Stellungnahme

des Gesamtverbandes der Deutschen Versicherungswirtschaft

ID-Nummer 6437280268-55

zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5000
Fax: +49 30 2020-6000

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +49 30 2020-6140
ID-Nummer 6437280268-55

Ansprechpartner: **BDIT**

E-Mail: **BDIT@gdv.de**

www.gdv.de

Zusammenfassung

Das Bundesinnenministerium hat am 09.12.2020 einen Referentenentwurf eines zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vorgelegt und bis zum folgenden Tag um Stellungnahme gebeten. Der GDV nimmt die Gelegenheit zur Kommentierung gern wahr.

Allerdings ist die Verfahrensweise – insbesondere die sehr kurze Stellungnahmefrist - ungewöhnlich und für einen effizienten Austausch zu Gesetzentwürfen in für die Zusammenarbeit mit betroffenen Verbänden ungeeignet.

Die Versicherungswirtschaft begrüßt das Vorhaben der Bundesregierung, die Cyberresilienz Deutschlands zu stärken. Die zunehmende Digitalisierung von Staat, Wirtschaft und Gesellschaft baut auf Cyber- und IT-Sicherheit auf und erfordert eine Kooperation aller Akteure. Hierzu war und ist die deutsche Versicherungswirtschaft ein verlässlicher Partner und wird weiterhin auf höchstem Niveau ihren Beitrag leisten. Der vorliegende Entwurf bildet dafür einerseits eine wichtige Basis.

Andererseits ist IT- bzw. Cybersicherheit kein rein nationales Thema. Die EU-Kommission hat als Bestandteil ihrer digitalen Finanzstrategie jüngst den Entwurf einer EU-Verordnung zur digitalen Resilienz im Finanzsektor zur Konsultation gestellt. Diese erhebt den umfassenden Anspruch, einen einheitlichen und unmittelbar geltenden Rechtsrahmen für die Überwachung und Minimierung von Risiken aus der Nutzung von Informations- und Kommunikationsrisiken (ICT) zu schaffen.

Eine bislang erfolgreiche Kooperation zwischen Behörden und Wirtschaft darf nicht durch eine unverhältnismäßige Bürokratisierung gefährdet werden. Die mit dem Gesetzentwurf verbundenen negativen Effekte – wie erheblicher Kostenzuwächse bei Unternehmen, der Gefahr von Doppelregulierung und Unsicherheiten – steht keine signifikante Erhöhung des IT-Sicherheitsniveaus gegenüber. Es ist zudem zu befürchten, dass sich die zusätzliche Komplexität negativ auf die Investitionen der Unternehmen auswirken.

Insbesondere sind die mit beträchtlichen Risiken für Unternehmen verbundene Detektion von Sicherheitslücken (§ 7b), die langfristige Speicherung von Daten, die bei der Angriffserkennung anfallen (§ 8a) sowie die Untersagung des Einsatzes kritischer Komponenten (§ 9b) zu nennen. Auch geht die Höhe der Bußgelder in § 14 bei Weitem über ein angemessenes Maß hinaus.

Inhaltsverzeichnis

Einleitung

Das Bundesministerium des Innern, für Bau und Heimat (BMI) hat am 09.12.2020 den Entwurf eines zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme in die Verbändeanhörung gegeben und um Stellungnahme am nächsten Tag gebeten.

Die deutsche Versicherungswirtschaft begrüßt das Vorhaben der Bundesregierung, die Cyberresilienz Deutschlands signifikant und ganzheitlich zu stärken. Die Digitalisierung von Staat, Wirtschaft und Gesellschaft basiert auf Cyber- und IT-Sicherheit und erfordert eine Kooperation aller betroffenen Akteure. Hierzu war und ist die deutsche Versicherungswirtschaft ein verlässlicher Partner und wird auch weiterhin ihren Beitrag leisten. Für ein reibungsfreies Funktionieren von digitalisierten (Geschäfts-) Prozessen der Versicherungsunternehmen ist ein hoher Grad an Cyberresilienz eine Grundvoraussetzung.

