United Internet AG

Elgendorfer Straße 57
56410 Montabaur
Deutschland
Tel. +49 2602 96-1100
Fax +49 2602 96-1011
info@united-internet.de
www.united-internet.de

Vorstand:
Ralph Dommermuth
(Vorsitzender)
Ralf Hartings
Markus Huhn

Vorsitzender
des Aufsichtsrats:
Philipp von Bismarck

Commerzbank AG,
Frankfurt am Main
IBAN:
DE71 5004 0000 0574 6227 00
BIC:
COBADEFFXXX

HRB Montabaur 5762
USt-ID Nr. DE 149 340 676

Oktober 2023

STELLUNGNAHME ZUM REFERENTENENTWURF[1] FÜR EIN NIS-2-UMSETZUNGS- UND CYBERSICHERHEITSSTÄRKUNGS-GESETZ (NIS2UmsuCG)

VORBEMERKUNGEN

Die United Internet AG begrüßt das mit dem Gesetzentwurf verbundene Ziel, die Cyberresilienz der Wirtschaft und Bundesverwaltung weiter zu stärken. Ein hohes Maß an Cybersicherheit ist eine wesentliche Voraussetzung, um sowohl die Funktionsfähigkeit gesellschaftlicher Kernbereiche als auch die Leistungsfähigkeit des Wirtschaftsstandorts sowie die Handlungsfähigkeit staatlicher Einrichtungen zu gewährleisten.

Die zur Erreichung dieses Ziels vorgesehenen Maßnahmen sollten so ausgestaltet werden, dass sie von den betroffenen Unternehmen realistischerweise und mit einem vertretbaren Aufwand in der Praxis umgesetzt werden können. Zudem müssen die Maßnahmen wirkungsvoll sein. Der Gesetzgeber sollte dabei auch berücksichtigen, dass es sich bei den vom NIS2UmsuCG erfassten Sektoren in der Regel um bereits hochgradig regulierte Wirtschaftsbereiche handelt, in denen die Unternehmen seit vielen Jahren umfassende und risikoadäquate Cybersicherheitsmaßnahmen auf dem Stand der Technik umsetzen. Von zentraler Bedeutung sind aus Unternehmenssicht darüber hinaus rechts- und planungssichere Vorgaben sowie ein hohes Maß an Kohärenz bzw. Widerspruchsfreiheit mit den Anforderungen des geplanten KRITIS-Dachgesetzes (KRITIS-DG).

Da diese Punkte im vorliegenden Referentenentwurf nicht ausreichend berücksichtigt werden, sind aus unserer Sicht Anpassungen am Gesetzentwurf erforderlich.

---

[1] Diese Stellungnahme bezieht sich auf den Ref-E mit Bearbeitungsstand 03.07.2023. Wir behalten uns vor, im Laufe des Gesetzgebungsverfahrens weitere Stellungnahmen abzugeben.

