bitkom

Stellungnahme

Juli 2025

Referentenentwurf zur Umsetzung der NIS-2-Richtlinie

Zusammenfassung

Mit der NIS-2-Richtlinie will die Europäische Union die digitale Resilienz ihrer Mitgliedstaaten stärken, Sicherheitsstandards vereinheitlichen, und kritische Infrastrukturen besser schützen. Angesichts zunehmender geopolitischer Spannungen und wachsender Cyberbedrohungen ist dieses Ziel nicht nur richtig, sondern überfällig. Bis Oktober 2024 hätte die Richtlinie in nationales Recht umgesetzt sein müssen. Deutschland hat diese Frist verpasst. Die Wirtschaft braucht daher schnellstmöglich Rechtssicherheit. Je mehr Zeit Deutschland bei der Umsetzung braucht, desto größer wird die Unsicherheit für betroffene Unternehmen – gerade im Vergleich zu anderen Mitgliedstaaten mit bereits abgeschlossener Umsetzung. Schon jetzt zeigen sich unterschiedliche Anforderungsniveaus in Europa, die grenzüberschreitende Tätigkeiten erschweren. Eine 1:1-Umsetzung der europäischen Vorgaben ohne zusätzliches nationales »Goldplating« ist nicht nur eine Frage der Praktikabilität, sondern auch der Wettbewerbsfähigkeit.

Die Bundesregierung erkennt diese Dringlichkeit nun an und priorisiert das Gesetzgebungsvorhaben. Die anberaumte Verbändeanhörung vor der Sommerpause ist daher ein notwendiger Schritt, um das Gesetz noch in der zweiten Jahreshälfte 2025 verabschieden zu können. Doch schon jetzt ist deutlich: Der aktuelle Entwurf löst viele Herausforderungen weiterhin nicht.

Ein zentrales Problem des vorliegenden Referentenentwurfs betrifft die geplanten Regelungen zur Informationssicherheit in der Bundesverwaltung. Der Entwurf lässt offen, ob künftig tatsächlich alle Behörden dem gleichen Schutzniveau unterliegen sollen. Derzeit ist unklar, ob § 29 Abs. 2 im weiteren Gesetzgebungsverfahren Bestand haben wird. Innerhalb der Bundesregierung scheint dazu bislang keine Einigung erzielt worden zu sein. Sollte es bei der Differenzierung bleiben, würden lediglich das Bundeskanzleramt und die Ministerien den strengen Anforderungen nach § 30 unterfallen, während für andere Einrichtungen der Bundesverwaltung niedrigere Mindeststandards gelten könnten. Diese Unklarheit stellt die Frage nach einem

90%

der deutschen Unternehmen rechnen im kommenden Jahr mit einem Anstieg von Cyberangriffen. (Bitkom, 2024)

konsistenten Sicherheitsniveau innerhalb der Bundesverwaltung. Auch bleibt der Ausschluss kommunaler Einrichtungen durch Entscheidung der Bundesländer weiterhin bestehen – ein schwerwiegendes strukturelles Defizit in der Abdeckung staatlicher Infrastrukturen, das bereits heute zu erheblichen Fragmentierungen in der nationalen Cybersicherheitsarchitektur und den entsprechenden Risiken führt.

Weiterhin fehlt eine erkennbare Abstimmung mit der geplanten Umsetzung der CER-Richtlinie (ehemals KRITIS-Dachgesetz). Diese betrifft insbesondere die physische Sicherheit kritischer Infrastrukturen – ein Bereich, der eng mit der digitalen Sicherheit verzahnt ist. Ohne eine abgestimmte Regelung besteht die Gefahr paralleler, nicht aufeinander abgestimmter Anforderungen an Unternehmen, die sowohl von NIS-2 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 sowie Rechtsunsicherheit in den Überschneidungsbereichen. Eine klare Koordinierung innerhalb des federführenden Ressorts erscheint notwendig, um Doppelregulierung und Reibungsverluste zu vermeiden.

Besondere Unsicherheit herrscht zudem bei der Frage, welche Unternehmen künftig konkret vom Gesetz erfasst sind. Die Neufassung der Schwellenwert-Klausel in § 28 Abs. 3 BSIG-E führt zu einer inhaltlichen Ausweitung des Anwendungsbereichs, ohne eine klare Definition für den Begriff der »vernachlässigbaren« Geschäftstätigkeit zu liefern. Dies erschwert eine verlässliche Betroffenheitsanalyse – sowohl für kleine und mittlere Unternehmen als auch für global tätige Anbieter mit breitem Leistungsspektrum. Während in früheren Entwürfen nur die kritische Geschäftstätigkeit maßgeblich war, rücken nun alle Aktivitäten in den Fokus – mit der Folge, dass auch Unternehmen mit nur geringem Anteil kritischer Leistungen potenziell einbezogen werden. Ohne klare Kriterien bleibt die Rechtslage unsicher.

Ebenso 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. Eine Klarstellung ist insbesondere deshalb notwendig, weil nun eine geteilte Fachaufsicht von BMI und BMDS über das BSI vorgesehen ist.

Diese und weitere Punkte werden im Folgenden im Detail aufgegriffen und zeigen auf, welche Anpassungen aus Sicht der Digitalwirtschaft notwendig sind, um eine praxisgerechte und rechtsklare Umsetzung der NIS-2-Richtlinie in Deutschland zu gewährleisten.

Die Kommentierung der Details bezieht sich aufgrund der Betroffenheit der Branche auf Artikel 1, Artikel 25 und Anlage 1.

Erfüllungsaufwand

Im Vergleich zum Regierungsentwurf 2024 ist der Erfüllungsaufwand für die Verwaltung von jährlich 122,28 Millionen Euro bzw. einmalig 38,21 Millionen Euro auf jährlich 320 Millionen Euro bzw. 177 Millionen Euro deutlich angestiegen. Dies stellt jedoch nur auf den ersten Blick eine zusätzliche Belastung für die öffentlichen Haushalte dar. Tatsächlich ist dieser Mehraufwand im Kontext der erheblichen finanziellen und sicherheitsrelevanten Schäden, die durch erfolgreiche Cyberangriffe auf die IT-Systeme der Verwaltung entstehen können, als gerechtfertigt einzuordnen. Es handelt sich hierbei um eine präventive Investition in die Resilienz staatlicher Strukturen, die mittelfristig nicht nur das Risiko schwerwiegender Vorfälle reduziert, sondern auch dazu beiträgt, Vertrauen in die digitale Leistungsfähigkeit der Verwaltung zu stärken. Die Bereitschaft, seitens der Bundesregierung in die Sicherheit der Verwaltung zu investieren, ist ausdrücklich positiv zu bewerten.

