VERBAND DEUTSCHER REEDER • BURCHARDSTRASSE 24 • 20095 HAMBURG

Per E-Mail

Bundesministerium des Innern und für Heimat
Referat CI 1 Grundsatz; Cyber- und Informationssicherheit
Dr. Daniel Meltzian,
Alt-Moabit 140
10557 Berlin

Verband
Deutscher
Reeder

ANSCHRIFT
Burchardstr. 24
D-20095 Hamburg

TELEFON
+49.40.35097-0

WWW
reederverband.de

Hamburg,
30.06.2025

vdr@
reederverband.de
Durchwahl -235

Referentenentwurf für ein Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung - Stellungnahme des Verbands Deutscher Reeder (VDR)

Sehr geehrter Herr Dr. Meltzian
sehr geehrte Damen und Herren,

wir danken Ihnen für die erneute Möglichkeit zur Stellungnahme zum Referentenentwurf für ein Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz). Gerne möchten wir diese Gelegenheit nutzen und nochmalig auf einige u.E. wesentliche Punkte hinweisen, die es bei den Regelungen zur Umsetzung der NIS-2-Richtlinie für den Bereich der Seeschifffahrt aber auch im Allgemeinen zu berücksichtigen gilt.

Diese fassen wir wie folgt zusammen:

- Keine Erfassung einzelner Schiffe
- Keine Anknüpfung an den ISM-Manager
- Differenzierung zwischen dispositiv tätigen Reedereien und bloßen Eignern
- Konzentration auf landseitige IT-Infrastruktur
- Klare Berücksichtigung international bestehender Standards (ISM, ISPS, BSI-Profile)
- Fehlende Übergangsfrist bzw. zu kurze Vorlaufzeit
- Fehlende Verzahnung mit dem KRITIS-Dachgesetz

1. Einordnung der Seeschifffahrt in den Geltungsbereich

Die Seeschifffahrt ist ein hochgradig internationaler und arbeitsteilig organisierter Sektor. Die überwiegende Zahl deutscher Reedereien betreibt keine eigene Liniendienste, sondern verchartert ihre Schiffe an sogenannte „Commercial Operator“, die dann für die operative Einsatzplanung und Ladungsdisposition verantwortlich sind.
Die Definition in Anlage 1 Nr. 2.3.1 des Referentenentwurfs, die auf "*Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt*" abstellt, ist in dieser Form daher zu weit gefasst. Sie differenziert nicht zwischen Reedereien mit dispositiver Steuerung und solchen, die lediglich Eigner oder Vercharterer sind. Wir empfehlen daher eine sachgerechte Eingrenzung, beispielsweise wie folgt:

"*Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, welche eine Anlage oder ein System zur operativen Steuerung von Seeschiffen nach einem festen Fahrplan oder zur Disposition des Schiffsraums von solchen Seeschiffen betreiben.*"

Diese Formulierung würde sicherstellen, dass nur solche Unternehmen erfasst werden, deren Ausfall erhebliche Auswirkungen auf die Versorgungssicherheit entfalten könnte.

2. Klare Abgrenzung zu ISM-/ISPS-Code und Ausschluss einzelner Schiffe

Die Cybersicherheit in der internationalen Seeschifffahrt unterliegt bereits umfassenden und verbindlichen Regelwerken, die gezielt auf die besonderen Risiken im Schiffsbetrieb zugeschnitten sind. Dazu zählen insbesondere:

- **ISM-Code (International Safety Management Code)**: Verlangt von ISM-Managern die Implementierung eines Sicherheitsmanagementsystems, das auch Maßnahmen zum Schutz vor Cyberangriffen einschließt. Die Umsetzung wird regelmäßig im Rahmen sogenannter "Office-Audits" durch den Flaggenstaat oder dessen beauftragte Organisationen kontrolliert https://www.deutsche-flagge.de/de/sicherheit/ism-code).
- **ISPS-Code (International Ship and Port Facility Security Code)**: Regelt den physischen Schutz von Schiffen und Hafenanlagen. Unternehmen müssen einen Company Security Officer (CSO) benennen, der für die Durchführung von Gefährdungsanalysen, die Ausarbeitung von Gefahrenabwehrplänen sowie deren Umsetzung verantwortlich ist. Diese Pläne müssen von den Flaggenstaaten genehmigt werden und unterliegen regelmäßiger Überwachung (https://www.deutsche-flagge.de/de/sicherheit/isps).
- **BSI-Grundschutzprofile**: In Deutschland existieren branchenspezifische IT-Grundschutzprofile des BSI für den Schiffsbetrieb und für landseitige Verwaltungsstandorte, die von Reedereien und ISM-Managern bereits angewendet werden (https://www.deutsche-flagge.de/de/sicherheit/ism-code/maritime-security).
- **Branchenspezifische Richtlinien**: Die international anerkannten "Guidelines on Cyber Security Onboard Ships" (ICS, BIMCO, IUMI, etc.) stellen den Stand der Technik für den maritimen Sektor dar und werden von Schiffsversicherern und Flaggenstaaten weltweit empfohlen. (https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf).

Diese etablierten Sicherheitsstandards sichern bereits heute das IT-Risiko einzelner Schiffe ab. Die zusätzliche Anwendung der Anforderungen aus dem NIS-2-Umsetzungsgesetz auf einzelne Schiffe wäre somit nicht nur redundant, sondern auch systematisch verfehlt.
Wir begrüßen daher ausdrücklich, dass einzelne Schiffe gemäß Anlage 1 Nr. 2.3.1 vom Geltungsbereich ausgenommen sind. Diese Klarstellung ist sachgerecht, da die Schiffe selbst bereits durch die genannten Sicherheitsregime abgesichert sind.

Die NIS-2-Pflichten müssen sich daher ausschließlich auf den Landbetrieb und zentrale IT-Infrastrukturen der relevanten Unternehmen aus dem Bereich der Schifffahrt beziehen, nicht auf einzelne Schiffe als abgrenzbare Einheiten.

3. Widerspruch: Anknüpfung an den ISM-Manager

Unabhängig von der allgemeinen Geltungsbereichsdefinition stellt sich im Gesetz die konkrete Frage, an welche Organisationseinheit innerhalb eines Unternehmens rechtlich angeknüpft wird.
Der Entwurf orientiert sich zur Bestimmung der betroffenen Unternehmen im Bereich der Seeschifffahrt an der Definition in Anhang I der Verordnung (EG) Nr. 725/2004 und damit mittelbar an der SOLAS-Definition für den "ISM-Manager". Diese Anknüpfungsentscheidung ist aus Sicht der Praxis widersprüchlich und verfehlt den Zweck der NIS-2-Richtlinie.

Der ISM-Manager ist ein technischer Betreiber im Sinne des Schiffsbetriebs, nicht jedoch für dispositive Steuerungsaufgaben oder kritische (Land) IT-Infrastruktur verantwortlich. In vielen Fällen wird diese Rolle von externen Dienstleistern außerhalb der EU wahrgenommen. Eine solche Struktur eignet sich daher nicht für die Durchsetzung von Sicherheits- und Meldepflichten nach dem NIS-2-Regime.
Die Anknüpfung sollte sachgerecht stattdessen an den Commercial Operator erfolgen, also auf das Unternehmen, das tatsächlich über IT-Infrastruktur für Flottensteuerung und, Routen- & Ladungsdisposition verfügt und damit sicherheitsrelevant im Sinne des NIS-2-Regimes ist. Dies entspricht auch der von uns unter Punkt 1 vorgeschlagenen sachgerechten Definition für den Geltungsbereich, die dispositiv tätige Unternehmen gezielt adressiert.