KERNPUNKTE

- Der Gesetzentwurf sieht vor, dass zahlreiche Regelungsinhalte in einer Rechtsverordnung konkretisiert oder überhaupt erst festgelegt werden sollen. Um Planungs- und Rechtssicherheit zu gewährleisten, sollten alle wesentlichen Aspekte unmittelbar im NIS2UmsCG geregelt und Rechtsverordnungen zur Konkretisierung einzelner Bestimmungen unmittelbar nach Inkrafttreten des Gesetzes verabschiedet werden.
- Unternehmen des Sektors „Informationstechnik und Telekommunikation“ benötigen zudem Rechtssicherheit hinsichtlich der Frage, ob (und wenn ja in welchem Umfang) für sie durch das NIS2UmsCG auch Anforderungen an die physiche Sicherheit eingeführt werden.
- Um eine einfache Rechtsanwendung sicherzustellen, müssen Vorgaben zur physischen Sicherheit und zur Cybersicherheit passgenau zueinander gestaltet werden. Einheitliche Begriffsdefinitionen sowie überschneidungs- und widerspruchsfreie Vorgaben im NIS2UmsCG und KRITIS-DG sind dabei zentral.
- Für Unternehmen, die sowohl unter das NIS2UmsCG als auch das KRITIS-DG fallen, sind klare und überschneidungsfreie behördliche Zuständigkeiten von zentraler Bedeutung. Auch ist es sinnvoll, behördenseitig eine zentrale Anlausfstelle (SPOC) für Unternehmen einzurichten, um den Informationsfluss möglichst effizient zu gestalten.
- Die vorgesehenen Meldepflichten sollten rein digital erbracht werden können und sich auf Informationen beschränken, die zur Erfüllung des gesetzlichen Auftrags der involvierten Aufsichtsbehörden unbedingt erforderlich sind.
- Es ist dringend geboten, dass das BSI zukünftig mehr verwertbare Informationen über Cyberbedrohungen mit der Wirtschaft teilt, um auf diese Weise einen aktiven Beitrag zu einem verbesserten Lagebild auf Seiten der Unternehmen zu leisten.
- Unternehmen benötigen Klarheit, welche Meldewege im Falle von Sicherheitsvorfällen bei Tochtergesellschaften mit Sitz im EU-Ausland eingehalten werden müssen.
- Für erstmalig unter die Cybersicherheitsregulierung fallende Unternehmen sollte das NIS2UmsCG angemessene Umset-

zungsfristen vorsehen. Alle erfassten Unternehmen sollten zudem die Möglichkeit erhalten, die Einhaltung der Anforderungen über bestehende Zertifizierungsverfahren nachzuweisen.

- Faire Verteilung von Verantwortlichkeiten entlang der Lieferkette: Vom NIS2UmsCG erfasste Unternehmen dürfen nicht für Sicherheitsmaßnahmen entlang der Lieferkette in die Verantwortung genommen werden, die außerhalb ihres Einflussbereichs liegen.

IM EINZELNEN

Planungs- und Rechtssicherheit

Der Referentenentwurf für ein NIS2UmsCG sieht vor, dass zahlreiche Regelungsinhalte in einer Rechtsverordnung konkretisiert oder überhaupt erst festgelegt werden. Dazu zählen auch wesentliche Inhalte wie beispielsweise die Frage der Anwendbarkeit der in Teil 3 Kapitel 2 NIS2UmsCG-E aufgeführten Pflichten (u.a. umzusetzende Risikomanagementmaßnahmen sowie Melde- und Nachweispflichten). Dieser Punkt soll nach § 28 Abs. 1 NIS2UmsCG-E erst in einer Rechtsverordnung abschließend festgelegt werden.

Im Sinne des Wesentlichkeitsgebots sollten entsprechende Aspekte jedoch unmittelbar im NIS2UmsCG-E geregelt werden. Dies würde zu einer deutlich verbesserten Planungssicherheit für Unternehmen führen. In Fällen, in denen die Konkretisierung einzelner Bestimmungen sinnvollerweise auf dem Verordnungsweg erfolgen sollte, muss der Gesetzgeber sicherstellen, dass die entsprechenden Verordnungen sehr zeitnah nach Inkrafttreten des NIS2UmsCG verabschiedet werden. Auch dies stellt eine wesentliche Voraussetzung dar, um für Unternehmen Planungs- und Rechtssicherheit zu gewährleisten.

Unternehmen des Sektors „Informationstechnik und Telekommunikation“, die nicht vollumfänglich vom Geltungsbereich des KRITIS-Dachgesetzes erfasst sein sollen (vgl. § 10 Abs. 3, § 11 Abs. 14 und § 12 Abs. 9 KRITIS-DG-E[2]), benötigen außerdem Rechtssicherheit hinisichtlich der Frage, ob für sie über das NIS2UmsCG Anforderungen an die physiche Sicherheit eingeführt werden. Aus der Gesetzesbegründung zu § 28 NIS2UmsCG-E (S. 108) resultiert jedoch eine Rechtsunsicherheit, da laut den dortigen Ausführungen erst in der

[2] KRITIS-DG-E mit Bearbeitungsstand 17.07.2023

Rechtsverordnung zum NIS2UmsCG bestimmt werden soll, ob auch Regelungen zur physischen Sicherheit eingeführt werden.

