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

Ansprechpartner	E-Mail	Fax	Durchwahl	Datum
Gerrit Wernke	gw@vatm.de	030 / 50 56 15 39	030 / 505 615 38	29.05.2024

Der **Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V. (VATM)** bedankt sich für die Gelegenheit einer Stellungnahme zum Referentenentwurf des Bundesministeriums des Innern und für Heimat für ein **Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheits-managements in der Bundesverwaltung** (NIS-2-Umsetzungs- und Cybersicherheits-stärkungsgesetz – NIS2UmsuCG).

Der VATM begrüßt die Veröffentlichung des aktuellen Referentenentwurfs und die damit einhergehende Möglichkeit zum breiten Austausch im Rahmen der Verbändeanhörung. Es ist positiv zu bewerten, dass im Laufe des Prozesses Verbesserungen eingegangen und umgesetzt wurden. Hierzu gehört, dass das BSI den Betreibern Kritischer Anlagen eine Frist von mindestens drei Jahren gewährt, um die Erfüllung der Anforderungen nach § 30 Abs. 1 erstmals nachzuweisen. Weiterhin ist auch die ersatzlose Streichung der Kategorie „*Unternehmen im besonderen öffentlichen Interesse*“ zu begrüßen. Künftig werden so neben Kritischen Anlagen nur noch wichtige sowie besonders wichtige Einrichtungen berücksichtigt. Dies trägt zur Stärkung der europaweiten Harmonisierung der Cybersicherheitsregulierung bei und beendet den deutschen Sonderweg des IT-Sicherheitsgesetzes 2.0 – ganz im Sinne der EU-Richtlinie.

Unabhängig dieser Punkte muss zu Beginn kritisch angesprochen werden, dass durch die erhebliche Verzögerung in den vergangenen Monaten eine besonders schwierige Situation entstanden ist, in der die Umsetzungsfrist im Oktober 2024 gerissen wird. Die wichtige EU-weite Harmonisierung in der Cybersicherheit wird dadurch enorm erschwert, dass andere Mitgliedstaaten 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 entsteht eine Rechtsunsicherheit für Unternehmen. Bei größeren Unternehmen besteht weiterhin eine erhebliche Verunsicherung bei möglichen Sicherheitsvorfällen vor Ablauf von Übergangs- und Nachweisfristen. Hier ist seitens des Gesetzgebers Klarheit zu schaffen.

Im Prozess hat der VATM abermals betont, dass die Umsetzung der NIS-2-Richtlinie eng mit dem KRITIS-DachG abgestimmt sein muss, um ein kohärentes und konsistentes Vorgehen zu gewährleisten. 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 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. Trotz diverser Verbesserungen zeigt die aktuell fehlende Konsultation der Gesetzentwürfe uneinheitliche Definitionen und Begrifflichkeiten, die Auslegungsprobleme verursachen könnten. Ein Beispiel liegt dabei in den Zuständigkeiten vom BSI im NIS2UmsuCG auf der einen und dem BBK im KRITIS DachG auf der anderen Seite, die durchaus konfliktbehaftet sind. Auf dieser Grundlage kann die EU-weite Harmonisierung der

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • Fax: 030 50561539 • E-Mail: vatm@vatm.de

Präsidium: David Zimmer (Präsident), Valentina Daiber (Vizepräsidentin), Michael Jungwirth, Wolfram Rinner, Karsten Rudloff, Dr. Marc Schütze, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Dr. Frederic Ufer

Cybersicherheit nicht wie angedacht erfüllt werden. Die Forderung bleibt, dass das NIS2UmsuCG und das KRITIS-DachG im Sinne des All-Gefahren-Ansatzes stärker aufeinander abgestimmt werden muss. Dies ist zusammen mit der zügigen Umsetzung beider Gesetzesvorhaben von großer Bedeutung für die Unternehmen in Deutschland.

