bitkom

Stellungnahme

Mai 2024

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Zusammenfassung

Angesichts der Cyberbedrohungslage unterstützt der Bitkom die Harmonisierung des Cybersicherheitsniveaus durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG). Wir begrüßen den Fortschritt durch den dritten Referentenentwurf und die bevorstehende Verbändeanhörung.

Positiv bewertet wird die dreijährige Frist für Betreiber Kritischer Anlagen zum Nachweis der Erfüllung der Anforderungen nach § 30 Abs. 1 sowie die Streichung der Kategorie „Unternehmen im besonderen öffentlichen Interesse“. Die geplante Online-Plattform zum Informationsaustausch zwischen wichtigen Einrichtungen und der Bundesverwaltung ist ein guter Schritt. Das BSI sollte die Entwicklung unbedingt in Abstimmung mit der Wirtschaft voranbringen. Wir begrüßen zudem die Abstimmung zwischen BMI und betroffenen Ressorts über erhebliche Sicherheitsvorfälle.

Auf der anderen Seite bestehen weiterhin Rechtsunsicherheiten für die Wirtschaft. Insbesondere KMU können ihre Betroffenheit vom NIS2UmsuCG oft nicht selbst abschätzen. Für mehr Rechtssicherheit muss der Referentenentwurf mit dem KRITIS-Dachgesetz abgestimmt werden. Eine fehlende Konsultation führt ansonsten zu Auslegungsproblemen und Konflikten zwischen Behörden. Klärungsbedarf besteht außerdem in § 30 bei Diensten, die in verschiedenen Geschäftsbereichen erbracht werden. Es sollte klar sein, ob alle IT-Systeme eines Unternehmens oder nur diejenigen, die direkt für relevante Dienstleistungen genutzt werden, abgedeckt sind. Empfohlen wird, die Definition auf die für kritische Dienstleistungen verwendeten IT-Systeme zu beschränken oder zumindest klarzustellen, dass unterschiedliche Risiken in die Risikobewertung einbezogen werden sollten.

Darüber hinaus kritisieren wir die Ausnahme kommunaler Verwaltungen von den NIS2UmsuCG-Vorgaben. Kommunale Dienstleistungen sind zentral für das tägliche Leben in Deutschland. Ein grundlegender Sicherheitsrahmen muss daher eingeführt werden, um diese Bereiche zu schützen. Die Hauptlast der Maßnahmen wird allein auf die Privatwirtschaft abgewälzt. Während diese Ihre volle Verantwortung annimmt, sehen wir mit Sorge, dass dies von staatlicher Seite nicht erfolgt. Somit bleiben Verwaltung und staatlich Einrichtungen die Schwachstelle für die Cybersicherheit in Deutschland. Eine integrative Herangehensweise, die alle Verwaltungsebenen einbezieht, ist notwendig, um die Cybersicherheit in der Breite zu erhöhen. Der Bitkom appelliert daher an das BMI, gemeinsam mit den Ländern und Kommunen einen inklusiven Ansatz zu verfolgen.

97%

der deutschen Unternehmen finden, dass Sicherheitsbehörden sie besser über die Cybersicherheitslage informieren sollten. (Bitkom, 2023)

Allgemeine Anmerkungen

Die Bedrohungslage im Cyberraum bleibt angespannt. Im vergangenen Jahr ist der deutschen Wirtschaft allein durch Cyberattacken ein Schaden in Höhe von 148,2 Mrd. Euro entstanden und die Unternehmen gehen davon aus, dass dies weiter stark ansteigen wird (Bitkom, 2023). Vor diesem Hintergrund ist es unerlässlich, die gesetzliche Verankerung und Governance der Informationssicherheit in Deutschland weiterzuentwickeln. Mit der NIS-2-Richtlinie (EU) 2022/2555 wurde auf europäischer Ebene dafür ein guter Kompromiss mit einer vernünftigen Balance zwischen gezielten regulatorischen Eingriffen und einer ganzheitlichen Stärkung der Cyber-Resilienz der EU gefunden.