Artikel 1: Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen

§ 2 Begriffsbestimmungen

Um eine einheitliche Gestaltung der NIS-2-Richtlinie in allen EU-Mitgliedsstaaten sicherzustellen, sowohl hinsichtlich der zu meldenden Vorfälle als auch ihrer Auswirkungen, ist es von entscheidender Bedeutung, dass die Mitgliedsstaaten eine gemeinsame Auslegungspraxis vereinbaren. Statt nationale Begriffsbestimmungen zu entwickeln, sollte die Bundesregierung im Rahmen der Umsetzung von Artikel 23 der NIS-2-Richtlinie (EU) 2022/2555 gemeinsam mit anderen Mitgliedsstaaten dieses gemeinsame Verständnis erarbeiten. Dabei ist es wichtig, die Begrifflichkeiten und Klassifizierungen, wie etwa »wichtige Unternehmen«, »besonders wichtige Unternehmen« und »kritische Infrastruktur Betreiber«, klarer abzugrenzen – etwa durch Regelbeispiele –, um eine einheitliche und nachvollziehbare Anwendung sicherzustellen. Dies würde dazu beitragen, eine kohärente und einheitliche Umsetzung der Meldepflichten zu gewährleisten.

Die »Kommunikationstechnik des Bundes«, die in § 2 Nr. 21 als Informationstechnik, die von einer oder mehreren Einrichtungen der Bundesverwaltung oder im Auftrag einer oder mehrerer Einrichtungen der Bundesverwaltung betrieben wird beschrieben wird, ist aus unserer Sicht zu wenig abgrenzungsscharf und sollte klarer definiert werden.

§ 2 Nr. 22 definiert die ‚kritische Anlage' als eine Anlage, die für die Erbringung einer kritischen Dienstleistung erheblich ist; die kritischen Anlagen werden durch Rechtsverordnung nach § 56 Abs.4 näher bestimmt. Hierzu sind im Zusammenhang mit der Regelung des § 56 vor allem vier Punkte hervorzuheben:

1. 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 oder Erleichterung des Scopes oder der Verpflichtungen erfolgt, wird hinterfragt und ist klärungsbedürftig.

2. Dass vor allem per Rechtsverordnung nach § 56 Abs. 4 BSIG-E die Schwellenwerte für Kritische Anlagen definiert werden, sehen wir als kritisch an. Zu begrüßen wäre, dass die Schwellenwerte im Gesetzgebungsverfahren für die NIS-2-Umsetzung bestimmt werden. Eine Bestimmung im Rahmen der Gesetzgebungsverfahren bringt Rechtssicherheit und beschleunigt die Umsetzung der Vorgaben. Heute bereits in der BSI-Kritis-Verordnung bestehende sektorspezifische Schwellenwerte sollten beibehalten werden; Einrichtungen, die unter den Schwellenwerten liegen, sollten als besonderes wichtige Einrichtungen respektive wichtige Einrichtungen gewertet werden.

3. Die Wirtschaftsverbände sollten 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. Nur so können rechtliche Vorgaben praxistauglich ausgestaltet sind. Die Streichung der entsprechenden Textstellen sollte zurückgenommen werden.

4. Trotz der vorgenommenen Anpassungen an die neuen Bezeichnungen der Ministerien fehlt das BMDS in der Aufzählung. Dabei besteht gerade beim BMDS aufgrund seiner Zuständigkeit für den TK-Netzausbau in Deutschland eine hohe Wahrscheinlichkeit für eine Betroffenheit. Neue Sicherheitsanforderungen an TK-Netzbetreiber oder TK-Infrastrukturen haben potenziell erhebliche Auswirkungen auf den Festnetz- und Mobilfunkausbau in Deutschland, die in den Entscheidungsprozess innerhalb der Bundesregierung einzubringen, zu bewerten und im Falle widerstreitender Interessen in Einklang zu bringen sind. Daher ist das BMDS zwingend in der Aufzählung des § 56 Abs. 4 zu ergänzen.

Aktuell besteht aus unserer Sicht die Gefahr einer Überregulierung für Rechenzentrumsbetreiber, da gemäß § 2 Nr. 35 eine weitreichende Einbeziehung aller benötigten Anlagen und Infrastrukturen, insbesondere der für die Stromverteilung, vorgesehen ist. Diese Regulierung geht deutlich über die Anforderungen der EU hinaus und könnte zu unnötigen Belastungen führen. Es ist daher wichtig, eine angemessene Balance zwischen Sicherheitsanforderungen und wirtschaftlicher Tragfähigkeit zu wahren, um die Effizienz und Wettbewerbsfähigkeit der betroffenen Unternehmen nicht zu gefährden.

Die in der Begründung zum vorliegenden Entwurf enthaltene Klarstellung zur Definition des Begriffs »Managed Services Provider« (Begründung zu §1 Nummer 26, S. 142) stellt eine inhaltliche Neuerung gegenüber dem Regierungsentwurf 2024 dar. Dort wird ausgeführt, dass ein bestimmter Kundenstamm keine Voraussetzung für die Einstufung als MSP sei und beispielsweise auch Unternehmen, die ausschließlich den zentralen IT-Betrieb einer Unternehmensgruppe übernehmen, grundsätzlich unter den Begriff MSP fielen. In mehreren anderen Mitgliedstaaten findet eine derart weitreichende Einbeziehung konzerninterner IT-Dienstleister nicht statt. Eine

einheitliche europäische Auslegung ist jedoch essenziell, um Rechtssicherheit und gleiche regulatorische Voraussetzungen zu schaffen. Es stellt sich die Frage, inwiefern konzerninterne MSP ein vergleichbares Systemrisiko für den Markt oder für Dritte darstellen wie externe Anbieter mit vielfältigem Kundenstamm. Vor diesem Hintergrund ist zu prüfen, ob die Einstufung von konzerninternen IT-Einheiten als MSP mit den Zielen der europäischen Gesetzgebung - insbesondere der risikobasierten Ausrichtung der NIS-2-Richtlinie - in Einklang steht. Klar ist jedoch, dass im Falle einer Gleichbehandlung interner und externer MSP mit erheblichen zusätzlichen Umsetzungs- und Nachweispflichten für Unternehmen in der gesamten EU zu rechnen wäre.

Die NIS-2-Richtlinie geht davon aus, dass hinter jedem Dienst und jeder Tätigkeit lediglich eine einzelne Einrichtung steht. Diese Annahme entspricht jedoch nicht der Realität der deutschen Wirtschaft. In der Praxis erbringen häufig mehrere Einrichtungen gemeinsam kritische Dienste oder Tätigkeiten, was zu Unklarheiten darüber führt, welche Unternehmen in arbeitsteiligen Konstellationen als Adressaten der Pflichten der NIS-2-Richtlinie anzusehen sind. Das deutsche Umsetzungsgesetz sollte eine Regelung enthalten, die klar festlegt, wie in arbeitsteiligen Konstellationen die Verantwortlichkeiten verteilt werden. Idealerweise sollte das deutsche Umsetzungsgesetz zudem eine eigenständige Definition des Betreiberbegriffs enthalten. Mindestens sollte klargestellt werden, dass Betreiber – unabhängig von den Eigentumsverhältnissen – jene sind, die tatsächlich, rechtlich oder wirtschaftlich einen bestimmenden Einfluss auf die Erbringung der regulierten Tätigkeiten oder Dienste ausüben.

