VATM e. V. ■ Reinhardtstr. 31 • 10117 Berlin

Herrn
MinR Dr. Daniel Meltzian
Bundesministerium des Innern
Leiter Referat CI 1
Grundsatz; Cyber- und Informationssicherheit

Ansprechpartner	E-Mail	Telefon	Datum
Gerrit Wernke	gw@vatm.de	030 / 814 760 80	03.07.202504.07.2025

VATM-Stellungnahme zum Referentenentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG

Der **Verband der Anbieter im Digital- und Telekommunikationsmarkt e. V. (VATM)** bedankt sich für die Gelegenheit einer Stellungnahme zum neuen Referentenentwurf des **Bundesministeriums des Innern** für ein **Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung** (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG).

Der VATM begrüßt die Veröffentlichung des abermals aktualisierten Referentenentwurfs und bedankt sich für die bis dahin durchgeführte breite Debatte im Rahmen der stattgefundenen Verbändeanhörungen – wohlgleich durch die kurzfristigen Änderungen zum Ende der letzten Legislaturperiode, damit einhergehende Diskussionen und einer Neuwahl weitere Verzögerungen hinzugekommen sind. Die Möglichkeit einer weiteren Verbändebeteiligung ist positiv zu bewerten, zumal bis dahin viele wichtige Punkte adressiert werden konnten. Es ist weiterhin positiv zu bewerten, dass im Laufe des Prozesses Verbesserungen eingegangen und umgesetzt wurden. Die Bundesregierung erkennt die Dringlichkeit dieses Vorhabens an. Eine Anhörung bereits vor der Sommerpause ist in Anbetracht der bereits verstrichenen Zeit sehr sinnvoll. Und dennoch: Es liegt ein gewisser Umsetzungsdruck mit noch vorliegenden Herausforderungen vor, denen nicht nur die Bundesregierung, sondern auch alle betroffenen Unternehmen in Deutschland gerecht werden müssen.

Die wichtige EU-weite Harmonisierung in der Cybersicherheit – die wir seitens des VATM bei verschiedenen Anhörungen im BMI nochmals betont haben – wird dadurch weiterhin erschwert, dass andere Mitgliedstaaten teils deutlich weiter in der Umsetzung sind und dementsprechend andere Fristen gelten. Die Anwendung für grenzüberschreitend tätige Unternehmen wird dadurch unnötig komplexer gemacht. Durch die Verzögerung besteht weiterhin eine Rechtsunsicherheit für Unternehmen. Bei größeren Unternehmen besteht zusätzlich eine erhebliche Verunsicherung bei möglichen Sicherheitsvorfällen vor Ablauf von Übergangs- und Nachweisfristen. Hier ist seitens des Gesetzgebers trotz des vergangenen Bemühens eines stringenten Zeitplans noch Klarheit zu schaffen.

Der neue Zeitplan selbst verdeutlicht, dass im Prozess eine enge Abstimmung im Sinne eines kohärenten und konsistenten Vorgehens mit dem KRITIS-DachG eigentlich weiter bestehen müsste, aber nun ein Stück aus dem Blick gelassen wurde. Nicht zuletzt wird dies auch in der NIS-2-Richtlinie (EU) 2022/2555 im Artikel 7 vorgegeben („*eine verstärkte Koordinierung zwischen den [...] zuständigen Behörden […] zum Zweck des Informationsaustauschs über Risiken, Bedrohungen und Sicherheitsvorfälle*“).

