GDV Gesamtverband der Versicherer

Stellungnahme

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
Lobbyregister-Nr. R000774

zum Referentenentwurf des Bundesministeriums des Innern:
Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

Inhalt

1. Zusammenfassung 2

2. Einleitung 2

2.1 Zu § 28 NIS-2-Umsetzunggesetz (Besonders wichtige und wichtige Einrichtungen): Besonderheit der unternehmenseigenen bzw. gruppeninternen IT-Dienstleister in der Versicherungswirtschaft 2

2.2 Zu § 28 Absatz 7 NIS-2-Umsetzungsgesetz (Besonders wichtige und wichtige Einrichtungen): Ausnahmeregelung 3

GDV

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, D-10002 Berlin
Telefon: +49 30 2020-5000 · Telefax: +49 30 2020-6000
Lobbyregister-Nr. R000774

Rue du Champ de Mars 23, B-1050 Brüssel
Telefon: +32 2 28247-30 · Telefax: +49 30 2020-6140
ID-Nummer 6437280268-55
www.gdv.de

Ansprechpartner
Betriebswirtschaft, IT und Prozesse

E-Mail
bdit@gdv.de

2.3 Zu § 38 BSI-Gesetz (Geschäftsleiterhaftung) 4

1. Zusammenfassung

Die deutsche Versicherungswirtschaft begrüßt das Vorhaben der Bundesregierung, die Cyberresilienz in Deutschland weiter zu stärken. Auch wenn Versicherungsunternehmen von der nationalen Umsetzung der NIS-2-Richtlinie nicht erfasst sind, besteht weiterhin die Gefahr einer Doppelregulierung.

Dies betrifft Teile der Versicherungskonzernstruktur (hier: gruppeninterne IT-Töchter), die weiterhin in den Anwendungsbereich fallen sollen. Wir regen daher an, dass gruppeninterne IT-Töchter konsequenterweise komplett ausgenommen werden, zumindest aber von den Meldeverpflichtungen nach §32.

2. Einleitung

Durch den Digital Operational Resilience Act (DORA: Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor) unterliegen Versicherungsunternehmen bereits umfassenden Vorgaben bzgl. der weiteren Stärkung der Cybersicherheit – z. B. Melde- und Nachweispflichten. Zur Vermeidung von Doppelregulierung hat der Europäische Gesetzgeber daher eine lex-specialis-Regelung in DORA aufgenommen. Die Versicherungsunternehmen sollen als Finanzunternehmen im Sinne von Art. 2 Abs. 2 der DORA-Verordnung entsprechend von NIS-2 ausgenommen sein.

Allerdings gilt dies nach dem definierten Anwendungsbereich nicht für deren gruppeninterne IT-Töchter. Wenn diese jedoch ausschließlich für eines bzw. mehrere der aus dem Anwendungsbereich ausgenommenen Versicherungsunternehmen IKT-Dienstleistungen erbringen, ist eine Regulierung über das NIS-2-Umsetzungsgesetz neben DORA nicht erforderlich. Zur Orientierung kann die Regelung des Artikel 31 Abs. 8 lit. iii) DORA-VO dienen, wonach gruppeninterne IKT-Dienstleister nicht als kritische IKT-Drittdienstleister anzusehen sind.

2.1 Zu § 28 NIS-2-Umsetzunggesetz (Besonders wichtige und wichtige Einrichtungen): Besonderheit der unternehmenseigenen bzw. gruppeninternen IT-Dienstleister in der Versicherungswirtschaft

Im Referentenentwurf zum NIS-2-Umsetzungsgesetz wird durch die Änderungen in Artikel 8 § 7 das Versicherungswesen und damit die Versicherungsunternehmen von der BSI-Kritisverordnung ausgenommen und sind daher keine Betreiber kritischer Anlagen nach §28 Abs. 1 Nummer 1.

Der Art. 2 Abs. 2 DORA benennt die in Art. 2 Abs.1 lit. a) bis t) DORA aufgeführten

Unternehmen als Finanzunternehmen, für die alle Bestimmungen aus DORA gelten. Hier gelten für Finanzunternehmen durch Ausnahme aus der BSI Kritisverordnung nur noch die Registrierungspflicht.

Von diesem Artikel ausgenommen sind die in Art. 2 Abs. 1 lit. u) DORA genannten IKT-Drittanbieterdienstleister. Auf diesen referenziert der §28 Abs. 6, so dass IT-Dienstleister den Bestimmungen des NIS-2-Umsetzungsgesetzes unterliegen.

