Stellungnahme des Bundesverbands der Deutschen Luftverkehrswirtschaft (BDL)

zum Referentenentwurf des Bundesministeriums des Innern und für Heimat

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

Stand: 28. Mai 2024

A. Zusammenfassung

Der vorliegende Referentenentwurf dient der Umsetzung der NIS2-Richtlinie in Deutschland und enthält Regelungsentwürfen für wichtige Einrichtungen und besonders wichtige Einrichtungen im BSI-Gesetz. Die deutsche Luftverkehrswirtschaft begrüßt ausdrücklich die erneute Einbindung der Wirtschaft hinsichtlich der nationalen Umsetzung der NIS2-Richtlinie.

Die vom europäischen Gesetzgeber vorgegebene Einordnung, nach welcher nahezu alle deutschen Luftverkehrsunternehmen mindestens als „besonders wichtige Einrichtungen“ klassifiziert werden, wertet die Branche grundsätzlich und weiterhin als deutlich überzogen.

Der Luftverkehrssektor in Deutschland unterliegt bereits heute einer Vielzahl spezialrechtlicher Cybersicherheitsregulierungen, welche bislang kaum ineinandergreifen. Diese sind neben dem BSIG in jedem Fall die unmittelbar geltenden EU-Verordnungen 300/2008 (Security-Grundverordnung) sowie 2018/1139 (Safety-Grundverordnung). In den der NIS2-Richtlinie vorangestellten Erwägungsgründen (Nummer 29) heißt es, dass Luftverkehrseinrichtungen, die bereits von den genannten spezialrechtlichen Normen erfasst sind, als konform eingestuft werden können. Die Luftverkehrswirtschaft begrüßt, dass der Gesetzgeber der Anregung teilweise folgt, dieser Besonderheit nun Rechnung zu tragen, indem bereits vorliegende Nachweise zumindest zur Erfüllung von Nachweispflichten für Betreiber kritischer Anlagen nach NIS2UmsuCG berücksichtigt werden können. Gleichzeitig wird darum gebeten, die Anforderungen für eine derartige Befreiung weiter zu spezifizieren und beide in Erwägungsgrund 29 der NIS2-Richtlinie genannten Verordnungen ((EG) 300/2008 und (EU) 2018/1139) unmittelbar im Gesetzestext zu berücksichtigen.

Ebenso ist positiv zu bewerten, dass Unternehmen im Anwendungsbereich des NIS2UmsuCG zur Nachweiserbringung eine Frist von mindestens drei Jahren gewährt werden soll. Diese Fristsetzung orientiert sich an einem realistischen Zeitplan, der Unternehmen in die Lage, versetzt die rechtlichen Anforderungen adäquat umsetzen zu können.

Allerdings ergeben sich aus Sicht der Luftverkehrswirtschaft weiterhin grundsätzliche Zweifel an der Tauglichkeit der geplanten Risikomanagementmaßnahmen, welche unbedingt im Kontext bereits existierender Spezialgesetze den Luftverkehrssektor betrachtet werden sollten. Von der in der NIS2-

Richtlinie genannten Möglichkeit zur Harmonisierung bestehender Cybersicherheitsverpflichtungen bei Luftverkehrseinrichtungen sollte darum zwingend Gebrauch gemacht werden.

Weitere inhaltliche Bedenken zum vorliegenden Referentenentwurf ergeben sich zu folgenden Bereichen:

1. § 2 BSIG-E: Unklare Begriffsbestimmungen
2. § 28 BSIG-E: Qualifizierung des Gesamtunternehmens als „besonders wichtige Einrichtung“ bereits bei Betrieb einer „kritischen Anlage“ unverhältnismäßig
3. § 30 BSIG-E: Unpräzise Eingrenzung des zu betrachtenden Scopes
4. § 30 Abs. 6 BSIG-E: Cybersicherheitszertifizierung für Bestandsanwendungen nicht praxistauglich
5. § 32 BSIG-E: Kurze Meldefristen wirken zulasten der Vorfallsbehandlung
6. § 38 BSIG-E: Unklare Schulungspflichten für Geschäftsleiter
7. § 60 BSIG-E: Überschreitung der Bußgeldobergrenzen

B. Im Einzelnen

1. § 2 BSIG-E: Unklare Begriffsbestimmungen

Gemäß § 2 Abs. 1 BSIG-E ergeben sich Begriffsbestimmungen, die aus Sicht der Luftverkehrswirtschaft einer Klarstellung bedürfen.

