen, Betreiber Kritischer Anlagen und wichtigen Einrichtungen sowie Domain-Name-Registry-Diensteanbieter ihren sich aus diesem Gesetz sowie dem [KRITIS-Dachgesetz] 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 ein Land seinen 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 ist nach wie vor unklar – es bedarf eindeutiger Verweise. In diesem Kontext ist zu klären, welcher Geschäftsführer / welche Geschäftsführerin 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 jene des Landes, in dem eine Tochtergesellschaft tätig ist.

Eine europäisch einheitliche Lösung ist grundsätzlich vorzugswürdig und jede Regelung in einem Mitgliedstaat, welche über die Anforderungen der NIS-2-Richtlinie hinausgeht, zu einer zusätzlichen Belastung für besonders wichtige Einrichtungen führt.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Referentenentwurf im Rahmen der Ressortberatungen sowie in den Beratungen in Bundestag und Bundesrat begrüßen:

(3a) Besonders wichtige Einrichtungen und wichtige Einrichtungen, die ihren Hauptsitz in Deutschland haben und für die aus Deutschland heraus ihre Cybersicherheitsgovernance erfolgt, müssen den Nachweispflichten nur in Deutschland nachkommen.

(3b) Besonders wichtige Einrichtungen und wichtige Einrichtungen, deren Hauptsitz in einem anderen EU-Mitgliedsstaat liegt, müssen 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, § 31 und § 34 dort nachkommen. Das Bundesamt kann das Unternehmen alle fünf Jahre auffordern, eine neuerliche Bescheinigung gemäß Satz 1 vorzulegen.

§ 36 Rückmeldungen des Bundesamts gegenüber meldenden Einrichtungen

Der Bundesverband der Deutschen Industrie e.V. (BDI) begrüßt ausdrücklich, dass das BSI zukünftig binnen 24 Stunden nach Eingang der Frühwarnung verpflichtet ist, dem meldenden Unternehmen eine Rückmeldung zukommen zu lassen. Insbesondere bewerten wir es positiv, dass das BSI auf Ersuchen der meldenden Einrichtung, Orientierungshilfen oder operative Beratung für die Durchführung möglicher Abhilfemaßnahmen zukommen lassen muss. Dies wird insbesondere für mittlere Unternehmen von herausgehobener Bedeutung zur effizienten Vorfallsbearbeitung sein.

§ 38 Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter 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 zusätzlich für besonders wichtige Einrichtungen definiert. Diese Differenzierung fehlt in § 38. 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 aufgelegt bekommt. Hier müsste die öffentliche Verwaltung auf Bundesebene eine Vorbildfunktion einnehmen.

Aus unserer Sicht bedarf es 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 Risikomanagement-Vorgaben 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.

Ferner sollte Absatz 2 gestrichen werden, da die NIS-2-Richtlinie keine entsprechenden Regelungen hinsichtlich eines Verzichts oder Vergleichs vorsieht. Inwiefern zum Beispiel die jeweiligen Aufsichtsgremien der Einrichtung zur Durchsetzung eines Anspruchs verpflichtet sind, sollte sich nach allgemeinen Grundsätzen bestimmen.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Referentenentwurf im Rahmen der Ressortberatungen sowie in den Beratungen in Bundestag und Bundesrat begrüßen:

~~*(2) Ein Verzicht der Einrichtung auf Ersatzansprüche aufgrund einer Verletzung der Pflichten nach Absatz 1 oder ein Vergleich der Einrichtung über diese Ansprüche ist unwirksam. Dies gilt nicht, wenn der Ersatzpflichtige zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrens mit seinen Gläubigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.*~~

§ 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 den Anforderungen nach § 30 Abs. 1 und § 32 erstmals nachweisen müssen. Diese Frist erhöht signifikant die Umsetzbarkeit der gesetzlichen Anforderungen.

Die Nachweispflichten für Betreiber Kritischer Anlagen sind in § 39 nicht hinreichend trennscharf formuliert, sodass nicht nur zum Betrieb Kritischer Anlagen genutzte Systeme, Komponenten und Prozesse umfasst wären. Betreiber Kritischer Anlagen haben laut Diskussionspapier die Erfüllung der Anforderungen nach § 30 Abs. 1 und § 32 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 gelisteten Risikomanagementmaßnahmen stehen jedoch unspezifisch im Bezug zu den informationstechnischen Systemen, Komponenten und Prozesse, 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- Es 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 stehen.

§ 57 Ermächtigung zum Erlass von Rechtsverordnungen

Die deutsche Industrie sieht es kritisch, dass erst per Rechtsverordnung nach § 57 Abs. 4 die Schwellenwerte für Kritische Anlagen definiert werden und diese nicht direkt im Rahmen der Gesetzgebungsverfahren für das NIS2UmsuCG und das KRITIS-Dachgesetz bestimmt werden. Eine direkte Bestimmung im Rahmen der Gesetzgebungsverfahren würde schnellere Rechtssicherheit für die Betroffenen bedeuten und zudem die Umsetzung der Vorgaben beschleunigen. In jedem Fall ist sicherzustellen, dass Kritische Anlagen identisch im NIS2UmsuCG und im KRITIS-Dachgesetz definiert werden.