Sinnvoll wäre hier aber eine Ausnahme für alle IKT-Drittdienstleister des Finanzsektors, die ausschließlich gruppenintern tätig sind. Diese Wertung entspräche auch dem Verständnis des Europäischen Gesetzgebers, der gruppeninterne IKT-Drittdienstleister von dem Überwachungsrahmen für kritische IKT-Drittanbieter nach DORA ausnimmt (Art. 31 Abs.8 lit. iii) DORA). Dies trägt dem Umstand Rechnung, dass die stark regulierten Finanzunternehmen regelmäßig größeren Einfluss auf die gruppeninternen IT-Dienstleister haben und die Einhaltung der strengen Sicherheitsanforderungen bereits hinreichend überwachen.

Wir regen daher weiterhin die Streichung der gruppeninternen IT-Dienstleister aus dem Anwendungsbereich des NIS-2-Umsetzungsgesetzes an:

§28 Abs. (6) Die §§ 30, 31, 32, 35, 36, 38 und 39 gelten nicht für
1. Finanzunternehmen nach Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 und Unternehmen, für welche die Anforderungen der Verordnung (EU) 2022/2554 auf Grund von § 1a Absatz 2 Kreditwesengesetz oder § 293 Absatz 5 Versicherungsaufsichtsgesetz gelten, **sowie deren gruppeninterne IKT-Dienstleister**.

2.2 Zu § 28 Absatz 7 NIS-2-Umsetzungsgesetz (Besonders wichtige und wichtige Einrichtungen): Ausnahmeregelung

§ 28 Abs. 7 NIS-2-Umsetzunggesetz (Achtung: wahrscheinliches Redaktionsversehen, hier wird auf Absatz 5 verwiesen, was eigentlich durch Hinzufügen des neuen Absatzes 3 nun 6 heißen müsste), nimmt Nicht-Finanzunternehmen, die Betreiber kritischer Anlagen beispielsweise nach § 5 der BSI-Kritisverordnung sind, von den Meldepflichten nach § 32 NIS-2-Umsetzunggesetz aus, soweit sie Anlagen für Finanzunternehmen betreiben.

Das ist sinnvoll, damit bei Sicherheitsvorfällen nicht ein doppelter Meldeaufwand betrieben werden muss. Nach der DORA-VO (vgl. Art. 28 Abs. 1 lit. a DORA) bleiben Finanzunternehmen auch bei Auslagerung auf IKT-Drittdienstleister für die Erfüllung der Anforderungen der DORA-VO voll verantwortlich. Zu diesen Anforderungen gehören auch die in Art. 19 Abs. 4 DORA-VO abgestuften Meldepflichten. Finanzunternehmen müssen also auch Sicherheitsvorfälle melden, die bei Anlagen auftreten, die für sie durch einen Dienstleister betrieben werden.

Derzeit hängt es von der Unternehmensgröße des IT-Dienstleisters ab, ob er der Meldepflicht nach § 32 unterliegt. Gerade kleinere IT-Dienstleister sind aber so von einer Meldepflicht betroffen.

Die DORA-VO unterscheidet aber nicht wie das NIS-2-Umsetzungsgesetz zwischen „Betreibern kritischer Anlagen“ und „besonders wichtigen Einrichtungen“ sowie „wichtigen Einrichtungen“. Wir schlagen daher folgende Änderung vor:

(7) § 32 gilt nicht für Betreiber kritischer Anlagen ***sowie besonders wichtige Einrichtungen und wichtige Einrichtungen****, soweit sie eine Anlage für Unternehmen nach Absatz 5 Nummer 1 betreiben.*

2.3 Zu § 38 BSI-Gesetz (Geschäftsleiterhaftung)

Wir begrüßen die gänzliche Streichung des in früheren Entwürfen noch enthaltenen Vergleichs- und Verzichtsverbots.

Die Neuformulierung von § 38 Abs. 2 sieht nunmehr vor, dass Geschäftsleitungen, die ihre Pflichten nach Abs. 1 verletzen, ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts haften (Satz 1). Nach dem BSIG haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten (Satz 2).

Nach unserer Einschätzung ist der neue § 38 Abs. 2 Satz 1 deklaratorisch. Der neue § 38 Abs. 2 Satz 2 statuiert eine Haftung, „wenn die für die Gesellschaft maßgeblichen Bestimmungen keine Haftungsregelung nach Satz 1“, d. h. keine Innenhaftung, enthalten. Da die Innenhaftung grundsätzlich im deutschen Gesellschaftsrecht angelegt ist, stellt sich die Frage nach der zu schließenden Lücke. Auch die Gesetzesbegründung enthält keine Hinweise zum konkreten Anwendungsbereich dieses Auffangtatbestands.

Wir regen an, die Gesetzesbegründung im weiteren Gesetzgebungsverfahren um entsprechende Erläuterungen zu ergänzen.

Berlin, den 03.07.2025