Es bleibt weiterhin dabei, dass mit dem NIS2UmsuCG und dem KRITIS-DachG eine einheitliche Regelung geschaffen werden muss, die physische Sicherheit und Cybersicherheit gemeinsam betrachtet. In der Praxis der VATM-Mitgliedsunternehmen sind diese eng miteinander verzahnt. Eine konkrete Benennung seitens des Gesetzgebers wäre sehr zu begrüßen. Durch den Regierungswechsel bestand ein Stück weit die Hoffnung, dass der Zeitverzug zwischen dem NIS2UmsuCG und dem KRITIS-DachG aufgehoben werden könnte und eine erkennbare Abstimmung mit der geplanten Umsetzung der CER-Richtlinie (ehemals KRITIS-Dachgesetz) stattfindet. Die physische Sicherheit kritischer Infrastrukturen – ein Bereich, der eng mit der digitalen Sicherheit verzahnt ist – ist hier konkret betroffen. Ohne eine abgestimmte Regelung besteht die Gefahr paralleler, nicht aufeinander abgestimmter Anforderungen an Unternehmen, die sowohl von NIS2 als auch von der CER-Richtlinie erfasst werden könnten. Eine klare Koordinierung vermeidet Doppelregulierung und Reibungsverluste.

Bei der Umsetzung der europäischen Vorgaben zur NIS 2 ist aus Sicht des VATM zusätzlich auf folgende Aspekte zu achten:

§ 1 – BSI-Kritisverordnung

In § 1 der BSI-Kritisverordnung wurden die Begriffsbestimmungen für „Betreiber“ und „kritische Dienstleistung“ ersatzlos gestrichen. Beide Begriffe sind allerdings an Dutzenden weiterer Fundstellen in der Verordnung und ihren Anhängen zu finden.

§ 2 – Begriffsbestimmungen (zu „kritische Infrastrukturen“ und „DNS-Diensteanbieter“)

Grundsätzlich sollte gelten: Es soll eine einheitliche Gestaltung der Meldepflichten in allen EU-Mitgliedstaaten sichergestellt werden, sowohl hinsichtlich der zu meldenden Vorfälle als auch ihrer Auswirkungen. Dabei ist es von entscheidender Bedeutung, dass die Mitgliedstaaten eine gemeinsame Auslegungspraxis vereinbaren. Keine nationalen Begriffsbestimmungen, sondern ein gemeinsames Verständnis, welches die Bundesregierung im Rahmen der Umsetzung von Artikel 23 der NIS-2-Richtlinie (EU) 2022/2555 gemeinsam mit anderen Mitgliedstaaten erarbeiten sollte. Dies kann dazu beitragen, eine kohärente und einheitliche Umsetzung der Meldepflichten zu gewährleisten.

Der § 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 werden im Zusammenhang mit der Regelung des § 56 weitere Punkte weiter unten ausformuliert.

Der Begriff „kritische Infrastrukturen“ wird sowohl im BSIG-E als auch in §§ 79, 136, 137, 141 und 142 TKG durch den Begriff „kritische Anlagen“ ersetzt. Die Auswirkungen dieser

Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • E-Mail: vatm@vatm.de

Begriffsänderung sind unklar. Weiterhin besteht Klärungsbedarf, ob daraus eine Erweiterung oder Erleichterung des Scopes oder der Verpflichtungen resultiert.

In den Begriffsbestimmungen des § 2 wird als DNS-Diensteanbieter definiert, wer „öffentlich verfügbare rekursive“ beziehungsweise „autoritative Dienste zur Auflösung von Domain-Namen“ anbietet. Das ist der exakte Wortlaut der NIS-2-Richtlinie (Artikel 6 Nummer 20). Nur in der Gesetzesbegründung ist der Versuch einer Einschränkung enthalten, der aber wirkungslos bleibt: „Werden DNS-Dienste als untrennbarer Teil eines Internetzugangsdienstes angeboten, ist der entsprechende Anbieter in der Regel nicht als eigenständiger DNS-Diensteanbieter zu betrachten. Autoritative DNS-Server zur Nutzung durch Dritte sind insbesondere solche, die nicht durch den zugehörigen Domaininhaber selbst betrieben werden, sondern grundsätzlich einer Vielzahl von Domaininhabern offensteht.“ Wer immer durch diese Auslegung aus der Verpflichtung durch die NIS 2 herausgenommen werden soll, ist als Zugangsanbieter ohnehin erfasst.

