Bundesverband

ASW-Positionspapier

Wichtige Stärkung der Wirtschaft & Behörden durch NIS-2

zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuDG)

Stand: 04. Juli 2025

Bundesverband

Das Wichtigste in Kürze

- Vereinheitlichung der verschiedenen Meldewege
- Strategische Nutzung von Informationen über Sicherheitsvorfälle für die gesamte Wirtschaft
- Hilfestellung durch Handreichungen für Lieferanten & Dienstleister in der Lieferkette
- Vertrauenswürdigkeitsüberprüfung von Mitarbeitern in besonderen Positionen
- Konkretisierung von Grundlegenden Schulungen & Sensibilisierungsmaßnahmen

Der ASW Bundesverband begrüßt den neuen Referentenentwurf für ein NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG). Dieser neue Entwurf weist eine erhebliche Qualitätssteigerung mit vielen positive Änderungen auf, welche die Sicherheit deutscher Unternehmen und Behörden wirksam stärken werden. Vor allem die Ernennung des BSI als zentrale Prüfstelle mit weiteren Prüfaufgaben, sowie die besondere Berücksichtigung der Behörden als Zielgruppe ist ein positives Signal.

Darüber hinaus finden sich jedoch Punkte, die noch nicht in ausreichender Form Berücksichtigung finden und daher eine Nachjustierung des Entwurfes erforderlich machen:

Verschiedene Meldepflichten

Die Verordnung DORA und die Richtlinie NIS-2 verfolgen unterschiedliche Zielrichtungen und gelten für jeweils klar definierte Bereiche mit eigenen Aufsichtsstrukturen. Unternehmen, die sowohl unter DORA als auch unter NIS-2 fallen, müssen derzeit jeweils separat melden. Die Pflichten bestehen nebeneinander und beruhen auf unterschiedlichen Rechtsgrundlagen.

Für viele Unternehmen wird die Vielzahl an Reportinganforderungen zunehmend zur Belastung, gerade im Zusammenspiel von Cyber-, Datenschutz- und KI-Regulierung. Es wäre wünschenswert, wenn eine Überprüfung zur Vereinheitlichung der Meldewege stattfindet.

Informationsaustausch (Plattform & strategische Nutzung von Informationen)

Die Einrichtung einer gemeinsamen digitalen Plattform, um Sicherheitsvorfälle verschiedener Art zu dokumentieren, begrüßen wir sehr. Wir begrüßen ebenfalls, dass das BSI weiteren Stellen die Teilnahme ermöglichen kann. Wir würden begrüßen, dass unter dem verwendeten Begriff „Stellen“ ebenfalls Spezialisten aus Unternehmen und nicht nur aus Behörden fallen. Dies ist durch die vage Formulierung nicht ersichtlich.

Der Entwurf sieht vor, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) Informationen über Sicherheitsvorfälle sammelt und diese ebenfalls auf der Plattform geteilt werden.

Wir schlagen drüber hinaus 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.

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

Sicherheit der Lieferkette

Unternehmen, die unter NIS2UmsuDG fallen, müssen gewährleisten, dass Ihre Lieferanten und Dienstleister einen hohen bzw. vergleichbaren Sicherheitsstandard vorweisen können. Dies wird dazu führen, dass zahlreiche Lieferanten und Dienstleister bei Inkrafttreten von NIS2UmsuDG wesentlich höhere Sicherheitsstandards vorweisen müssen als sie derzeit können. Viele werden von den neuen Anforderungen unvorbereitet überrascht werden.

Wir empfehlen daher, dass Unternehmen die Verpflichtung haben sollten, ihren Dienstleistern eine konkrete Handreichung zur Verfügung zu stellen, um diese bei der Einhaltung/Errichtung von Sicherheitsmaßnahmen zu unterstützen. Ansonsten sehen wir eine Benachteiligung kleinerer und mittlerer Lieferanten und Dienstleister in der Lieferkette.

Nicht vorhandene Vertrauenswürdigkeitsüberprüfung von Mitarbeitenden

Das NIS2UmsuDG fokussiert sich auf umfassende Risikomaßnahmen und eine Zulassung von IT-Hardware, erwähnt jedoch nicht die Zuverlässigkeitsüberprüfung von Mitarbeitenden.

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.

Grundlegende Schulungen & Sensibilisierungsmaßnahmen

Im Maßnahmenkatalog des Kapitels Risikomanagement [§30 (2)] stellt sich beim Punkt 7 die Frage, was unter „grundlegenden Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik“ zu verstehen ist. In welchem Turnus sollen die Schulungen stattfinden? Was gilt als Schulung? Reicht ein Infoblatt als PDF mit nützlichen Tipps oder ein E-Learning? Soll der Lernerfolg von Schulungen überprüft werden – falls ja, wie? Reicht ein einfaches Absolvieren der Lerninhalte? Usw.

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.

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