Der Bitkom ist weiterhin überzeugt von der europäischen Idee für einen ganzheitlich gestärkten und harmonisierten Cybersecurity-Regulierungsrahmen. Wir begrüßen die Veröffentlichung des dritten Referentenentwurfs und die Möglichkeit zum breiten Austausch mit Stakeholdern im Rahmen der Verbändeanhörung. Es ist positiv zu bewerten, dass das Gesetz den Betreibern Kritischer Anlagen eine Frist von mindestens drei Jahren gewährt, um die Erfüllung der Anforderungen nach § 30 Abs. 1 erstmals dem BSI gegenüber nachzuweisen. Ebenso begrüßen wir die ersatzlose Streichung der Kategorie „Unternehmen im besonderen öffentlichen Interesse“, wodurch künftig neben Kritischen Anlagen nur noch wichtige sowie besonders wichtige Einrichtungen berücksichtigt werden. Dies trägt zur Stärkung der europaweiten Harmonisierung der Cybersicherheitsregulierung bei und beendet den deutschen Sonderweg des IT-Sicherheitsgesetzes 2.0.

Durch Verzögerungen sind wir aktuell jedoch in einer Situation, in der die Umsetzungsfrist im Oktober 2024 möglicherweise nicht eingehalten werden kann. Dadurch entstehen zweierlei Probleme. Erstens schadet dies der EU-weiten Harmonisierung in der Cybersicherheit, da andere Mitgliedsstaaten bereits fortgeschritten sind und damit andere Umsetzungsfristen gelten. Der deutsche Gesetzgeber verschärft diese Situation, indem er sich von der Struktur der NIS-2-Richtlinie (EU) 2022/2555 entfernt, was die Anwendung für grenzüberschreitend tätige Unternehmen unnötig komplex macht und indem er über die Anforderungen der EU erhöhte Verpflichtungen aufnimmt, die zu einem erheblichen Aufwand und zu Doppelregulierungen führen. Zweitens entsteht durch die Verzögerung eine Rechtsunsicherheit für Unternehmen. Viele Unternehmen, insbesondere KMU, können nicht ohne externe Beratung ihre Betroffenheit vom NIS2UmsuCG absehen oder sind sich gar nicht bewusst, dass sie möglicherweise in den Geltungsbereich fallen. Auch bei größeren Unternehmen besteht Verunsicherung hinsichtlich möglicher Sicherheitsvorfälle vor Ablauf von Übergangs- und Nachweisfristen. Wir bitten in Hinblick auf diese genannten Punkte um Klarstellung seitens des Gesetzgebers.

Bei der Weiterentwicklung der Cybersicherheitsstrategie Deutschlands ist auch zu beachten, dass diese eng mit der Nationalen Sicherheitsstrategie und dem KRITIS-Dachgesetz abgestimmt sein muss, um ein kohärentes und konsistentes Vorgehen zu gewährleisten. Die NIS-2-Richtlinie (EU) 2022/2555 sieht in Artikel 7 lit. g „eine verstärkte Koordinierung zwischen den [...] zuständigen Behörden [...] zum Zweck des Informationsaustauschs über Risiken, Bedrohungen und Sicherheitsvorfälle“ vor. Es gilt daher mit dem NIS2UmsuCG und dem KRITIS DachG ein einheitliches Verständnis

darüber zu entwickeln, wie physische Sicherheit und Cybersicherheit gemeinsam umgesetzt werden können. In der Unternehmenspraxis sind diese Bereiche eng miteinander verzahnt und sollten nicht isoliert voneinander betrachtet und umgesetzt werden müssen. Aktuell führt fehlende Konsultation der Gesetzentwürfe zu uneinheitlichen Definitionen und Begrifflichkeiten, die Auslegungsprobleme verursachen können. Dies zeigt sich beispielsweise in den konfliktbehafteten Zuständigkeiten vom BSI im NIS2UmsuCG auf der einen Seite und dem BBK im KRITIS DachG auf der anderen Seite. Die angestrebte EU-weite Harmonisierung der Cybersicherheit kann auf dieser Grundlage nicht ausreichend erreicht werden. NIS2UmsuCG und das KRITIS DachG sollten daher stärker aufeinander abgestimmt und wesentliche Regelungsinhalte im Sinne des All-Gefahren-Ansatzes besser harmonisiert werden. Die zügige Novellierung der BSI-KRITIS-Verordnung ist ebenfalls von Bedeutung, um Sektoren anhand von Schwellwerten und Anlagekategorien zu definieren.