§ 60 Sanktionsvorschriften

Mit dem in § 60 enthaltenen Verweis auf das Ordnungswidrigkeitengesetz sieht der Gesetzgeber eine Verzehnfachung der Bußgeldhöhe vor, wodurch er in nicht akzeptablem Maße die in der NIS-2-Richtlinie enthaltenen Bußgeldobergrenzen für eine Vielzahl von Unternehmen überschreitet. Bei wichtigen

Einrichtungen mit einem Jahresumsatz von 1,4 Milliarden Euro würde diese Verzehnfachung zu einem höheren Höchstbußgeld führen als EU-weit vorgesehen. Bei besonders wichtigen Einrichtungen mit einem Jahresumsatz von einer Milliarde Euro würde dies zu einem höheren Höchstbußgeld führen als EU-weit vorgesehen. Die deutsche Industrie erachtet Bußgelder grundsätzlich als probates Mittel, um die Beachtung und Implementierung von gesetzlichen Anforderungen zu forcieren. Gleichwohl müssen Bußgelder stets angemessen sein. Die eklatante Überschreitung des EU-weit vorgesehenen Bußgeldrahmens im NIS2UmsuCG sollte nichtsdestotrotz zwingend gestrichen werden, da sie Unternehmen am Standort Deutschland in ungerechtfertigt hohem Maße im Verhältnis zu Wettbewerbern im EU-Ausland benachteiligt.

Die deutsche Industrie fordert daher den Gesetzgeber zu folgender Änderung an § 60 auf:

(5) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 1 Buchstabe a mit einer Geldbuße bis zu zwei Millionen Euro~~, wobei § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten anzuwenden ist,~~ sowie in den Fällen des Absatzes 2 Nummer 1 Buchstabe c, Nummern 5, 10, 11, 12 und 13 mit einer Geldbuße bis zu fünfhunderttausend Euro und in den Fällen des Absatzes 2 Nummer 1 Buchstabe b und des Absatzes 3 mit einer Geldbuße bis zu einhunderttausend Euro geahndet werden.

§ 64 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

Die deutsche Industrie unterstützt ausdrücklich die Möglichkeit, dass das BSI die Umsetzung der Anforderungen nach § 30, § 32 und § 33 überprüfen kann – dies trägt erheblich dazu bei, dass es ein Level-Playing-Field für alle Wirtschaftsakteure gibt. Wir fordern das Bundesministerium des Innern und für Heimat jedoch auf, dass analog zu § 39 Abs. 1 Satz 1 die Aufforderung zum erstmaligen Nachweis der Umsetzung der Anforderungen gemäß § 30 Abs. 1 frühestens drei Jahre nach Inkrafttreten des NIS2UmsuCG gestellt werden darf.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Referentenentwurf im Rahmen der Ressortberatungen sowie in den Beratungen in Bundestag und Bundesrat begrüßen:

(1) Das Bundesamt kann einzelne besonders wichtige Einrichtungen verpflichten, Audits, Prüfungen oder Zertifizierungen von unabhängigen Stellen zur Prüfung der Erfüllung der Anforderungen nach den §§ 30, 31 und 32 durchführen zu lassen. *Die erstmalige Aufforderung nach Satz 1 erfolgt frühestens drei Jahre nach erstmaliger Registrierung.*

(3) Das Bundesamt kann von besonders wichtigen Einrichtungen Nachweise über die Erfüllung einzelner oder aller Anforderungen nach den §§ 30, 31 und 32 verlangen. Soweit das Bundesamt von seinem Recht nach Absatz 1 Gebrauch gemacht hat, kann es hierbei auch die Übermittlung der Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel sowie die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln die Vorlage eines geeigneten Mängelbeseitigungsplans im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder der sonst zuständigen Aufsichtsbehörde verlangen. Das Bundesamt kann die Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen. *Die erstmalige Überprüfung nach Satz 1 erfolgt frühestens drei Jahre nach erstmaliger Registrierung.*

(5) Das Bundesamt kann bei besonders wichtigen Einrichtungen die Einhaltung der Anforderungen nach diesem Gesetz überprüfen. Es kann sich bei der Durchführung der Überprüfung eines qualifizierten unabhängigen Dritten bedienen. Die besonders wichtige Einrichtung hat dem Bundesamt und den

in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung erhebt das Bundesamt Gebühren und Auslagen bei der jeweiligen besonders wichtigen Einrichtung nur, sofern das Bundesamt auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach § 30 Absatz 1 begründeten. *Die erstmalige Überprüfung nach Satz 1 erfolgt frühestens drei Jahre nach erstmaliger Registrierung.*

§ 65 Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen

Die deutsche Industrie unterstützt ausdrücklich die Möglichkeit, dass das BSI die Umsetzung der Anforderungen nach § 30, § 32 und § 33 überprüfen kann – dies trägt erheblich dazu bei, dass es ein Level-Playing-Field für alle Wirtschaftsakteure gibt. Wir fordern das Bundesministerium des Innern und für Heimat jedoch auf, dass analog zu § 39 Abs. 1 Satz 1 die Aufforderung zum erstmaligen Nachweis der Umsetzung der Anforderungen gemäß § 30 Abs. 1 frühestens drei Jahre nach Inkrafttreten des NIS2UmsuCG gestellt werden darf.

Die deutsche Industrie würde die Umsetzung folgender Änderungen am vorliegenden Referentenentwurf im Rahmen der Ressortberatungen sowie in den Beratungen in Bundestag und Bundesrat begrüßen:

§ 65 Rechtfertigen Tatsachen die Annahme, dass eine wichtige Einrichtung die Anforderungen aus den §§ 30, 31 und 32 nicht oder nicht richtig umsetzt, so kann das Bundesamt die Einhaltung der Anforderungen nach den §§ 30, 31 und 32 überprüfen und Maßnahmen nach § 64 treffen. *Die erstmalige Überprüfung nach Satz 1 erfolgt frühestens drei Jahre nach erstmaliger Registrierung.*

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: D1844