GDV Gesamtverband der Versicherer

STELLUNGNAHME

Stellungnahme

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
Lobbyregister-Nr. R000774

zum Entwurf eines Gesetzes zur Stärkung der Cybersicherheit

Inhaltsverzeichnis

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

1. Zusammenfassung

Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) teilt grundsätzlich das gesetzgeberische Ziel die Cybersicherheit in Deutschland weiter zu stärken. Insbesondere die Möglichkeit des Bundesamts für Sicherheit in der Informationstechnik (BSI) sich resilient im Cyberraum aufzustellen und die Erkenntnislage zu Cyberbedrohungen zu verbessern ist positiv zu bewerten.

Kritisch zu betrachten ist aus Sicht des GDV vor allem, dass unter dem Grundsatz der Stärkung der Cybersicherheit in Deutschland eine Reihe neuer, teilweise erheblicher, Eingriffsbefugnisse für die deutschen Sicherheitsbehörden entstehen.

2. Konkrete Punkte

Zu § 11 Abs. 1 BSIG (Hilfsersuchen)

Der § 11 Abs. 1 BSIG gibt vor, dass Unternehmen, die als besonders wichtige beziehungsweise wichtige Einrichtungen klassifiziert werden, nach eigenem Ersuchen Unterstützung vom BSI bei „Cyberangriffen“ erhalten können.

Eine Erweiterung um vom Digital Operational Resilience Act (DORA) regulierte Unternehmen könnte sinnvoll sein, um besser auf die Bedrohungslage der Finanz- und Versicherungsbranche zu reagieren. Gerade bei kleinen oder mittelgroßen Versicherungsunternehmen bzw. solchen, die keine ausgelagerte IT-Tochter haben und daher nicht vom BSIG reguliert werden, könnte dies eine sinnvolle Maßnahme zu Stärkung der Cybersicherheit sein.

Zu § 15 Abs. 6 (Anforderung von Informationen)

Die Regelung des § 15 Abs. 6 verpflichtet Anbieter öffentlich zugänglicher Telekommunikationsdienste und geschäftsmäßige Anbieter von digitalen Diensten, auf Anforderung des BSI ihnen bekannte sicherheitsrelevante technische Informationen, die Rückschlüsse auf Schadaktivität, Schwachstellen, Verwundbarkeiten oder aktuelle Bedrohungen für die Sicherheit ihrer informationstechnischen Systeme bereitzustellen.

Der GDV setzt sich in diesem Zusammenhang für eine anonymisierte und aggregierte Rückkopplung der Informationen an die KRITIS-Unternehmen bzw. auch an DORA-regulierte Unternehmen, die nicht der KRITIS-VO unterliegen bzw. nicht vom Anwendungsbereich des BSIG umfasst sind, ein. Dies könnte die Resilienz der kritischen Infrastruktur stärken.

Zu § 31 Abs. 2 (Angriffserkennung)

§ 31 Abs. 2 BSIG gibt vor, dass Betreiber kritischer Anlagen die Daten aus ihrer verpflichtenden Angriffserkennung per Schnittstelle an das BSI weiterleiten müssen.

Auch in diesem Zusammenhang setzt sich der Gesamtverband der Deutschen Versicherungswirtschaft für eine Rückkopplung der bereitgestellten Informationen an die KRITIS-Unternehmen bzw. durch DORA-regulierte Unternehmen, die nicht der KRITIS-VO unterliegen bzw. nicht vom Anwendungsbereich des BSIG umfasst sind, ein.

3. Verbesserung des Informationsaustauschs

Stärkung der kritischen Infrastruktur
Seit der Streichung der Versicherungsbranche aus der BSI-KRITIS-Verordnung im Rahmen des NIS-2-Umsetzungsgesetzes, hat sich der Informationsfluss zwischen Versicherungsunternehmen und dem BSI in Bezug auf Cyberbedrohungen verschlechtert. Versicherungen erhalten durch die Deregistrierung als KRITIS Unternehmen bspw. keine direkten Informationen mehr zu kompromittierten Identitäten ihrer Kunden, obwohl diese Informationen dem BSI vorliegen und in der Vergangenheit mit Versicherungsunternehmen geteilt wurden.

Diese Veränderung sollte nicht das Ergebnis der Vermeidung einer Doppelregulierung von Versicherungen durch NIS-2 und dem Digital Operational Resilience Act sein und läuft zudem konträr zum gesetzgeberischen Ziel von DORA, die Stärkung der Resilienz von Finanzunternehmen zu fördern, bzw. der NIS-2 Richtlinie, die Cybersicherheit zu stärken.

Denkbar wäre beispielsweise die Einführung einer gesetzlichen Grundlage, die eine Weitergabe von Informationen durch das BSI sowohl an KRITIS Unternehmen als auch an von DORA regulierte Unternehmen zulässt ohne neue Berichtspflichten für Versicherungsunternehmen bzw. deren IT-Töchter einzuführen. Dadurch könnte dem Ziel von DORA, die Stärkung der Resilienz von Finanzunternehmen im Bereich der Informationssicherheit, Rechnung getragen und gleichzeitig Doppelregulierung vermieden werden.

Stärkung der gesamtwirtschaftlichen Cyberresilienz
Durch die in § 15 Abs. 6 und § 31 Abs. 2 BSIG geplanten Datenerhebungen soll die durch bereits bestehende Meldepflichten (z.B. NIS2, DORA und CRA) bestehende, behördliche Grundlage zu Stärkung der Cybersicherheit weiter wachsen. Das Potenzial dieser Daten zur Stärkung der gesamtwirtschaftlichen Cyberresilienz, die über wichtige und besonders wichtige Einrichtungen hinausgeht, wird bisher nicht hinreichend ausgeschöpft.

Dabei könnten diese Daten – in anonymisierter und aggregierter Form – einen erheblichen Mehrwert für die gesamte Wirtschaft sowie die wissenschaftliche Forschung entfalten. Derzeit mangelt es diesen Akteuren jedoch an einem

ausreichenden Zugang zu verlässlichen und umfassenden Informationen über Cybervorfälle und Bedrohungslagen. Dabei sind diese Daten eine wesentliche Grundlage, um Risiken fundiert zu analysieren, Entwicklungen frühzeitig zu erkennen und wirksame Präventionsmaßnahmen abzuleiten.

Der GDV schlägt daher die Schaffung einer Rechtsgrundlage für eine solche sachgerechte Datennutzung vor, um die Forschung und Cyberresilienz der Wirtschaft insgesamt zu stärken.

Berlin, den 17.03.2026