Bei der Umsetzung der europäischen Vorgaben ist dabei aus Sicht des VATM ganz allgemein auf folgende Aspekte besonderer Wert zu legen:

- Die europaweit einheitliche Umsetzung der NIS-2-Richtlinie ist von wesentlicher Bedeutung und sollte das Hauptziel auf EU-Ebene und in den Mitgliedstaaten sein.
- Dazu gehört insbesondere die Kohärenz der Sicherheitsmaßnahmen und der Meldepflichten. Dies wird die Komplexität insbesondere für multinationale Unternehmen verringern und einen Flickenteppich aus abweichenden oder sogar widersprüchlichen nationalen Anforderungen vermeiden.
- Die Cybersicherheitsverpflichtungen müssen gestrafft werden, um sich überschneidende und/oder widersprüchliche Verpflichtungen und unnötige Belastungen oder Kosten zu vermeiden. Dies kann nur erreicht werden, wenn bei der Umsetzung die Komplexität und das Zusammenspiel der Richtlinie mit anderen Regelwerken (z. B. DORA & CRE) berücksichtigt wird. Gleiches gilt mit Blick auf Cybersicherheitsbestimmungen im nationalen Fachrecht (bspw. im TKG).
- Die Telekommunikationsanbieter unterliegen seit 2013 der Sicherheits- und Ausfallsicherheitsregulierung und verfügen daher bereits über umfangreiche Sicherheitsstrategien und solide Erfahrungen bei der Umsetzung der NIS-Anforderungen angesichts der EECC-NIS-Anforderungen. Dazu gehört auch eine effiziente Arbeitsbeziehung mit den nationalen Regulierungsbehörden, die beibehalten werden sollte.
- Vor diesem Hintergrund sollte bei der nationalen Implementierung darauf geachtet werden, dass bestehende Sicherheitspraktiken dieser Unternehmen nicht geändert werden müssen, um die NIS2-Vorgaben zu erfüllen. Aufgrund des gleichen, bereits bestehenden Sicherheitsniveaus erscheint deshalb eine Ausnahme der Unternehmen sinnvoll, um damit keine zusätzlichen bürokratischen Hürden ohne gleichzeitige Steigerung des Schutzniveaus aufzubauen.
- Die Bundesregierung sollte davon absehen, die Verwendung bestimmter Technologien vorzuschreiben. Dies bedeutet, dass die Unternehmen die Technologie gemäß internationaler Normen wählen können, die besser zu ihren Geschäftsmodellen und Systemen passt. Das gewährleistet, dass die Vorschriften nicht veraltet sind, wenn sich die Technologie ändert und verbessert.
- Angesichts des dynamischen Charakters der Entwicklungen im Bereich der Cybersicherheit müssen Standards und Zertifizierungen durch von der Industrie geleitete, globale Normungsgremien wie 3GPP entwickelt werden. Nach dem EU-Cybersicherheitsgesetz (EU Cybersecurity Act) sollten solche Systeme nur freiwillig sein. Mit NIS2 soll dies außer Kraft gesetzt werden, indem die Regelungen verbindlich werden. Die Verwendung bestimmter Technologien soll erst dann vorgeschrieben werden, wenn sie sich für die Wirtschaftsakteure (unabhängig von ihrer Größe) als

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • Fax: 030 50561539 • E-Mail: vatm@vatm.de

Präsidium: David Zimmer (Präsident), Valentina Daiber (Vizepräsidentin), Michael Jungwirth, Wolfram Rinner, Karsten Rudloff, Dr. Marc Schütze, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Dr. Frederic Ufer

betrieblich und wirtschaftlich tragfähig erwiesen haben. Die nationale Umsetzung in der Bundesrepublik sollte dies aufgreifen.