Dennoch ist das Vorgehen des Gesetzgebers diesbezüglich zu kritisieren. So ist das IT-Sicherheitsgesetz aus dem Jahr 2015 nicht – wie dort verankert – evaluiert worden, sondern es wurde über zwei Jahre im BMI, ohne Einbindung der betroffenen Sektoren, ein neuer Entwurf entwickelt, der den bisherigen Ansatz des kooperativen Miteinanders von Staat und Wirtschaft nicht mehr verfolgt.

Als Gesetzgeber ist der Staat dazu aufgefordert, einen regulatorischen Rahmen vorzugeben und so zu gestalten, dass bundesweit das Sicherheitsniveau gestärkt wird. Dabei muss ein besonderes Augenmerk auf die realistische Umsetzbarkeit in den regulierten Unternehmen gerichtet sein. Der regulatorische Rechtsrahmen muss klare und verhältnismäßige Vorgaben machen. Das IT-Sicherheitsgesetz 2.0 könnte hierfür den geeigneten Rahmen bieten, lässt jedoch im Referentenentwurf (RefE) vom 09.12.2020 die notwendige Rechtsklarheit vermissen und ist in seinen Vorgaben zu weitreichend und/oder unbestimmt.

Zudem lässt der Gesetzentwurf die notwendige Referenzierung auf europäische Regulierung und Initiativen – wie den Digital Operational Resilience Act (DORA) und die ICT Guidelines von EIOPA – vermissen. Schon um die Wettbewerbsfähigkeit im europäischen Kontext zu erhalten, sollte ein nationaler Alleingang und damit eine Doppelregulierung deutscher Unternehmen verhindert werden. Für die Versicherungswirtschaft als Adressat dieser Regulierungen stellt sich die dringende Frage nach dem (zukünftigen) Verhältnis zu den nationalen Vorgaben. Hinzu kommt, dass Versicherungsunternehmen sich zusätzlich sektorspezifischen Anforderungen an ihre IT-Sicherheit ausgesetzt sehen. Ein derart komplexes Regime mit verschiedenen Regulierungsebenen und möglicherweise konkurrierenden Anforderungen wäre aus Compliance-Sicht kaum mit verhältnismäßigem Aufwand zu bewältigen. Wir möchten daher an das BMI appellieren, die evtl. Redundanz des Gesetzentwurfs mit europäischen und sektoralen Vorgaben zur IT-Sicherheit in den Blick zu nehmen.

§ 3 Absatz 1 Nummer 20 – Aufgaben des Bundesamtes

Der Ansatz, das BSI als oberste deutsche Cybersicherheitsbehörde zu stärken, wird seitens der deutschen Versicherungswirtschaft grundsätzlich begrüßt. Nach § 3 Abs. 1 Nr. 20 BSIG-E soll das BSI die Entwicklung und Veröffentlichung eines Standes der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte übernehmen. Dies ist allerdings abzulehnen. Der Stand der Technik entsteht durch das Agieren aller Beteiligten (Entwickler, Hersteller und Unternehmen als Nutzer) und ist einer sich ständig ändernden Dynamik ausgesetzt. Diese Dynamik kann und sollte der Gesetzgeber bzw. eine Behörde nicht beeinflussen.

Ob ein System dem Stand der Technik entspricht, kann immer nur zum gegenwärtigen Zeitpunkt oder maximal im Nachgang festgestellt werden. Ein Festlegen eines Standes der Technik durch das BSI könnte daher dazu führen, das geführte und veröffentlichte Listen bzgl. des Standes der Technik bereits bei der Bekanntmachung wieder überholt sind, da Forschung und Entwicklung bereits neue Erkenntnisse haben. Der Markt bietet zudem ausreichend kompetente Akteure, die sich laufend einer Beschreibung des aktuellen Standes der Technik widmen und öffentlich zur Verfügung stellen, anhand derer sich die Politik und Wirtschaft orientieren können.

Sollte diese neue Kompetenz des BSI bestehen bleiben, könnte es zu Verzerrungen durch die Entstehung möglicher Monopole kommen, die zudem ein lukratives Ziel für Angreifer darstellen könnten. Durch das Festlegen eines Standes der Technik könnten Hersteller sowie deren Produkte nicht mehr berücksichtigt werden, die vor dem Festlegen der Kriterien genutzt werden konnten. Dadurch würde nur noch die Nutzung von Produkten gewisser Hersteller ermöglicht werden. Auch außerhalb dieser Systeme darf das BSI nicht den Stand der Technik für Sicherheitslösungen definieren und deren Nutzung erzwingen.