Aus Gründen der Rechts- und Planungssicherheit ist es zudem wichtig, dass bei behördlichen Prüfvorgängen nach dem NIS2UmsCG, bspw. im Kontext des § 41 BSIG-neu (bisheriger §9b BSIG), Klarheit in Bezug auf Fristen, Stichtage u.ä. besteht. Auch sollte der im Zuge der NIS2-Umsetzung angepasste nationale Rechtsrahmen eine Genehmigung als Rechtsfolge vorsehen. Die alleinige Untersagungsmöglichkeit im bisherigen §9b BSIG führt in der Praxis dazu, dass sich die Inbetriebnahme von unproblematischen Komponenten bis zum Fristablauf unnötig in der Schwebe befindet. Dies kann zu Verzögerungen beim Netzausbau führen.

Kohärenz mit dem KRITIS-Dachgesetz

Auch unabhängig von der konkreten Frage, ob im Zuge der Umsetzung des NIS2UmsCG Anforderungen an die physische Sicherheit für Unternehmen des Sektors „Informationstechnik und Telekommunikation“ eingeführt werden, müssen Vorgaben zur physischen Sicherheit und zur Cybersicherheit passgenau zueinander gestaltet werden. Dies ist eine wesentliche Voraussetzung, um eine einfache und praktikable Rechtsanwendung für alle Unternehmen sicherzustellen. Einheitliche Begriffsdefinitionen sowie überschneidungs- und widerspruchsfreie Vorgaben im NIS2UmsCG und KRITIS-DG sind dabei zentral.

Behördliche Zuständigkeiten

Im Zuge der laufenden Ausgestaltung des gesetzlichen Rahmens für die Cybersicherheit (NIS2UmsCG) und die physische Sicherheit (KRITIS-DG) Kritischer Infrastrukturen sind darüber hinaus eindeutige und überschneidungsfreie Regelungen in Bezug auf die behördlichen Zuständigkeiten erforderlich. Diese Regelungen müssen berücksichtigen, dass KRITIS-Unternehmen auch nach den für sie geltenden spezialgesetzlichen Regelungen (z.B. dem TKG) einer aufsichtsbehördlichen Kontrolle (z.B. durch die BNetzA) unterliegen. In diesem Zusammenhang ist es sinnvoll, für Unternehmen einen Single-Point-of-Contact (SPOC) unter den Behörden einzurichten, damit Informationen bzw. Meldungen ‚in‘ und ‚aus‘ den Unternehmen ohne Zeitverlust und möglichst wirksam und zielgerichtet verarbeitet werden können.

Meldeverfahren

Die im NIS2UmsCG verpflichtend vorgeschriebenen Vorfallsmeldungen sollten rein digital erfolgen können. Zur Vermeidung unverhältnismäßiger bürokratischer Aufwände sollten sich die Meldungen auf Informationen beschränken, die zur Erfüllung des gesetzlichen Auftrags der involvierten Aufsichtsbehörden unbedingt erforderlich sind. Die vom NIS2UmsCG erfassten Unternehmen sind auf entsprechende Entlastungen dringend angewiesen, zumal der Referentenentwurf in § 31 für zukünftige Sicherheitsvorfälle ein mehrstufiges Meldesystem vorsieht.

- Nach unserer Überzeugung dürfen Berichts- und Meldewege darüber hinaus keine „Einbahnstraße“ darstellen: So ist es dringend geboten, dass das BSI zukünftig mehr Informationen über Cyberbedrohungen und Cybersicherheitsvorfälle mit der Wirtschaft teilt, um auf diese Weise einen aktiven Beitrag zu einem verbesserten Lagebild auf Seiten der vom NIS2UmsCG erfassten Unternehmen leistet. Dies ist nicht zuletzt vor dem Hintergrund der veränderten geopolitischen Rahmenbedingungen sowie den von staatlichen Akteuren ausgehenden Bedrohungen von zentraler Bedeutung.