Nach § 2 Abs. 1 Nr. 9 f. BSIG-E wird die Definition eines „erheblichen Sicherheitsvorfalls“ mit Kann-Bestimmungen in Verbindung gesetzt, wonach das Kriterium der Erheblichkeit nicht erfüllt würde. Die Definition bezieht sich außerdem allgemein auf Sicherheitsvorfälle und nicht spezifisch auf „Cyber“-Sicherheitsvorfälle, die jedoch zentraler Gegenstand des NIS2UmsuCG sind. Diese Unklarheit ist nicht auf die NIS2-Richtlinie rückführbar, da dort zwischen Sicherheitsvorfällen und Beinahe-Vorfällen unterschieden wird. Ebenso bezieht sich die Definition Nr. 38 „Sicherheitsvorfall“ des NIS2UmsuCG nur auf tatsächliche Beeinträchtigungen.

Um folgende Präzisierung gebeten:

§ 2 Abs. 1 Nr. 10

> *„erheblicher Cyber-Sicherheitsvorfall“ ein Sicherheitsvorfall, der*
>
> *a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat ~~oder verursachen kann;~~ oder*
>
> *b) andere natürliche oder juristische Personen durch erhebliche materielle oder im-materielle Schäden beeinträchtigt hat ~~oder beeinträchtigen kann,~~*
>
> *soweit nach Absatz 2 keine weitergehende Begriffsbestimmung erfolgt;*

Ferner wird durch § 2 Abs. 1 Nr. 21 BSIG-E der Begriff „kritische Anlage“ in das NIS2UmsuCG überführt. Die Ausgestaltung erfolgt in Referenz auf § 28 Abs. 7 i.V.m. § 58 Abs. 4 BSIG-E mittels einer Rechtsverordnung unter dem NIS2UmsuCG, dabei handelt sich um die bereits existierenden BSI-KritisV (vgl. Gesetzesbegründung S. 171 zu § 58 Abs. 4 BSIG-E).

Sobald eine Rechtsverordnung nach § 4 Abs. 4 KRITIS-DachG vorliegt ändert sich dieser Bezug entsprechend Art. 29 Abs. 2 i.V.m. Art. 2 NIS2UmsuCG: § 28 Abs. 7 sowie § 58 Abs. 4 BSIG-E werden gestrichen und die Begriffsbestimmung in § 2 Abs. 1 Nr. 21 BSIG-E referenziert fortan auf das KRITIS-DachG. Mit dieser Regelung soll sichergestellt werden, dass zu jedem Zeitpunkt immer jeweils nur eine Verordnung zur KRITIS Bestimmung Gültigkeit besitzt. Um sicherzustellen, dass auch während der derart ausgestalteten Übergangsphase bis zur gemeinschaftlichen Anwendung der neuen KRITIS-DachG-VO keine abweichende Bestimmung „kritischer Anlagen" erfolgt sollten die Definitionen des NIS2UmsuCG und des KRITIS-DachG aufeinander abgestimmt sein und sich außerdem an der bestehen BSI-KritisVO orientieren.

Im bekannten zweiten Entwurf des KRITIS-DachG (RefE-2 vom 21.12.2023, 17:05) bestanden noch die folgenden Problemstellungen, welche sich durch die oben beschriebene Referenz nun auch auf das NIS2UmsuCG beziehen:

Im KRITIS-DachG-E wird statt auf „erhebliche Versorgungsengpässe oder Gefährdungen" (vgl. BSIG & BSI-KritisVO) auf „langfristige Versorgungsengpässe oder Gefährdungen" abgestellt. Hier sollte einheitlich von „erhebliche Versorgungsengpässe oder Gefährdungen" gesprochen werden.

Die BSI-KritisVO referiert abstrakt auf „erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit. Dem gegenüber bezieht das KRITIS-DachG potenzielle „langfristige Versorgungsengpässe oder Gefährdungen" auf „wirtschaftliche Tätigkeiten, die öffentliche Sicherheit oder Ordnung, die öffentliche Gesundheit, wichtige gesellschaftliche Funktionen oder die Erhaltung der Umwelt". Dies entspricht den (neuen) Faktoren aus der CER-Richtlinie, kann aber vor allem auch in Verbindung mit § 4 KRITIS-DachG-E als Ausweitung betrachtet werden.

Aus Sicht der Luftverkehrswirtschaft ist diese Unklarheit zu beheben, damit die Referenz des NIS2UmsuCG auf das KRITIS-DachG nicht zu einer erneuten Ausweitung führt.

