Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)524

Stellungnahme

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
Lobbyregister-Nr. R000774

zum Gesetzentwurf der Bundesregierung:
Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

BT-Drucksache 20/13184

Inhalt

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

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 grundsätzlich 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

- entweder komplett ausgenommen werden (siehe 2.1) oder
- zumindest eine Gleichbehandlung der kleinen und großen IT-Töchter (siehe 2.2) umgesetzt wird.

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 Artikel 2 Absatz 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 Regierungsentwurf zum NIS-2-Umsetzungsgesetz werden in Kapitel 1 „Anwendungsbereich“ in § 28 Abs. 5 (Besonders wichtige Einrichtungen und wichtige Einrichtungen) Finanzunternehmen und damit im Ergebnis die Versicherungswirtschaft über die Nennung von DORA als lex specialis ausgenommen.

Der hier einschlägig zitierte Artikel 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. In diesem Artikel ausgenommen sind die in Artikel 2 Abs. 1 lit. u) DORA genannten IKT-Drittanbieterdienstleister. Sinnvoll wäre hier 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 (5) 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 6 NIS-2-Umsetzungsgesetz (Besonders wichtige und wichtige Einrichtungen): Ausnahmeregelung

§ 28 Abs. 6 NIS-2-Umsetzunggesetz nimmt Nicht-Finanzunternehmen, die Betreiber kritischer Anlagen 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.

Die DORA-VO unterscheidet aber nicht wie das NIS-2-Umsetzunggesetz zwischen „Betreibern kritischer Anlagen“ und „besonders wichtigen Einrichtungen“ sowie „wichtigen Einrichtungen“.

Dies hat zur Folge, dass für die beiden niedrigeren Gefährdungskategorien eine gesteigerte, weil doppelte Meldepflicht entsteht:

- Nicht-Finanzunternehmen, die Betreiber kritischer Anlagen sind und diese Anlagen für Finanzunternehmen betreiben, müssen richtigerweise nicht nach NIS-2-Umsetzungsgesetz melden, weil das Finanzunternehmen nach DORA meldet.

- Nicht-Finanzunternehmen, die „nur“ besonders wichtige oder wichtige Einrichtungen sind und Anlagen für Finanzunternehmen betreiben, müssen dagegen nach NIS-2-Umsetzungsgesetz melden, obwohl das Finanzunternehmen bereits nach DORA meldet.

Wir regen daher an, die Ausnahme aller gruppeninternen IT-Dienstleister aus den in §32 hinterlegten Meldepflichten des NIS-2-Umsetzungsgesetzes durch folgende Ergänzung des §28 Abs. 6 umzusetzen:

(6) § 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.*

Berlin, den 31.10.2024