Die Entscheidung, kommunale Verwaltungen auf Wunsch der Länder sowie Bundeseinrichtungen von den Vorgaben des NIS2UmsuCG auszunehmen, wird in unserer Mitgliedschaft mit Sorge aufgenommen. Kommunale Dienstleistungen sind von zentraler Bedeutung für das tägliche Leben der Bürgerinnen, Bürger und Unternehmen. Ein Ausfall essenzieller Dienste würde nicht nur unmittelbare und erhebliche Auswirkungen auf die betroffene Bevölkerung und Wirtschaft haben, sondern könnte auch das Vertrauen in die Funktionsfähigkeit staatlicher Strukturen nachhaltig erschüttern. Vor diesem Hintergrund ist eine Stärkung der Cybersicherheit in diesen Bereichen unabdingbar und von höchster Priorität. Anstatt aus Gründen des vermeintlich hohen Aufwands auf spezifische Vorgaben für die Kommunen zu verzichten, wäre die Einführung eines grundlegenden Sicherheitsrahmens, eine angemessene und praktikable Alternative. Ein solcher Rahmen könnte beispielsweise bei Asylverfahren den notwendigen Schutz für eingestufte Daten gewährleisten, ohne die Ressourcen der kommunalen Verwaltungen übermäßig zu belasten. Dafür stehen bereits heute eine Vielzahl an etablierten Standards zur Absicherung zu Verfügung, die den Kommunen auch im „Weg in die Basis-Absicherung“ (WiBA) an die Hand gegeben werden.

Es ist aus unserer Sicht nicht nachvollziehbar, dass die Hauptlast der Umsetzung der Cybersicherheitsmaßnahmen erneut auf die Privatwirtschaft abgewälzt wird, während wesentliche Teile der öffentlichen Verwaltung ausgenommen bleiben. Dies steht in direktem Widerspruch zum erklärten Ziel der NIS-2-Richtlinie (EU) 2022/2555, die Resilienz und Sicherheit in der Daseinsvorsorge umfassend zu stärken. Eine integrative Herangehensweise, die auch die kommunalen Verwaltungen einschließt, ist unerlässlich, um die Cybersicherheit in allen Bereichen des öffentlichen Lebens zu erhöhen. Wir appellieren daher an das BMI, die bestehenden Ausnahmen zu überdenken und in Zusammenarbeit mit den Ländern einen inklusiven Ansatz zu verfolgen, der den Schutz und die Sicherheit der gesamten Bevölkerung gewährleistet.

Um Unternehmen und Behörden noch effektiver zu schützen, schlagen wir zudem vor, dass neben organisatorischen und technischen Maßnahmen auch die Mitarbeitenden in die Sicherheitsstrategien einbezogen werden. Regelmäßige Schulungen und Sensibilisierungsprogramme sind hierbei entscheidend. Die Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden in sicherheitsrelevanten Bereichen zur

Unternehmensresilienz beitragen. Derzeit fehlt jedoch eine gesetzliche Grundlage, die eine rechtssichere Prüfung von Bewerbenden, Mitarbeitenden und Dienstleistenden ermöglicht. Eine möglicher Lösungsansatz wäre die Option zur freiwilligen Vertrauenswürdigkeitsüberprüfung aus Artikel 14 der Resilience-of-Critical-Entities-Richtlinie ((EU) 2022/2557) in die deutschen Gesetze zu übernehmen. Diese Prüfung sollte durch staatliche Stellen erfolgen, wofür ein geeigneter rechtlicher Rahmen dafür zu schaffen ist. Die Überprüfung soll zudem die bestehende staatliche Sicherheitsüberprüfung im Geheim- und vorbeugenden personellen Sabotageschutz ergänzen und nahtlos in das bestehende System integriert werden.