Die NIS-2-Richtlinie erfasst im Sektor der Anbieter digitaler Dienste auch Anbieter von Online-Marktplätzen. Zur Definition von Online-Marktplätzen verweist die Richtlinie auf Art. 2 lit. n der UGP-Richtlinie 2005/29/EG. Demnach gilt jeder Dienst, der es Verbrauchern mithilfe von Software, einschließlich einer Website, eines Teils einer Website oder einer Anwendung, die vom oder im Namen des Gewerbetreibenden betrieben wird, ermöglicht, Fernabsatzverträge mit anderen Gewerbetreibenden oder Verbrauchern abzuschließen, als Online-Marktplatz. Im Referentenentwurf wird auf § 312l Abs. 3 BGB verwiesen, ohne dass dies einen sachlichen Unterschied bewirkt. Unternehmen, die einen Webshop betreiben, eröffnen Dritten jedoch zunehmend die Möglichkeit, über ihre Plattform Waren im eigenen Namen zu verkaufen. Da dies allerdings in der Regel nur in geringem Umfang geschieht, ist es nicht sachgerecht, solche Marktplätze einem kritischen Sektor zuzuordnen. Die Systematik der NIS-2-Richtlinie deutet darauf hin, dass der europäische Gesetzgeber insbesondere solche Marktplätze erfassen wollte, die maßgeblich zum Absatz von Waren Dritter beitragen und deshalb eine kritische Funktion erfüllen. Daher sollte eine Ausnahme für Anbieter vorgesehen werden, bei denen der Online-Marktplatz nur einen unwesentlichen Teil der Gesamttätigkeit ausmacht.

Hersteller von Medizinprodukten, chemischen Erzeugnissen und vielen weiteren Produkten werden auch von der NIS-2-Richtlinie erfasst. Im europäischen Recht existieren jedoch verschiedene Definitionen des Herstellerbegriffs. Die NIS-2-Richtlinie und der Referentenentwurf lassen jedoch offen, welche davon im Rahmen der NIS-2-Umsetzung maßgeblich sein soll. Da die Herstellerbegriffe zu unterschiedlichen Ergebnissen bei der Anwendbarkeit führen, ist eine Klarstellung zur Vermeidung von

Rechtsunsicherheit dringend erforderlich. Da die NIS-2-Richtlinie ein hohes Cybersicherheitsniveau in der EU zum Ziel hat, sollte ein spezifischer, cybersicherheitsrechtlicher Herstellerbegriff zugrunde gelegt werden, der jene Akteure erfasst, die für den Schutz der Produktion verantwortlich sind.

§ 3 Aufgaben des Bundesamtes

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 eine NIS-2-Umsetzung keine Berücksichtigung. Wir regen an, diesen Verweis im Entwurf aufzunehmen, um durch das Gesetz sicherzustellen, dass Maßnahmen zur breiten Implementierung qualifizierter Vertrauensdienste gefördert werden. Generell befürworten wir auch andere Maßnahmen, die diese Zielsetzung unterstützen.

§ 6 Informationsaustausch

Es ist zu begrüßen, dass das BSI künftig eine Online-Plattform zum Informationsaustausch mit wichtigen Einrichtungen und der Bundesverwaltung betreiben wird. Im Vorfeld mangelte es jedoch an einer ausreichenden Einbindung der Wirtschaft, und die wiederholte Verzögerung der Bereitstellung des Portals ist aus Sicht der Unternehmen problematisch. Eine frühzeitige und transparente Veröffentlichung wäre hilfreich, um sich rechtzeitig mit den Funktionen und Anforderungen vertraut machen zu können. Ein offener Austausch mit der Wirtschaft kann dazu beitragen, die Plattform praxisnah auszugestalten – entsprechendes Feedback wird gerne eingebracht.

Für die Vorgabe der Teilnahmebedingungen auf der Online-Plattform nach § 6 Abs. 2 durch das BSI sollten hohe operative Aufwände vermieden werden, um auch KMU eine niedrigschwellige Beteiligung am Informationsaustausch zu ermöglichen. Auch eine Vereinheitlichung der Plattform zur Umsetzung von Informationspflichten aus anderen Gesetzesvorhaben wie der Umsetzung der CER-Richtlinie würde weiter zu einer lösungsorientierten Nutzung beitragen. Neben dem digitalen Austausch von Informationen ist es wichtig, die unabhängige Partnerschaft kritischer Infrastrukturen (UP KRITIS) fortzusetzen, um den persönlichen und vertrauensvollen Kontakt zwischen den Beteiligten zu gewährleisten.

§ 14 Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen

Das BSI kann zur Erfüllung seiner Aufgaben informationstechnische Produkte und Systeme untersuchen und ist berechtigt, von den Herstellern alle erforderlichen Auskünfte, insbesondere über technische Einzelheiten, zu verlangen. Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen weitergegeben und veröffentlicht werden, wenn dies der Aufgabenerfüllung dient. Bis zum Inkrafttreten des CRA als EU-weit geltender Rechtsrahmen für Produkte mit digitalen Elementen, ist das hier

vorgesehene Vorgehen eine angemessene Übergangslösung. Ab dem Inkrafttreten des CRA muss unbedingt gewährleistet werden, dass es keine parallelen Formen der Marktaufsicht gibt.

Aktuell geht jedoch weder aus dem Gesetzentwurf noch aus der Begründung hervor, wie sichergestellt werden soll, dass einerseits das Interesse der Allgemeinheit an der Aufklärung von Sachverhalten und andererseits das Interesse des Herstellers an der Geheimhaltung produkt- oder servicebezogener Informationen gewahrt bleibt. Insbesondere ist das Verhältnis der entsprechenden Auskunftsrechte zum GeschGehG gänzlich unklar. Der Gesetzgeber muss daher 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 für eine Schwachstelle kein schneller Patch verfügbar ist, sollte diese nur vertraulich kommuniziert werden. Dies verhindert, dass Kunden und Betreiber durch die Veröffentlichung von Angriffsmöglichkeiten geschädigt werden. Das BSI muss die Hersteller über die Beschreibung der Angriffsmöglichkeit sowie rechtzeitig vor der Veröffentlichung über den Inhalt der vom BSI geplanten externen Kommunikation informieren. Den Herstellern ist, im Sinne des Responsible Disclosure Verfahrens, vor der Veröffentlichung ausreichend Zeit zur Behebung des Problems einzuräumen.

