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

des Bundesministeriums des Innern (BMI)

Berlin, 04.07.2025

Das Deutsche Verkehrsforum (DVF) bedankt sich für die Möglichkeit zur Kommentierung des Referentenentwurfs für ein Gesetz zur Umsetzung der NIS2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz - NIS2UmsuCG) mit Stand 23.06.2025.

Nachfolgend einige Anmerkungen:

- Das DVF begrüßt, dass im vorliegenden Entwurf der Nachweiszeitraum über die umgesetzten Anforderungen des neuen BSIG für die Einrichtungen der Bundesverwaltung gestrafft wurde (§ 43 Abs. 4). Dieser soll analog zu den Vorgaben für die in den Geltungsbereich der Richtlinie fallenden Unternehmen drei Jahre betragen.
- Kritisch ist zu sehen, dass im vorliegenden Entwurf eine Entkoppelung vom KRITIS-DachG vorgenommen wurde. Das KRITIS-DachG zur Umsetzung der Resilienz-Richtlinie war bislang mit der NIS2-Umsetzung verwoben: So sollten die Gesetze aufeinander abgestimmt werden, u.a. um Vorgaben zur Erbringung von Meldepflichten und Nachweisverfahren zu synchronisieren. Diese Vernetzung ist im aktuellen Entwurf weitestgehend gelöscht, sollte mit Blick auf die Handhabbarkeit der Vorgaben und dem Ziel der Reduzierung bürokratischen Aufwands jedoch dringend wiederaufgenommen werden (siehe hierzu auch der Punkt „Harmonisierung mit weiterer einschlägiger Regulatorik, insbesondere KRITIS-DachG“)

An einigen Stellen sehen wir darüber hinaus nach wie vor Konkretisierungs- bzw. Anpassungsbedarf – insbesondere da, wo die Anforderungen des vorliegenden Entwurfes in Teilen strenger sind als in der NIS2 vorgegeben:

Zu § 28 BISG Besonders wichtige Einrichtungen und wichtige Einrichtungen

- Der § 28 Abs. 1 Nr. 4 beschriebene Anwendungsbereich scheint von dem der NIS2-Richtlinie erheblich abzuweichen: Nach unserem Verständnis sind hier Unternehmen

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.]
- Bei den Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen sollte konkretisiert werden, dass aufgrund des Betriebs einer „kritischen Anlage“ gemäß § 28 Abs. 8 auch nur der diese „kritische Anlage“ betreffende Unternehmensteil den speziellen Anforderungen an „besonders wichtige Einrichtungen“ nach § 31 unterfällt.

Zu § 30 BISG Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

- In der NIS2 wird von der Beherrschung von Risiken für die Erbringung der Dienste gesprochen, das NIS2UmsuCG spricht in § 30 Abs. 1 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.
- Für die Pflichten von Betreibern besonders wichtiger und wichtiger Einrichtungen enthält § 30 Abs. 2 einen Katalog von mindestens zu treffenden Maßnahmen. Nur für Betreiber besonders wichtiger Anlagen (und darunter Betreiber kritischer Anlagen) wird in Absatz 7 ausdrücklich die Möglichkeit zur Einführung branchenspezifischer Sicherheitsstandards zur Gewährleistung der Anforderungen nach Abs. 1 vorgesehen. Offen und zu klären bleibt demnach, inwiefern Betreiber wichtiger Einrichtungen ebenso ihre Übereinstimmung mittels geeigneter Standards nachweisen können. Ferner sollte klargestellt werden, dass der Nachweis der Übereinstimmung für Betreiber wichtiger Einrichtungen nur anlassbezogen erforderlich ist.

Zu § 34 BSIG Besondere Registrierungspflicht für bestimmte Einrichtungsarten

- Die Definition der Hauptniederlassung und die Auswirkung von § 34 Abs. 1 Nr. 3 (Anschrift der Hauptniederlassung) 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 **Anlage 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.
- **Anlage 2** Punkt 1.1.1 bezeichnet weiterhin KEP-Dienstleister pauschal, ohne Bezug auf den Betrieb relevanter informationstechnischer Systeme oder deren Größe bzw. Versorgungsgrad:
    - Somit würden Vertragsunternehmen (Subunternehmer) stets dann einbezogen, wenn sie die relativ niedrigen Schwellenwerte nach § 28 Abs. 2 Nr. 3 erreichen, womit jedes Logistikunternehmen, das als Teil seiner Geschäftstätigkeiten als Anbieter von Postdienstleistungen gem. PostG registriert ist, potenziell einer zweiten Markteintrittshürde begegnete.

