Stellungnahme

des Gesamtverbandes der Deutschen Versicherungswirtschaft

zum Referentenentwurf des Bundesministeriums des Innern

Erste Verordnung zur Änderung der BSI-Kritisverordnung

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5452
Fax: +49 30 2020-6452

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +32 2 28247-39
ID-Nummer 6437280268-55

Ansprechpartner:
Patrik Maeyer
Leiter (komm.) Betriebswirtschaft und Informationstechnologie

E-Mail: p.maeyer@gdv.de

www.gdv.de

Zusammenfassung

Der Gesamtverband der Deutschen Versicherungswirtschaft begrüßt die Stärkung der IT-Sicherheit kritischer Infrastrukturen durch das IT-Sicherheitsgesetz. Für die Versicherungsunternehmen ist es von besonderer Bedeutung, dass die sensiblen Daten der Kunden verantwortungsvoll und unter Wahrung der notwendigen Sicherheitsstandards verarbeitet werden.

Aus diesem Grund wurde bereits 2010 das Krisenreaktionszentrum für IT-Sicherheit der deutschen Versicherungswirtschaft GmbH (LKRZV) als Single Point of Contact (SPOC) im Rahmen des Umsetzungsplans KRITIS gegründet.

Der Verband dankt für die kooperative und transparente Zusammenarbeit zur Entwicklung branchenspezifischer Schwellenwerte. Trotz der gemeinsamen Vorarbeit zu dieser Rechtsverordnung ergeben sich noch einige ergänzende Anmerkungen.

1. Allgemeine Anmerkungen zum Entwurf der Rechtsverordnung

Der Verband begrüßt die Verankerung der im kooperativen Verfahren gemeinsam erarbeiteten Schwellenwerte für die Bereiche Lebensversicherung und Komposit in dem vorliegenden Entwurf für eine Rechtsverordnung (RVO) gemäß § 10 I BSIG. Damit wird unter Beachtung der Einheit der Rechtsordnung die bereits in § 8 Versicherungsaufsichtsgesetz (VAG) vorgegebene Spartentrennung bei der Feststellung der Kritikalität von Versicherungsleistungen berücksichtigt. Dennoch verweist der Verband nochmals auf die Sektorstudie[1], wonach ein IT-Vorfall in der Versicherungsbranche sowohl aufgrund in der Regel nicht zeitkritischer Verfahren als auch aufgrund der zeitversetzten Abwicklung von Leistungs- und Schadensfällen der Versicherungsnehmer keine kritischen Auswirkungen im Sinne des IT-Sicherheitsgesetzes hat. Die nun abgeleiteten Schwellenwerte, die sich auf Leistungs- und Schadensfälle beziehen, sind vertretbar. Es sollte jedoch auch im Sinne des von der Bundesregierung gesetzten Ziels des Bürokratieabbaus regelmäßig hinterfragt werden, ob mit der vorgelegten RVO tatsächlich kritische Infrastrukturen besser geschützt werden.

Zu Regelungen, die die private Krankenversicherung betreffen, wird auf den Verband der Privaten Krankenversicherung e.V. verwiesen.

2. Zu den Regelungen im Einzelnen

2.1. § 7 Abs. 8 RVO:

„Abweichend von § 1 Nummer 2 hat im Sektor Finanz- und Versicherungswesen bestimmenden Einfluss auf eine Kritische Infrastruktur, wer die tatsächliche Sachherrschaft ausübt. Die rechtlichen und wirtschaftlichen Umstände bleiben insoweit unberücksichtigt.“

Es bedarf einer Klarstellung des angestrebten Anwendungsbereichs dieser Norm auf Kopfstellen im Bereich der Zahlungssysteme. Andernfalls könnten im Versicherungsbereich auch IT-Dienstleister entgegen der Intention des Verordnungsgebers erfasst werden, die teilweise als externe Dienstleister für verschiedene Versicherungskonzerne tätig sind.