Wenn der Hersteller einer signifikant verbreiteten Software nicht willens ist, eine Schwachstelle zu patchen (bspw. bei EoL-Status der Software ohne Upgrade-Möglichkeit oder Aufgabe der Geschäftstätigkeit), sollte das BSI die Möglichkeit haben, die Veröffentlichung des Codes unter der GPL-Version 3 zu erwirken.

§ 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen

Die Änderung der Schwellenwert-Klausel in § 28 Abs. 3 BSIG-E stellt eine wesentliche inhaltliche Anpassung gegenüber den bisherigen Entwürfen dar. Während dort lediglich die »der Einrichtungsart zuzuordnende Geschäftstätigkeit« als Grundlage der Betroffenheitsprüfung diente, werden nun sämtliche Geschäftstätigkeiten eines Unternehmens in den Blick genommen – es sei denn, sie können klar als vernachlässigbar eingestuft werden. Damit wird eine deutlich strengere Auslegung etabliert, die potenziell auch Unternehmen erfasst, die nur in geringem Umfang kritische Tätigkeiten ausüben. Problematisch ist dabei, dass bislang nicht eindeutig geklärt ist, ab welchem Umfang eine Tätigkeit als »vernachlässigbar« gilt. Diese Unschärfe führt zu Rechtsunsicherheit und erschwert es betroffenen Einrichtungen, ihre Einordnung verlässlich vorzunehmen. Eine Klarstellung, etwa durch Schwellenwerte oder konkrete Abgrenzungskriterien, wäre ist daher dringend erforderlich. Erfolgen könnte dies beispielsweise über eine Anpassung der Sektordefinitionen, z.B. eine Beschränkung der Energieerzeugung auf "Haupttätigkeiten" oder die Festlegung von Schwellenwerten in der KRITIS-VO.

Während privatwirtschaftliche Unternehmen die Anforderungen erfüllen müssen, bleiben relevante kommunale Einrichtungen weiterhin vom Anwendungsbereich

ausgeschlossen, mit Verweis auf die konkurrierende Gesetzgebung der Länder. Dies ist für eine ganzheitliche nationale Cybersicherheitsabwehr weder förderlich noch akzeptabel. Lediglich wenn diese Einrichtungen Waren oder Dienstleistungen gegen Entgelt für Einrichtungen der Bundesverwaltung anbieten, fallen sie in den Anwendungsbereich des Gesetzes (Artikel 1 § 28 Abs. 9). Dadurch wird versäumt, eine einheitliche Cybersicherheitsstrategie zu entwickeln, die ein hohes Niveau der Cybersicherheit auf allen Ebenen der Verwaltung ermöglicht. Wir sprechen uns daher dafür aus, in Koordination mit den Ländern auch kommunale Einrichtungen in den Anwendungsbereich der NIS-2-Umsetzung aufzunehmen.

Hinsichtlich der Definition von wichtigen Einrichtungen sollte im deutschen Umsetzungsgesetz zur NIS-2-Richtlinie eine klare und systematische Unterscheidung zwischen Herstellern und Anbietern vorgenommen werden. Die europäische Richtlinie sieht im Anwendungsbereich (Artikel 2) sowie bei der Einordnung wesentlicher und wichtiger Einrichtungen (Artikel 3) vor, dass insbesondere die in den Anhängen I und II gelisteten Tätigkeiten – wie etwa die Herstellung von Datenverarbeitungsgeräten gemäß Anhang II, Punkt 5 (b) – unmittelbar erfasst sind. Der aktuelle Entwurf des BSIG-E weitet diesen Anwendungsbereich jedoch erheblich aus, indem er in § 28 Abs. 2 Nr. 3 auch Einrichtungen einbezieht, die Waren oder Dienstleistungen entgeltlich anbieten. Damit erfolgt eine Interpretation, die über die ursprüngliche Intention der EU-Richtlinie hinausgeht und eine nationale Verschärfung darstellt. Eine differenzierte Betrachtung zwischen Herstellungs- und Vertriebstätigkeiten wäre im Sinne einer 1:1-Umsetzung angebracht und würde helfen, zusätzliche Anforderungen für bestimmte Marktakteure zu vermeiden.

§ 29 Einrichtungen der Bundesverwaltung

Es bestehen weiterhin erhebliche Bedenken hinsichtlich der vorgesehenen Regelungen zur IT-Sicherheit in der Bundesverwaltung. Der aktuell vorliegende Referentenentwurf lässt weiterhin die Möglichkeit offen, dass lediglich die Bundesministerien und das Bundeskanzleramt dem Regime des § 30 unterfallen, während für die übrigen Einrichtungen der Bundesverwaltung lediglich Mindeststandards gelten würden, die hinter dem Niveau des IT-Grundschutzes zurückbleiben. Zwar ist derzeit unklar, ob die entsprechende Formulierung in § 29 Abs. 2 im weiteren Gesetzgebungsverfahren Bestand haben wird, da innerhalb der Bundesregierung noch keine Einigung erzielt wurde. Dennoch wirft die geplante Differenzierung grundsätzliche Fragen auf – insbesondere, ob die Bundesverwaltung künftig insgesamt dem gleichen Schutzniveau unterliegen wird wie die Wirtschaft. Dabei gilt bereits seit 2017 der Umsetzungsplan Bund, der die obersten Bundesbehörden zur Anwendung des IT-Grundschutzes verpflichtet.

Ein Verzicht auf die Ausweitung des IT-Grundschutzes auf die gesamte Bundesverwaltung im Rahmen der NIS-2-Umsetzung würde faktisch zu einer Absenkung des Cyber-Sicherheitsniveaus innerhalb der Bundesverwaltung führen – insbesondere, wenn sich die bisherige Regelungslage im Gesetz fortsetzt. Eine solche Entscheidung stünde nicht nur im Widerspruch zu Forderungen, die unter anderem im Rahmen der öffentlichen Anhörung des Bundestages erhoben wurden, sondern würde auch problematische Signale an die Wirtschaft senden. Unternehmen, die durch die

Umsetzung des NIS 2 Umsetzungsgesetzes erheblich belastet werden, könnten das Fehlen einer Vorbildfunktion der öffentlichen Hand als Glaubwürdigkeitsdefizit wahrnehmen.

Besonders kritisch wäre, wenn auch sicherheitsrelevante Behörden wie das BKA und das BSI von der verbindlichen Einhaltung des IT-Grundschutzes ausgenommen blieben. Angesichts der sensiblen Daten, die diese Institutionen verwalten, und ihrer unverzichtbaren Funktionalität im Krisenfall wäre eine höhere Sicherheitsanforderung dringend geboten.

Die Begründung, eine Ausweitung des IT-Grundschutzes sei aus Kostengründen nicht realisierbar, erscheint nicht überzeugend. Die nun notwendigen Maßnahmen hätten bereits vor Jahren umgesetzt werden sollen, sodass die anfallenden Kosten eher als technische Schulden zu betrachten sind. Zudem ist allgemein bekannt, dass die Folgekosten von Cybervorfällen die Ausgaben für Prävention bei weitem übersteigen. Bitkom appelliert daher eindringlich, den IT-Grundschutz für die gesamte Bundesverwaltung verbindlich vorzuschreiben, um ein hohes Sicherheitsniveau nachhaltig sicherzustellen.