Abschließend ist anzumerken, dass auch für die Begriffsbestimmung „kritische Dienstleistung" nach § 2 Abs. 1 Nr. 23 BSIG-E der oben beschriebene Sachverhalt zutrifft und damit anzupassen ist.

2. § 28 BSIG-E: Qualifizierung des Gesamtunternehmens als „besonders wichtige Einrichtung" bereits bei Betrieb einer „kritischen Anlage" unverhältnismäßig

Bei der Qualifizierung als „besonders wichtige Einrichtung" sollte nur der Unternehmensteil, welcher eine "kritische Anlage" gemäß § 28 Abs. 1 Nr. 4 betreibt, den speziellen Anforderungen an „kritische Anlagen" unterliegen. Dabei ist zweifelsfrei sicherzustellen, dass die Beschaffenheit und der Betrieb der informationstechnischen Systeme, Komponenten und Prozesse, die das Unternehmen für die Erbringung der Dienste der kritischen Anlage nutzt, innerhalb des Gesamtbetriebs eindeutig abgrenzt sind. Anderenfalls wären die betroffenen Unternehmen gezwungen, Unternehmensteile, die Betreiber der „kritischen Anlage" sind, unternehmensrechtlich in ein verbundenes Unternehmen auszugliedern, um eine Betroffenheit des Gesamtunternehmens zu verhindern.

Erforderlich ist auch eine Klarstellung, welche Anforderungen bei Unternehmen, die sowohl „kritische Anlagen" betreiben sowie Konzernteile, die aufgrund anderer Geschäftsaktivitäten als „besonders wichtige" respektive „wichtige Einrichtungen" einzustufen wären, einschlägig sind. Vor allem angesichts des fehlenden spezifischen Bezuges der Risikomanagementmaßnahmen nach § 30 BSIG-E auf die „kritische Anlage" ist diese Ausdifferenzierung notwendig. Es sollte ausschließlich aufgrund des

Betriebs einer „kritischen Anlage“ gemäß § 28 Abs. 6 BSIG-E auch nur der diese „kritische Anlage“ betreffende Unternehmensteil den speziellen Anforderungen an „besonders wichtige Einrichtungen“ nach § 31BSIG-E unterfallen. 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. Es muss sichergestellt werden, dass (besonders) „wichtigen Einrichtungen“ durch den Betrieb einer „kritischen Anlage“ regelmäßig kein unverhältnismäßiger Mehraufwand entsteht. Diese Klarstellung ist auch im Hinblick auf die Bußgeldvorschriften nach § 61 BSIG-E notwendig.

Auch hinsichtlich § 28 Abs. 3 i.V.m. § 2 Abs. 1 Nr. 12 und § 38 BSIG-E sollte der Bezug klarer formuliert werden. So wird darum gebeten, im Falle einer Aktiengesellschaft oder Holding nur der eigentlich betroffene Unternehmensteil – welcher die relevante (kritische) Dienstleistung erbringt –angesprochen wird.

3. § 30 BSIG-E: Unpräzise Eingrenzung des zu betrachtenden Scopes

Aus Sicht der Luftverkehrswirtschaft ist die in § 30 Abs. 1 BSIG-E vorgenommene Eingrenzung des zu betrachtenden Scopes unpräzise und umfassender als durch die NIS2-Richtlinie vorgegeben. So ist gemäß der NIS2-Richtlinie eine Beherrschung von Risiken für die Erbringung der Dienste vorgesehen, während im derzeitigen Entwurf des NIS2UmsuCG auf die Vermeidung von Störungen (und die Verringerung von Auswirkungen) referenziert wird. Folglich fehlt ein qualifizierender Faktor, wonach die Störung überhaupt Relevanz für die Diensterbringung hat und es somit ein zu beherrschendes Risiko gibt.

Bei besonders wichtigen Einrichtungen sollte sich der Scope der betroffenen IT-Systeme deutlich auf die zur Erbringung der Dienstleistung erforderlichen Anlagen beziehen. Die aktuelle Formulierung könnte so interpretiert werden, dass auch „Support-Prozesse“ und Informationsportale (z. B. Lohnabrechnung, Onboarding, digitale Speisepläne) zu berücksichtigen sind, weil sie für die Mitarbeiter, welche die Dienstleistung erbringen, benötigt werden.

