HDE Handelsverband Deutschland

Stellungnahme

Referentenentwurf des Bundesministeriums des Innern für ein Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG).

Stand: 4. Juli 2025

I. Einleitung

Der Handelsverband Deutschland (HDE) ist die Spitzenorganisation des deutschen Einzelhandels. Insgesamt erwirtschaften in Deutschland rund 280.000 Einzelhandelsunternehmen mit drei Millionen Beschäftigten an 400.000 Standorten einen Umsatz von rund 630 Milliarden Euro jährlich.

Der HDE bedankt sich für die Möglichkeit, Stellung zum Referentenentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) des Bundesministerium des Innern (BMI) für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland zu nehmen.

II. Position des HDE

- **Allgemeine Ausführungen**

1. Der Gesetzgeber sollte die Kongruenz mit dem KRITIS-DachG und seinen definierten Sektoren und der dortigen zuständigen Behörde (aktuell Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)) herstellen
2. Der Gesetzgeber sollte die zügige Novellierung der BSI-KRITIS-Verordnung durchführen, die weiterhin aussteht und die Sektoren mit Schwellwerten (nach Versorgungsgrad) sowie Anlagekategorien definiert.
3. Der Gesetzgeber sollte die Arbeitsfähigkeit des BSI in erster Linie der Planstellen als Gegenstand künftiger Haushaltsaufstellungsverfahren sicherstellen.
4. Da es keine Umsetzungsfrist für Unternehmen gibt, dafür aber laut Gesetz Nachweise/Prüfungen durch das BSI erst nach 3 Jahren nach in Kraft treten möglich sind, besteht für den Zwischenzeitraum eine Unsicherheit für Unternehmen. Diese können dann nur auf den Ermessenspielraum des BSI hoffen, dass mit einem guten Reporting/Nachweis durch Unternehmen über die bisher ergriffenen Maßnahmen im Fall eines Vorfalls, keine Sanktionierung stattfindet.

- **Zu § 11 Abs. 1**

„(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Einrichtung der Bundesverwaltung oder einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung um einen herausgehobene Fall, so kann das Bundesamt auf Ersuchen der betroffenen Einrichtung oder des betroffenen Betreibers oder einer anderen für die Einrichtung oder den Betreiber zuständigen Behörde die Maßnahmen treffen, dir zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen System erforderlich sind.“

Es bedarf einer Definition und Erläuterung eines „herausgehobenen Falls“, z. B. anhand technischer Parameter, Schwellenwerte für Schadenshöhe oder gesellschaftlicher Relevanz.

- **Zu § 11 Abs. 2**

Handelsverband Deutschland e. V. (HDE)
Dara Kossok-Spieß | Netzpolitik und Digitalisierung | kossok-spiess@hde.de
Ulrich Binnebößel | Zahlungsverkehr, Logistik, Online-Redaktion | binneboessel@hde.de
Am Weidendamm 1A | 10117 Berlin | kontakt@hde.de

„Ein herausgehobener Fall nach Absatz 1 liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder wenn die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichem Interesse ist“

Es bedarf einer spezifischeren Angabe, ab wann von einem Angriff von besonderer Qualität zusprechen ist.

- **Zu § 28 Abs. 3**

„Rechtfertigen Tatsachen die Annahme, dass eine wichtige Einrichtung Verpflichtungen nach § 30 Absatz 1 Satz 1, § 32 Absatz 1 bis 3 und § 38 Absatz 3 nicht oder nicht richtig umsetzt, so kann das Bundesamt deren Einhaltung überprüfen und Maßnahmen nach § 61 treffen.“

Der HDE begrüßt diese Änderung zum Ursprungsentwurf. Gerade im Handel ist die Installation der Ladepunkte zum einen nur ein Nebengeschäft und eine zusätzliche Dienstleistung, die der Kundenbindung und Steigerung der Umsätze im Kerngeschäft dienen soll. Zum anderen ist Installation der Ladepunkte für Handelsunternehmen aber vor allem eine Verpflichtung nach Gebäude-Elektromobilitätsinfra-struktur-Gesetz (GEIG). Das Gleiche gilt für Betreibung von Erzeugungsanlagen: Handelsunternehmen werden durch landesspezifische PV-Pflichten verpflichtet, PV-Anlagen zu betreiben. Aus diesen Verpflichtungen dürfen für Handelsunternehmen – durch die Umsetzung der NIS-Richtlinie ins nationale Recht – keine weiteren um-fangreichen Berichtspflichten ergeben, nur weil sie Ladepunkte / PV-Anlagen betreiben (müssen).

