

Stellungnahme

zum Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG)

DSLV Bundesverband Spedition und Logistik e. V.

Friedrichstraße 155-156 | Unter den Linden 24
10117 Berlin

Telefon: +49 30 4050228-0

E-Mail: info@dslv.spediteure.de

www.dslv.org | de.linkedin.com/company/spediteure

Lobbyregister beim Deutschen Bundestag | Registernummer: R000415

Transparenz-Register der EU | Identifikationsnummer: 7455137131-52

Stand: 28. Mai 2024

Zum Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG) vom 7. Mai 2024 nimmt der DSLV wie folgt Stellung:

Der Logistiksektor unterstützt das Ziel der NIS-2-Richtlinie, das Gesamtniveau der Cybersicherheit in der EU zu steigern. Die Regelungen der NIS-2-Richtlinie sollten dabei möglichst ohne wesentliche Verschärfungen bzw. Erweiterungen in deutsches Recht übernommen und nur die rechtssystematisch notwendigen Anpassungen vorgenommen werden. Eine übermäßige Bürokratiebelastung des Mittelstands, die die überwiegende Mehrheit der Logistikunternehmen in Deutschland ausmacht, sollte unter allen Umständen vermieden werden.

Der DSLV Bundesverband Spedition und Logistik unterstützt als Mitglied des Branchenarbeitskreises Transport und Verkehr (BAK TuV) zudem die aktuelle Stellungnahme des Technischen Arbeitskreises (TAK) Regulierung des UP KRITIS.

Darüber hinaus bitten wir darum, die folgenden Punkte zu berücksichtigen.

Besonders wichtige und wichtige Einrichtungen in der Logistik

Der DSLV begrüßt die Entscheidung, den Logistiksektor nicht als Subsektor im Annex 1 im Sektor Transport und Verkehr aufzunehmen. Dies entspricht der Systematik der europäischen NIS-2-Richtlinie und verhindert die Regulierung von kleinen Speditionsunternehmen, die für sich genommen keine Relevanz für die Versorgungssicherheit Deutschlands haben.

Entgegen dieser Grundsatzentscheidung können bestimmte Speditionen allerdings weiterhin unter die Regulierung fallen. Der DSLV begrüßt in dem Zusammenhang zwar, dass bei einer Prüfung der Betroffenheit nur diejenigen Teile der Einrichtung einzubeziehen sind, die tatsächlich im Bereich der in den Anlagen 1 und 2 genannten Definitionen der Einrichtungskategorien tätig sind (Seite 144 des Referentenentwurfs). Trotzdem droht in den folgenden Bereichen eine Regulierung von kleinen und mittelständischen Marktteilnehmern, deren Ausfall keine spürbaren Auswirkungen auf den Wirtschaftsstandort Deutschland hätte:

- ➔ In Anlage 1 steht im Subsektor Luftverkehr unter 2.1.2 am Ende „Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben“. Was damit gemeint ist, ergibt sich weder aus dem Gesetz selbst noch aus den Erläuterungen. Es ist naheliegend, einen gewissen Organisationszusammenhang („zugehörig“) mit dem Flughafen anzunehmen, wie sie z. B. bei Abfertigungsgesellschaften vorliegen. Fraglich ist auch, ob lediglich ein räumlicher oder darüberhinausgehend auch ein funktioneller Zusammenhang bestehen muss. Eine klarere Formulierung bzw. eine Klärung im Besonderen Teil des Gesetzesentwurfs würde dabei helfen, Rechtsunsicherheiten zu vermeiden.
- ➔ In Anlage 1 unter 2.2.2. werden „Eisenbahnverkehrsunternehmen nach § 2 Nummer 3 AEG, einschließlich Betreiber einer Serviceeinrichtung nach § 2 Nummer 9 AEG“ in Verbindung mit Anlage 2 Nummer 2 bis 4 des Eisenbahnregulierungsgesetzes (ERegG) als

Betreiber von wichtigen oder besonders wichtigen Einrichtungen eingeordnet. Dies betrifft überwiegend Eisenbahnverkehrsunternehmen. Über den Zusatz „Betreiber einer Serviceeinrichtung“ sind allerdings auch nach Anlage 2 Nummer 2 b ERegG Betreiber von Güterterminals betroffen. Dies umfasst z. B. multimodale Logistikterminals, Railports oder Speditionen mit eigenem Gleisanschluss. Dies sind in der Mehrzahl kleinere, inhabergeführte Speditionsunternehmen mit weniger als 100 Mitarbeitern. Eine Regulierung dieser Marktteilnehmer ist nicht zielführend.