- Die Verwendung des Kriteriums der "Hauptniederlassung"[1] sollte der Standard für Unternehmen mit komplexen Geschäftsmodellen und grenzüberschreitender Präsenz sein. Es sollte vermieden werden, dass Tochtergesellschaften einer europaweiten Gruppe unter die getrennte und gleichzeitige Zuständigkeit ihrer jeweiligen Mitgliedstaaten fallen. Der aktuelle Gesetzentwurf sieht genau dies aber vor.
- Geschäftsmodelle können komplex sein, und es kann kein einheitliches Konzept für die Managementstrukturen geben. Das NIS2UmsuCG sollte den betroffenen Unternehmen die Möglichkeit geben, zu entscheiden, wo die Verantwortung und Haftung für das "Management" liegt, auch wenn dies außerhalb der EU sein sollte.
- In Erwägungsgrund 124 der NIS2-Richtlinie wird dargelegt, dass die Mitgliedstaaten ihre Prioritäten für die Überwachung anhand verschiedener Kriterien oder Maßstäbe festlegen können. Wir plädieren nachdrücklich dafür, dass große Unternehmens-kunden eine starke Verhandlungsposition haben und die Sicherheitsrisiken für ihr Geschäft und die Dienste, auf die sie angewiesen sind, besser verstehen. Dies äußert sich in starken vertraglichen Verpflichtungen einschließlich SLAs, Audit-Rechten und Dokumentationsanforderungen. Somit haben Unternehmen, die Dienst-leistungen für diese Unternehmenskunden erbringen, bereits einen zusätzlichen Anreiz, strenge Sicherheitspraktiken zu gewährleisten. Die Bundesregierung sollte dies bei der Umsetzung klar zum Ausdruck bringen und noch stärker als im bisherigen Entwurf entsprechende Ausnahmen formulieren.
- Artikel 37 der Richtlinie ermöglicht es den zuständigen Behörden, zusammen-zuarbeiten und auf Ersuchen eines anderen Mitgliedstaat Aufsichts- oder Durch-setzungsmaßnahmen zu verlangen. Um Doppelarbeit und einen erhöhten Aufwand für grenzüberschreitend tätige Unternehmen zu vermeiden, sollten solche Maßnahmen nur dann verlangt werden, wenn ein klarer Bedarf besteht und die Informationen nicht im Rahmen der bestehenden Aufsichtstätigkeit der zuständigen Behörde eingeholt werden können. Der Gesetzentwurf zum NIS2UmsuCG sollte diesen Aspekt aufgreifen und deutlich herausstellen.

[1] Einrichtung, die über operative und verwaltungstechnische Fähigkeiten zur Umsetzung von Cybersicherheitsmaßnahmen verfügt

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • Fax: 030 50561539 • E-Mail: vatm@vatm.de

Präsidium: David Zimmer (Präsident), Valentina Daiber (Vizepräsidentin), Michael Jungwirth, Wolfram Rinner, Karsten Rudloff, Dr. Marc Schütze, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Dr. Frederic Ufer

Weiterhin merken wir zu den folgenden konkreten Punkten an:

§ 2 Begriffsbestimmungen (insb. zu den Berichts- und Meldepflichten)

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 Mitgliedstaaten ein gemeinsames Verständnis erarbeiten. Dadurch würde eine kohärente und einheitliche Umsetzung der Meldepflichten gewährleistet. Es ist besonders wichtig, dass für eine einheitliche Ausgestaltung der Meldepflichten in den EU-Mitgliedstaaten, sowohl hinsichtlich der zu meldenden Vorfälle als auch ihrer Auswirkungen, die Mitgliedstaaten eine gemeinsame Auslegungspraxis vereinbaren. Unternehmen benötigen zudem Klarheit, welche Meldewege im Falle von Sicherheitsvorfällen bei Tochtergesellschaften mit Sitz im EU-Ausland eingehalten werden müssen.

Der Gesetzentwurf sollte weiterhin deutlich machen, dass Telekommunikationsanbieter, die nur Geschäftskunden bedienen, nicht verpflichtet sind, die Öffentlichkeit über Bedrohungen oder Cybervorfälle zu informieren, da sie keine direkten Beziehungen zu Verbrauchern haben. Meldepflichten gehen aktuell insofern am tatsächlichen Bedarf vorbei und erzeugen stattdessen weitere bürokratische Hürden.

Um zu vermeiden, dass die zuständigen Behörden mit Meldungen überschwemmt werden, sollten die Schwellenwerte für die Meldung von Vorfällen auf ein angemessenes Niveau festgelegt werden. Dabei ist bspw. die Verwendung von absoluten Schwellenwerten (z. B. 1 Million betroffene Nutzer) anstelle von qualitativen Kriterien zu empfehlen. Letztere sind schwieriger in automatisierte Meldesysteme einzubauen und führen zu einer übermäßigen Meldung unbedeutender Vorfälle.

Der VATM begrüßt, dass das Bundesinnenministerium nun „im Benehmen“ mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz durch Rechtsverordnung bestimmen kann, wann ein Sicherheitsvorfall als erheblich im Sinne von Absatz 1 Nummer 10 anzusehen ist.

Auf der anderen Seite besteht aus Sicht des VATM aktuell die Gefahr einer Überregulierung für Rechenzentrumsbetreiber, die sich durch die weitreichende Einbeziehung aller benötigten Anlagen und Infrastrukturen, insbesondere der für die Stromverteilung im § 2 Abs. 1 Nr. 34 ergibt. Diese Regelung geht weit über die Anforderungen der EU hinaus und führt zu unnötigen Belastungen. Wir sprechen uns hier für einen angemessenen Ausgleich zwischen Sicherheitsanforderungen und wirtschaftlicher Tragfähigkeit aus, um die Effizienz und insbesondere auch Wettbewerbsfähigkeit der betroffenen Unternehmen nicht zu gefährden.