§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Das Sicherheitsziel «Authentizität" findet sich nicht in § 30 Abs. 1, da davon ausgegangen wird, dass dieses bereits im Ziel »Integrität« enthalten ist. Wir möchten darauf aufmerksam machen und empfehlen dringend eine Wiederaufnahme. Authentizität wird schließlich klar in der europäischen NIS-2-Richtlichinie als Sicherheitsziel benannt. Authentizität adressiert die Identitäten, insbesondere maschinelle Identitäten, die für die digitale Transformation eminent wichtig sind. Die EU-Fachgremien haben mit Absicht Authentizität als Ziel aufgenommen, da Integrität das Identitäts-Thema nicht abbildet.

Weiterer Handlungsbedarf in § 30 besteht in den unzureichenden Formulierungen im Gesetzestext bzw. in den Erläuterungen zum Verständnis des Begriffs "Erbringung ihrer Dienste", wodurch die konkrete Reichweite der Pflichten nach § 30 Abs. 1 weiterhin 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 bzw. 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.

Aber selbst ohne das Betreiben verschiedener Geschäftsbereiche ist unklar, warum ein derart weiter Begriff und damit die Ausdehnung der Pflichten auf die gesamte Unternehmens-IT erforderlich sind. Selbst wenn man sich vom bisherigen, bei KRITIS-Betreibern angewandten anlagenbezogenen Begriff lösen würde, ist nicht ersichtlich, warum diese Ausweitung im Hinblick auf die Schutzziele notwendig ist. Dies gilt insbesondere für die Einrichtungen, die nur aufgrund des Betriebs einer kritischen Anlage als besonders wichtige Einrichtung gelten. Ziel ist der Schutz der Versorgungssicherheit von Deutschland in bestimmten Sektoren. Sofern ein Unternehmen im verarbeitenden Gewerbe in den Anwendungsbereich fällt, sollten etwa Produktion und Logistik geschützt werden, etwa auch ein Warenwirtschaftssystem. Aber eine allgemeine Webseite des Unternehmens muss beispielsweise keinen erheblichen Einfluss auf die Versorgungssicherheit ausüben.

Wir empfehlen vor diesem Hintergrund zu prüfen, ob

- **entweder** das Merkmal „Erbringung ihrer Dienste“ auf informationstechnische Systeme, Komponenten und Prozesse, die sie für die Erbringung der Dienste im sektorbezogenen Teilbereich oder zum Betrieb ihrer kritischen Anlage benötigen, beschränkt wird
- **oder** jedenfalls folgende oder eine vergleichbare Klarstellung aufzunehmen, um hinreichend deutlich zum Ausdruck zu bringen, dass die unterschiedliche Risikoexposition und die grundsätzlich geringeren Auswirkungen möglicher Sicherheitsvorfälle außerhalb des sektorbezogenen Teilbereichs zwingend in die Risikobewertung nach § 30 Abs. 1 BSIG-RefE einzubeziehen sind: "Vielmehr sind die hier gemeinten Dienste sämtliche Aktivitäten der Einrichtung, für die IT-Systeme eingesetzt werden, dies beinhaltet beispielsweise auch Büro-IT oder andere IT-Systeme, die durch die Einrichtung betrieben werden, aber nicht unmittelbar für die Erbringung ihrer Dienste genutzt werden. Bei der Risikoexposition der Risiken und Auswirkungen eines Ausfalls oder einer Störung solcher IT-Systemen ist die fehlende Unmittelbarkeit besonders zu berücksichtigen."

Durch den Verweis in § 30 Abs. 3 auf Artikel 21 Abs. 5 der NIS-2-Richtlinie (EU) 2022/2555 wird ein Allgefahren-Ansatz angesetzt, bei dem »die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen« sind. Bestimmte Branchen sind zwar weitestgehend von diesen Anforderungen der europäischen Richtlinie ausgenommen, eine Überlappung gerade im OT-Bereich ist aus unserer Sicht jedoch nicht auszuschließen. Dies erfordert eine Klarstellung in der NIS-2-Umsetzung, um nicht über die harmonisierten Anforderungen hinauszugehen und einen erheblichen Mehraufwand für betroffene Unternehmen zu vermeiden.

Da die CSA-Schemata bislang keine konkreten Vorgaben zum Anwendungsbereich der Schutzniveaus enthalten, sollte der Gesetzgeber § 30 Abs. 6 präziser ausgestalten. Die derzeit allgemein gehaltene Regelung lässt Interpretationsspielraum, wonach nur höchstzertifizierte Lösungen zum Einsatz kommen dürfen. Dies berücksichtigt jedoch nicht den unterschiedlichen Sensitivitätsgrad der verarbeiteten Daten. Eine differenzierte Ausgestaltung ist erforderlich, um den Schutzbedarf angemessen abzubilden und eine praktikable Umsetzung zu gewährleisten.

Außerdem sprechen wir uns dafür aus, dass das Vorschlagsrecht für branchenspezifische Sicherheitsstandards gemäß § 30 Abs. 9 auch auf wichtige Einrichtungen und nationale Standardisierungsorganisationen ausgeweitet wird. Die Ausweitung dieser Möglichkeit würde die Einbindung von Stakeholdern über die KRITIS-Betreiber hinaus befördern und so zu einer höheren Akzeptanz und Verbreitung von B3S beitragen und gleichzeitig die Kompatibilität mit den in internationalen Normen enthaltenen Stand der Technik befördern und so auch Anpassungskosten reduzieren. Gleichzeitig halten wir es für unerlässlich, dass branchenspezifische Sicherheitsstandards, die eine Eignungsfeststellung durchlaufen haben, vom BSI frei und öffentlich zugänglich bereitgestellt wird. Nur so kann sichergestellt werden, dass alle Betreiber, Dienstleister und Berater auf dem gleichen Wissensstand sind und die Sicherheitsanforderungen einheitlich umgesetzt werden. Dies wäre auch im Sinne eines grundlegenden Prinzips zum Stand der Technik, das Transparenz und Nachvollziehbarkeit gewährleistet.

Abschließend ist aufgrund der Regelung des Inkrafttretens, welche keine Umsetzungsfrist vorsieht - und somit zur Implementierung der Maßnahmen nach § 30 BSIG-E keinerlei Umsetzungsfrist zugestanden wird - eine Frist mindestens bis zur nächsten Nachweispflicht bei Kritischen Infrastrukturen für die Umsetzung der Risikomanagementmaßnahmen zu gewähren. Eine solche Übergangsfrist sollte insbesondere auch für die Dokumentationspflicht gemäß Abs. 1 gelten.

