Bundesverband E-Commerce und
Versandhandel Deutschland e.V.
www.bevh.org

- Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh) -

Stellungnahme zum Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie

Berlin, den 03.07.2024

Ansprechpartnerinnen: Daniela Bleimaier, daniela.bleimaier@bevh.org
Elisa Rudolph, elisa.rudolph@bevh.org

Der **Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh)** repräsentiert als die Interessenvertretung der Branche der in Deutschland aktiven Online- und Versandhändler Unternehmen aller Größen und aller denkbaren Handelsformen (Online, Multichannel, Katalog, TV-Shopping, Plattformhändler und -betreiber). Die Mitglieder des bevh stehen für mehr als 80% des gesamten Branchenumsatzes. Darüber hinaus sind dem Verband mehr als 130 Dienstleister aus dem Umfeld der E-Commerce-Branche angeschlossen.

Wir bedanken uns für die Möglichkeit der Stellungnahme hinsichtlich der beabsichtigten Umsetzung der NIS-2-Richtlinie und möchten uns dazu wie folgt äußern.

Zunächst sei vorab darauf hingewiesen, dass eine stärkere Klarheit in den nationalen Regelungen den betroffenen Unternehmen nicht beim Verständnis, sondern auch bei der Umsetzung der Vorgaben helfen wird. Es wird daher nochmals appelliert, die bisherigen Vorgaben hinsichtlich Klarheit und Praktikabilität nachzuschärfen. Für die betroffenen Unternehmen ist es wichtig, dass diesen eine verständliche und klare Orientierungshilfe zur Verfügung gestellt wird, konkret dazu, welche Risikomanagementmaßnahmen sie ergreifen müssen und wann von einem „erheblichen Sicherheitsvorfall“, der die Meldepflichten gem. § 32 NIS2UmsuCG-E auslöst, auszugehen ist.

Zudem im Einzelnen:

1. Kongruenz mit dem KRITIS-DachG und den definierten Sektoren sowie der zuständigen Behörde (BBK)

Die Übereinstimmung mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (KRITIS-DachG) und den darin definierten Sektoren ist von entscheidender Bedeutung. Aktuell ist das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) die zuständige Behörde. Es ist essenziell, dass die Sektoren gemäß den Vorgaben des KRITIS-DachG klar definiert und ihre spezifischen Bedürfnisse

und Gefährdungen berücksichtigt werden. Dies stellt sicher, dass die Schutzmaßnahmen zielgerichtet und effektiv sind, um die Sicherheit und Resilienz der kritischen Infrastrukturen zu gewährleisten.

2. Zügige Novellierung der BSI-KRITIS-Verordnung

Aus der Sicht des bevh ist eine Novellierung der BSI-KRITIS-Verordnung unerlässlich. Die Verordnung sollte zügig aktualisiert werden, um die Sektoren mit entsprechenden Schwellwerten (basierend auf dem Versorgungsgrad) und spezifischen Anlagekategorien klar zu definieren. Eine präzise und aktuelle Verordnung ermöglicht es den Betreibern kritischer Infrastrukturen, die notwendigen Schutzmaßnahmen zielgerichtet umzusetzen und die gesetzlichen Anforderungen zu erfüllen.

3. Arbeitsfähigkeit des BSI

Das BSI spielt eine zentrale Rolle bei der Beratung, Unterstützung und Überwachung der Betreiber kritischer Infrastrukturen. Eine ausreichende personelle und finanzielle Ausstattung sowie der Zugang zu modernster Technologie sind notwendig, um den hohen Anforderungen und dynamischen Bedrohungslagen gerecht zu werden. Die Arbeitsfähigkeit des Bundesamts für Sicherheit in der Informationstechnik (BSI) muss deshalb gewährleistet und kontinuierlich verbessert werden.