Wir möchten an dieser Stelle außerdem darauf hinweisen, dass die wörtliche Übersetzung des Begriffs „Access Control“ zu einer fehlerhaften Interpretation führen kann. Statt dem bisher gewählten Wort „Zugriffskontrolle“ scheint vielmehr „Zugriffssteuerung“ die Bedeutung im Sinne der europäischen Richtlinie wiederzugeben.

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

§ 2 Begriffsbestimmungen

Um eine einheitliche Gestaltung der Meldepflichten 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. Dies würde dazu beitragen, eine kohärente und einheitliche Umsetzung der Meldepflichten zu gewährleisten.

Die Definition von „Informationssicherheit“ in § 2 Abs. 1 Nr. 16 begrüßen wir insofern, als dass sie den angemessenen „Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen“ vorsieht. Wir möchten an dieser Stelle ausdrücklich darauf hinweisen, dass die Ziele der NIS-2-Richtlinie (EU) 2022/2555 nur durch einen entsprechenden holistischen Ansatz erreicht werden können. Dementsprechend müssen alle technischen und organisatorischen Aspekte zum Schutz von Informationen, sowohl analog als auch digital, einbezogen werden. Entsprechende Anpassungen wurden auch im Verlaufe des Referentenentwurfs für ein NIS2UmsuCG gemacht, beispielsweise mit dem Austausch von „Cybersicherheit“ zu „Informationssicherheit“ in § 43 Abs. 2. An anderer Stelle, wie in § 38 Abs. 1 wird jedoch weiter auf „Cybersicherheit“ verwiesen, was entsprechend angepasst oder durch eine weitere Begriffsdefinition abgesichert werden sollte.

Mit der aktuellen Begriffsdefinition von „Managed Service Providern“ gemäß § 2 Abs. 1 Nr. 25 wird aus unserer Sicht jegliche Form der MSP in den Anwendungsbereich des NIS2UmsuCG genommen. Dies umfasst auch konzerninterne Dienstleister. Sollte dieser Umfang intendiert sein, würden wir uns für eine dahingehenden Hinweis in der Definition aussprechen.

Aktuell besteht aus unserer Sicht die Gefahr einer Überregulierung für Rechenzentrumsbetreiber, da gemäß § 2 Abs. 1 Nr. 34 eine weitreichende Einbeziehung aller benötigten Anlagen und Infrastrukturen, insbesondere der für die Stromverteilung, vorgesehen ist. Diese Regulierung geht 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.

Darüber hinaus begrüßen wir die in Absatz 2 vorgesehene Möglichkeit des BMI, im Benehmen mit anderen betroffenen Ressorts durch Rechtsverordnung festzulegen, wann ein Sicherheitsvorfall als erheblich im Sinne der einschlägigen Vorschriften anzusehen ist. Diese gemeinsame Entscheidungsfindung ermöglicht einen zielgerichteten Umgang mit Sicherheitsvorfällen und trägt somit zur Verbesserung der Sicherheitslage bei.

§ 3 Aufgaben des Bundesamtes

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

§ 6 Informationsaustausch

Wir begrüßen, dass das BSI eine Online-Plattform zum Informationsaustausch mit wichtigen Einrichtungen und der Bundesverwaltung betreiben wird. Es ist essenziell, dass BMI und BSI vorab eine Testversion des BSI Information Sharing Portals vorlegen und es gemeinsam mit der Wirtschaft weiterentwickeln, um zielgruppengerechte Lageinformationen bereitzustellen. Wir stehen bereit, um uns am Austausch dazu zu beteiligen und konstruktives Feedback zu geben.