- ➔ In Anlage 2 ist im Sektor Transport und Verkehr die Branche Post- und Kurierdienste aufgeführt. Dies umschließt Anbieter von Postdienstleistungen nach § 4 Nr. 1 PostG, einschließlich Anbieter von Kurierdiensten. Der DSLV weist darauf hin, dass in einem separaten Verfahren momentan das PostG im Rahmen des Postrechtsmodernisierungsgesetz überarbeitet wird. Sollte sich daraus eine Änderung der Definition des Anbieters von Postdienstleistungen ergeben, kann dies auch eine veränderte Betroffenheit nach NIS2UmsuCG ergeben, durch die nicht nur ein Großteil von Stückgutspeditionen reguliert werden könnte, wenn der Begriff auf diese ausgedehnt wird, sondern, wenn die Marktzugangsregelung auch auf den Transport (Hauptlauf) von Postsendungen erweitert wird, auch potentiell jedes Straßengüterverkehrsunternehmen in Deutschland sowie aus anderen Mitgliedstaaten, das Ladungen zwischen den Standorten der eigentlichen Anbieter von Postdienstleistungen bewegt. Im Kontext der Cybersicherheit erscheint eine solch weitreichende Verpflichtung der Transportwirtschaft schon deshalb unverhältnismäßig, weil der Transport von Behältern in den Netzwerken durch solche Auftragnehmer keine Verknüpfung mit den Versandsystemen der Anbieter impliziert (hier werden allein die Behälter durch den jeweils verladenden bzw. empfangenden Anbieter im System angemeldet).

Einrichtungen der Bundesverwaltung, § 29 BSIG

Die fortgesetzten Cyberangriffe auf Kommunen und Behörden, die teils erhebliche Auswirkungen auf Wirtschaft und Gesellschaft haben, verdeutlichen die Notwendigkeit, die öffentliche Verwaltung auf allen föderalen Ebenen in den Anwendungsbereich des BSIG aufzunehmen. Die Vorfälle in Anhalt-Bitterfeld und Schwerin zeigen, welche Folgen es hat, wenn wichtige Verwaltungsdienstleistungen ausfallen und dadurch wesentliche Planungs- und Genehmigungsverfahren unterbrochen werden. Während der breite Anwendungsbereich auch viele mittelständische und kleine Unternehmen umfasst, nimmt der Staat hier eine besondere Rolle ein und entzieht sich seiner eigentlichen Verantwortung. Es ist entscheidend, dass Bundes-, Landes- und Kommunalbehörden einheitlich als besonders wichtige Stellen definiert werden, um sie in den Anwendungsbereich des BSIG einzubeziehen. Eine bloße Einstufung als wichtige Einrichtungen reicht für einen funktionierenden Staat nicht aus. Diese umfassende Einbeziehung ist unerlässlich, um das Ziel der NIS-2-Richtlinie (EU) 2022/2555 zu erreichen, nämlich eine EU-weite Harmonisierung der Cybersicherheit. Nur durch die vollständige Integration aller Verwaltungsebenen kann die Wirksamkeit der Maßnahmen zur Stärkung der Cybersicherheit in der öffentlichen Verwaltung in ganz Europa gewährleistet werden.

- ➔ Der Gesetzesentwurf sollte insoweit erweitert werden, dass auch Behörden auf Landes- und Kommunalebene in den Adressatenkreis des BSIG einbezogen und als besonders wichtige Einrichtungen aufgenommen werden.

Meldepflichten, § 32 BSIG

Die in § 32 normierten Meldepflichten bedürfen für eine rechtssichere Anwendung in der Praxis der Konkretisierung. Spezifisch stellt sich die Frage, welche Umstände eine substantiierte Kenntnis über die Qualität eines Vorfalls gemäß der Definition in § 2 Absatz 1 Nr. 9 oder einer Rechtsverordnung nach § 2 Absatz 2 begründen. Die im Entwurf gegebene Erläuterung zu § 32 Absatz 1 „*dass eine Mitarbeiterin oder ein Mitarbeiter der Einrichtung innerhalb seiner Arbeitszeit Kenntnis über einen erheblichen Sicherheitsvorfall erlangt*“, müsste dahingehend spezifiziert werden, dass es sich um Beschäftigte mit ausreichender Sachkunde handelt und die Kenntnis auf eine notwendige Analyse der betreffenden Störung bzw. ihrer Ursachen folgt. Insbesondere Erstmeldungen nach Nr. 1 sollten nicht vorsorglich erfolgen müssen.

- ➔ Die in der Begründung zum Entwurf gegebene Erklärung zu Kenntniserlangung über einen erheblichen Sicherheitsvorfall sollte konkretisiert werden. Es muss sich insoweit um eine substantiierte Kenntnis handeln, als dass zunächst für qualifizierte Stellen im Unternehmen eine grundlegende Beurteilung möglich ist.
- ➔ Ebenso notwendig erscheint eine Festlegung für solche Fälle, in denen bereits eine andere nationale Aufsichtsbehörde in die Behandlung eines erheblichen Sicherheitsvorfalls einbezogen wurde.

