HDE Handelsverband Deutschland

20. April 2021

EU-Vorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit (NIS 2)

Hintergrund

- Die EU-Kommission hat am 16. Dezember 2020 eine neue EU-Cybersicherheitsstrategie sowie neue Vorschriften zur Erhöhung der Widerstandsfähigkeit kritischer Einrichtungen vorgelegt, um Europas kollektive Abwehrfähigkeit gegen Cyberbedrohungen zu stärken.
- Um auf die zunehmenden Risiken durch Digitalisierung und Vernetzung zu reagieren, soll dabei auch die *Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union* von 2013 überarbeitet werden.
- Die überarbeitete NIS-Richtlinie soll mittlere und große Einrichtungen aus einer größeren Anzahl von Sektoren erfassen, wobei deren strategische Bedeutung zum Maßstab genommen werden soll.
- Die NIS 2 soll zudem höhere Sicherheitsanforderungen an Unternehmen stellen, sich der Sicherheit der Lieferketten widmen und strengere Aufsicht- und Durchsetzungsanforderungen durch die nationalen Behörden vorsehen.
- Es obliegt nun dem Europäischen Parlament und dem Rat, die vorgeschlagene NIS-2-Richtlinie zu prüfen und anzunehmen. Das Europäische Parlament hat angekündigt im Mai 2021 einen Berichtsentwurf vorzulegen und seine Position bis Ende des Jahres 2021 anzunehmen.

Position

- Wir unterstützen das Ziel der Kommission, die Widerstandsfähigkeit von Einrichtung und deren Schutz gegen Cyberangriffe zu stärken. Allerdings bitten wir darum, insbesondere vier Punkte bei der Ausgestaltung der Vorschriften zu berücksichtigen:

1. Anwendungsbereich (Artikel 2 und Anhang 1)

- Mit der NIS 2 soll der Anwendungsbereich auf zahlreiche weitere Sektoren ausgeweitet werden, inkl. dem Verkauf von Lebensmitteln. Es sollte jedoch sichergestellt werden, dass jede Erweiterung primär von wissenschaftlichen Überlegungen geleitet und nicht das Ergebnis politischer Interessen ist. Dies bezieht sich insbesondere auf den Einfluss der laufenden Covid-19-Pandemie. Der öffentliche Diskurs ist von einem unterschiedlichen, teilweise irreführenden Verständnis von kritischen Infrastrukturen geprägt. Der Begriff wurde weniger unter dem Aspekt dessen gesehen, was *schützenswert* ist, sondern mehr unter dem Aspekt dessen, was funktionieren und aufrechterhalten werden muss. Deshalb empfehlen wir, sich im Rahmen der NIS-Richtlinie auf Cyber-Bedrohungen zu konzentrieren und die **Aufrechterhaltung der lokalen Lebensmittelversorgung nicht mit der Kritikalität der IT von Branchen der kritischen Infrastruktur zu verwechseln**. Die NIS-Richtlinie sollte von letzterem Standpunkt aus betrachtet und durchdacht werden.
- Deshalb sollte sich die Kommission an klare Definitionen halten und eine (wissenschaftlich) ungerechtfertigte Aufblähung dessen, was als kritische Infrastruktur zu betrachten ist, vermeiden. Dies wird auch von der Folgenabschätzung[1] unterstützt: Während in den meisten Sektoren die Befragten dazu neigten, die Erweiterung des Anwendungsbereichs der NIS-Richtlinie zu begrüßen, waren die Ergebnisse im Lebensmittelhandel gemischter, denn nur die Hälfte der Befragten unterstützte die Idee, in den Anwendungsbereich aufgenommen zu werden.
- Die Ausweitung des Anwendungsbereichs sollte daher grundsätzlich nur Unternehmen von systemischer Relevanz umfassen. Selbst ein Großteil von mittleren Unternehmen hat aber keinen kritischen Anteil an der Versorgungssicherheit eines Mitgliedstaates oder der EU und sollte bei einer Ausnahmeregelung berücksich-

[1] https://data.consilium.europa.eu/doc/document/ST-14150-2020-ADD-4/en/pdf (Seite 41)