Im Sinne des risikobasierten Ansatzes sollte die Umsetzung und Auswahl von verhältnismäßigen und wirksamen Risikomanagementmaßnahmen dadurch verbessert werden, dass eine noch stärkere Orientierung an den Anforderungen entlang der NIS2-Richtlinie erfolgt. Die inhaltliche Abweichung zwischen Art. 21 Abs. 1 NIS2-Richtlinie zur Beherrschung von Risiken und § 30 Abs. 1 BSIG-E zur Vermeidung von Störungen sollte im Sinne der Rechtsklarheit und der europäischen Harmonisierung in § 30 Abs. 1 BSIG-E behoben werden.

4. § 30 Abs. 6 BSIG-E: Cybersicherheitszertifizierung für Bestandsanwendungen nicht praxistauglich

Gemäß § 30 Abs. 6 BSIG-E wird dem Gesetzgeber die Möglichkeit zur Festlegung verpflichtender Cybersicherheitszertifizierungen, auch für Bestandsanwendungen, eröffnet. Zwar haben die Mitgliedsstaaten nach der NIS2-Richtlinie die Option eine solche verpflichtende Zertifizierung vorzusehen, es ist jedoch anzuzweifeln, ob die umfassende Ermächtigung im NIS2UmsuCG notwendig und zielführend ist. Besonders da weder Regeln zur Anhörung betroffener Kreise noch zu Übergangszeiten oder möglichen Entschädigungszahlungen vorgesehen sind. Eine Cybersicherheitszertifizierung für IKT-Produkte, IKT-Dienste und IKT-Prozesse für besonders wichtige Einrichtungen und wichtige

Einrichtung zu verlangen ist praxisfern und nur sehr eingeschränkt umsetzbar. So beauftragen Unternehmen der Luftverkehrswirtschaft z. B. zunehmend Dienstleister zur Erbringung bestimmter Aufgaben, bei denen sie keinen Einfluss auf deren Cybersicherheitszertifizierung bzw. deren eingesetzte Systeme und ohnehin kein Durchgriffsrecht haben. Über dies würden sich durch Rezertifizierungen (bspw. bei älterer Bestandsinfrastruktur ohne Cybersicherheitszertifikat) oder durch Neubeschaffungen unverhältnismäßig hohe Beschaffungskosten und Vorlaufzeiten ergeben.

Für Bestandsinfrastrukturen, welche z. B. seit mehr als zehn Jahren im Einsatz sind und Hersteller weder eine Cybersicherheitszertifizierung vorlegen oder entsprechende Zertifizierung durch das BSI negativ beschieden wird, ist das mit unverhältnismäßigen Kosten und mit sehr hohen Vorlaufzeiten verbunden.

Für Unternehmen, welche spezialgesetzlich bereits umfassend reguliert sind, z. B. entsprechend der Luftfahrt-Grundverordnung EU (DVO) 2018/1139, sollte außerdem auf eine zusätzliche Zertifizierung über Cybersicherheitszertifizierungsschemata nach dem EU Cybersecurity Act verzichtet werden.

Im Kontext der Risikomanagementmaßnahmen gemäß § 30 NIS2UmsuCG sollte zudem unbedingt die bereits existierende Regulierungslandschaft für den Luftfahrtsektor Berücksichtigung finden. Das NIS2UmsuCG sollte daher die in der NIS2-Richtlinie genannte Möglichkeit zur Harmonisierung bestehender Cybersicherheitsverpflichtungen bei Luftverkehrseinrichtungen aufgreifen (vgl. Erwägungsgrund 29). Im Anwendungsbereich der NIS2-Richtlinie liegende Unternehmen in der Luftverkehrswirtschaft (u. a. Luftfahrtunternehmen, Flughäfen) müssen bereits vergleichbare Anforderungen (siehe Cybersicherheitsmaßnahmen nach der DVO (EU) 2019/1583 oder nach DVO (EU) 2018/1139 bzw. nachfolgend PART-IS) erfüllen, unabhängig davon, ob sie bisher in den Wirkungsbereich der geltenden BSI-KritisVO fallen. Das BSI sollte prüfen können, ob diese Anforderungen und die darin enthaltenen Vorgaben gleichwertig zu denen des NIS2UmsuCG sind. Sollte dies der Fall sein, sind Doppelstrukturen und -anforderungen zwingend zu vermeiden. Eine derartige Regelung könnte vergleichbar zu jener die branchenspezifischen Sicherheitsstandards betreffend unter § 30 Abs. 12 BSIG-E geschaffen werden.