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • Fax: 030 50561539 • E-Mail: vatm@vatm.de

Präsidium: David Zimmer (Präsident), Valentina Daiber (Vizepräsidentin), Michael Jungwirth, Wolfram Rinner, Karsten Rudloff, Dr. Marc Schütze, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Dr. Frederic Ufer

§ 6 Informationsaustausch

Mit der Online-Plattform des Bundesamtes für Sicherheit in der Informationstechnik zum Informationsaustausch mit anderen wichtigen Einrichtungen und der Bundesverwaltung wird ein auch aus unserer Sicht wichtiges Tool betrieben. Wichtig dabei muss es sein, dass das Bundesinnenministerium gemeinsam mit dem BSI vorab eine Testversion des Information Sharing Portals vorlegt, um es gemeinsam mit der Wirtschaft weiterzuentwickeln. Nur so können effiziente Lageinformationen bereitgestellt werden. Aus unserer Sicht ist es darüber hinaus dringend geboten, dass das BSI zukünftig mehr verwertbare Informationen über Cyberbedrohungen mit der Wirtschaft teilt, um auf diese Weise einen Beitrag zu einem verbesserten Lagebild zu leisten.

Kritisch wird gesehen, dass die Vorgabe der Teilnahmebedingungen auf der Online-Plattform nach § 6 Abs. 2 durch das BSI zu erhöhten operativen Aufwänden führen wird. Darüber hinaus würde analog zur Forderung einer bestmöglichen Harmonisierung mit dem KRITIS DachG eine Vereinheitlichung der Plattform zur Umsetzung von Informationspflichten aus anderen Gesetzesvorhaben zu einer lösungsorientierten Nutzung beitragen. Es ist somit wichtig, dass neben dem digitalen Austausch von Informationen der Umsetzungsplan KRITIS (UP KRITIS) fortgesetzt wird, um die vertrauensvolle Zusammenarbeit zwischen den Beteiligten zu gewährleisten.

§ 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen (Anwendung des § 30 BSIG für Telekommunikationsunternehmen)

Auch im neuen Referentenentwurf des NIS2-Umsetzungsgesetz werden die Pflichten des § 30 BSIG den Telekommunikationsunternehmen weiterhin auferlegt. Da viele der in § 30 BSIG vorhandenen Pflichten bereits durch das Telekommunikationsgesetz (TKG), insbesondere durch die Anforderungen des Sicherheitskonzeptes nach §§ 165 ff. TKG, abgedeckt sind, würden in Ansehung des TKG redundante Anforderungen mit möglicherweise unterschiedlichen Zuständigkeiten geschaffen.

1. Redundanz und Doppelaufwand

Die Einführung des § 30 BSIG für Telekommunikationsunternehmen führt zu einer doppelten Regulierung, da die Anforderungen durch die BNetzA (§ 167 TKG) größtenteils bereits im TKG festgelegt und verankert sind. Die zusätzlichen Berichtspflichten verursachen somit unnötigen bürokratischen Doppelaufwand und erhöhen die Kosten für die betroffenen Unternehmen. Eine Harmonisierung der Anforderungen ausschließlich innerhalb des TKG würde diese Redundanz vermeiden und die Effizienz in Bezug auf Umsetzung der Sicherheitsmaßnahmen erhöhen.

Auch müssen Doppelzuständigkeiten vermieden werden. Derzeit ist die Bundesnetzagentur (BNetzA) für die Überwachung der Sicherheitsanforderungen im Telekommunikationssektor nach §§ 165 ff. TKG zuständig; diese hat sich nach den Vorgaben des TKG ohnehin mit dem

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • Fax: 030 50561539 • E-Mail: vatm@vatm.de

Präsidium: David Zimmer (Präsident), Valentina Daiber (Vizepräsidentin), Michael Jungwirth, Wolfram Rinner, Karsten Rudloff, Dr. Marc Schütze, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Dr. Frederic Ufer

BSI über die Anforderungen abzustimmen, welche an das Sicherheitskonzept des TKG zu stellen sind. Mit der Einführung des § 30 BSIG könnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) nun als faktisch zweite Aufsichtsbehörde hinzutreten. Dies würde zu einer Verkomplizierung der Aufsichtsstruktur führen und könnte zudem zu widersprüchlichen Anforderungen und Verzögerungen bei der Durchsetzung führen. Eine einheitliche Aufsicht durch die BNetzA ist daher schon aus Sicht der Effizienz der Sicherheitsmaßnahmen geboten.

