Bundesverband

ASW-Positionspapier

Sicherheitsmeldungen müssen in Handlungsempfehlungen münden

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

Stand: 20. Oktober 2023

Der ASW Bundesverband begrüßt die Einbeziehung der Wirtschaft in den Prozess der Umsetzung der NIS-2-Richtlinie in Deutschland und möchte hiermit wichtige Anmerkungen zum vorliegenden Diskussionspapier und Umsetzungsprozess geben.

1. Unklarheit bezüglich des NIS-2-Umsetzungsgesetzes

Der vorliegende Referentenentwurf für die Umsetzung von NIS-2 enthält Regelungen zur persönlichen Haftung der Vorstände, die über die Anforderungen von NIS-2 hinausgehen. Es besteht jedoch Unklarheit darüber, ob dieser Entwurf das geplante NIS-2-Umsetzungsgesetz ersetzen soll. Wir benötigen Klarheit darüber, ob der aktuelle Gesetzgebungsprozess weiterhin gültig ist oder ob dieser Referentenentwurf als Ersatz vorgesehen ist.

2. Strategische Nutzung von Sicherheitsinformationen

Der Entwurf sieht vor, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) Informationen über Sicherheitsvorfälle sammelt. Der ASW Bundesverband schlägt vor, dass das BSI explizit den Auftrag erhält, diese Informationen auszuwerten und strategische Empfehlungen an die Wirtschaft und Politik abzuleiten. Ähnlich der OWASP Top 10 sollte eine Liste der wichtigsten Maßnahmen erstellt werden, die deutsche Unternehmen ergreifen sollten, um sich effektiv vor Cyberbedrohungen zu schützen.

Wir schlagen vor, dass das BSI den Auftrag erhält, Erkenntnisse über vergangene Sicherheitsvorfälle für eine konzertierte Vorfallerkennung als IOC (Indicators of Compromise) mit der deutschen Wirtschaft zu teilen und die Erfahrungen aus beispielhaften Vorfällen als anonymisierte Lessons Learned und Best Practices aufzubereiten. So könnte die gesamte deutsche Wirtschaft aus diesen Vorfällen lernen, auch wenn diese nicht bei ihnen selbst stattgefunden haben.

Das BSI erhält über die gemeldeten Sicherheitsvorfälle die Möglichkeit Angriffsvektoren, Grundursachen und die Bedingungen für die Wirksamkeit und Nicht-Wirksamkeit von Sicherheitsmaßnahmen zu untersuchen. Die Möglichkeit zur Auswertung und Nutzbarmachung dieser Informationen sollte dringend genutzt werden.

3. Klare Definitionen von erheblichen Sicherheitsvorfällen

Die im Referentenentwurf enthaltenen Definitionen von erheblichen Sicherheitsvorfällen sind zu vage und könnten zu praktischen Problemen führen. Wir empfehlen klarere und präzisere Definitionen, die sich an bewährten Praktiken in einigen Branchen orientieren.

Man könnte auf die Verordnung EU 2018/151 zurückgreifen, darin werden in Artikel 4 erhebliche Auswirkungen definiert. (Art. 4 Verordnung (EU) 2018/151 - Erhebliche Auswirkungen eines Sicherheitsvorfalls, https://lexparency.de/eu/32018R0151/ART_4/).

Alternativ könnte für die Definition auf die EBA/GL/2021/03 der European Banking Authority aufgebaut werden, die einem vergleichbaren Ziel dienen (Revised Guidelines on major incident reporting under PSD2). Dort werden ebenfalls Vorgaben zur Definition und Abgrenzung erheblicher Sicherheitsvorfälle gemacht, die über die allgemeinen Punkte des Referentenentwurfs hinaus gehen und sich in der Praxis bewährt haben.

4. Anpassung der Meldefristen

Die vorgeschlagenen Meldefristen von 24 Stunden sollten auf 72 Stunden verlängert werden, um eine bessere Abstimmung mit den Meldefristen der Datenschutz-Grundverordnung (DSGVO) zu erreichen.

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

5. Cybersecurity-Anforderungen

Die vorgeschlagenen Anforderungen an die Cybersecurity bei Behörden und Firmen, sollte noch einmal überarbeitet werden. Als Beispiel “Angriffserkennung” ist zu unkonkret und auch nicht von großem Nutzen, da eine Erkennung keine Verteidigung enthält. Besser wären architektonische Vorschläge wie IT-Notfallplanung, BCM oder auch ISMS (Information Security Management System) als Vorgaben zur Absicherung und Erkennung, mit Vorschlägen zur Verteidigung durch IT-Technologien als Basis.

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