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 04.07.2025

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.

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.

Wir appellieren, dass das KRITIS-DachG in enger Abstimmung mit dem vorliegenden Verfahren erfolgt, um einen Gleichlauf der Vorgaben gewährleisten zu können. Dies ist unerläßlich um Rechtssicherheit für betroffene Unternehmen zu schaffen und keine Unsicherheiten zu erzeugen.

2. 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.

3. Empfehlung zur Erweiterung von § 31BSIG-E: 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 BSIG-E spricht ausschließlich von Angriffserkennung. Dies erscheint nicht ausreichend.

Wir empfehlen daher, die Angriffserkennung um die Angriffs**prävention** 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 im Einzelfall 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.

4. Klarstellung in § 28 Abs. 3 BSIG-E

Die Regelung sieht eine Ausnahme für solche Geschäftstätigkeiten vor, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung „vernachlässigbar“ sind. Diese Formulierung ist unklar und unbestimmt und führt daher zu Rechtsunsicherheiten. Auch unter Bezugnahme auf die entsprechende Gesetzesbegründung wird nicht klar, wann eine Geschäftstätigkeit vernachlässigbar ist. Soweit ersichtlich dürfte dies auch gegen die Vorgaben der EU-Richtlinie verstoßen. Das BMI wird um Klarstellung der gesetzlichen Regelung ersucht, um hier eine rechtlich saubere Handhabe für die betroffenen Unternehmen zu schaffen.

5. § 62 BSIG-E Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen

Die gewählte Formulierung führt zu Unklarheit. Nicht nachvollziehbar ist, welche Tatsachen erfasst sind und folglich dann auch, wann konkret das Bundesamt Überprüfungsmaßnahmen ergreifen kann. Mit Blick auf die Regelung der Richtlinie sollte das BSI klarstellen, in welchen Fällen das Bundesamt einschreiten kann.

6. Weitere Klarstellung

Der Begriff des „Rechenzentrumsdienstes“ ist nachzuschärfen, da dieser nach der Definition auch konzerninterne Gesellschaften betrifft, die nicht nach außen tätig werden. Eine Einbeziehung auch dieser in den Anwendungsbereich erscheint als nicht notwendig.