§ 31 Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

§31 Abs. 2 sieht vor, dass kritische »Komponenten und Prozesse« der Angriffserkennung unterliegen sollen. Insbesondere bei Prozessen erscheint dies jedoch nicht praktikabel, da »Komponenten und Prozesse« nicht direkt an eine Angriffserkennung angeschlossen werden können. Eine solche Maßnahme ist technisch nur bei »Systemen« umsetzbar.

§ 32 Meldepflichten

Auch hinsichtlich der Meldefristen im Zusammenhang mit der Meldung von Sicherheitsvorfällen gibt es weiterhin offene Fragen. Die auf europäischer Ebene festgelegte Frist für die erste Meldung innerhalb von 24 Stunden wird als zu kurz erachtet, insbesondere für kleinere und mittlere Unternehmen, die von NIS-2 betroffen sind. Diese Frist kann leider nicht mehr geändert werden, weshalb es nunmehr notwendig ist, zumindest klarzustellen, dass die 24-Stunden-Frist entweder ab dem Zeitpunkt gilt, an dem das betroffene Unternehmen tatsächlich Kenntnis von dem Vorfall erlangt oder - noch sinnvoller - ab dem Zeitpunkt, an dem das betroffene Unternehmen tatsächlich die Signifikanz des Vorfalls, die zu einer Meldepflicht führt, festgestellt hat.

Diese Klarstellung ist für kleinere und mittlere Unternehmen von zentraler Bedeutung, da sie andernfalls gezwungen wären, einen IT-Service rund um die Uhr bereitzustellen,

was für viele Unternehmen im Anwendungsbereich der vorliegenden Richtlinie nicht praktikabel ist. Im Fall eines Angriffs, der beispielsweise an einem Wochenende oder an Feiertagen stattfindet, wäre es für diese Unternehmen unmöglich, die Meldepflichten innerhalb von 24 Stunden zu erfüllen. Bitkom fordert daher eine präzise Regelung, die sicherstellt, dass die Frist zur Meldung erst zu einem der o.g. Zeitpunkte zu laufen beginnt, um die praktische Umsetzbarkeit für alle Unternehmen zu gewährleisten. Die Klarstellung ist auch für solche Konstellationen relevant, in denen die betroffene Einrichtung Leistungen an einen IT-Dienstleister ausgelagert hat und für die Erfüllung ihrer Meldepflicht auf eine Information durch diesen IT-Dienstleister angewiesen ist.

Zudem sollte der Gesetzgeber sicherstellen, dass die Anforderungen im Meldewesen so effizient und digital wie möglich umgesetzt werden. Hierzu sollte ein vollständig digitalisiertes Meldeportal eingerichtet werden, das über effiziente Schnittstellen zur Automatisierung verfügt, Mehrfachmeldungen vermeidet und eine zentrale Anlaufstelle bietet. Unternehmen sollte zudem die Möglichkeit eingeräumt werden, Meldungen in englischer Sprache einzureichen, um den internationalen Anforderungen gerecht zu werden. Eine solche Maßnahme stärkt zugleich einen gesamtheitlichen europäischen Ansatz mit einheitlichen und parallelen Regelungen. Zwischenmeldungen sollten auf das notwendige Minimum reduziert werden, um den administrativen Aufwand und die Belastung der Ressourcen zu minimieren.

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

Ursprünglich war in § 38 Abs. 1 die Formulierung vorgesehen, wonach die Geschäftsleitung »Risikomanagementmaßnahmen zu genehmigen« hat. Dies entsprach der Systematik der NIS-2-Richtlinie (EU) 2022/2555 und ist inhaltlich nachvollziehbar. Die zwischenzeitlich vorgenommene Änderung in »Risikomanagementmaßnahmen umzusetzen« ist hingegen kritisch zu bewerten. 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 nach § 38 Abs. 1 geeignete Dritte beauftragen kann. Die Letztverantwortung verbleibt dabei weiterhin bei der Geschäftsleitung.

§ 39 Nachweispflichten für Betreiber kritischer Anlagen

Viele Betreiber Kritischer Infrastrukturen, deren nächste Nachweisfrist nach § 8a BSIG im vierten Quartal 2025 oder im ersten Quartal 2026 liegt, befinden sich derzeit in konkreter Vorbereitung oder bereits in laufenden Auditverfahren. Sollte das neue BSIG-E im Zuge der NIS-2-Umsetzung im Herbst 2025 in Kraft treten, wäre unklar, wie mit diesen laufenden Prüfungen umzugehen ist – insbesondere, ob Nachweise nach

bisherigem Recht noch angenommen werden können, wenn die neue Rechtslage bereits gilt, aber noch keine neue Frist festgelegt wurde. Ein vollständiger Prüfzyklus umfasst in vielen Fällen einen Zeitraum von bis zu sechs Monaten und kann mit erheblichem personellen und organisatorischen Aufwand verbunden sein. Entsprechend groß ist die Unsicherheit bei den betroffenen Unternehmen, ob ein geplanter oder laufender Nachweis zum Zeitpunkt der Vorlage überhaupt noch rechtskonform ist oder erneut durchgeführt werden müsste.

Um Planungs- und Rechtssicherheit für Betreiber, Prüfer und Aufsicht zu schaffen, sollte der Gesetzgeber klarstellende Übergangsregelungen im BSIG-E verankern. So ließe sich § 39 Abs. 3 BSIG-E um eine Regelung ergänzen, nach der Betreiber ihre Nachweise in einem Zeitraum von zwölf Monaten nach Inkrafttreten des Gesetzes weiterhin nach den bisherigen Anforderungen erbringen können, sofern ihre ursprüngliche Frist in diesen Zeitraum gefallen wäre. Eine solche Regelung würde sowohl das Risiko doppelter Prüfzyklen minimieren als auch das BSI von unnötigen Einzelfallprüfungen entlasten. Ergänzend sollte das BSI frühzeitig kommunizieren, in welchem Umfang sich Prüfumfang und Anforderungen künftig verändern werden, sowie klarstellen, dass Nachweise bereits vor Ablauf der Frist eingereicht werden dürfen. Dies würde einen geordneten und rechtssicheren Übergang unterstützen.

§ 41 Untersagung des Einsatzes kritischer Komponenten

Bitkom unterstützt ausdrücklich das Ziel des Gesetzgebers, Kritische Infrastrukturen wirksam zu schützen. Schon in der Bitkom-Stellungnahme zum IT-Sicherheitsgesetz 2.0 wurde die rechtssichere und hinreichend genaue Definition Kritischer Funktionen gefordert, um Kritische Komponenten klar identifizieren zu können. Entscheidend ist, dass solche Komponenten nur dann als kritisch eingestuft werden, wenn ihre Beeinträchtigung in der jeweiligen Einsatzumgebung den KRITIS-Schutzzielen zuwiderläuft.