Handelsverband Deutschland (HDE) e. V.
Fabian Fechner | Stellv. Büroleiter | E-Mail: fechner.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brüssel | Telefon: +32 (0) 2 737 03 76 | Fax: +32 (0) 2 230 84 97
www.einzelhandel.de

tigt werden– insbesondere da die Folgenabschätzung (Seite 71) von einer Kostensteigerung von 22% ausgeht – was wir noch für deutlich zu niedrig halten. Der Aufwand und die Maßnahmen verursachen pro Betrachtungsgegenstand Kosten von mindestens 100.000 € in den ersten zwei Jahren. Der Geltungsbereich würde zu tausenden neuen, betroffenen Unternehmen führen. Alleine im Lebensmittelbereich würde sich die Anzahl der betroffenen Betriebe verhundertfachen. Daher unser **Lösungsvorschlag mit Bezug auf die Versorgungskritikalität**: Wird die **Versorgung von mehr als 0,5 % der Bevölkerung des jeweiligen Mitgliedsstaates** durch eine Einrichtung erbracht, ist diese Einrichtung wesentlich oder wichtig im Sinne dieser Richtlinie. Dies würde auch die unterschiedlichen wirtschaftlichen Rahmenbedingungen (z.B. Preisniveau) innerhalb der Mitgliedstaaten adäquat berücksichtigen. Sollte dieser Lösungsvorschlag nicht mehrheitsfähig sein, so sollte die bisherige Ausnahme für Kleinst- und Kleinunternehmern (Art. 2 Abs. 1) – welche wir ausdrücklich unterstützen - auf mittelständische Unternehmen ausgeweitet werden (EU-KMU-Definition).

2. Harmonisierung, Konsistenz & Vermeidung von legislativen Dopplungen

- Da viele unserer Mitgliedsunternehmen in verschiedenen EU-Mitgliedsstaaten tätig sind, erkennen wir den Mehrwert der Harmonisierung der NIS 2.0 an. Allerdings stellt sich die Frage ob eine Minimalharmonisierung (Art. 3) ausreichend ist, um sicherzustellen, dass grenzüberschreitend agierende Unternehmen nicht **in jedem Mitgliedstaat unterschiedliche Anforderungen** zu erfüllen haben. Wenn es hier nationale Unterschiede geben würde, würde dies zu einem deutlichen Zusatzaufwand führen.

3. Verantwortung entlang der Lieferkette (Artikel 18)

- Unternehmen haben es in der Lieferkette oft mit großen, globalen Lieferanten zu tun, gegen die sie wenig oder gar keinen Einfluss haben. Ein wesentliches oder wichtiges **Unternehmen sollte daher nicht haften, wenn ein Zulieferer die Anforderungen nicht erfüllt,** zumindest dann nicht, wenn es alles in seiner Macht Stehende getan hat, um im Rahmen des Vertrags sicherzustellen, dass der Zulieferer ein risikoadäquates Maß an Cybersicherheit aufrechterhält.
- Die **Verantwortung für die Sicherheit der Lieferkette liegt bei den Herstellern** bzw. Lieferanten der jeweiligen Lösungen. Nur diese kennen vollumfänglich die von ihnen verwendeten Datenspeicher- und -verarbeitungsdienste, sowie die verwalteten Sicherheitsdienste und -prozesse. Die Verantwortung für die Sicherheit in der Lieferkette sollte daher aufgrund des begrenzten Kenntnis- und Einflussbereiches der Betreiber nicht auf diese abgewälzt und stattdessen auf multinationaler und regulatorischer Ebene direkt an die Hersteller und Dienstleister adressiert werden.
- Darüber hinaus bleibt der Vorschlag unklar, was die konkreten Auswirkungen der in Artikel 18 Nummer 2d genannten Anforderungen an die "Sicherheit der Lieferkette" sind. Da Ziffer 2d "sicherheitsrelevante Aspekte in Bezug auf die Beziehungen zwischen jedem Unternehmen und seinen Lieferanten oder Dienstleistern" beinhaltet, ist unklar, wie wesentliche und wichtige Unternehmen sicherstellen sollen, dass ein Lieferant oder Dienstleister die von der EU-Kommission als notwendig erachteten Anforderungen einhält.

4. Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung (Artikel 21)

- Die potenzielle Verpflichtung von Betreibern zum Einsatz von zertifizierten IKT-Produkten, -Diensten und -Prozessen ist nicht praxisgerecht und innovations- und reaktionsfeindlich. Eine Konsolidierung der eingesetzten Lösungen führt zu Monokulturen und bringt neue systemische und grenzüberschreitende Risiken. Die Ausnutzung einzelner Schwachstellen gefährdet dadurch ganze Sektoren oder wirkt ggf. sogar sektorübergreifend. Wir fordern daher, diesen Artikel zu streichen.

Handelsverband Deutschland (HDE) e. V.
Fabian Fechner | Stellv. Büroleiter | E-Mail: fechner.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brüssel | Telefon: +32 (0) 2 737 03 76 | Fax: +32 (0) 2 230 84 97
www.einzelhandel.de