Unternehmen benötigen außerdem Klarheit, welche Meldewege im Falle von Sicherheitsvorfällen bei Tochtergesellschaften mit Sitz im EU-Ausland eingehalten werden müssen. Der Referentenentwurf enthält dazu keine expliziten Ausagen, sodass an diesem Punkt noch Konkretisierungsbedarf besteht.

Umsetzungsfristen und Nachweise

Durch die Vorgaben der europäischen NIS2-Richtlinie werden zukünftig signifikant mehr Unternehmen als bisher von der KRITIS-Regulierung erfasst sein. Für erstmalig erfasste Unternehmen sollte das NIS2UmsCG daher angemessene bzw. in der Praxis realistischerweise zu bewältigende Umsetzungsfristen vorsehen.

Alle erfassten Unternehmen sollten zudem die Möglichkeit erhalten, die Einhaltung der Anforderungen des NIS2UmsCG über bestehende Zertifizierungsverfahren nachzuweisen. Wir begrüßen es ausdrücklich, dass in § 30 Abs. 2 NIS2UmsCG-E in Bezug auf die Umsetzung der verpflichtend vorgegebenen Risikomanagementmaßnahmen zumindest auf „einschlägige europäische und internationale Normen“ verwiesen wird. Das Gesetz sollte jedoch auch explizit die Möglichkeit vorsehen, dass die Umsetzung von Risikomanagementmaßnahmen

durch etablierte Zertifizierungen (etwa nach ISO 27001 oder BSI-Grundschutz) rechtssicher nachgewiesen werden kann.

Sicherheit der Lieferkette

Die verpflichtend vorgeschriebenen Risikomanagementmaßnahmen nach § 30 NIS2UmsCG-E müssen explizit auch die „Sicherheit der Lieferkette“ mitberücksichtigen. In diesem Zusammenhang bedarf es einer fairen Verteilung von Verantwortlichkeiten entlang der Lieferkette: Insbesondere dürfen nach § 30 NIS2UmsCG-E verpflichtete Unternehmen nicht für Sicherheitsaspekte entlang der Lieferkette in die Verantwortung genommen werden, die außerhalb ihres Einflussbereichs liegen. Die in § 30 Abs. 8 NIS2UmsCG-E genannten Aspekte, beispielsweise die „Gesamtqualität der Produkte und der Cybersicherheitspraxis“ von Lieferkettenakteuren, liegen jedoch nicht vollumfänglich in der Verantwortungs- und Einflusssphäre der verpflichteten Unternehmen. Die Bestimmungen in § 30 Abs. 8 NIS2UmsCG-E enthalten zudem verschiedene unbestimmte Rechtsbegriffe (etwa die im vorangegangenen Satz zitierten Begriffe „Gesamtqualität“ und „Cybersicherheitspraxis“), wodurch die Einhaltung der Bestimmungen zusätzlich erschwert wird. Darüber hinaus müssen die Regelungen zur Sicherheit der Lieferkette Fallkonstellationen mitberücksichtigen, in denen externe Dienstleister für Unternehmen operative Cybersicherheitsmaßnahmen durchführen.

ÜBER UNITED INTERNET

Die United Internet AG ist mit über 27 Mio. kostenpflichtigen Kundenverträgen und rund 40 Mio. werbefinanzierten Free-Accounts ein führender europäischer Internet-Spezialist. Kern von United Internet ist eine leistungsfähige „Internet-Fabrik“ mit 10.500 Mitarbeitenden, ca. 3.700 davon in Produkt-Management, Entwicklung und Rechenzentren. Neben einer hohen Vertriebskraft über etablierte Marken wie 1&1, GMX, WEB.DE, IONOS, STRATO und 1&1 Versatel steht United Internet für herausragende Operational Excellence bei weltweit über 67 Mio. Kunden-Accounts.

ANSPRECHPARTNER

Manuela-Andrea Pohl, Head of Public Affairs
mpohl@united-internet.de | 030 200093 8820
Otto-Ostrowski-Straße 7, 10249 Berlin

Oliver Klein, Senior Public Affairs Manager
oklein@united-internet.de | 030 200093 8825
Otto-Ostrowski-Straße 7, 10249 Berlin

Lobbyregister R001932
EU-Transparenzregister: Nr. 31650149406-33