Gleichzeitig müssen bei der Ausgestaltung der Kriterien die EU-rechtlichen Grundsätze der Nichtdiskriminierung, des fairen Wettbewerbs, des Marktzugangs und der Verhältnismäßigkeit gewahrt bleiben. Risikobewertungen sollten auf transparenten Verfahren, technischen Parametern und international anerkannten Cybersicherheitsstandards – wie etwa ISO 27001 – basieren. Dabei ist das bestehende EU-Recht zu berücksichtigen, das bereits Anforderungen an Unternehmensführung, Risikomanagement und Sicherheit in der Lieferkette vorsieht.

Offen bleiben 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. Ein kurzfristiger Ersatz von oftmals jahrelang genutzten Komponenten könnte daher unter Umständen nicht möglich sein.

Die Festlegung technischer Vorgaben sollte im Rahmen von Rechtsverordnungen erfolgen. Nur so kann sichergestellt werden, dass sektorspezifische Anforderungen sowie die fachliche Expertise aus der Praxis angemessen berücksichtigt werden.

Verbände und weitere relevante Akteure sollten dabei kontinuierlich in die Ausgestaltung und regelmäßige Aktualisierung der Kriterien eingebunden sein, um deren Wirksamkeit und Anschlussfähigkeit an den Stand der Technik zu gewährleisten.

§ 43 Informationssicherheitsmanagement

Es ist grundsätzlich zu begrüßen, dass das BSI verpflichtet wird, gemeldete Schwachstellen unverzüglich an die verantwortlichen Hersteller oder Produktverantwortlichen zur Behebung weiterzuleiten, sofern diese nicht bereits öffentlich bekannt sind. Auch die vorgesehene Verpflichtung der Bundesministerien zur Meldung entdeckter Schwachstellen stellt einen wichtigen Schritt zur Stärkung der IT-Sicherheit im staatlichen Bereich dar. Ein funktionierender Schwachstellenmeldeprozess ist essenziell, um bestehende Sicherheitslücken schnell zu schließen und potenzielle Angriffsvektoren zu minimieren.

Allerdings ist kritisch zu bewerten, dass der Entwurf weiterhin Ausnahmen für Sicherheitsbehörden sowie für Vereinbarungen mit nicht näher benannten »Dritten« vorsieht. Diese Ausnahmen schaffen erhebliche Sicherheitsrisiken, da nicht nachvollziehbar ist, mit welchen Akteuren solche Vereinbarungen getroffen werden dürfen und welche Schwachstellen davon konkret betroffen sind. Die fehlende Transparenz in diesem Bereich untergräbt das Ziel einer umfassenden Schwachstellenbeseitigung und kann dazu führen, dass Lücken über längere Zeiträume hinweg offenbleiben – mit potenziell gravierenden Auswirkungen auf die Sicherheit nationaler IT-Systeme und Netzwerke.

Um dem entgegenzuwirken, sollte der Entwurf dahingehend überarbeitet werden, dass Schwachstellen ausnahmslos und ohne zeitliche Verzögerung an die jeweiligen Hersteller gemeldet werden – unabhängig davon, ob sie durch Ministerien, das BSI, Sicherheitsbehörden oder andere Stellen identifiziert wurden. Eine solche Klarstellung würde nicht nur zur Schließung bestehender Regelungslücken beitragen, sondern auch das Vertrauen in die staatliche IT-Sicherheitsarchitektur stärken. Nur durch vollständige Transparenz und einheitliche Meldepflichten lässt sich das Risiko erfolgreicher Cyberangriffe wirksam reduzieren und die IT-Sicherheit auf nationaler Ebene nachhaltig verbessern.

§ 44 Vorgaben des Bundesamtes

Positiv hervorzuheben ist, dass in § 44 die in früheren Entwürfen vorgesehene Abschwächung der Umsetzungspflicht des IT-Grundschutzes für nachgeordnete Behörden nicht weiterverfolgt wird. Gleichzeitig ergibt sich aus der Regelung in § 29 Abs. 2, wonach die vollständige Einbeziehung der Bundesbehörden in die Vorgaben des § 30 erneut in Frage gestellt wird, ein Konflikt. Nachgeordnete Behörden, die teils einen höheren Schutzbedarf aufweisen und deren Ausfall potenziell größere kurzfristige Auswirkungen auf die Gesellschaft haben kann als der Ausfall von Ministerien, würden unter Umständen nur reduzierte Schutzmaßnahmen umsetzen müssen. Im Sinne eines kohärenten Schutzniveaus wäre es daher folgerichtig, dass mit der Umsetzung der Mindestanforderungen aus dem IT-Grundschutz – wie in § 44 vorgesehen – zugleich auch die Anforderungen aus § 30 erfüllt würden. Dies entspräche dem Ziel eines

harmonisierten Cybersicherheitsniveaus, das der Bitkom ausdrücklich unterstützt. Darüber hinaus ist zu beachten, dass sich aus den kurzfristig anstehenden Änderungen im IT-Grundschutz je nach Regelungsgehalt zusätzliche Umsetzungspflichten für entsprechend betroffene Dienstleister ergeben können.

§ 46 Informationssicherheitsbeauftragte der Ressorts

Unklar bleibt der aktuelle Entwurf hinsichtlich der konkreten Ausgestaltung der Rolle eines Chief Information Security Officer (CISO) für den Bund. Zwar sieht § 48 BSIG vor, dass die Bundesregierung eine Koordinatorin oder einen Koordinator für Informationssicherheit bestellt. Laut Begründung soll diese Person als zentrale Anlaufstelle für Maßnahmen der Informationssicherheit in der Bundesverwaltung fungieren und die Ressorts bei der Umsetzung entsprechender Vorgaben unterstützen. Damit wird zumindest ein Rahmen für eine koordinierende Rolle auf Bundesebene skizziert.

Allerdings bleibt der Entwurf bei der weiteren Ausgestaltung dieser Funktion vage. Die konkrete organisatorische Verankerung, etwa zur Einordnung in bestehende Verwaltungsstrukturen oder zur Ausstattung mit fachlichen und personellen Ressourcen, wird nicht gesetzlich geregelt, sondern einem späteren Kabinettsbeschluss überlassen. Bei einem so zentralen Element wie dem CISO Bund wäre ein höherer Grad an gesetzlicher Konkretisierung wünschenswert, um Verbindlichkeit und Wirksamkeit sicherzustellen.

Zudem sollte der Gesetzgeber der vielfach anerkannten Anforderung Rechnung tragen, dass ein CISO möglichst unabhängig agieren können muss – insbesondere zur Vermeidung von Interessenkonflikten bei der Bewertung sicherheitsrelevanter Maßnahmen. Eine gesetzlich verankerte organisatorische Unabhängigkeit und klare Aufgabenbeschreibung würden nicht nur die Position selbst stärken, sondern auch zur Effektivität und Glaubwürdigkeit des Informationssicherheitsmanagements auf Bundesebene beitragen.