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 dem KRITIS DachG würde weiter zu einer lösungsorientierten Nutzung beitragen. Neben dem digitalen Austausch von Informationen ist es wichtig, den Umsetzungsplan KRITIS (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 intern 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.

§ 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen

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 des NIS2UmsuCG aufzunehmen.

§ 29 Einrichtungen der Bundesverwaltung

Die anhaltenden Cyberangriffe auf Kommunen und Behörden, die teilweise weitreichende Folgen für Wirtschaft und Gesellschaft haben, verdeutlichen die Dringlichkeit, die öffentliche Verwaltung auf allen Ebenen des föderalen Staates in den Anwendungsbereich des NIS2UmsuCG einzubeziehen. Die Fälle aus Anhalt-Bitterfeld und Schwerin zeigen die Folgen, wenn wichtige Verwaltungsdienstleistungen nicht zur Verfügung stehen und dabei beispielsweise wichtige Planungs- und Genehmigungsverfahren ausgesetzt sind. Während die Verantwortung durch den weitreichenden Anwendungsbereich auch viele mittlere und kleine Unternehmen trifft, nimmt sich der Staat hier eine Sonderrolle und entzieht sich der eigentlichen Verantwortung.

Es ist unerlässlich, dass Bundesbehörden, Landes- und Kommunalbehörden einheitlich als besonders wichtige Stellen definiert werden, um sie in den Anwendungsbereich des NIS2UmsuCG einzubeziehen. Ausnahmen davon oder Einstufungen als lediglich wichtige Einrichtungen, sollten aus unserer Sicht nicht vorgenommen werden. Dafür sollte sich das BMI insbesondere in Koordination mit den Ländern einsetzen. Die ganzheitliche Einbeziehung ist von entscheidender Bedeutung, um das beabsichtigte Ziel der NIS-2-Richtlinie (EU) 2022/2555 zu erreichen, nämlich eine EU-weite Harmonisierung der Cybersicherheit zu gewährleisten. Nur durch eine umfassende Integration aller Verwaltungsebenen kann die Wirksamkeit von Maßnahmen zur Stärkung der Cybersicherheit in der öffentlichen Verwaltung in ganz Europa gewährleistet werden.

§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Das Sicherheitsziel “Authentizität” ist in § 30 Abs. 1 nicht mehr aufgeführt, wohingegen es unter § 2 Nr. 22 weiterhin aufgeführt wird. Wir möchten darauf aufmerksam machen und um eine Wiederaufnahme bitten. Authentizität wird schließlich klar in der europäischen NIS2-Richtlichinie als Sicherheitsziel benannt. Sollte sich das BMI an dieser Stelle an den internationalen Begrifflichkeiten Confidentiality, Integrity and Availability (CIA) orientiert haben, wäre eine Klarstellung in der Begründung wünschenswert.

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.

Dieses Ergebnis überrascht umso mehr, da bei der Berechnung der Schwellenwerte zur Ermittlung des Anwendungsbereichs nach § 28 nur die Kennzahlen berücksichtigt werden sollen, die auf den sektorbezogenen Teilbereich des Unternehmens entfallen (Begründung zu § 28 Abs. 3, S. 144). Damit soll sichergestellt werden, dass Unternehmen, "deren hauptsächliche Geschäftstätigkeit jedoch nicht einer Einrichtungskategorie gemäß Anlage 1 oder 2 dieses Gesetzes zuzuordnen ist, nicht in unverhältnismäßiger Weise erfasst werden" (Begründung zu § 28 Abs. 3 BSIG-RefE, S. 144). Das oben darstellte weite Begriffsverständnis von "Erbringung ihrer Dienste" läuft diesem Zweck aber gerade zuwider. Diese Frage ist nicht nur für die Reichweite der Pflichten des § 30 BSIG-RefE selbst von zentraler Bedeutung. Dies hat auch weitere Auswirkungen, wie beispielsweise den Umfang der zu erstellenden notwendigen Dokumentation oder die Anordnung von Prüfungen durch Behörden. So sollte auch in den Nachweispflichten nach § 39 deutlich klargestellt sein, dass diese nur den Geltungsbereich der kritischen Anlage umfassen und nicht darüber hinaus gehen. Auch die Beurteilung eines relevanten erheblichen Sicherheitsvorfalls für die Meldepflichten nach § 32 BSIG-RefE wird erleichtert, wenn der Anwendungsbereich klarer, weil enger ist.