Die bestehenden Sicherheitsanforderungen nach §§ 165 ff. TKG sind bereits umfassend und berücksichtigen den aktuellen Stand der Technik. Sie decken die notwendigen technischen und organisatorischen Maßnahmen ab, um die Sicherheit der Telekommunikationsnetze zu gewährleisten. Sollten dennoch spezifische Anforderungen als notwendig erachtet werden, die im Katalog des § 30 BSIG aufgeführt sind, können diese durch eine Erweiterung des Anforderungskatalogs nach § 167 TKG integriert werden. Dies würde sicherstellen, dass alle Anforderungen konsistent und innerhalb eines kohärenten regulatorischen Rahmens bleiben.

2. Streichung der Anwendung des § 30 BSIG

Die Anwendung des Anforderungskatalogs in § 30 BSIG für Telekommunikationsunternehmen führt in diesem Bereich zu einer unnötigen Doppelregulierung mit der Gefahr von Ineffizienzen und einem erhöhten Ressourcen- und Kostenaufwand.

Es wird vorgeschlagen, die Anwendung des § 30 BSIG über § 28 Abs. 4 BSIG für Telekommunikationsunternehmen zu streichen, um sicherzustellen, dass Telekommunikationsunternehmen weiterhin nur den Anforderungen des TKG unterliegen. Sollte ein Delta zwischen den Anforderungen des BSIG und den Vorgaben der §§ 165 ff. TKG bestehen, sollte dies durch eine Erweiterung des Anforderungskatalogs nach § 167 TKG gelöst werden. Dies ermöglicht eine gezielte und bedarfsgerechte Anpassung der Sicherheitsanforderungen, ohne die Aufsichtsstrukturen zu verkomplizieren. Eine einheitliche Regulierung durch das TKG, ergänzt durch einen erweiterten Anforderungskatalog nach § 167 TKG, gewährleistet eine effiziente und konsistente Sicherheitsüberwachung innerhalb der bereits bestehenden Strukturen.

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

Die aktuelle Formulierung in § 38 NIS2UmsCG zeigt eine über den europäischen Rechts-rahmen hinausgehende Anforderung auf. Dabei hat der europäische Gesetzgeber die sogenannte „Managerhaftung“ in der NIS-2-Richtlinie in Art. 20 Abs. 1 allgemein sowie in Art. 32 Abs. 6 (besonders wichtige Einrichtungen) klar definiert. Diese differenzierte Definition fehlt aktuell in § 38 und sollte aus Sicht des VATM in das nationale Umsetzungsgesetz aufgenommen werden.

Es bleibt unklar, in welchem Umfang die Delegation von Verantwortlichkeiten auf Unternehmensangehörige im Zuge der Einhaltung der Risikomanagement-Vorgaben zur IT-

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • Fax: 030 50561539 • E-Mail: vatm@vatm.de

Präsidium: David Zimmer (Präsident), Valentina Daiber (Vizepräsidentin), Michael Jungwirth, Wolfram Rinner, Karsten Rudloff, Dr. Marc Schütze, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Dr. Frederic Ufer

Sicherheit noch möglich ist. Dies gilt insbesondere auch aus der Sicht einer Konzernstruktur. Es muss klargestellt werden, wie die Umsetzung von Cybersicherheitsmaßnahmen durch Dritte weiterhin möglich ist. Hier ist Rechtsklarheit vonnöten.

Da die NIS-2-Richtlinie keine entsprechenden Regelungen hinsichtlich eines Verzichts oder Vergleichs vorsieht, sollte darüber hinaus Absatz 2 gestrichen werden. Es sollte nach dem Maßstab allgemeiner Grundsätze bestimmt werden, inwiefern bspw. die jeweiligen Aufsichtsgremien der Einrichtung zur Durchsetzung eines Anspruchs verpflichtet sind.