Zu § 56 BSIG Ermächtigung zum Erlass von Rechtsverordnungen

- Der im **§56 Abs. 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.

Zu § 61 BSIG Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen

- § 61 Abs. 3 des Entwurfs besagt, dass das Bundesamt erst nach 3 Jahren Audits u.a. anordnen darf, insofern greifen die Sanktionsvorschriften für eine Zuwiderhandlung dagegen auch erst entsprechend verzögert, was sich in § 65 Abs. 2 Nr. 1 widerspiegelt, der von der Zuwiderhandlung gegen eine vollziehbare Anordnung spricht.
- Die sonstigen Sanktionen gegen die übrigen Vorgaben des Gesetzes, wie beispielsweise Meldepflichten, Dokumentationspflichten über die erforderlichen Maßnahmen nach § 30 etc. greifen nach unserer Lesart aber sofort, siehe § 65 Abs. 2 Nr. 2 (und die Ziffern danach) des Entwurfs. Dies ist in Anbetracht der Kürze der Zeit durchaus bedenkenswert. Denn wenn eine Einrichtung die „Einhaltung einer Verpflichtung dokumentieren“ muss, dann muss sie hierfür bereits in der Lage sein, die Verpflichtung zu erfüllen. Da hier auf § 30 Abs. 2 verwiesen wird, sprechen wir letztlich von sämtlichen Vorgaben, die im Kern in NIS2 enthalten sind (Einhaltung des Standes der Technik, Incident Management, Sicherheit der Lieferkette…). Insbesondere § 65 Abs. 2 Nr. 3 halten wir deshalb ohne Übergangsfrist für schwierig.
- Liest man § 65 Abs. 2 Nr. 3 nun wiederum in Verbindung mit § 61 Abs. 3, könnte man den Entwurf auch so verstehen, dass man zwar ab Tag 1 verpflichtet ist, eine Dokumentation zu erstellen, diese erst nach > 3 Jahren vorgelegt werden muss. Hier sollte dringend nachgeschärft werden, um für die betroffenen Unternehmen Rechtssicherheit herzustellen.

Zu § 62 BSIG Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen

- Konkretisierungsbedarf sehen wir bei den Vorgaben des § 62 zu Aufsichtsmaßnahmen des Bundesamts, wenn Tatsachen die Annahme rechtfertigen, dass eine wichtige Einrichtung die gesetzlichen Verpflichtungen nicht oder nicht richtig umgesetzt hat. Was rechtfertigt die Annahme bzw. wie wird diese substantiiert? Hier sollte die vorherige Gelegenheit des Unternehmens zur Stellungnahme aufgenommen werden.

Harmonisierung mit weiterer einschlägiger Regulatorik, insbesondere KRITIS-DachG

- In den Gesetzesinitiativen zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der

Bundesverwaltung sowie zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-DachG) ist grundsätzlich eine größtmögliche Harmonisierung sicherzustellen, beispielsweise in den folgenden Punkten:

- Grundsätzliche Anforderungen des Risikomanagements (§ 30 Abs. 1) an KRITIS-Betreiber, wichtige und besonders wichtige Einrichtungen im Bereich Risikomanagement sind seitens des Gesetzgebers zu harmonisieren.
- Technische und organisatorische Maßnahmen zur Absicherung der Anlagen (§ 30 Abs. 2) sind in Gleichklang zu bringen. Insbesondere § 30 Abs. 2 Nr. 1-5, 7 und 10 finden in jedem Fall in den Bereichen Cyber sowie Physical Resilience Anwendung. Daraus abgeleitete Mindestanforderungen in den jeweils gültigen Verordnungen sind zu vereinheitlichen, um synergetische Anforderungskataloge sowie branchenspezifische Sicherheitsstandards gesetzesübergreifend zu ermöglichen und Prüfungen zu vereinfachen.
- Vorgaben zur Art und Weise der Nachweiserbringung (§ 39) müssen zwischen beiden Gesetzen gleich sein. Andernfalls sind die dafür notwendigen Ressourcen zur Prüfung und Nachweiserbringung durch Doppelstrukturen auf Prüfer- sowie auf zu Prüfendenseite deutlich höher. Ziel muss es sein, den Betreibern die Möglichkeit zu eröffnen, durch eine Nachweisprüfung alle Anforderungen des Gesetzesgebers zu erfüllen.
- Vorgaben zu Meldepflichten, -verfahren und entsprechenden Fristen sind in beiden Gesetzen gleichermaßen darzustellen. § 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. In diesem Kontext muss auch 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 Sicherheitslücken betroffener Produkte (§13 Abs. 2) über eine gemeinsame Plattform erfolgen.