4. Empfehlung zur Erweiterung von §31: Angriffserkennung und -prävention

Die Sicherstellung der Sicherheit und Resilienz kritischer Infrastrukturen erfordert eine konsequente und vorausschauende Herangehensweise, die sowohl auf der Erkennung als auch auf der Prävention von Angriffen basiert. Nur durch eine umfassende Strategie kann der Schutz kritischer Systeme und Dienste gewährleistet werden. Der derzeitige §31 spricht ausschließlich von Angriffserkennung. Wir empfehlen daher, die Angriffserkennung um die Angriffsprävention zu erweitern. Ein präventiver Ansatz, kombiniert mit der Angriffserkennung, ist von entscheidender Bedeutung. Wenn ausschließlich Angriffserkennungen (wie SIEM und DER/XDR) eingesetzt werden, ist bei der Erkennung oft bereits wertvolle Zeit verstrichen, was zu spät sein kann. Durch die Einbindung von Präventionsmaßnahmen, insbesondere die Anwendung von Continuous Threat Exposure Management (CTEM), kann eine kontinuierliche Risikoanalyse und frühzeitige Identifizierung potenzieller Bedrohungen ermöglicht werden. Dies verbessert die Sicherheitslage erheblich, da Risiken proaktiv minimiert und Angriffe bereits im Vorfeld verhindert werden können.

5. Konsolidierung von Meldeprozessen der verschiedenen Gesetze und Verordnungen

Es wird angeregt, dass eine übergeordnete bzw. eine einheitliche Stelle geschaffen wird, die alle Meldungen zu Sicherheitsvorfällen erfasst und verarbeitet. Zur Unterstützung und Erleichterung für betroffene Unternehmen sollte es lediglich eine Stelle geben, an die Sicherheitsvorfälle gemeldet werden sollen. Diese zentrale Stelle sollte ausreichend mit Ressourcen ausgestattet sein.

Durch eine zentrale Anlaufstelle wird es auch Cyberkriminellen schwerer gemacht, wieder und wieder mit den gleichen Angriffskampagnen erfolgreich zu sein.

Soweit die Meldungen von Sicherheitsvorfällen für alle Organisationen und Unternehmen auch einsehbar sind, kann dies dazu beitragen, dass die jeweilige Angriffswellen unterbrochen werden. Zudem werden Unternehmen dabei überstützt, sich effektiv vor bekannt gewordenen Angriffen oder bestimmten Angriffsmustern zu schützen. So können die begrenzten Ressourcen gezielter und risikoorientierter eingesetzt werden. Priorisierung ist dabei ein wirksames Mittel für einen effizienten Ressourcen Einsatz. Mit einem entsprechenden Informationssystem ließen sich final Risiken und auch Schäden frühzeitig gegensteuern.

Die zentrale Stelle sollte die Informationen zu Sicherheitsvorfällen, sog. IOC (Indicator of Compromise) in einer standardisierten, ggf. pseudonymisierten Form automatisiert abrufbar bereitstellen.

6. Begrenzung der Ausnahmen

Öffentliche Einrichtungen, insbesondere die der Bundesverwaltung dürfen keinesfalls pauschal vond er Verfplichtung zur Umsetzung der Vorgaben ausgenommen werden, da diese häufig Ziel von Cyberangriffen sind und gerade an dieser Stelle besser geschützt werden müssen.

Final sollte darüber hinaus auch berücksichtigt werden, dass die Anzahl an betroffenen Unternehmen weitaus größer ist, als die der eigentlich Verpflichteten. Insbesondere ist darauf hinzuweisen, dass durch die Aufnahme der Verpflichtung zur Sicherstellung einer sicheren Lieferkette auch Unternehmen, die zwar nicht selbst betroffen, aber mittelbar betroffen sind, eigene Kontrollen etablieren und die Vorgaben zumindest in großen Teilen auch umsetzen müssen. Hier bedarf es zusätzlicher Aufklärung und Unterstützung von Wirtschaftsunternehmen.