§ 6 – Informationsaustausch

Der VATM begrüßt, dass das BSI künftig eine Online-Plattform zum Informationsaustausch mit wichtigen Einrichtungen und der Bundesverwaltung betreiben wird. Eine frühzeitige und transparente Veröffentlichung wäre in diesem Zusammenhang hilfreich, um sich rechtzeitig mit den Funktionen und Anforderungen vertraut machen zu können. Bereits jetzt stellen viele Mitgliedsunternehmen Rückfragen zur Umsetzung der Richtlinie. Ein offener Austausch mit der Wirtschaft kann dazu beitragen, die Plattform praxisnah auszugestalten.

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.

§ 28 – Anwendungsbereich

In § 28 Abs. 3 wird der Kreis der Unternehmen eingeschränkt, der immer dann von der Anwendung der Regulierung als wichtige oder besonders wichtige Einrichtung auszunehmen sei, wenn die Zumessung auf der Grundlage einer „vernachlässigbaren“ Geschäftstätigkeit erfolgte. Abgesehen davon, dass dies europarechtlich genauso zweifelhaft sein dürfte wie die vorherige Formulierung, die bei der size-cap-rule „auf die Geschäftstätigkeit abstellen“ wollte, bleibt sie wohl weitgehend wirkungslos. Unternehmen, die nur wegen einer Solarstromanlage auf dem Dach in den Anwendungsbereich zu fallen drohen, dürften ein seltener Ausnahmefall sein.

Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • E-Mail: vatm@vatm.de

Die Neuformulierung führt zu einer erheblichen Erweiterung des Anwendungsbereichs des Gesetzes. Während in den vorangegangenen Entwürfen die „der Einrichtungsart zuzuordnende Geschäftstätigkeit“ als Grundlage der Betroffenheitsprüfung diente, sollen nun sämtliche Geschäftstätigkeiten eines Unternehmens in den Blick genommen werden, außer sie können klar als vernachlässigbar eingestuft werden. Die Folge ist eine deutlich strengere Auslegung, die potenziell auch Unternehmen erfasst, die nur in geringem Umfang kritische Tätigkeiten ausüben. Problematisch ist dabei, dass bislang nicht definiert 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 wünschenswert.

§ 30 – Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen (Begriff „Cyberhygiene“)

Die Streichung des Begriffs „Cyberhygiene" in den Mindestsicherheitsanforderungen des § 30 Abs. 2 Nr. 7 ist mit einer vollständigen Umsetzung der Richtlinie unvereinbar. „Cyberhygiene” durch „Sensibilisierungsmaßnahmen“ ersetzen zu wollen ist ein Kategorienfehler. Die Richtlinie fordert in Erwägungsgrund 49 grundlegende Verfahren („Software- und Hardware-Updates, Passwortänderungen, die Verwaltung neuer Installationen, die Einschränkung von Zugriffskonten auf Administratorenebene und die Sicherung von Daten”) – die Sensibilisierungsmaßnahmen für die „Cyberhygiene” folgen in Erwägungsgrund 50. Das ist im aktuellen Gesetzesentwurf formal falsch umgesetzt. Die Streichung der „Cyberhygiene” ist auch nicht konsequent erfolgt: In den Änderungen des EnWG ist sie im neuen § 5c weiterhin vorhanden.

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

Die ursprüngliche Formulierung in § 38 Abs. 1, wonach die Geschäftsleitung „Risiko-managementmaßnahmen zu genehmigen“ hat, entsprach der Systematik der NIS-2-Richtlinie (EU) 2022/2555 und war inhaltlich dementsprechend nachvollziehbar. Die in der Zwischenzeit vorgenommene Änderung in „Risikomanagementmaßnahmen umzusetzen“ ist hingegen seitens des VATM kritisch zu bewerten. Eine solche Umsetzung erfordert spezifische Fachkenntnisse im Bereich der Informationssicherheit, über die die Geschäftsleitung in der Regel nicht verfügt. Sachlich betrachtet liegen diese Aufgaben bei den entsprechend qualifizierten Fachabteilungen innerhalb der Organisation. Es wäre daher konsequent und auch folgerichtig, zur ursprünglichen Formulierung zurückzukehren. Ergänzend sollte 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.

Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • E-Mail: vatm@vatm.de

§ 41 – Untersagung des Einsatzes kritischer Komponenten

Die Sicherheit unserer Netzinfrastruktur ist unbestritten ein hohes Gut, weshalb der VATM, das Vorhaben des Gesetzgebers kritische Infrastrukturen effektiv zu schützen, unterstützt. § 41 des NIS2UmsuCG legt weiterhin strenge Anforderungen an den Einsatz kritischer Komponenten fest. Wir befürworten außerdem, dass eine kluge Abwägung unter Federführung des BMI beim Einsatz der kritischen Komponenten berücksichtigt wird.

Ferner muss gewährleistet werden, dass die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Informationstechnik, und nach Anhörung der betroffenen Wirtschaftsverbände sowie von Vertretern der Wissenschaft, die kritischen Funktionen und Komponenten festlegt, um wirtschaftliche, technologische und gesellschaftliche Nachteile zu vermeiden.

§ 56 – Ermächtigung zum Erlass von Rechtsverordnung

Die ersatzlose Streichung der vorgesehenen Beteiligungsrechte für Wissenschaft, KRITIS-Betreiber und Wirtschaftsverbände bei der Definition von KRITIS-Dienstleistungen (§ 56 Abs.4) und Sicherheitsvorfällen (§ 56 Abs. 5) ist fachlich nicht nachvollziehbar.

Die Wirtschaftsverbände sollten bei der Entwicklung von Rechtsverordnungen, die die Wirtschaft selbst auch betreffen, weiterhin angehört werden. Die bisherige Praxis der Anhörung im Bereich des IT-Sicherheitsrechts sollte unbedingt fortgesetzt werden, um rechtliche Vorgaben praxistauglich zu gestalten. Die Streichung entsprechender Textstellen sollte in der Folge rückgängig gemacht werden. Die strukturierte Einbindung der Wirtschaft hätte für praxisnahe und akzeptierte Regelungen gesorgt.

Die Schwellenwerte für „Kritische Anlagen“ werden vor allem durch Rechtsverordnungen nach § 56 Abs. 4 BSIG-E festgelegt. Es ist kritisch zu sehen, dass diese im Gesetzgebungsverfahren für das NIS2UmsuCG bestimmt werden sollten, um Rechtssicherheit zu gewährleisten und die Umsetzung zu beschleunigen. Bereits bestehende sektorspezifische Schwellenwerte in der BSI-Kritisverordnung sollten beibehalten werden, wobei Einrichtungen unterhalb dieser Schwellenwerte als besonders wichtige Einrichtungen gewertet werden sollten.

Auffällig ist weiterhin trotz der vorgenommenen Anpassungen an die neuen Bezeichnungen der Ministerien das Fehlen des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS) in der Vertreterliste. Gerade bei ebenenübergreifenden Digitalisierungsfragen und aufgrund der Zuständigkeit für den TK-Netzausbau in Deutschland wäre dessen Einbindung für kohärente Entscheidungen essentiell. Neue Sicherheitsanforderungen an TK-Netzbetreiber oder TK-Infrastrukturen haben potenziell erhebliche Auswirkungen auf den Festnetz- und Mobilfunkausbau in Deutschland und sind daher in den Entscheidungsprozess innerhalb der Bundesregierung einzubringen, zu bewerten und im Falle widerstreitender Interessen in Einklang zu bringen. Daher ist das BMDS zwingend in der Aufzählung des § 56 Abs. 4 zu ergänzen.

Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • E-Mail: vatm@vatm.de

Zum Artikel 25: Änderung des Telekommunikationsgesetzes

Technische und organisatorische Schutzmaßnahmen in der Ergänzung des § 165 TKG.