Aus diesem Grund sollten solche Kriterien wie die Mitarbeiteranzahl und die Umsatzgröße auf die Tätigkeit der Unternehmen als Ladepunktbetreiber / Betreiber von Erzeugungsanlagen abzielen und nicht auf die Gesamtmitarbeiteranzahl / Gesamtumsatz. Denn obwohl die Schwellenwerte bereits in der europäischen NIS-2-Richtlinie enthalten sind, beinhaltet die NIS-2-Richtlinie auch den Grad der Kritikalität als Kriterium. Für die Rechtssicherheit der Unternehmen und Planbarkeit von Investitionen ist eine Definition der vernachlässigbaren geringfügigen Tätigkeit vorteilhaft.

- **Zu § 30 Abs. 6**

„Besonders wichtige Einrichtungen und wichtige Einrichtung dürfen durch Rechtsverordnung nach § 58 Absatz 3 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden, wenn diese über eine Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel k9 der Verordnung (Eu) 2019/881 verfügen.“

Es bedarf einer genauen Spezifikation oder bestenfalls abschließender Aufzählung von IKT -Produkten, -Dienste, und -Prozessen oder Kategorisierung der betroffenen Produkte, um Planungs- und Investitionssicherheit herzustellen.

- **Zu § 31**

„Für Betreiber kritischer Anlagen gelten für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, im Vergleich zu anderen informationstechnischen Systemen, Komponenten und Prozessen besonders wichtiger Einrichtungen über das Schutzniveau dieser Einrichtungen hinausgehende Maßnahmen nach § 30 Absatz 1 Satz 1 als verhältnismäßig, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht.“

Handelsverband Deutschland e. V. (HDE)
Dara Kossok-Spieß | Netzpolitik und Digitalisierung | kossok-spiess@hde.de
Ulrich Binnebößel | Zahlungsverkehr, Logistik, Online-Redaktion | binneboessel@hde.de
Am Weidendamm 1A | 10117 Berlin | kontakt@hde.de
www.einzelhandel.de

Eine genauere Ausdifferenzierung der Verhältnismäßigkeit, sollten hier platziert werden.

Die in §31 vorgesehene Fokussierung auf Angriffserkennung (z. B. SIEM/XDR) greift zu kurz. Ergänzend sollte der Entwurf auch **präventive Maßnahmen** (wie CTEM – Continuous Threat Exposure Management) explizit benennen. Wenn nur Angriffserkennungen eingesetzt werden, ist bei der Erkennung bereits viel Zeit verstrichen und oft zu spät.

- **§ 36 Abs. 2**

„(2) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Si-cherheitsvorfall zu verhindern oder zu bewältigen, oder liegt die Offenlegung des erhebli-chen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann das Bundesamt nach Anhörung der betreffenden Einrichtung diese dazu verpflichten, die Öffentlichkeit über den erheblichen Sicherheitsvorfall zu informieren."

Es bedarf einer genauen Spezifikation, wann ein solches Szenario „erforderlich" ist und welche konkreten Kriterien für eine Offenlegung erfüllt sein müssen.

- **§ 38 Abs. 1-3**

„(1) Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen."

Durch eine Streichung des Zusatzes Risikomanagement „im Bereich Cybersicherheit zu billigen" wird der Geltungsbereich der Maßnahmen deutlich vergrößert. An dieser Stelle bedarf es einer Konkretisierung auf welches Risikomanagement sich bezogen wird und umzusetzen ist.

„(2) Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten"

Eine nähere Konkretisierung, inwieweit der Geschäftsleiter für einen schuldhaft verursachten Schaden haftet, sollte definiert werden.

„(3) Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik und die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste zu erwerben."

