Stellungnahme

zum Diskussionspapier zur Umsetzung der NIS-2 Richtlinie in Deutschland

(Diskussionspapier Bearbeitungsstand: 27. September 2023)

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: 20. Oktober 2023

Zum Diskussionspapier des BMI zur Umsetzung der NIS-2-Richtlinie in Deutschland nimmt der DSLV wie folgt Stellung:

Der Logistiksektor unterstützt das Ziel der NIS-2 Richtlinie, das Gesamtniveau der Cybersicherheit in der EU zu steigern. Das Diskussionspapier bewertet der Bundesverband Spedition und Logistik (DSLV) inhaltlich grundsätzlich positiv.

Nachweispflichten für Betreiber kritischer Anlagen, §§ 30, 31

Betreiber kritischer Anlagen haben die Erfüllung der Anforderungen nach § 30 Absatz 1 und § 31 dem Bundesamt für Sicherheit in der Informationstechnik (BSI) auf geeignete Weise nachzuweisen. Damit soll der bisherige § 8a BSIG fortgeführt werden. Dieser sieht jedoch unter Verweis auf § 8a Absatz 1 Satz 1 BSIG vor, dass das Schutzziel der Maßnahmen auf die „Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen“ abzielt. Die unter § 30 BSIG-E gelisteten Risikomanagementmaßnahmen stehen jedoch unspezifisch im Bezug zu den informationstechnischen Systemen, Komponenten und Prozessen, die sie für die „Erbringung ihrer Dienste“ nutzen. Diese Diskrepanz wird zu Unklarheiten bei der Umsetzung führen. Es bedarf daher einer genaueren Definition, was unter diesen Diensten zu verstehen ist.

Nach Verständnis des DSLV können im Falle der Kritis-Betreiber darunter nur die Dienste verstanden werden, die von der kritischen Anlage erbracht werden. Im Falle der Qualifizierung eines Unternehmens als „besonders wichtige Einrichtung“ ausschließlich aufgrund des Betriebs einer „kritischen Anlage“ gem. § 28 Abs. 1 Nr. 4 BSIG-E sollte daher auch nur der diese „kritische Anlage“ betreffende Unternehmensteil den speziellen Anforderungen an „besonders wichtige Einrichtungen“ unterliegen. Dies ist insbesondere vor dem Hintergrund sinnvoll, wenn die von der kritischen Anlage erbrachte Dienstleistung in keinem Zusammenhang mit den im sonstigen Kerngeschäft erbrachten Dienstleistungen der betroffenen Einrichtung stehen.

➔ Der Entwurf sollte insoweit konkretisiert werden, dass die Definition der „Erbringung von Diensten“ nur solche Dienste umfasst, die von der kritischen Anlage erbracht werden. Nur dieser Unternehmensteil der kritischen Anlage sollte dann auch den Anforderungen an besonders wichtige Einrichtungen unterliegen.

Die wesentlichen Unterschiede zwischen Betreibern besonders wichtiger und wichtiger Einrichtungen bestehen in Verpflichtungen zur Teilnahme am Informationsaustausch (nach § 6), sowie für Betreiber kritischer Anlagen in wiederkehrenden Nachweispflichten (nach § 39). 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 Anlagen (und darunter Betreiber kritischer Anlagen) wird in § 30 Absatz 9 ausdrücklich die Möglichkeit zur Einführung branchenspezifischer Sicherheitsstandards zur Gewährleistung der Anforderungen nach § 30 Absatz 1 vorgesehen. Offen bleibt demnach, inwiefern Betreiber wichtiger Einrichtungen ebenso ihre Übereinstimmung mittels

geeigneter Standards nachweisen können. Nach Ansicht des DSLV wäre letztlich der Nachweis der Übereinstimmung für Betreiber wichtiger Einrichtungen nur anlassbezogen erforderlich.

Für Betreiber sowohl besonders wichtiger wie auch wichtiger Einrichtungen ist eine Registrierungspflicht vorgesehen (§ 33). Nach Ansicht des DSLV sind als „Einrichtungen" die jeweiligen Unternehmen gemeint (ohne Einzelanlagen). Insbesondere bei international agierenden Konzernunternehmen stellt sich die Frage, ob nach Absatz 1 Nr. 2 geforderte Kontaktdaten in Deutschland sein sollen oder ein zentraler Kontakt bei der mit dem Betrieb und der Überwachung der IT-Systeme betrauten Stelle (in einem Konzernunternehmen) als Kontaktstelle fungieren kann. Nur letzteres erscheint sinnvoll, da grenzüberschreitend tätige Unternehmen zumeist über zentrale Systeme verfügen und Personal mit umfänglicher Kenntnis der Systemeigenschaften und -architektur in solchen zentralen Stabsfunktionen beschäftigt ist. Aus demselben Grund sollte die Kommunikation des BSI und an das BSI auch in Englisch erfolgen. Schon weil die NIS-2 in allen EU-Staaten in ähnlichen Pflichten für Unternehmen mündet, sind die zentrale Betreuung von Risikomanagementmaßnahmen, Meldepflichten und Englisch als Verkehrssprache aus Sicht des DSLV zwingend vorzusehen.

- ➔ Der Entwurf sollte klarstellen, dass die Kontaktstelle in Unternehmen nach § 33 Absatz 1 Nr. 2 sowie insbesondere Pflichten aus den §§ 30 bis 35 auch von den internationalen Zentralabteilungen von Konzern mit Niederlassungen in Deutschland wahrgenommen werden können. Englisch sollte gleichwertig zu Deutsch für die Kommunikation mit der nationalen Behörde vorgesehen werden.
- ➔ 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.

<u>Meldepflichten, § 32</u>

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 Rechtverordnung 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

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 § 60 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 überwachen hätten, macht deutlich, dass dies kein Beitrag zu einer ernsthaften und kohärenten Cybersicherheitsstrategie betreffender Unternehmen darstellt.

➔ 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 fällt. 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.

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 600.000 Beschäftigten und einem jährlichen Branchenumsatz in Höhe von 135 Milliarden Euro wesentlicher Teil der drittgrößten Branche Deutschlands sind (Stand: Juli 2022).

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.