§ 41 Untersagung des Einsatzes kritischer Komponenten

Mit dem IT-Sicherheitsgesetz 2.0 wurde bereits umfangreich über die Erarbeitung einer rechtssicheren und hinreichend genauen Definition kritischer Funktionen diskutiert, um kritische Komponenten klar identifizieren zu können. Auch weiterhin ist es notwendig, dass eine Liste mit klar formulierten kritischen Komponenten und eindeutig definierten technischen Vorgaben vorliegt. Denn im Sinne des Gesetzes können Komponenten mit kritischen Funktionen nur dann kritisch sein, wenn ihre Funktionalitäten in Bezug auf die Einsatzumgebung im Falle ihrer Beeinträchtigung den KRITIS-Schutzzielen zuwiderlaufen. Spezifikationen erfolgen sektorspezifisch im Rahmen einer Rechtsverordnung unter Beteiligung der betroffenen KRITIS-Sektoren und Betreiber kritischer Anlagen.

Die Gefährdungslage einer Funktion wird wesentlich vom aktuellen Stand der Technik beeinflusst und ist somit nicht statisch. Die Erstbewertung und Re-Evaluierung kritischer Komponenten und Funktionen muss daher einem Wirkmechanismus folgen, der Planungs- und Investitionssicherheit von Unternehmen sowie die Einhaltung gesetzlicher Fristen ermöglicht.

§ 55 Konformitätsbewertung und Konformitätserklärung

Bzgl. des Konformitätsbewertung und -erklärung stellt sich die dringende Frage mit Verweis auf die Ziele, die mit der Neueinführung des § 55 zur Konformitätserklärung verfolgt werden. Es gilt zu klären, ob diese Regelung dem Cyber Resilience Act (CRA) vorgreifen soll. Aus Sicht des VATM muss im Sinne einer klaren und kohärenten Gesetzgebung in der Cybersicherheit eine sorgfältige Prüfung erfolgen, um potenzielle Missverständnisse zu vermeiden. Zusätzlich gilt es zu betonen, dass der zusätzlich eingeführte Konformitätsnachweis neue bürokratische Hürden schaffen könnte.

Sollte sich bei der Prüfung der genannten Punkte herausstellen, dass § 55 den europäischen Sicherheitsbemühungen entgegenwirkt, plädieren wir für eine Streichung dieser Regelung. Das Ziel der EU-weiten Harmonisierung gemäß der NIS-2-Richtlinie (EU) 2022/2555 sollte nicht gefährdet werden.

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • Fax: 030 50561539 • E-Mail: vatm@vatm.de

Präsidium: David Zimmer (Präsident), Valentina Daiber (Vizepräsidentin), Michael Jungwirth, Wolfram Rinner, Karsten Rudloff, Dr. Marc Schütze, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Dr. Frederic Ufer

§ 65 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

Hier gilt es ebenfalls kritisch zu prüfen, inwiefern die nach § 65 geschaffenen Untersagungsbefugnisse des BSI gegenüber der Geschäftsführung, des Vorstandes und rechtlichen Vertretern der Unternehmen rechtlich umsetzbar sind.

Weiterhin zu den Änderungen des Telekommunikationsgesetzes:

Mit Bezug auf die Anlage 2 des Sicherheitskataloges ist es wichtig, mögliche Änderungen am §§165 ff. TKG bei Veröffentlichung genau zu beobachten und zu überprüfen. Dadurch können potenzielle Auswirkungen auf die Telekommunikationsunternehmen und die Branche besser verstanden und angemessen darauf reagiert werden.

Wesentliche Änderungen in der Anlage 2 des Sicherheitskataloges (z. B. der Liste der kritischen Funktionen) würden einen Mehraufwand und ggf. eine Entschleunigung von Innovationen bedeuten. Dies sollte der Gesetzgeber im Blick behalten.

Dem VATM gehören die größten deutschen Wettbewerbsunternehmen im Telekommunikationsmarkt an, aber auch regional anbietende Netzbetreiber, TK-Diensteanbieter sowie zahlreiche innovative Technologie- und Serviceanbieter. Als führender deutscher Telekommunikationsverband steht er für die mit Abstand meisten Kundenbeziehungen im Markt. Seine 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 89 Mrd. Euro vorgenommen. Sie investieren auch mit großem Abstand am stärksten in den zukunftssicheren Glasfaserausbau direkt bis in die Häuser.

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • Fax: 030 50561539 • E-Mail: vatm@vatm.de

Präsidium: David Zimmer (Präsident), Valentina Daiber (Vizepräsidentin), Michael Jungwirth, Wolfram Rinner, Karsten Rudloff, Dr. Marc Schütze, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Dr. Frederic Ufer