Verantwortlichkeiten, § 38 BSIG

Die Verantwortlichkeit für Geschäftsleiter nach § 38 geht in vielen Fällen ins Leere bzw. könnte unbillige Haftungsrisiken für Leiter nationaler Unternehmensteile begründen. In internationalen Konzernunternehmen, deren IT-Systeme zentral betrieben und überwacht werden, haben nationale Geschäftsleiter keinen Einfluss auf wesentliche Aspekte des Risikomanagements nach § 30. Die in § 61 normierten Sanktionsmöglichkeiten gegenüber der juristischen Person des nationalen Unternehmens stellen in diesen Fällen das einzig angemessene und auch hinreichende Instrument dar. Allein die Vorstellung, dass Geschäftsleiter in mehreren (möglicherweise allen) EU-Staaten zentrale Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und zu überwachen hätten, macht deutlich, dass dies kein Beitrag zu einer ernsthaften und kohärenten Cybersicherheitsstrategie betreffender Unternehmen darstellt. Die Pflicht zu "billigen", i. S. v. zustimmen oder gutheißen, bedeutet insbesondere bei international agierenden Konzernunternehmen ein "zur Kenntnis nehmen", da kein direkter Einfluss auf die Struktur und den Betrieb relevanter Prozesse besteht.

- ➔ Die Obliegenheiten für Geschäftsleiter nach § 38 sind zumindest dahingehend zu präzisieren, dass diese nur greifen, sofern der Betrieb und das Risikomanagement von IT-Systemen in deren Verantwortung fallen. Insbesondere die Vorsehung einer zwingenden Norm in Absatz 2 verkennt die Realität zentral, d. h. aus dem Ausland, betriebener

IT-Systeme und geht daher vorschnell über die Vorgaben des Artikel 20 der NIS-2-Richtlinie hinaus.

Nachweispflichten für Betreiber kritischer Anlagen, § 39 BSIG

Für die Pflichten von Betreibern besonders wichtiger und wichtiger Einrichtungen enthält § 30 Absatz 2 einen Katalog von mindestens zu treffenden Maßnahmen. Nur für Betreiber besonders wichtiger und kritischer Anlagen wird in § 30 Absatz 8 und 9 ausdrücklich die Möglichkeit zur Einführung branchenspezifischer Sicherheitsstandards zur Gewährleistung der Anforderungen nach § 30 Absatz 1 vorgesehen. Offen bleibt weiterhin, inwiefern Betreiber wichtiger Einrichtungen ebenso ihre Übereinstimmung mittels geeigneter Standards nachweisen können.

- ➔ Dem BSI sollte analog zu § 30 Absatz 9 aufgegeben werden, allgemeine IT-Sicherheitsstandards (bspw. ISO 27.001) sowie sonstige Bedingungen für den Nachweis der Übereinstimmung im Kontext international verbundener Unternehmen zu bewerten. Es sollte (auch für wichtige Einrichtungen) klargestellt werden, inwieweit welche Zertifizierungen zur Erfüllung der Anforderungen ausreichen, wie dies beispielsweise in der Begründung zu § 44 Abs. 1 für die Vorgaben des Bundesamtes zur Informationssicherheit der Einrichtungen der Bundesverwaltung erfolgt.

Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen, § 40 BSIG

Aus § 40 insbesondere aus den Absätzen 3 und 4 lässt sich entnehmen, dass das Bundesamt bei erheblichen Sicherheitsvorfällen, die zwei oder mehr Mitgliedstaaten betreffen, verpflichtet ist, den Sicherheitsvorfall und die ihm aufgrund der Meldepflichten nach § 32 zugegangenen Informationen an die zuständigen Behörden der anderen betroffenen Mitgliedstaaten und an die ENISA weiterzuleiten. Zusammenfassend wäre dies so zu interpretieren, dass bei einem erheblichen Sicherheitsvorfall, der mehrere Mitgliedstaaten betrifft, nur Meldepflichten gegenüber dem Bundesamt oder einer anderen nationalen Behörde der betroffenen Mitgliedstaaten zu erfüllen sind. Die Notwendigkeit von Mehrfachmeldungen bei grenzüberschreitenden Sicherheitsvorfällen entfielen damit.

Für die nationalen Pflichten in einem anderen Mitgliedstaat wäre dort (für die ebenfalls betroffene dortige Geschäftseinheit) auf die Meldung an/durch das BSI zu verweisen. Es ist unbedingt zu vermeiden, dass in einem Krisenfall Ressourcen für das Meldewesen gebunden werden.