[1] Studie P107 Finanz- und Versicherungswesen: Analyse Kritischer Infrastrukturen in Deutschland; Stand: 18.12.2015; V104 – Überarbeitung

Dies kann bei betroffenen IT-Dienstleistern zu erheblicher Rechtsunsicherheit führen, da diesen weder die Anwendungen noch die Zahl etwaiger Leistungs- und Schadensfälle, welche von ihren Kunden auf ihren Systemen betrieben werden, bekannt sind. Ein Einblick in die auf den Systemen des IT-Dienstleisters befindlichen Informationen des Versicherers ist weder rechtlich noch tatsächlich möglich, sodass eine Ermittlung der notwendigen Informationen zur Feststellung, ob eine Meldepflicht nach dem Entwurf der Rechtsverordnung besteht, rechtskonform nicht umsetzbar wäre, da der Schutz von Betriebsgeheimnissen und die Einhaltung des Datenschutzes durch die IT-Dienstleister nutzenden Versicherungsunternehmen gewahrt werden muss.

Um diese Unklarheit zu vermeiden, sollte die Formulierung einschränkend auf die Kopfstellen im Bereich der Zahlungssysteme wie folgt angepasst werden:[2]

„Abweichend von § 1 Nummer 2 hat im Sektor Finanz- und Versicherungswesen die Anlagenkategorien des Teils 3 Nummern 1, 2, 3 und 4 bestimmenden Einfluss auf eine Kritische Infrastruktur, wer die tatsächliche Sachherrschaft ausübt. Die rechtlichen und wirtschaftlichen Umstände bleiben insoweit unberücksichtigt."

2.2. Anhang 6, Teil 1, Nr.1, Lit. u-z:

„Im Sinne von Anhang 6 sind

u) Vertragsverwaltungssystem für das Versicherungsvertragsverhältnis
System zur Speicherung und Verarbeitung von Informationen zum Versicherungsvertragsverhältnis.

v) Leistungssystem Lebensversicherung
System zur Leistungsbearbeitung im Bereich Lebensversicherung.

w) Leistungssystem der Sozialversicherungsträger (SVT)
Integriertes Anwendungssystem zur Erfassung, Prüfung und Berechnung von Renten- und sonstigen Entgeltersatzleistungen nach § 29 des vierten Buches Sozialgesetzbuch in der jeweils geltenden Fassung

x) Leistungssystem Krankenversicherung

[2] Änderungsvorschläge sind durch Unterstreichungen gekennzeichnet

System zur Leistungsbearbeitung im Bereich Krankenversicherung.

y) Schadensystem (Komposit)
System zur Schadensermittlung im Bereich Schaden- und Unfallversicherungen

z) Auszahlungssystem
System zur Auszahlung der Entschädigung bzw. Versicherungsleistung an den Zahlungsempfänger."

Es bestand in den Vorarbeiten zum Entwurf der Rechtsverordnung Einvernehmen, dass allenfalls Leistungs- bzw. Schadenssysteme im Bereich der Versicherungswirtschaft kritisch im Sinne des IT-Sicherheitsgesetzes sein könnten. Dies sollte – konsistent mit den übrigen Legaldefinitionen, welche jeweils auf die Leistungs- bzw. Schadenssysteme Bezug nehmen – sich auch an dieser Stelle widerspiegeln.

Daher sollte in Lit. y) der Begriff „Schadensermittlung" durch „Schadenbearbeitung" ersetzt werden.

Die Schadensermittlung, die gegebenenfalls durch einen externen Gutachter erfolgt, ist nicht als kritische Dienstleistung im Sinn der Rechtsverordnung ausgewiesen. Vielmehr soll die Schadenbearbeitung in der Kompositversicherung erfasst werden, zumal diese entsprechend IT-gestützt in den von Versicherungsunternehmen betriebenen IT-Systemen erfolgt.

2.3. Anhang 6, Teil 1, Nr. 3:

„Abweichend von Nummer 1 gilt eine Anlage, die den Anlagenkategorien des Teil 3 Spalte B Nummer 5.1.3, 5.1.6 und 5.1.9 zuzuordnen ist, zum 1. April des Kalenderjahres, das auf die drei Kalenderjahre folgt, deren durchschnittlicher Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur."