5. § 32 BSIG-E: Kurze Meldefristen wirken zulasten der Vorfallsbehandlung

Mit dem NIS2UmsuCG sollen umfangreiche Meldepflichten eingeführt werden. Dabei ist jedoch unbedingt zu berücksichtigen, dass die Meldepflichten und Wege des NIS2UmsuCG und des KRITISDachG aufeinander abgestimmt sind und keine Doppelstrukturen entstehen. Ferner sollte für Vorfallsmeldungen entsprechend § 32 BSIG-E für Betreiber kritischer Anlagen das bestehende BSI-Melderegime weiter genutzt werden können.

Um die Anforderungen für die betroffenen Unternehmen beherrschbar zu halten, sollte außerdem die Identifikation der zu meldenden Vorfälle verbessert werden: Entsprechend § 32 Abs. 1 BSIG-E hat die Erstmeldung bei einem erheblichen Sicherheitsvorfall innerhalb von 24 h nach Kenntnisnahme zu erfolgen. Dies sollte nur für die Systeme gelten, die für die Erbringung der Dienstleistung relevant sind. Angesichts der derzeit noch unzureichenden Definition „erheblicher Sicherheitsvorfälle“, welche derzeit ebenfalls Beinahe-Vorfälle umfasst, sollte außerdem die nach Art. 23 Abs. 1 Satz 1 NIS2-Richtlinie erfolgte Klarstellung übertragen werden, dass nur solche Vorfälle zu berichten sind, bei denen tatsächlich eine erhebliche Auswirkung auf die Erbringung der Dienste festzustellen war.

6. § 38 BSIG-E: Unklare Schulungspflichten für Geschäftsleiter

Die NIS2-Richtlinie sieht umfangreiche Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen vor. Anders als im NIS2UmsuCG ist dort jedoch keine entsprechende Regelung hinsichtlich eines Verzichts oder Vergleichs enthalten, § 38 Abs. 2 BSIG-E sollte daher ersatzlos gestrichen werden.

Vor allem sind jedoch weitere Klarstellungen hinsichtlich der Möglichkeiten der Delegation der Umsetzung der Anforderungen aus § 30 BSIG-E und der Schulungspflichten erforderlich. Gerade aus Sicht einer Konzernstruktur sind die Anforderungen in § 38 i.V.m. § 2 Abs. 1 BSIG-E (Definition einer Geschäftsleitung) als praxisfern zu betrachten. Dies gilt im Besonderen auch für die Schulungspflichten – da die Geschäftsleitung üblicherweise nicht in die Abwicklung des operativen Tagesgeschäfts eingebunden ist, sollte die unbedingt die Möglichkeit gegeben sein, alternativ auch nachgelagerte Führungsebenen in Vertretung für die Geschäftsleitung schulen zu können.

7. § 60 BSIG-E: Überschreitung der Bußgeldobergrenzen

Mit dem in § 60 enthaltenen Verweis auf das Ordnungswidrigkeitengesetz sieht der Gesetzgeber eine Verzehnfachung der Bußgeldhöhe vor, wodurch er in nicht akzeptablem Maße die in der NIS2-Richtlinie enthaltenen Bußgeldobergrenzen für die Unternehmen der Luftverkehrswirtschaft signifikant überschreitet.

Die deutsche Luftverkehrswirtschaft erachtet Bußgelder grundsätzlich als probates Mittel, um die Beachtung und Implementierung von gesetzlichen Anforderungen zu forcieren. Gleichwohl müssen Bußgelder stets angemessen sein. Die eklatante Überschreitung des EU-weit vorgesehenen Bußgeldrahmens im NIS2UmsuCG sollte nichtsdestotrotz zwingend gestrichen werden, da deutsche Luftverkehrsunternehmen in ungerechtfertigt hohem Maße im Verhältnis zu Wettbewerbern im EU-Ausland benachteiligt werden.

Bundesverband der Deutschen Luftverkehrswirtschaft e. V. (BDL)
Haus der Luftfahrt | Friedrichstraße 79 | 10117 Berlin

Der Bundesverband der Deutschen Luftverkehrswirtschaft (BDL) wurde 2010 als gemeinsame Interessenvertretung der deutschen Luftverkehrswirtschaft gegründet. Mitglieder des Verbandes sind Fluggesellschaften, Flughäfen, die Deutsche Flugsicherung und weitere Leistungsanbieter im deutschen Luftverkehr.