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. 2 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 im NISUmsuCG, um nicht über die harmonisierten Anforderungen hinauszugehen und einen erheblichen Mehraufwand für betroffene Unternehmen zu vermeiden.

Außerdem sprechen wir uns dafür aus, dass das Vorschlagsrecht für branchenspezifische Sicherheitsstandards gemäß § 30 Absatz 9 auch auf wichtige Einrichtungen ausgeweitet wird. Mit der Bewährung dieser Möglichkeit durch KRITIS-Betreiber würde solch eine Ausweitung die Vorteile von B3S noch weiter in die Breite tragen, um mehr Einrichtungen aktiv zu beteiligen.

§ 41 Untersagung des Einsatzes kritischer Komponenten

Bitkom unterstützt weiterhin das Ansinnen des Gesetzgebers, Kritische Infrastrukturen, soweit technisch und personell möglich, wirksam zu schützen. Schon in unserer Stellungnahme zum IT-Sicherheitsgesetz 2.0 forderten wir, die rechtssichere und hinreichend genaue Definition Kritischer Funktionen, um Kritische Komponenten klar fassen/identifizieren zu können. Es bedarf auch weiterhin einer Liste mit klar formulierten kritischen Komponenten und eindeutig definierten technischen Vorgaben. Diese bzw. Komponenten mit kritischen Funktionen können i. S. dieses Gesetzes nur dann kritisch sein, wenn ihre Funktionalitäten in Bezug auf die Einsatzumgebung im Falle ihrer Beeinträchtigung den KRITIS-Schutzzielen zuwiderlaufen. Spezifikationen erfolgen Sektor spezifisch im Rahmen einer Rechtsverordnung unter Beteiligung der betroffenen KRITIS-Sektoren und Betreiber kritischer Anlagen.

§ 54 Zertifizierung

Bitkom begrüßt die Anpassung in § 54 Abs. 8, wonach Sicherheitszertifikate anderer anerkannter Zertifizierungsstellen aus dem Bereich der Europäischen Union vom Bundesamt anerkannt werden können, sofern sie eine Sicherheit aufweisen, die den Sicherheitszertifikaten des Bundesamtes gleichwertig ist und die Gleichwertigkeit vom Bundesamt festgestellt wurde. Es ist sicherzustellen, dass die Gleichwertigkeit von Sicherheitszertifikaten aller nationalen Zertifizierungsstellen, die heute beispielsweise

schon in der SOGIS (Senior Officials Group Information Systems Security) oder auch im „EUCC scheme“ (European Cybersecurity Scheme on Common Criteria) integriert sind, ohne Verzögerung vom Bundesamt festgestellt werden. Die neue Regelung ermöglicht eine koordinierende europäische Zertifizierungslandschaft, trägt zum Gelingen eines digitalen europäischen Binnenmarktes bei und entlastet die Unternehmen bei ihren Zertifizierungsvorhaben. Neue administrative Pflichten, die seitens der Unternehmen bewältigt werden müssen, müssen vermieden werden.

Ferner sollte mit Blick auf § 54 Abs. 5 vor einer Vermischung von technischen Regeln und Kriterien mit politischen Bewertungen vermieden werden, da ersteres dem Bundesamt und zweiteres dem BMI obliegt. Unnötiger Mehraufwand und Bürokratie sollten vermieden werden. Potenzielle Entscheidungen nach § 54 Abs. 5 müssen frühzeitig und öffentlich durch das Bundesministerium des Innern und für Heimat gegenüber der Industrie und dem Bundesamt angezeigt werden, um Planungs- und Investitionssicherheit zu schaffen.

