

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

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

Berlin, den 28.05.2024

Ansprechpartnerinnen: Daniela Bleimaier, [daniela.bleimaier@bevh.org](mailto:daniela.bleimaier@bevh.org)  
Elisa Rudolph, [elisa.rudolph@bevh.org](mailto: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.

## 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.