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

September 2024

STELLUNGNAHME ZUM REGIERUNGSENTWURF FÜR EIN NIS-2-UMSETZUNGS- UND CYBERSICHERHEITSSTÄRKUNGS-GESETZ (NIS2UmsuCG)

VORBEMERKUNGEN

Ein hohes Maß an Cybersicherheit ist eine zentrale Voraussetzung für die erfolgreiche Digitalisierung von Staat, Wirtschaft und Gesellschaft. Die United Internet AG begrüßt daher ausdrücklich das mit dem NIS2UmsuCG verbundene Ziel einer Stärkung der Cyberresilienz Deutschlands.

Um den vom NIS2UmsuCG erfassten Unternehmen Planungssicherheit zu bieten, sollte das Gesetz in den kommenden Monaten zügig verabschiedet werden. Die darin enthaltenen Anforderungen sollten so ausgestaltet werden, dass diese von den Unternehmen realistischerweise und mit einem vertretbaren Aufwand umgesetzt werden können. Der Gesetzgeber sollte dabei auch berücksichtigen, dass es sich bei vielen vom NIS2UmsuCG erfassten Sektoren um bereits hochgradig regulierte Wirtschaftsbereiche handelt, in denen die Unternehmen seit vielen Jahren umfassende und risikoadäquate Cybersicherheitsmaßnahmen auf dem Stand der Technik umsetzen. Von besonderer Bedeutung ist für Unternehmen zudem ein hohes Maß an Rechtssicherheit, etwa durch eindeutige Begriffsdefinitionen sowie klar definierte Verantwortlichkeiten im NIS2UmsuCG.

Um dies sicherzustellen, sind aus unserer Sicht Anpassungen an dem im Juli 2024 vorgelegten Regierungsentwurf notwendig.

KERNPUNKTE

- Das NIS2UmsuCG sollte den erfassten Unternehmen die Möglichkeit einräumen, die Einhaltung der im Gesetz vorgesehenen Risikomanagementmaßnahmen über bestehende bzw. etablierte Zertifizierungsverfahren nachzuweisen.
- Da vom NIS2UmsuCG weitreichende Auswirkungen auf sektorspezifische Regelungsregime (u.a. im Telekommunikationsbereich) ausgehen, müssen entsprechende Wechselwirkungen unbedingt mitberücksichtigt werden.
- Gesetzliche Vorgaben zur physischen Sicherheit und zur Cybersicherheit müssen passgenau zueinander gestaltet werden. Einheitliche Begriffsdefinitionen sowie überschneidungs- und widerspruchsfreie Vorgaben im NIS2UmsuCG und KRITIS-DG sind dabei zentral. Gleiches gilt in Bezug auf behördliche Zuständigkeiten.
- Die im NIS2UmsuCG 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.
- Faire Verteilung von Verantwortlichkeiten entlang der Lieferkette: Vom NIS2UmsuCG erfasste Unternehmen dürfen nicht für Sicherheitsmaßnahmen entlang der Lieferkette in die Verantwortung genommen werden, die außerhalb ihres Einflussbereichs liegen
- Wichtige Legaldefinitionen wie „Cloud-Computing-Dienst“ und „Rechenzentrumsdienst“ müssen im NIS2UmsuCG nachgeschärft und klarer voneinander abgegrenzt werden, um eine rechtssichere Auslegung zu ermöglichen.

.

IM EINZELNEN

(1) Nachweise

Alle vom NIS2UmsuCG erfassten Unternehmen sollten die Möglichkeit erhalten, die Einhaltung der Anforderungen des Gesetzes über bestehende bzw. etablierte Zertifizierungsverfahren nachzuweisen. Wir begrüßen es ausdrücklich, dass im Regierungsentwurf in § 30 Abs. 2 BSIG-neu in Bezug auf die Umsetzung der verpflichtend vorgegebenen Risikomanagementmaßnahmen auf „einschlägige europäische und internationale Normen“ verwiesen wird. Zudem sieht § 39 BSIG-neu vor, dass Betreiber kritischer Anlagen die Umsetzung wesentlicher Vorgaben durch „Sicherheitsaudits, Prüfungen oder Zertifizierungen“ nachweisen können.

