Stellungnahme des Deutschen Verkehrsforums e.V. zum

Entwurf für ein Gesetz 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)

Berlin, 27.05.2024

Vorbemerkung

Das Deutsche Verkehrsforum e.V. (DVF) ist die verkehrsträgerübergreifende politische Vertretung des Mobilitätssektors im Personen- und Güterverkehr. Unsere rund 170 Mitglieder sind vorwiegend große und mittelständische Unternehmen, die sowohl Infrastrukturen betreiben als auch Waren zustellen und Personen befördern und damit überwiegend in den Anwendungsbereich der NIS-2-Richtlinie fallen. Da wir sowohl über unsere Mitgliedsunternehmen, als auch selbst im UP KRITIS engagiert sind, unterstützen wir dessen Stellungnahme, die Sie hier abrufen können.

Nachfolgend noch einige Punkte, die wir in diesem Zusammenhang herausstellen möchten:

- Wir begrüßen, dass der vorliegende Referentenentwurf bereits einige der Hinweise, die wir im Rahmen der Konsultation zum Diskussionspapier für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie im Oktober letzten Jahres gegeben haben, aufgreift. Beispielhaft sei hier Festsetzung der Dreijahresfrist zwischen Inkrafttreten des Gesetzes und die Verpflichtung zur Erbringung von Nachweisen über die Erfüllung von Anforderungen mit Blick auf besonders wichtige Einrichtungen analog zur Frist von Betreibern kritischer Anlagen genannt (§ 65, (3)).

An einigen Stellen sehen wir jedoch nach wie vor Konkretisierungs- bzw. Anpassungsbedarf:

- **Die Anforderungen des vorliegenden Entwurfes sind in Teilen strenger, als in der NIS-2 vorgegeben:**

Zu § 28 (1) Nr. 4 BISG

  - Der hier beschriebene Anwendungsbereich scheint von dem der NIS2-Richtlinie erheblich abzuweichen: Nach unserem Verständnis sind Unternehmen vom Anwendungsbereich des § 28 Abs. 1 Nr. 4 BSIG-E als „*besonders wichtige*

Einrichtung“ umfasst, die nach der NIS2-Richtlinie nicht betroffen wären. Das deutsche Umsetzungsgesetz geht damit aus unserer Sicht „ohne Not“ weit über den Anwendungsbereich der europäischen Richtlinie hinaus, mit ganz erheblichen finanziellen Auswirkungen auf die betroffenen Unternehmen. Zudem ist nicht klar, warum man auf europäischer Ebene von „wesentlichen“ und „wichtigen“ Einrichtungen spricht, wohingegen der deutsche Gesetzgeber „wichtige“ und „besonders wichtige“ Einrichtungen (anders) definiert. Etwas vereinfacht gesagt: Der Fokus der europäischen Richtlinie liegt auf den Betreibern kritischer Infrastrukturen, das deutsche Umsetzungsgesetz verpflichtet einen Großteil der Lieferkette gleich direkt gesetzlich mit.

- Zudem ist nicht ganz klar, wie die Definition des Anwendungsbereichs in der aktuellen Fassung zu verstehen ist: Den Satz *„Eine juristische Person, die anderen juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet, die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen ist“*, könnte man so verstehen, dass jeder Dienstleister oder Lieferant (bei einer entsprechenden Mitarbeiteranzahl/ bei entsprechendem Umsatz) einer in Anlage 1 bestimmten Einrichtungsart, unabhängig von der Art seiner geleisteten Tätigkeit/ gelieferten Ware in den Anwendungsbereich des Gesetzes fiele. Mit anderen Worten könnte man die aktuelle Definition einer „besonders wichtigen Einrichtung“ so verstehen, dass auch der Kaffeelieferant der Deutschen Bahn (bei einer entsprechenden Mitarbeiteranzahl/ bei entsprechendem Umsatz) in den Anwendungsbereich des Gesetzes fiele, was - liest man Abs. 1 in Verbindung mit Abs. 3 - wohl nicht gewünscht ist. [Der Relativsatz im Gesetzentwurf scheint den falschen Bezug zu haben, denn intendiert ist vermutlich, dass sowohl die Geschäftstätigkeit des Lieferanten/ des Dienstleisters als auch seine entgeltlich angebotene Ware oder Dienstleistung einen Bezug zu einer in Anlage 1 bestimmten Einrichtungsart haben müssen?]

Zu § 30 (1) BISG

- In der NIS-2 wird von der Beherrschung von Risiken für die Erbringung der Dienste gesprochen, das NIS2UmsuCG spricht jedoch von der Vermeidung von Störungen in informationstechnischen Systemen, Komponenten und Prozesse, die für die Erbringung ihrer Dienste genutzt werden. Hier fehlt ein qualifizierender Faktor, dass die Störung überhaupt Relevanz für die Diensterbringung hat und es somit ein zu beherrschendes Risiko gibt.
- Mit Blick auf steigende Harmonisierungsanforderungen innerhalb der EU sowie weitere europäische Regelungen (z.B. den CRA) sollten aus unserer Sicht nationale Alleingänge bei der Umsetzung europäischer Vorgaben vermieden werden und die Regelungen der NIS2-Richtlinie möglichst ohne wesentliche Verschärfungen bzw. Erweiterungen in deutsches Recht übernommen werden.
- Für Produkte/Dienste, für die spezialgesetzliche Regelungen vorliegen, die hinsichtlich ihrer Cybersicherheitsanforderungen von der EU KOM als ausreichend angesehen werden, sollten diese berücksichtigt werden.