4. Fehlende Übergangsfrist bzw. zu kurze Vorlaufzeit

Zu guter Letzt möchten wir mit dem Fehlen jeglicher Übergangsfristen im aktuellen Entwurf einen aus unserer Sicht besonders kritischen Punkt ansprechen. Der vorliegende Entwurf sieht eine unmittelbare Inkraftsetzung aller vorgesehenen Regelungen vor, die teilweise einen erheblichen Erfüllungsaufwand für die betroffenen Unternehmen mit sich bringen. Zwar ergibt sich dies letztlich aus den Vorgaben der EU-NIS-2-Richtlinie, die am 27.12.2022 im Amtsblatt L333 der Europäischen Union veröffentlicht worden und am zwanzigsten Tag nach ihrer Veröffentlichung in Kraft getreten ist. Die Mitgliedstaaten müssen die Richtlinie innerhalb von 21 Monaten nach ihrem Inkrafttreten in nationales Recht umsetzen. Eine frühere gesetzgeberische Umsetzung in Deutschland hätte allerdings eine angemessene Frist zur Vorbereitung und Umsetzung für die betroffenen Unternehmen ermöglicht.

Vor dem Hintergrund der bestehenden Herausforderungen in Sachen Erfüllungsaufwand erachten wir es für äußerst problematisch, dass der Wirtschaft keine ausreichende Vorlaufzeit für die Erfüllung der teils sehr umfassenden zusätzlichen Anforderungen eingeräumt wird. In den Erläuterungen auf Seite 118 des Entwurfs wird ausgeführt, dass rund 2.950 besonders wichtige Einrichtungen und rund 17.900 wichtige Einrichtungen einem erheblichen Erfüllungsaufwand unterliegen werden. Die Kalkulation geht dabei von einem geschätzten Aufwand von 1.100 Stunden für wichtige Einrichtungen und 2.752 Stunden für besonders wichtige Einrichtungen aus, wie in der Tabelle auf Seite 118 dargestellt.

Angesichts der aktuellen Situation auf dem Arbeitsmarkt, insbesondere der knappen Verfügbarkeit von IT-Security-Spezialisten, ist die Umsetzung der erforderlichen Maßnahmen innerhalb eines Jahres bereits als äußerst ambitioniert, wenn nicht gar illusorisch zu betrachten. Die betroffenen Unternehmen benötigen eine realistische Zeitspanne, um die geforderten Maßnahmen adäquat umsetzen zu können. Eine entsprechende Übergangsfrist ist somit unumgänglich, um die Einhaltung der neuen Regelungen sicherstellen zu können und um gleichzeitig die wirtschaftliche Stabilität und operative Kontinuität der betroffenen Einrichtungen zu gewährleisten.

5. Fehlende Verzahnung mit dem KRITIS-Dachgesetz

Kritisch ist zu sehen, dass der vorliegende Entwurf im Vergleich zur Vorversion aus dem Jahr 2024 die ursprünglich vorgesehene Verzahnung mit dem KRITIS-Dachgesetz (KRITIS-DachG) weitgehend aufgibt. Dieses Gesetz zur Umsetzung der Resilienz-Richtlinie zielte gemeinsam mit der NIS-2-Umsetzung auf ein abgestimmtes Regelungssystem für besonders sensible Einrichtungen.
Im Referentenentwurf 2024 war vorgesehen, zentrale Regelungsbereiche – wie Meldepflichten, Nachweisverfahren und Aufsichtsstrukturen – zwischen beiden Gesetzen zu synchronisieren. Im aktuellen Entwurf vom Juni 2025 finden sich dazu keine ausdrücklichen Bezüge mehr. Stattdessen erscheinen die Vorschriften nun isoliert und sektorspezifisch, ohne sektorübergreifende Anschlussfähigkeit.
Dies steht aus unserer Sicht im Widerspruch zum Ziel, den bürokratischen Aufwand zu reduzieren und Unternehmen mit mehrfacher Relevanz (z. B. NIS-2 und KRITIS-DachG) nicht

mit doppelten Pflichten und Verfahren zu belasten. Wir empfehlen daher nachdrücklich, die ursprünglich beabsichtigte Systemharmonisierung wiederaufzunehmen.

Für Rückfragen stehen wir selbstverständlich jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen
VERBAND DEUTSCHER REEDER