BDL
Bundesverband der Deutschen Luftverkehrswirtschaft

07/2025

Stellungnahme des Bundesverbands der Deutschen Luftverkehrswirtschaft (BDL)

zum Referentenentwurf des Bundesministeriums des Innern und für Heimat

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

Stand: 4. Juli 2025

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. Von der in der NIS2-Richtlinie genannten Möglichkeit zur Harmonisierung bestehender Cybersicherheitsverpflichtungen bei Luftverkehrseinrichtungen sollte Gebrauch gemacht werden und die Ergebnisse der begrüßenswerten aktuellen europäischen Harmonisierungsbestrebungen in diesem Sektor aufgenommen werden. Auch bzgl. der Meldepflichten zu Cybersicherheitsvorfällen, die sich aus der NIS-2 und den spezialrechtlichen Regeln ergeben, wäre eine weitere Harmonisierung und Zentralisierung der Meldestellen wünschenswert.

Große Bedenken verursacht auch die Abkehr von einer abgestimmten Veröffentlichung des NIS2UmsuCG und des die CER-Richtlinie umsetzenden KRITIS-Dachgesetz (KRITIS-DG). Hier sind uneinheitlichen KRITIS-Definitionen und Geltungsbereiche zu befürchten, die zu einem signifikanten Mehraufwand in den betroffenen Unternehmen führen würden.

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
   § 28 Abs. (3) BSIG-E: unklarer Rechtsbegriff „geringfügiger Nebentätigkeiten“
3. § 30 BSIG-E: Unpräzise Eingrenzung des zu betrachtenden Scopes
4. § 30 Abs. 6 BSIG-E: Cybersicherheitszertifizierung für Bestandsanwendungen nicht praxistauglich
   § 30 BSIG: Weitere Harmonisierung Risikomanagementmaßnahmen für Sektor
5. § 32 BSIG-E: VorfallsbehandlungMeldepflichten entsprechend Schutz und Regelungsziel
6. § 38 BSIG-E: Unklare Schulungspflichten für Geschäftsleiter
7. § 56 Ermächtigung zum Erlass von Rechtsverordnungen; Anhörung der Wirtschaftsverbände
8. § 60 BSIG-E: Überschreitung der Bußgeldobergrenzen

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.

Die **Gesetzesbegründung zu § 2 Abs. 1 Nr. 26 „Managed Service Betreiber“** (MSP) führt aus, dass ein bestimmter Kundenkreis keine Voraussetzung für die Einstufung als MSP sei und somit auch Unternehmen unter den Begriff und somit den Anwendungsbereich des Gesetzes fallen könnten, die ausschließlich den zentralen IT-Betrieb eines Unternehmensverbundes übernehmen. Verbunden mit den Änderungen in § 28 Abs. (3) & (4) ist diese Auslegung kritisch zu sehen und könnte zu einer deutlichen Ausweitung der Betroffenheit führen. Ohne die Möglichkeit der Abstellung auf die zuzuordnende Geschäftstätigkeit(en) des Unternehmensverbundes könnte somit ein wesentlicher Anteil von Unternehmen alleinig angesichts des zentralen IT-Betrieb als besonders wichtige Einrichtung erfasst werden. Konzerninterne IT-Dienstleistungen sollten regulatorisch im Kontext des Gesamtkonzerns betrachtet werden. Eine zentrale IT sollte daher betrachtet werden, wenn das Verbundunternehmen einem der kritischen Sektoren zuzuordnen ist.

Nach **§ 2 Abs. 1 Nr. 11** 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. 40 „Sicherheitsvorfall“ des NIS2UmsuCG nur auf tatsächliche Beeinträchtigungen.

Um folgende Präzisierung gebeten:

> *„erheblicher Cyber-Sicherheitsvorfall“ ein Sicherheitsvorfall, der*
>
> *a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder*
>
> *b) andere natürliche oder juristische Personen durch erhebliche materielle oder im-materielle Schäden beeinträchtigt hat,*

soweit nach Absatz 2 keine weitergehende Begriffsbestimmung erfolgt;

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. 1 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. 8 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. 4 i.V.m. § 2 Abs. 1 Nr. 13 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. § 28 Abs. (3) BSIG-E: unklarer Rechtsbegriff „geringfügiger Nebentätigkeiten“

