Bundesverband

ASW-Positionspapier

Stellungnahme des dritten Referenten-entwurfs NIS2

Zum Diskussionspapier für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland

Stand: 28. Mai 2024

Bundesverband

Vorwort

Das Internet ist der Tatort des 21. Jahrhunderts.

Innerhalb der letzten fünf Jahre haben wir eine rasante Zunahme von Cyberkriminalität erlebt. Die Akteure sind dabei längst nicht mehr nur Hackergruppierungen, sondern mittlerweile auch staatlich gesteuerte Angreifer wie z.B. Nachrichtendienste. Die aktuelle Weltlage verschärft die Lage massiv und zeigt auf, wie wichtig eine gemeinsame, zielführende Strategie für den Cyber-Schutz ist.

Der dritte Referentenentwurf ist aus unserer Sicht ein wichtiger Schritt zur Stärkung des Cybersicherheitsniveaus für den Wirtschaftsstandort Deutschland. Insbesondere die Möglichkeit, sich bei der Verbandsanhörung in den konstruktiven Austausch zu begeben, begrüßen wir sehr.

Positive Anmerkungen:

1. Nachweispflichten

Unternehmen, die in den Anwendungsbereich des NIS2UmsuCG fallen, erhalten mehr Freiraum für die Umsetzung, da Nachweispflichten frühestens drei Jahre nach Inkrafttreten des Gesetzes eingefordert werden können. Die Übergangszeit nimmt so Druck von den Unternehmen und verhindert „Schnellschüsse“ bei der Umsetzung und Implementierung. Es bleibt zudem genügend Zeit für einen fachlichen Austausch zwischen den Unternehmen sowie die Umsetzung von Best-Practice Fällen.

Negative Anmerkungen:

1. Nicht vorhandene Vertrauenswürdigkeitsüberprüfung von Mitarbeitenden

Das NIS2UmsuCG fokussiert sich auf umfassende Risikomaßnahmen und eine Zulassung von IT-Hardware, erwähnt jedoch nicht die Zuverlässigkeitsüberprüfung von Mitarbeitenden geht. An dieser Stelle erlauben wir uns die Frage: Was bringt einem Unternehmen die allerbeste Technik und Absicherung, wenn Mitarbeitende absichtlich physische Sicherheitslücken schaffen?

Das Thema Pre-Employment Screening beschäftigt die Sicherheitsabteilungen von Unternehmen seit Jahren und ist häufig mit hohen Aufwänden sowie Kosten verbunden. Gleichzeitig hat sich das Verfahren jedoch als effektiv erwiesen, insbesondere bei der Vergabe von hohen leitenden Positionen, die immer häufiger mit einer entsprechenden Sicherheitsfreigabe verknüpft ist. Die Durchführung einer Zuverlässigkeitsüberprüfung bei der Vergabe von sicherheitskritischen Stellen sollte über ein einheitliches Verfahren erfolgen und insbesondere für KMUs eine Kostenübernahme beinhalten.

2. Informationsaustausch – Gemeinsame Plattform

Die Einrichtung einer gemeinsamen digitalen Plattform, um Sicherheitsvorfälle verschiedener Art zu dokumentieren, begrüßen wir sehr. Nur so können neue Angriffsmethoden, Schwachstellen in Systemen oder ähnliches frühzeitig identifiziert und entschärft werden. Zurzeit liegt die Entwicklung dieser Plattform beim BSI. Damit

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Bayerischer Platz 6 | 10779 Berlin
Telefon +49 (0)30 246 37 175 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

diese Plattform funktioniert und von Unternehmen proaktiv genutzt wird, ist es unerlässlich, die Wirtschaft und Verbände bei der Entwicklung und alle Entwicklungsstufen der Plattform miteinzubeziehen.

Erhalten die Nutzer unzureichendes Feedback nach einer Meldung, oder aber die Bedienung ist zu kompliziert bzw. nicht selbsterklärend, werden die Unternehmen und insbesondere KMUs die Plattform meiden. Eine Rückgewinnung der Nutzer ist dann mit erheblichem Mehraufwand verbunden und gestaltet sich schwierig.

3. Risikomanagement – Schulungen Cybersicherheit und Cyberhygiene

Bei der Beschreibung der Maßnahmen verweist das NIS2UmsuCG unter anderem darauf dass:

„Die Maßnahmen sollen den Stand der Technik einhalten und müssen mindestens die folgenden Themen umfassen: §30 (2)“ […]

- **Schulungen Cybersicherheit und Cyberhygiene**

Prinzipiell ist dieser Maßnahmenkatalog zu begrüßen jedoch finden wir, dass insbesondere die Punkte **Schulungen Cybersicherheit und Cyberhygiene** wesentlich ausführlicher definiert werden müssen. Dies beginnt mit einer klaren Abgrenzung der beiden Begriffe Cyberhygiene und Cybersicherheit, da es hier häufig zu thematischen Überschneidungen kommt. Wir halten den Ausdruck der Cybersicherheit bzw. Schulungen der Cybersicherheit als ausreichend.

Unabhängig von der Definition von Cybersicherheit sollten dezidierte Fragen geklärt werden was mit „Schulungen Cybersicherheit“ gemeint ist, u. a.:

- In welchem Turnus sollen die Schulungen stattfinden?
- Was gilt als Schulung? Reicht ein Infoblatt als PDF mit nützlichen Tipps oder eine Schulung bzw. E-Learning?
- Soll der Lernerfolg von Schulungen überprüft werden – falls ja, wie? Reicht ein einfaches Absolvieren der Lerninhalte?
- Wie werden die Nachweise über die Schulungen geführt? Wem sollen sie gemeldet werden?
- Welche Inhalte müssen in einer Schulung, die den Titel „Cybersicherheit“ trägt, vermittelt werden?
- Werden die zu vermittelnde Inhalte jährlich vom BSI aktualisiert?
- Wird eine Möglichkeit der Kostenkompensation gewährt? Sobald ein Dozent, eine Awareness-Kampagne oder ein E-Learning eingekauft werden, bewegen sich die Kosten rasch im vierstelligen Bereich.