Das Gesetz sollte jedoch auch für alle anderen erfassten Unternehmen explizit die Möglichkeit vorsehen, dass die Umsetzung von Risikomanagementmaßnahmen durch etablierte Zertifizierungen (etwa nach ISO 27001 oder BSI-Grundschutz) rechtssicher nachgewiesen werden kann.

(2) Auswirkungen auf sektorspezifische Regelungsregime

Als Artikelgesetz sieht das NIS2UmsuCG (zum Teil weitreichende) Änderungen in zahlreichen Fachgesetzen wie etwa dem Telekommunikationsgesetz (TKG) vor. Diese Wechselwirkungen müssen im Gesetzgebungsprozess unbedingt berücksichtigt werden. So ist es beispielsweise für Unternehmen des Telekommunikationssektors von zentraler Bedeutung, dass eine Doppelregulierung mit dem TKG vermieden wird.

In diesem Zusammenhang ist ausdrücklich zu begrüßen, dass der TK-Sektor im Regierungsentwurf durch die Bestimmungen in § 28 Abs. 4 BSIG-neu grundsätzlich von wesentlichen Regelungsinhalten des BSIG ausgenommen wird und diese Regelungsinhalte durch Art. 26 NIS2UmsuCG ins sachnähere TKG überführt werden. Problematisch ist jedoch folgende, im gleichen Absatz enthaltene Einschränkung: „Satz 1 gilt nicht für die dort aufgeführten besonders wichtigen und wichtigen Einrichtungen, soweit sie über die in Satz 1 Nummer 1 und 2 genannten Anlagen hinaus weitere kritische Anlagen nach § 2 Nummer 22 betreiben oder aufgrund weiterer Tätigkeiten einer der in Anlage 1 oder 2 bestimmten Einrichtungsarten zuzuordnen sind.“

Diese Einschränkung würde in der Praxis dazu führen, dass TK-Unternehmen, die weitere Dienste im NIS2-Geltungsbereich anbieten, de facto einer Doppelregulierung durch das TKG und BSIG unterliegen würden.

Die aus dem NIS2UmsuCG resultierenden Änderungen auf gesetzlicher Ebene bedingen in den betroffenen Branchen darüber hinaus häufig auch Anpassungen untergesetzlicher Regelwerke. Diese Anpassungen müssen zeitnah und unter Beteiligung aller betroffenen Kreise erfolgen. Hier sehen wir insbesondere die sektorspezifischen Aufsichtsbehörden (etwa die BNetzA) in der Verantwortung, rechtzeitig alle Stakeholder zu konsultieren und diese eng in die Anpassung entsprechender Regelwerke mit einzubeziehen.

(3) Kohärenz mit dem geplanten KRITIS-Dachgesetz

Gesetzliche Vorgaben zur physischen Sicherheit und zur Cybersicherheit müssen 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 in beiden Regelungsbereichen sind hierfür zentral.

Im Zuge der laufenden Ausgestaltung des gesetzlichen Rahmens für die Cybersicherheit (NIS2UmsuCG) und die physische Sicherheit Kritischer Infrastrukturen (KRITIS-DG) sind zudem 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.

(4) Meldeverfahren und bi-direktioner Informationsaustausch

Nach § 32 Abs. 4 BSIG-neu soll das BSI dazu ermächtigt werden, „die Einzelheiten zur Ausgestaltung des Meldeverfahrens und zur Konkretisierung der Meldungsinhalte" festzulegen. Das Meldeverfahren sollte dabei in der Praxis so ausgestaltet werden, dass Vorfalls-

meldungen rein digital erfolgen können. Zur Vermeidung unverhältnismäßiger bürokratischer Aufwände sollten sich die Meldungen zudem auf Informationen beschränken, die zur Erfüllung des gesetzlichen Auftrags der involvierten Aufsichtsbehörden unbedingt erforderlich sind.

