GDV Gesamtverband der Versicherer

STELLUNGNAHME

Stellungnahme

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
Lobbyregister-Nr. R000774

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

Inhalt

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

Zusammenfassung

Die deutsche Versicherungswirtschaft begrüßt das Vorhaben des Bundesinnenministeriums, die Cyberresilienz in Deutschland weiter zu stärken. Auch wenn Versicherungsunternehmen von der nationalen Umsetzung der NIS-2-Richtlinie grundsätzlich nicht erfasst sind, nehmen wir erneut die Gelegenheit zur Stellungnahme gerne wahr, da Teile einer Versicherungskonzernstruktur weiterhin in den Anwendungsbereich fallen sollen.

1. 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. Hier kann man sich u.E. auch an der Regelung des Artikel 31 Abs. 8 lit. iii) DORA-VO orientieren, wonach gruppeninterne IKT-Dienstleister nicht als kritische IKT-Drittdienstleister anzusehen sind.

Wir begrüßen die erkennbaren Verbesserungen bei der Ausgestaltung der Geschäftsleiterhaftung, insbesondere die vollständige Streichung des im früheren Entwurf noch enthaltenen Vergleichs- und Verzichtsverbots.

1.1 Zu § 28 BSI-Gesetz (Besonders wichtige und wichtige Einrichtungen): Besonderheit der unternehmenseigenen bzw. gruppeninternen IT-Dienstleister in der Versicherungswirtschaft

Im Referentenentwurf 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.

Wie komplex die Einbeziehung der gruppeninternen IT-Töchter sowohl in das nationale als auch das europäische Cybersicherheitsregime werden kann, lässt sich anhand der vorgesehenen Vorfallsmeldungen verdeutlichen, die sowohl aus NIS-2 als auch aus DORA heraus zu erfolgen haben:

Beispiel: Bei der gruppeninternen IT-Tochter kommt es zu **einem** Vorfall, der Auswirkungen auf den Geschäftsbetrieb einzelner Töchter hat oder haben könnte. Folgende Meldungen müssen nun von den Beteiligten abgesetzt werden:

1. Die **IT-Tochter** meldet den Vorfall nach § 32 NIS2UmsuCG innerhalb von 24 Stunden **an das BSI**.
2. Die **IT-Tochter** meldet den Vorfall nach DORA **an die einzelnen Versicherungsunternehmen** (z. B. Kranken-, Leben- und Sachversicherung) des Konzerns.
3. Die **einzelnen Versicherungsunternehmen** melden - je nach Betroffenheit - den Vorfall nach Art. 19 Abs. 1 DORA innerhalb von 4 Stunden nach Einstufung als kritisch **an die BaFin**, spätestens jedoch nach 24 Stunden.
4. Das **BSI stellt der BaFin** nach § 32 Abs. 5 NIS2UmsuCG „unverzüglich die bei ihm eingegangenen Meldungen zur Verfügung“ (siehe Nr. 1).
5. Die **BaFin** wiederum **übermittelt** nach Art 19 Abs. 6 c) DORA „zeitnah“ Einzelheiten zu dem Vorfall **an das BSI** (siehe Nr. 3).

Zudem ist hier anzumerken, dass nach derzeitigem Stand weder Meldeinhalt noch Meldeweg aus den beiden Regularien aufeinander abgestimmt sind, so dass unterschiedlich gemeldete Inhalte in unterschiedlichen Formaten aus unterschiedlichen Meldewegen dann dahingehend verglichen werden müssen, ob es sich um einen oder mehrere Vorfälle handelt.

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 gruppeninternen IKT-Dienstleister***.

1.2 Zu § 38 BSI-Gesetz (Geschäftsleiterhaftung)

Wir begrüßen die gänzliche Streichung des in § 38 Abs. 2 a.F. 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 03.07.2024