Der Versuch des Gesetzgebers durch die in § 28 Abs. (3) vorgenommene Ergänzung zu vermeiden, dass geringfügige Nebentätigkeiten zu einer unverhältnismäßigen Identifizierung als wichtige oder besonders wichtige Einrichtung führen könnten ist begrüßenswert. Jedoch könnte er für bereits betroffene Einrichtungen zu vermeidbaren Zusatzaufwänden führen, da selbst bei eindeutiger Betroffenheit zusätzliche „vernachlässigbare Geschäftsbetriebe“ zu identifizieren wären. Hinzu kommt, dass derzeit kein einheitliche Auslegung „vernachlässigbarer Geschäftsbetriebe“ besteht. Eine weitere Klarstellung des derzeit unklaren Rechtsbegriffes „vernachlässigbare Geschäftsbetriebe“ und die folgende Ergänzung ist daher erforderlich:

§ 28 Abs. (3) BSIG-E

> *Bei der Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 können solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind. Wurde eine Einrichtung bereits als besonders wichtige Einrichtungen oder wichtige Einrichtungen registriert, so kann die Betrachtung „vernachlässigbare Geschäftsbetriebe“ unterbleiben.*

In diesem Sinne sollte sich auch für die Bestimmung hinsichtlich der Schwellenwerte die Zuordnung der Einrichtung auf die Geschäftstätigkeit(en) für die eine Registrierung erfolgen soll, weiterbestehen und die Formulierung unter § 28 Abs. (4) Nr. 1 wiederaufgenommen werden:

(4) Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nach den Absätzen 1 und 2 ist auf

1. die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen und könnte außerdem auch Verbundunternehmenregelung negativ beeinflussen.

4. § 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.

5. § 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.

6. § 30 BSIG: Weitere Harmonisierung Risikomanagementmaßnahmen für Luftfahrtsektor

Auch im Kontext der Risikomanagementmaßnahmen gemäß § 30 NIS2UmsuCG sollte zudem 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 NIS2-UmsuCG sollte daher die in der NIS-2-Richtlinie genannte Möglichkeit zur Harmonisierung bestehender Cybersicherheitsverpflichtungen bei Luftverkehrseinrichtungen aufgreifen (vgl. Erwägungsgrund 29 NIS2) bzw. die Ergebnisse der begrüßenswerten Harmonisierungsbestrebungen in diesem Sektor auf europäischer Ebene aufnehmen.

§ 32 BSIG-E: Meldepflichten entsprechend Schutz und Regelungsziel

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.

7. § 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.

Die vorgenommen Änderungen sind zu begrüßen, da nun im Gesetzestext ein klarer Verweis auf die gesellschaftsrechtlichen Bestimmungen besteht. Dennoch sind 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. Es muss mindestens die Freiheit bestehen, Schulungen in Umfang, Dauer und Inhalt entsprechend der operativen Rolle im Unternehmen anpassen zu können.

8. § 56 Ermächtigung zum Erlass von Rechtsverordnungen; Anhörung der Wirtschaftsverbände

Es ist zwingend erforderlich, dass die Wirtschaftsverbände bei der Entwicklung von Rechtsverordnungen, die die Wirtschaft betreffen, angehört werden. Die Anhörung trägt erheblich dazu bei, dass rechtliche Vorgaben möglichst praxistauglich ausgestaltet sind.

Den vom Bundesministerium des Innern im Gesetzgebungsverfahren mehrfach vorgetragenen Verweis auf die Geschäftsordnung der Bundesregierung, nach der Anhörungen von Verbänden grundsätzlich vorgesehen sind, erachten wir als nicht ausreichend. Zumal die Anhörung im aktuellen Entwurf uneinheitlich geregelt ist, § 56 Abs. 1 & 2 fordern eine Anhörung, in den für die Wirtschaft besonders wichtigen Abs. 3-5 ist keine Anhörung im Gesetzestext verankert. Die Anhörung von Verbänden sollte einheitlich in den einschlägigen Fachgesetzen verpflichtend verankert werden. Dies ist insbesondere auch hinsichtlich der nun unabgestimmten Umsetzung der NIS-2-Richtlinie und der CER-Richtlinie erforderlich, die absehbar zu zwei parallelen KRITIS-VO führen wird.

9. § 65 BSIG-E: Überschreitung der Bußgeldobergrenzen

Mit dem in § 65 Abs. (5) BSIG-E enthaltenen Verweis auf das Gesetz über Ordnungswidrigkeiten (OWiG) 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.

Kontakt

Dr. Isabel Weiß
Leiterin Security

Isabel.weiss@bdl.aero
+49 30 520 077-125

Bundesverband der Deutschen Luftverkehrswirtschaft e. V. (BDL)
Haus der Luftfahrt / Friedrichstraße 79 / 10117 Berlin / www.bdl.aero

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.