- ➔ In der Gesetzesbegründung sollte klargestellt werden, dass bei einem erheblichen Sicherheitsvorfall, der mehrere Mitgliedstaaten betrifft, Meldepflichten nur gegenüber *einer* nationalen Behörde der betroffenen Mitgliedstaaten zu erfüllen sind. Mehrfachmeldungen bei grenzüberschreitenden Sicherheitsvorfällen sind nicht notwendig. Langfristig sollten alle darauf hinwirken, die Meldepflichten europaweit zu vereinfachen und zu bündeln.

Ermächtigung zum Erlass von Rechtsverordnungen, § 58 BSIG

Die Verordnungsermächtigungen in § 58 bestimmen, dass die Definition eines „als bedeutend anzusehenden Versorgungsgrads anhand von branchenspezifischen Schwellenwerten“ durch das „etablierte Verfahren“ bestimmt werden soll (Seite 172 des Referentenentwurfs). Demnach soll es eine gemeinsame Verordnung zur Kategorisierung von Anlagen nach BSIG und KRITIS-Dachgesetz geben.

- ➔ Der DSLV spricht sich für einheitliche und klare Maßstäbe bei der Bestimmung der Schwellenwerte von wichtigen, besonders wichtigen und kritischen Einrichtungen aus und insbesondere die Hinweise in den Begründungen einheitlich zu gestalten. Die Beteiligung der Branchenverbände ist unbedingt zu gewährleisten, um ungeeignete, praxisfremde Schwellenwerte zu vermeiden.

Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen, § 66 BSIG

§ 66 erscheint zu unbestimmt und bedarf nach Ansicht des DSLV einer Einschränkung bzw. Klarstellung. In der vorliegenden Formulierung könnten bereits bloße oder unbestätigte Eindrücke oder Annahmen zu Durchsetzungsmaßnahmen und somit zu einer quasi vorsorglich verordneten Offenlegungspflicht führen.

- ➔ Gegebenenfalls sollte den Berteibern von betroffenen Einrichtungen vor Durchführung von Durchsetzungsmaßnahmen ausdrücklich Gelegenheit zur Stellungnahme gegeben werden.



Verbandsstruktur, Leistungsprofil und Leitlinien

Als Spitzen- und Bundesverband repräsentiert der DSLV durch 16 regionale Landesverbände die verkehrsträgerübergreifenden Interessen der 3.000 führenden deutschen Speditions- und Logistikbetriebe, die mit insgesamt 610.000 Beschäftigten und einem jährlichen Branchenumsatz in Höhe von 138 Milliarden Euro wesentlicher Teil der drittgrößten Branche Deutschlands sind (Stand: November 2023).

Die Mitgliederstruktur des DSLV reicht von global agierenden Logistikkonzernen, 4PL- und 3PL-Providern über inhabergeführte Speditionshäuser (KMU) mit eigenen LKW-Flotten sowie Befrachter von Binnenschiffen und Eisenbahnen bis hin zu See-, Luftfracht-, Zoll- und Lagerspezialisten.

Speditionen fördern und stärken die funktionale Verknüpfung sämtlicher Verkehrsträger. Die Verbandspolitik des DSLV wird deshalb maßgeblich durch die verkehrsträgerübergreifende Organisations- und Steuerungsfunktion des Spediteurs bestimmt.

Der DSLV ist politisches Sprachrohr sowie zentraler Ansprechpartner für die Bundesregierung, für die Institutionen von Bundestag und Bundesrat sowie für alle relevanten Bundesministerien und -behörden im Gesetzgebungs- und Gesetzumsetzungsprozess, soweit die Logistik und die Güterbeförderung betroffen sind.

Gemeinsam mit seinen Landesverbänden ist der DSLV Berater und Dienstleister für die Unternehmen seiner Branche. Als Arbeitgeberverbände und Sozialpartner vertreten die DSLV-Landesverbände die Branche in regionalen Tarifangelegenheiten.

Der DSLV ist Mitglied des Europäischen Verbands für Spedition, Transport, Logistik und Zolldienstleistung (CLECAT), Brüssel, der Internationalen Föderation der Spediteurorganisationen (FIATA), Genf, sowie assoziiertes Mitglied der Internationalen Straßentransport-Union (IRU), Genf. In diesen internationalen Netzwerken nimmt der DSLV auch Einfluss auf die Entwicklung des EU-Rechts in Brüssel und Straßburg und auf internationale Übereinkommen der UN, der WTO, der WCO, u. a.

Die Mitgliedsunternehmen des DSLV fühlen sich den Zielen der Sozialen Marktwirtschaft und der Europäischen Union verpflichtet.