Nach unserer Überzeugung dürfen Berichts- und Meldewege zudem keine „Einbahnstraße“ darstellen. Wir begrüßen daher ausdrücklich die in § 6 BSIG-neu vorgesehene Online-Plattform des BSI zum Informationsaustausch mit wichtigen Einrichtungen, besonders wichtigen Einrichtungen und Einrichtungen der Bundesverwaltung. In der Umsetzungspraxis wird es darauf ankommen, dass über diese Plattform tatsächlich ein bi-direktionaler Informationsaustausch zustande kommt. Denn aus unserer Sicht ist es 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. Dies ist nicht zuletzt vor dem Hintergrund der veränderten geopolitischen Rahmenbedingungen sowie den von staatlichen Akteuren ausgehenden Bedrohungen von zentraler Bedeutung.

Der Regierungsentwurf sieht in Art. 26 Nummer 5 ferner vor, die in § 168 Abs. 1 TKG enthaltene doppelte Meldepflicht von Vorfällen (Meldung sowohl gegenüber dem BSI als auch der BNetzA) fortzuschreiben. Wir plädieren für eine Abschaffung der doppelten Meldepflicht, da diese in der Praxis zu unverhältnismäßigen administrativen Mehraufwänden führt. Im Sinne eines Single Point of Contact-Prinzips sollten Telekommunikationsunternehmen ihren Meldepflichten durch eine zentrale Meldung an die BNetzA nachkommen können.

(5) Klar definierte und faire Verantwortlichkeiten

Vom NIS2UmsuCG erfasste Unternehmen sind auf eindeutige und in der Praxis umsetzbare Vorgaben in Bezug auf das Risikomanagement angewiesen. Die Risikomanagementmaßnahmen nach § 30 Abs. 2 BSIG-neu umfassen explizit auch die „Sicherheit der Lieferkette“. In der Praxis muss hierbei unbedingt eine faire Verteilung von Verantwortlichkeiten entlang von Lieferketten sichergestellt werden. Insbesondere dürfen Unternehmen nicht für Sicherheitsaspekte entlang der Lieferkette in die Verantwortung genommen werden, die außerhalb ihres jeweiligen Einflussbereichs liegen. In der Gesetzesbegründung zu § 30 Abs. 2 wird zudem darauf verwiesen, dass Einrich-

tungen bei der Umsetzung von Maßnahmen zur Sicherheit der Lieferkette auch Aspekte wie die „Gesamtqualität der Produkte“ oder die „Cybersicherheitspraxis“ ihrer Anbieter und Diensteanbieter berücksichtigen müssen. Hierbei handelt es sich um unbestimmte Rechtsbegriffe, die die Umsetzung der Vorgaben zur Sicherheit der Lieferkette zusätzlich erschweren.

Art. 26 Nummer 3 NIS2UmsuCG-E sieht vor, die Risikomanagementmaßnahmen des § 30 BSIG-neu ins TKG (durch Anpassung des § 165 TKG) aufzunehmen. Mit Blick auf die vorgesehenen Anforderungen zur Lieferkettensicherheit sollte auch an dieser Stelle sichergestellt werden, dass es zu einer fairen Verteilung von Verantwortlichkeiten entlang der Lieferkette kommt und dass unbestimmte Rechtsbegriffe möglichst konkretisiert werden.

Unklar ist aus unserer Sicht zudem grundsätzlich, wie die geplanten Regelungen zur Lieferkettensicherheit Fallkonstellationen mitberücksichtigen, in denen externe Dienstleister für vom NIS2UmsuCG erfasste Unternehmen operative Cybersicherheitsmaßnahmen durchführen.

(6) Eindeutige Begriffsdefinitionen

Die im Regierungsentwurf in § 2 BSIG-neu legaldefinierten Begriffe „Cloud-Computing-Dienst“ und „Rechenzentrumsdienst“ bedürfen aus unserer Sicht nach wie vor einer klareren Abgrenzung, etwa mit Blick auf die Einordnung von Infrastructure-as-a-Service-Diensten, um Rechtsunsicherheiten auf Seiten der Unternehmen zu vermeiden.

ÜBER UNITED INTERNET

Die United Internet AG ist mit über 28 Mio. kostenpflichtigen Kundenverträgen und über 39 Mio. werbefinanzierten Free-Accounts ein führender europäischer Internet-Spezialist. Kern von United Internet ist eine leistungsfähige „Internet-Fabrik“ mit 11.000 Mitarbeitenden. 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.

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