Um ein vermutlich redaktionelles Versehen zu beheben und den mit der Norm angestrebten Bereich der Kompositversicherung abzubilden, müsste die Nummerierung wie folgt angepasst werden: „…Nummer 5.1.3, 5.1.7 und 5.1.10…"

2.4. Anhang 6, Teil 1, Nr. 5:

„Stehen mehrere Anlagen derselben Art in einem engen betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in Teil 3 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als Kritische Infrastruktur. Ein enger betrieblicher Zusammenhang ist gegeben, wenn die Anlagen

a) mit gemeinsamen Betriebseinrichtungen verbunden sind,
b) einem vergleichbaren technischen Zweck dienen und
c) unter gemeinsamer Leitung stehen."

Die Norm muss rechtsklar so gestaltet werden, dass nicht die Spartentrennung in Versicherungskonzernen, die aus mehreren, rechtlich unabhängigen Versicherungsunternehmen unterschiedlicher Sparten bestehen, ausgehebelt wird. Vielmehr muss die Norm auf gleiche und gemeinsam betriebene Anlagenkategorien beschränkt werden.

Gemäß § 8 VAG sind Versicherungsunternehmen zur Spartentrennung verpflichtet, sodass der Betrieb in einem Versicherungsunternehmen jeweils nur eine der drei genannten Sparten Lebens-, Kranken- und Kompositversicherung umfassen darf. Versicherungskonzerne können jedoch aus mehreren, rechtlich unabhängigen Versicherungsunternehmen verschiedener Sparten bestehen. Dabei wird die Spartentrennung innerhalb eines Konzerns auch innerhalb der IT-Systeme und -Anlagen beachtet, meist bis auf die Anwendungsebene. Wie bereits oben angemerkt, ist die im Entwurf der Rechtsverordnung grundsätzlich angelegte Spartentrennung mithin sachgerecht, steht im Einklang mit Regelungen des Versicherungsaufsichtsrechts und bildet rechtliche wie sachliche Gegebenheiten zutreffend ab.

Die vorstehende Regelung würde jedoch systemwidrig dazu führen, dass eben diese Spartentrennung faktisch aufgehoben würde. Dies würde auch zu einer sachlich nicht gerechtfertigten Ausweitung der mittels der Schwellenwerte festgelegten Feststellung der Kritikalität von IT-Anlagen in der Versicherungswirtschaft führen. Würde die Spartentrennung durch die vorgenannte Norm jedenfalls in Versicherungskonzernen faktisch obsolet, stünde dies im eklatanten Widerspruch zu Sinn und Zweck der für die einzelnen Sparten gesondert festgelegten Schwellenwerte. Im Falle eines IT-Sicherheitsvorfalls in einer gemeinsamen Anlage, in der in unterschiedlichen Sparten jeweils weniger jährliche Leistungs- und

Schadensfälle verarbeitet werden als in den Schwellenwerten angegeben, wären auch dann keine kritischen Auswirkungen auf die Gesamtwirtschaft oder Gesellschaft zu erwarten, wenn über die Sparten hinweg kumulativ der Schwellenwert für eine Sparte erreicht würde.

Beispiel:
Ein Versicherungskonzern betreibt eine gemeinsame IT-Anlage, in der für verschiedene Konzerntöchter Leistungs- und Schadensfälle verarbeitet werden. Jährlich werden hier für die Konzerntochter im Bereich der Lebensversicherung 300.000 Leistungsfälle und für die Konzerntochter im Bereich der Kompositversicherung 210.000 Schadensfälle in getrennten Anwendungssystemen verarbeitet. Fiele die gemeinsame Anlage aus, wären mithin maximal 300.000 Lebensversicherungen und 210.000 Kompositversicherungen betroffen, was auch bei zeitgleichem Eintreten nicht zu einem kritischen Effekt für Wirtschaft oder Gesellschaft führen würde, da gänzlich unterschiedliche Sachverhalte betroffen wären.

Mithin bedarf die Norm der Klarstellung, dass nur gleiche Anlagenkategorien, die gemeinsam betrieben werden, erfasst sein sollen.