Bezugnehmen auf die Neugestaltung des § 165 Abs. 2 mit der Ergänzung (2a) zur Ausweisung der Mindestanforderungen für Risikomanagementmaßnahmen im Bereich der Cybersicherheit ist es zwingend erforderlich und zu erwarten, dass ein Abgleich mit dem Sicherheitskatalog der BNetzA stattfindet. Hier sollte die BNetzA aufgrund der dort niedergelegten Anforderungen den Sicherheitskatalog überarbeiten. Im Zuge dessen gilt es, die folgenden Punkte noch einmal zu berücksichtigen:

- § 165 Abs. 2 Satz 3 (neu): In der Neufassung sind neue Abwägungskriterien für die Angemessenheit der technischen und organisatorischen Vorkehrungen und sonstigen Maßnahmen hinzugekommen. In der vorangegangenen Fassung war der Stand der Technik noch maßgeblich. Dabei ist eine Spezifikation des Ausmaßes der Risikoexposition, der Größe des Betreibers sowie der Eintrittswahrscheinlichkeit, der Schwere des Vorfalls sowie der gesellschaftspolitischen und wirtschaftlichen Auswirkungen zu erwarten.

- § 165 Abs. 2a: 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. Der „gefahrenübergreifende Ansatz“ war bislang nicht gesetzlich vorgeschrieben. Es sollte noch einmal hinterfragt werden, ob sich aus der Formulierung neue Verpflichtungen ergeben. Dem Implementing Regulations (Annex) der EU sind alle weiteren aufgenommenen Punkte zu entnehmen. Auch hier machen die Punkte einen Abgleich mit dem Sicherheitskatalog der BNetzA erforderlich. Somit ist auch hier zu erwarten, dass die BNetzA den Sicherheitskatalog überarbeiten wird.

- Darüber hinaus ist die Regelung des § 165 Abs. 2a Nr. 4 besonders hervorzuheben: In Bezug auf die Harmonisierung der Neuregelungen sollte ein Abgleich mit § 30 Abs. 2 Nr. 4 erfolgen und der Passus „zwischen den einzelnen Einrichtungen“ in Bezug auf die Lieferkette unter Verbleib der Regelung „zu unmittelbaren Anbietern oder Diensteanbietern“ gestrichen werden.

- § 165 Abs. 2 (2b): Die Geschäftsleitungen von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, sind verpflichtet, die von diesen Einrichtungen nach Absatz 2 zu ergreifenden Maßnahmen umzusetzen und ihre Umsetzung zu überwachen. Wir verweisen dabei auf die Ausführungen zu § 38 weiter oben. Wir möchten darauf hinweisen, dass auch hier zur ursprünglichen Formulierung „zu genehmigen“ zurückzukehren ist. Diese wird der Rolle der Geschäftsleitung als verantwortliche Instanz ohne operative Überforderung gerecht. Ergänzend sollte zwingend gesetzlich klargestellt werden, dass die Geschäftsleitung zur Erfüllung ihrer Pflichten geeignete Dritte beauftragen kann. Die Letztverantwortung verbleibt dabei weiterhin bei der Geschäftsleitung.

Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • E-Mail: vatm@vatm.de

Dem VATM gehören die größten deutschen Telekommunikationsunternehmen an, insgesamt rund 180 auch regional anbietende Netzbetreiber, Diensteanbieter, aber auch Zulieferunternehmen. Zudem steht der Verband für wichtige Investoren, die den Glasfaserausbau in Deutschland deutlich voranbringen werden. Die VATM-Mitgliedsunternehmen versorgen 80 Prozent aller Festnetzkunden und nahezu alle Mobilfunkkunden außerhalb der Telekom. Seit der Marktöffnung im Jahr 1998 haben die Wettbewerber im Festnetz- und Mobilfunkbereich Investitionen in Höhe von rund 127 Milliarden Euro vorgenommen. Sie investieren auch am stärksten in den zukunftssicheren Glasfaserausbau direkt bis in die Häuser. 86 Prozent der Haushalte, die gigabitfähige Anschlüsse nutzen, sind Kunden der Wettbewerber.

Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • E-Mail: vatm@vatm.de

Präsidium: Valentina Daiber (Präsidentin), Wolfram Rinner (Vizepräsident), Timm Degenhardt, Markus Hendrich, Michael Jungwirth, Michael Martin, Carina Panek, Karsten Rudloff, Rickmann v. Platen, Soeren Wendler • Geschäftsführer: Dr. Frederic Ufer