- Bei den Anforderungen an die **Risikomanagementmaßnahmen** von Betreibern kritischer Anlagen sollte konkretisiert werden, dass aufgrund des Betriebs einer „kritischen Anlage“ gemäß § 28 Abs. 6 auch nur der diese „kritische Anlage“ betreffende Unternehmensteil den speziellen Anforderungen an „besonders wichtige Einrichtungen“ nach **§ 31** unterfällt.

- **Zu §34 BSIG Registrierungspflicht für bestimmte Einrichtungsarten: Abs. 1 Nr. 3 (Anschrift der Hauptniederlassung)**

Die Definition der Hauptniederlassung und die Auswirkung auf die Tochtergesellschaften in einem Konzernkonstrukt ist nach wie vor unklar. Die Verweise sind hier noch anzupassen. In Bezug auf die Hauptniederlassungsfrage für den IT-Betrieb sei vorweggenommen, dass hier noch einige Punkte unklar sind:

  - Welcher Geschäftsführer haftet innerhalb eines Konzernkonstrukts? Der Geschäftsführer der Hauptniederlassung bei einem Fehler der Tochtergesellschaft oder der Geschäftsführer der Tochtergesellschaft? Können die Umsetzungen der Anforderungen aus § 30 und der Schulungspflichten delegiert werden?
  - Welcher Stand der Technik ist verpflichtend umzusetzen und in welchen Mitgliedsstaaten?
  - Wie sieht es aus, wenn die Anforderungen des Mitgliedsstaats der Hauptniederlassung höher (alternativ niedriger) sind als in dem Mitgliedsstaat der Tochtergesellschaft?
  - Gilt die Nachweispflicht nur für den Mitgliedsstaat der Hauptniederlassung?

- Klärungsbedarf gibt es aus unserer Sicht auch bei denen in **Anhang 1** unter 2.1.2. einbezogenen „Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben“. Was damit gemeint ist, ergibt sich weder aus dem Gesetz selbst noch aus den Erläuterungen.

- Die in **Anlage 2** erfasste Branche Post- und Kurierdienste umschließt Anbieter von Postdienstleistungen nach § 4 Nr. 1 PostG, einschließlich Anbieter von Kurierdiensten. Da in einem separaten Verfahren momentan das PostG im Rahmen des Postrechtsmodernisierungsgesetz überarbeitet wird, kann dies auch eine veränderte Betroffenheit nach NIS2UmsuCG ergeben, sollte sich aus dem laufenden Gesetzgebungsverfahren eine Änderung der Definition des Anbieters von Postdienstleistungen ergeben – was höchst wahrscheinlich ist und potentiell den größten Teil der mittelständischen Transportunternehmen betreffen könnte.

- **Der im §58 (4) BSIG** gestrichene, für die Wirtschaft sehr wichtige Punkt zur „Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der Wirtschaftsverbände beim Erlass oder Änderung der Verordnung zur Identifizierung von Kritischen Anlagen“, sollte wieder aufgenommen werden.

- **§ 12 KRITIS-DachG** des Referentenentwurfs vom 21. Dezember 2023 sieht nach dem Grundsatz „ein Vorfall, eine Meldung“ ein einheitliches Meldeportal sowie eine einheitliche Meldestelle für Vorfälle gemäß KRITIS-DachG und NIS2UmsuCG vor. Hierfür bedarf es eines bundeseinheitlichen Vollzuges des KRITIS-DachG, da andernfalls in Sektoren wie bspw. Wasser, Abfallwirtschaft und ÖPNV – und damit auch in Querverbundsunternehmen – eine Zersplitterung der behördlichen Zuständigkeit und des Meldewesens nicht nur bei der Resilienz, sondern auch im Bereich der Cybersicherheit droht. Um dies zu verhindern, muss eine Regelung zur Anbindung der Landesbehörden an ein einheitliches Meldeportal und eine einheitliche Meldestelle erfolgen, um im Falle eines landesgrenzüberschreitenden Vorfalls die Notwendigkeit von Mehrfachmeldungen durch das betroffene Unternehmen zu vermeiden.

  Im Sinne der Einheitlichkeit und besseren Handhabbarkeit für die Unternehmen sollten umgekehrt auch die Warnungen an die Hersteller von von Sicherheitslücken betroffener Produkte (§13 (2)) über eine gemeinsame Plattform erfolgen. Ferner sollte § 13 (3) dahingehend konkretisiert werden, dass Warnungen, die nicht entfernt werden, alle sechs Monate (Entwurf: „regelmäßig“) zu überprüfen sind.

- Im Bundesamt für Sicherheit in der Informationstechnik sollte zudem ein entsprechender Personalaufbau vorgesehen und sichergestellt werden, um die zusätzlichen Aufgaben und Kompetenzen ohne Engpässe bewältigen zu können.