§ 55 Konformitätsbewertung und Konformitätserklärung

In § 55 wird aus unserer Sicht nicht deutlich, welche konkreten Ziele mit der Einführung der Konformitätserklärung verfolgt werden sollen. Auch ist unklar, inwieweit dieser Abschnitt in der NIS-2-Richtlinie (EU) 2022/2555 verankert ist. Die Konformitätsbewertung scheint vielmehr der Einführung des CRA vorzugreifen, was einen isolierten Ansatz innerhalb der EU bedeuten würde. Um die Ziele der NIS-2-Richtlinie (EU) 2022/2555 zu erreichen, sprechen wir uns daher dafür aus, die Freiwilligkeit der Konformitätsbewertung, ähnlich wie in § 57, für Unternehmen deutlicher zu kennzeichnen. Es sollte vermieden werden, dass mit der deutschen Umsetzung EU-Vorgaben ausgeweitet werden.

§ 56 Ermächtigung zum Erlass von Rechtsverordnungen

Wie zu § 2 ausgeführt, fehlt das BMDS bei der Aufzählung der zu beteiligen Ministerien und ist aus den zu § 2 angeführten Gründen zu ergänzen.

Zudem wurde die in früheren Entwürfen vorgesehene Beteiligung von Wissenschaft, KRITIS-Betreibern und Wirtschaftsverbänden bei der Definition von KRITIS-Dienstleistungen (§ 56 Abs. 4) sowie bei der Festlegung erheblicher Sicherheitsvorfälle (§ 56 Abs. 5) im aktuellen Entwurf ersatzlos gestrichen. Die damit verbundenen Beteiligungsrechte hätten eine sachgerechte und praxisnahe Ausgestaltung der jeweiligen Regelungsinhalte unterstützt. Es ist bedauerlich, dass diese Möglichkeit zur strukturierten Einbindung relevanter Expertise nicht weiterverfolgt wurde. Eine gesetzlich verankerte Konsultation zentraler Stakeholder würde zur fachlichen Qualität und zur Akzeptanz der Regelungen gleichermaßen beitragen. (vgl. hierzu auch die Ausführungen unter § 2 Begriffsbestimmungen).

§ 61 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

§ 61 regelt die Zuständigkeit des Bundesamtes für die Überwachung der Einhaltung der Vorschriften bei wichtigen und besonders wichtigen Einrichtungen sowie bei kritischen Anlagen. Mit Abs. 11 wird eine Berichtspflicht des BSI gegenüber den Datenschutzaufsichtsbehörden eingeführt, sofern bei Sicherheitsvorfällen auch personenbezogene Daten betroffen sein könnten. Diese Vorgabe ist nur dann sinnvoll und praktikabel, wenn sich zugleich klarstellt, dass betroffene Unternehmen in solchen Fällen nicht zusätzlich eine eigenständige Meldung an die Datenschutzaufsicht abgeben müssen. Eine doppelte Meldepflicht wäre nicht nur redundant, sondern würde auch zu erheblichem administrativem Mehraufwand führen.

Darüber hinaus bleibt unklar, wie sich die vorgesehenen Audits von bestehenden Verfahren wie dem KRITIS-Nachweis unterscheiden. Es fehlt an einer Standardisierung der Auditverfahren sowie an einer Abgrenzung zu bereits etablierten Formaten. Ohne eine klare Definition der Anforderungen und Abläufe besteht das Risiko paralleler Prüfstrukturen, die zu Rechtsunsicherheit und unnötiger Belastung der betroffenen Einrichtungen führen. Da ein großer Teil der besonders wichtigen Einrichtungen gerade nicht zu den Betreibern kritischer Anlagen gehört, sollte sich die Nachweiserbringung und Auditmöglichkeit auf das Nötigste beschränken.

§ 62 Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen

§ 62 BSIG-E differenziert nicht ausreichend zwischen wichtigen und besonders wichtigen Einrichtungen im Hinblick auf die Ausgestaltung der behördlichen Maßnahmen. Zwar sieht die NIS-2-Richtlinie selbst für beide Kategorien ein vergleichbares Schutzniveau vor, der deutsche Entwurf schafft jedoch auch auf Ebene der behördlichen Durchsetzung keine abgestufte Vorgehensweise.

Gerade bei wichtigen Einrichtungen, zu denen in hohem Maße auch kleine und mittlere Unternehmen zählen, ist eine differenzierte Herangehensweise notwendig. Diese Unternehmen verfügen oft nicht über dieselben personellen oder finanziellen Ressourcen wie besonders wichtige Einrichtungen oder Betreiber kritischer Anlagen. Eine Gleichbehandlung bei den regulatorischen Anforderungen und den damit verbundenen Eingriffsbefugnissen der Behörde würde für viele dieser Einrichtungen eine unverhältnismäßige Belastung bedeuten. Es wäre daher sachgerecht, im Gesetz klarzustellen, dass die behördlichen Maßnahmen im Verhältnis zur Bedeutung und Risikolage der jeweiligen Einrichtung stehen müssen.

Artikel 25: Änderung des Telekommunikationsgesetzes

§ 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 Anbieter 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

Abs. 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Abs. 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, sind verpflichtet, die von diesen Einrichtungen nach Abs. 2 zu ergreifenden Maßnahmen umzusetzen und ihre Umsetzung zu überwachen. Hier verweisen wir auf die Ausführungen zu § 38 in diesem Dokument und möchten darauf hinweisen, dass auch hier zur ursprünglichen Formulierung »zu genehmigen« zurückzukehren ist, die der Rolle der Geschäftsleitung als verantwortliche Instanz ohne operative Überforderung gerecht wird. Ergänzend sollte gesetzlich klargestellt werden, dass die Geschäftsleitung zur Erfüllung ihrer Pflichten geeignete Dritte beauftragen kann. Die Letztverantwortung verbleibt dabei weiterhin bei der Geschäftsleitung.

§ 168 Meldung eines Sicherheitsvorfalls

Für Telekommunikationsunternehmen bedingt die Neuregelung des § 168 TKG eine doppelte Meldepflicht von erheblichen Vorfällen - dies sowohl an das BSI als auch an die Bundesnetzagentur (vgl. Artikel 25 § 168 Abs. 1 und 3 TKG). Vor allem die Anwendung für grenzüberschreitend tätige Unternehmen wird sehr komplex und es werden über die Forderungen der EU hinausgehende Verpflichtungen aufgenommen, die zu einem erheblichen Aufwand und zu nicht nachvollziehbarer Doppelregulierung führt. Die Anpassung der Meldepflicht nach Artikel 25 § 168 Abs. 1 TKG-E ist vorzusehen.

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 Abs. 1 (4) als besonders wichtige Einrichtung eingestuft.

Spalte A	Spalte D
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.*

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Felix Kuhlenkamp | Bereichsleiter Sicherheitspolitik
T +49 30 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Sicherheitspolitik