HDE Handelsverband Deutschland

Stellungnahme

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

Stand: 27. Mai 2024

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 Bundesministeriums des Innern und für Heimat (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, und
3. Der Gesetzgeber sollte die Arbeitsfähigkeit des BSI sichern
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 § 2 Nr. 27**

„27. „Online-Marktplatz“ ein Dienst nach § 312l Absatz 3 BGB;“

Es bedarf einer konkreten Darstellung einschließlich Beispielen der Begriffsbestimmung „Online-Markplatz“.

- **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.“

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

Es bedarf einer Definition und Erläuterung eines „herausgehobenen Falls“.

- **Zu § 30 Abs. 6**

„(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 von IKT -Produkten, -Dienste, und -Prozessen.

- **Zu § 31**

In §31 wird nur von Angriffserkennung gesprochen. Erweiterung um Angriffserkennung [und -prävention]. Präventionsansatz (gepaart mit Angriffserkennung) ist das A und O, denn wenn nur Angriffserkennungen (wie z.B. hier SIEM und DER/XDR) eingesetzt werden, ist bei der Erkennung bereits viel Zeit verstrichen und oft zu spät). Bei der Angriffsprävention kommen Entwicklungen der Continuous Threat Exposure Management (CTEM) zum Tragen, die mit technischen Maßnahmen eine kontinuierliche Risikoanalyse ermöglichen.

- **§ 36 Abs. 2**

„(2) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Sicherheitsvorfall zu verhindern oder zu bewältigen, oder liegt die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann das Bundesamt nach Anhörung der betreffenden Einrichtung die Öffentlichkeit über den erheblichen Sicherheitsvorfall informieren oder die Einrichtung verpflichten, dies zu tun.“

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

- **§ 41 Abs. 1**

„(1) Ein Betreiber kritischer Anlagen hat den geplanten erstmaligen Einsatz einer kritischen Komponente gemäß § 2 Absatz 1 Nummer 22 dem Bundesministerium des Innern und für Heimat vor ihrem Einsatz anzuzeigen.“

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

- **§ 41 Abs. 3**

„Vor Ablauf der Frist von zwei Monaten nach Anzeige nach Absatz 1 ist der Einsatz nicht gestattet. Das Bundesministerium des Innern und für Heimat 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.

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

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.

- **Zur Anlage 1 und 2**

Aus Handelssicht gibt es neue Kategorien von besonders wichtigen oder wichtigen Einrichtungen in Anlage 1 und 2:

1. **Ladepunktbetreiber:** angeführt in Anlage 1; Definition nach §2 Abs. 8 LSV (Betreiber ist, wer unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Ein-fluss auf den Betrieb eines Ladepunkts ausübt). Sie gehören zu besonders wichtigen und/oder wichtigen Einrichtungen je nach Größe bzw. Umsatz

2. **Betreiber von Erzeugungsanlagen:** angeführt in Anlage 1; Definition gemäß § 3 Nr. 18d EnWG (Erzeugungsanlage ist eine Anlage zur Erzeugung von elektrischer Energie)

Zu Punkt 1 und 2, Ladepunktbetreiber und Betreiber von Erzeugungsanlagen: nach Erwägungsgrund 15 der NIS-2-Richtlinie (siehe Erläuterungen oben) sollte nicht allein die Größe des Unternehmens nach Mitarbeiteranzahl und Umsatzgröße entscheidend sein, sondern auch der „Grad ihrer Kritikalität in Bezug auf ihren Sektor oder die Art der von ihnen erbrachten Dienste sowie ihre Größe“ der Einrichtungen. 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-Elektromobilitätsinfrastruktur-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 umfangreichen 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.

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