§ 55 Konformitätsbewertung und Konformitätserklärung

In § 55 des NIS2UmsuCG 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 Cyber Resilience Act (CRA) vorzugreifen, was einen isolierten Ansatz innerhalb der EU bedeuten würde. Dies widerspricht dem Ziel, ein einheitliches Cybersicherheitsniveau zu erreichen. Der Bitkom plädiert daher für ein koordiniertes und gemeinsames Vorgehen auf europäischer Ebene, um eine Fragmentierung in den Mitgliedstaaten zu vermeiden. Zusätzlich möchten wir betonen, dass der neu eingeführte Konformitätsnachweis, der auf BSI-Anforderungen basiert, unnötige bürokratische Hürden für die Unternehmen schaffen würde.

Um die Ziele der NIS-2-Richtlinie (EU) 2022/2555 zu erreichen, sprechen wir uns daher für die Streichung von § 55 aus. Mit diesem harmonisierten und weniger bürokratischen Ansatz kann die Cybersicherheit in der EU effektiv gestärkt werden.

§§ 63/64 Zuständigkeit des Bundesamtes sowie Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten

§ 63 legt die Zuständigkeit des Bundesamtes für die Einhaltung der Vorschriften aus Teil 3 (§§ 28-50) für wichtige Einrichtungen und besonders wichtige Einrichtungen sowie für kritische Anlagen in Deutschland fest. Mit § 64 wird diese Zuständigkeit bei IT-Dienstleistungen auf Unternehmensteile oder Beteiligungen in EU-Mitgliedsstaaten erweitert, wenn der Hauptsitz des Unternehmens/Konzerns in Deutschland liegt. Das hätte in der jetzigen Formulierung die Konsequenz, dass das deutsche rechtliche Konzept der „kritischen Anlagen“ auch im europäischen Ausland gelten würde, wenn der Hauptsitz des Betreibers in Deutschland liegt. Dies ist führt zum Export der

erhöhten deutschen KRITIS-Anforderungen in das europäische Ausland. Dies gilt es zu vermeiden, weil es über die eigentlichen Anforderungen der NIS2 hinausgeht und in anderen EU-Mitgliedsstatten nicht umsetzbar wäre.

§ 65 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

Die nach § 65 geschaffenen Untersagungsbefugnisse des BSI gegenüber der Geschäftsführung, des Vorstandes und rechtlichen Vertretern der Unternehmen müssen im Hinblick auf ihre rechtliche Umsetzbarkeit kritisch geprüft werden. Zudem sollten die Haftungsfragen für potenziell verursachte Schäden durch eine Unternehmensübernahme eindeutig geklärt werden.

Artikel 23: Änderungen des Telekommunikationsgesetzes (FNA 900-17)

Für Telekommunikationsunternehmen bleibt es bei einer nicht nachvollziehbaren doppelten Meldepflicht von Vorfällen sowohl an das BSI als auch an die BNetzA (vgl. Artikel 23 § 168 Abs. 1 TKG). Ferner bleibt unklar, warum die Regelung bzgl. der einzuholenden Garantieerklärungen von Herstellern kritischer ITK-Komponenten aufgenommen wurde, obgleich das Bundesministerium des Innern und für Heimat bereits im Oktober 2022 die entsprechende Allgemeinverfügung für den TK-Sektor widerrufen hatte. Diese Ungewissheiten erschweren eine kohärente Umsetzung und schaffen Verwirrung in der Branche.

Zusätzlich könnten wesentliche Änderungen in der Anlage 2 des Sicherheitskataloges (z. B. der Liste der kritischen Funktionen) einen Mehraufwand und ggf. eine Entschleunigung von Innovationen bedeuten. Daher ist es wichtig, mögliche Änderungen am §§165 ff. TKG bei Veröffentlichung genau zu beobachten und zu überprüfen, um potenzielle Auswirkungen auf die Telekommunikationsunternehmen und die Branche insgesamt zu verstehen und angemessen darauf reagieren zu können.

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 | Referent Sicherheitspolitik
T 030 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Sicherheitspolitik