Der Absatz bedarf einer Konkretisierung hinsichtlich der Ausgestaltung der Schulungen sowie der Anforderungen an entsprechende Schulungen. Darüber hinaus bedarf es einer Konkretisierung, welche Person der Geschäftsführung eines Unternehmens als Geschäftsleitung an entsprechenden Schulungen teilnehmen sollte. Zudem braucht es unterstützende Angebote und entsprechende budgetäre Finanzierung, um Unternehmen bei der Vermittlung der Inhalte zu unterstützen. Hier sieht der HDE sowohl das BSI als auch die Kompetenzzentren in einer herausgehobenen Rolle.

Handelsverband Deutschland e. V. (HDE)
Dara Kossok-Spieß | Netzpolitik und Digitalisierung | kossok-spiess@hde.de
Ulrich Binnebößel | Zahlungsverkehr, Logistik, Online-Redaktion | binneboessel@hde.de
Am Weidendamm 1A | 10117 Berlin | kontakt@hde.de

- **§ 41 Abs. 1**

„Ein Betreiber kritischer Anlagen hat den geplanten erstmaligen Einsatz einer kritischen Komponente gemäß § 2 Nummer 23 dem Bundesministerium des Innern vor ihrem Einsatz anzuzeigen."

Es bedarf einer genauen Definition und Spezifikation der „kritischen Komponente".

„Vor Ablauf der Frist von zwei Monaten nach Anzeige nach Absatz 1 ist der Einsatz nicht gestattet. Das Bundesministerium des Innern kann die Frist gegenüber der Einrichtung um weitere zwei Monate verlängern, wenn die Prüfung besondere Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist."

Es bedarf einer Definition und Konkretisierung des Prüfungsvorgangs.

Aus zeitkritischen Gründen bedarf es eines Alternativprozesses, zur Ermöglichung des Einsatzes einer noch nicht abschließend geprüften „kritischen Komponente", um eine Aufrechterhaltung des Geschäftsbetriebs einer kritischen Anlage zu gewährleisten.

- **§ 61 Abs. 9**

„Sofern besonders wichtige Einrichtungen den Anordnungen des Bundesamtes nach diesem Gesetz trotz Fristsetzung nicht nachkommen, kann das Bundesamt dies der jeweils zuständigen Aufsichtsbehörde mitteilen. Die zuständige Aufsichtsbehörde kann, wenn ein Zusammenhang zwischen Durchsetzungsmaßnahme und Anordnung besteht, als letztes Mittel

> 1. die dieser Einrichtung erteilte Genehmigung nach dem jeweiligen Fachrecht vorüber-gehend ganz oder teilweise aussetzen und
>
> 2. unzuverlässigen Geschäftsleitungen die Ausübung der Tätigkeit, zu der sie berufen sind (§ 2 Nummer 13), vorübergehend untersagen"

Es bedarf eines Zwischenschritts, bevor die entsprechende Aufsichtsbehörde involviert wird. Das Bundesamt sollte in Kontakt mit der besonders wichtigen Einrichtung treten, um mögliche Ursachen der Fristverletzung zu berücksichtigen.

- **§ 62**

„Rechtfertigen Tatsachen die Annahme, dass eine wichtige Einrichtung Verpflichtungen nach § 30 Absatz 1 Satz 1, § 32 Absatz 1 bis 3 und § 38 Absatz 3 nicht oder nicht richtig umsetzt, so kann das Bundesamt deren Einhaltung überprüfen und Maßnahmen nach § 61 treffen."

Eine Ausdifferenzierung einer nicht richtigen Umsetzung sollte angegeben werden. Dabei sollte definiert werden, ab wann eine nicht richtige Umsetzung erfolgt ist, und differenziert werden zu keiner Umsetzung respektive einer richtigen Umsetzung.

Handelsverband Deutschland e. V. (HDE)
Dara Kossok-Spieß | Netzpolitik und Digitalisierung | kossok-spiess@hde.de
Ulrich Binnebößel | Zahlungsverkehr, Logistik, Online-Redaktion | binneboessel@hde.de
Am Weidendamm 1A | 10117 Berlin | kontakt@hde.de