Diese Fragen mögen für Konzerne unerheblich sein, da hier bereits Lernplattformen und eigene Abteilungen wie „Learning and Development“ vorhanden sind. KMUs verfügen jedoch in den seltensten Fällen über solche Abteilungen und Möglichkeiten.
Bei der Klärung dieser Fragen sollten ebenfalls Wirtschaft und Verbände mit einbezogen werden.

4. Sicherheit der Lieferkette

Artikel 16, 5c (3) 3.

„Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern.“

Zurzeit diskutieren viele Unternehmen darüber, ob sie unter NIS2UmsuCG fallen oder nicht – häufig kommen sie dabei zu dem Schluss, dass dies nicht der Fall ist. Dabei wird außer Acht gelassen, dass Unternehmen, die unter NIS2UmsuCG fallen, gewährleisten müssen, dass Ihre Lieferanten und Dienstleister einen hohen bzw. vergleichbaren Sicherheitsstandard vorweisen können. Dies wird dazu führen, dass zahlreiche Unternehmen bei Inkrafttreten von NIS2UmsuCG wesentlich höhere Sicherheitsstandards vorweisen müssen als sie derzeit können. Viele werden von den neuen Anforderungen unvorbereitet überrascht werden. Wir sehen in der Automobilbranche bereits eine ähnliche Situation: Unternehmen müssen TISAX zertifiziert sein um als Lieferant oder Dienstleister in diesem Sektor auftreten zu können.

Wir empfehlen daher einen transparenten sowie einheitlichen Sicherheitsstandard für die Zulieferer bzw. Dienstleister von Unternehmen, die unter NIS2UmsuCG fallen. Ähnlich wie es bereits nach dem TISAX Standard durchgeführt wird.

Artikel 1: § 29 Einrichtungen der Bundesverwaltung

Die Streichung der Verwaltungen der Länder und Kommunen aus NIS2UmsuCG erachten wir auf mehreren Ebenen als das falsche Signal.

Es ist ein zumindest fragwürdiges Zeichen an die Wirtschaft wenn Unternehmen, KMUs und auch Zulieferer die neuen Anforderungen umsetzen müssen, die öffentliche Hand jedoch nicht. Gerade hier sollte mit gutem Beispiel vorangegangen werden, da die Wirtschaft auf eine funktionierende Verwaltung angewiesen ist.

Die jüngsten Cyber-Attacken auf kommunale Einrichtungen haben gezeigt, dass die öffentliche Hand ein beliebtes Ziel darstellt und Ausfälle von kommunalen Verwaltungsdiensten erhebliche Auswirkungen haben. Ein Ausfall von kommunalen Dienstleistungen kann z.B. in sozialen Brennpunkten ein Mittel der Destabilisierung sein. Es ist daher unerlässlich, dass die öffentliche Hand ebenfalls hohe Sicherheitsstandards erfüllen muss.

Ein weiterer Punkt, der für Unverständnis innerhalb der Wirtschaft sorgt, ist die Exklusion von Leitern von Einrichtungen hinsichtlich der Haftbarkeit nach *„§38 (3) Leiter von Einrichtungen der Bundesverwaltung gelten nicht als Geschäftsleitung.“*

Während die Geschäftsleitung eines jeden Unternehmens, das unter NIS2UmsuCG fällt, zahlreiche Pflichten (Schulungen und dergleichen) erfüllen muss, gilt dies nicht mehr für die Geschäftsleitung von Einrichtungen der Bundesverwaltung.

Dadurch wird die Akzeptanz der NIS2UmsuCG in der Wirtschaft gefährdet, da schwer zu erklären ist, warum die Geschäftsleitung eines KMU alle Anforderungen und Haftbarkeiten erfüllen muss, die Geschäftsleitung von einer größeren Einrichtung der Bundesverwaltung jedoch nicht.

Schlusswort

Als Bundesverband der Allianz für Sicherheit in der Wirtschaft e.V. haben wir uns dem Wirtschaftsschutz verpflichtet und begrüßen die kommende NIS2UmsuCG. Die von uns angeführten Punkte stellen einen Ausschnitt der für uns relevanten Punkte dar. Wir stehen jederzeit für eine konstruktive Diskussion und Zusammenarbeit zur Verfügung.

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Bayerischer Platz 6 | 10779 Berlin
Telefon +49 (0)30 246 37 175 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

Die Allianz für Sicherheit in der Wirtschaft e.V. (ASW Bundesverband) vertritt die Sicherheitsinteressen der deutschen Wirtschaft auf Bundes- und EU-Ebene gegenüber der Politik, den Medien und den zentralen Sicherheitsbehörden. Der ASW Bundesverband arbeitet mit Unternehmen der freien Wirtschaft, Entscheidungsträgern der Sicherheitspolitik und -Behörden sowie unterschiedlichen Universitäten und Forschungseinrichtungen dauerhaft zusammen. Er wird getragen von den deutschen regionalen Sicherheitsverbänden sowie diversen fachspezifischen Bundesverbänden und Fördermitgliedern. Mehr zum ASW Bundesverband finden Sie unter: https://asw-bundesverband.de

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Bayerischer Platz 6 | 10779 Berlin
Telefon +49 (0)30 246 37 175 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de