Ergänzend wird darauf verwiesen, dass die Normenklarheit dahingehend fehlt, was damit gemeint ist, dass Schwellenwerte zusammen erreicht oder überschritten werden, so dass auch hier eine Klarstellung erforderlich wäre. Ein Addieren der Schwellenwerte der in einer gemeinsamen Anlage verarbeiteten Leistungs- und Schadensfälle würde, wie oben ausgeführt, die Spartentrennung obsolet werden lassen und die Feststellung der Kritikalität einer Anlage über die mittels der Schwellenwerte festgelegten Kriterien hinaus erweitern. Auch die Lesart, dass im Falle des Überschreitens eines von bis zu drei unterschiedlichen Schwellenwerten, die für Anlagen der Versicherungswirtschaft gelten, auch die übrigen Anlagen in einer gemeinsamen Anlage durch die Hintertür zu kritischen Infrastrukturen würden, führte zu einer unverhältnismäßigen Ausweitung des Anwendungsbereichs und würde ebenso die Spartentrennung aushebeln.

Da dies wohl nicht der Absicht des Verordnungsgebers entspricht, wird diesseitig die folgende Formulierung vorgeschlagen:

„Stehen mehrere Anlagen derselben Anlagenkategorie, in einem engen betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten den in Teil 3 Spalte D für diese Anlagenkategorie genannten Schwellenwert zusammen, gilt die

gemeinsame Anlage als Kritische Infrastruktur. Ein enger betrieblicher Zusammenhang ist gegeben, wenn die Anlagen

a) mit gemeinsamen Betriebseinrichtungen verbunden sind,
b) einem vergleichbaren technischen Zweck dienen und
c) unter gemeinsamer Leitung stehen."

2.5. Anhang 6, Teil 2 Berechnungsformeln zur Ermittlung der Schwellenwerte

Um der Besonderheiten der Lebensversicherungssparte Rechnung zu tragen, bedarf es der Definition in der Rechtsverordnung, was als Leistungsfall in die Ermittlung der Schwellenwerte einfließt. Der Verband schlägt daher die Ergänzung der Rechtsverordnung um einen weiteren Punkt vor.

Zu verweisen ist hierbei auf die in der Vorbereitung der Erarbeitung der Rechtsverordnung besprochene Intention, dass im Bereich der Lebensversicherung für die Ermittlung des Schwellenwertes auf die Zahl derjenigen ablaufenden Verträge, die eine Leistung (Zahlung) des Versicherungsunternehmens auslösen, abgestellt wird. Nur in diesen Fällen kann von einer kritischen Dienstleistung im Sinne der Rechtsverordnung ausgegangen werden. Weiterhin sollen regelmäßige Zahlungen jeweils nur zum Zeitpunkt der initialen Leistungsbearbeitung, bei der etwa die Höhe der fälligen (monatlichen) Leistung festgestellt wird, bzw. der Zahlungsstart in die Berechnung einbezogen werden. Dies ist nur folgerichtig, da Anhang 6 Teil 1 Nr. 1 Lit. v) auf die Leistungsbearbeitung abstellt, die auch bei regelmäßigen Zahlungen nur einmal, nämlich zu Beginn des Bewilligungszeitraums, durchgeführt wird.

Der zusätzliche Punkt der Rechtsverordnung könnte wie folgt ausgestaltet werden:

„Bei den für die Anlagenkategorien des Teils 3 Nummer 5.1.1, 5.1.4 und 5.1.8 genannten Schwellenwerten werden nur ablaufende Verträge mit Auszahlung der Versicherungsleistung i.S.d. Anhang 6, Teil 1, Nr.1, Lit. z eingerechnet. Unabhängig von der Zahlungsweise (einmalig, monatlich oder sonst wiederkehrend) wird jeder Leistungsfall nur einmalig, bei wiederkehrenden Auszahlungen nur bei der erstmaligen Leistungsbearbeitung i.S.d. Anhang 6, Teil 1, Nr.1, Lit. v, einbezogen."

Berlin, den 14.03.2017