§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden

Das BSI soll durch § 7b BSIG-E in die Lage versetzt werden, zur „Detektion von Sicherheitslücken und anderen Sicherheitsrisiken bei Einrichtungen des Bundes oder der in § 2 Absatz 13 und 14 genannten Unternehmen Maßnahmen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen (Portscans) durchführen, …“ zu können. Die deutsche Versicherungswirtschaft lehnt diese neue Befugnis für das BSI ab. Zum einen könnte die Sicherheit und Verfügbarkeit der Systeme durch den Scan gefährdet werden, da dem BSI im Vorfeld nicht klar sein kann, wie weit es durch die Detektion in die Systeme eindringt und diese sogar beeinflusst. Zum anderen ist nicht geregelt, wer für Schäden haftet, die durch die Detektion verursacht werden. Weiterhin sind die Art und der Umfang der Detektion nicht klar definiert. Hier muss ein klarer

Rechtsrahmen geschaffen werden. Die Maßnahmen müssen sich auf das absolut Notwendige zur Detektion der Sicherheitslücken beschränken, dürfen nicht über einen Portscan hinausgehen und eine Kompromittierung der Systeme muss ausgeschlossen sein.

Sollte an dieser Regelung festgehalten werden, müssten neben den Haftungsfragen auch geklärt werden, wie die betroffenen Betreiber im Vorfeld über Umfang, Form und Zeitraum der Detektion informiert werden, wie das BSI die Detektion nachvollziehbar dokumentiert und garantiert, dass nur eine Detektion der Schwachstelle durchgeführt wird, keine Kompromittierung der Systeme vorgenommen wird und keine Hintertür verbleibt.

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastruktur

In §8a Abs. 1 sollen die Wörter „spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1“ durch die Wörter „spätestens bis zum ersten Werktag, der auf die erstmalige oder erneute Bestimmung einer Anlage als Kritische Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 folgt“ ersetzt werden. Das bedeutet, dass für Unternehmen, die bereits als Kritische Infrastruktur gelten und die Schwellenwerte nicht zwischenzeitlich wieder unterschreiten, statt der bisherigen zweijährigen Umsetzungsfrist nunmehr eine Frist von maximal sechs Monaten und 72 Stunden eingeräumt wird, wenn die Verkündung auf einen Freitag fallen würde. Eine derartige Verkürzung ist in keiner Weise nachvollziehbar. Die Begründung zu dieser Anpassung, dass die Übergangsfrist durch das Datum des Inkrafttretens der Rechtsverordnung (RVO) bereits verstrichen sei, kann zumindest nicht für Unternehmen geltend gemacht werden, die die Schwellenwerte erstmalig überschreiten. Auch der Verweis auf die RVO mit einer Umsetzungsfrist von mindestens drei Monaten ist nicht akzeptabel. Die Änderung des Abs. 1 ist daher zurückzunehmen.

§ 8a Abs. 1a BSIG-E schreibt vor, dass die Betreiber Kritischer Infrastrukturen auch Systeme zur Angriffserkennung einzusetzen haben. Hier müssen die eingesetzten Systeme zur Angriffserkennung geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten.

Die Unternehmen haben schon im Eigeninteresse und im Rahmen des Risikomanagements entsprechende Systeme etabliert. Hier sollte daher eine starre gesetzliche Vorschrift unterbleiben. Ein automatisiertes Erfassen und Auswerten von Angriffsmerkmalen ist in der betrieblichen Praxis gar nicht sinnvoll, da immer eine fallbezogene Analyse erfolgen muss, um neue Angriffsvektoren oder -logiken erkennen zu können.

Nach § 8a Abs. 1b BSIG-E müssen Betreiber Kritischer Infrastrukturen für die Angriffserkennung und -nachverfolgung relevante nicht personenbezogene Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, mindestens vier Jahre spei-

chern. Dies ist abzulehnen, da hier Datenmengen in Terabyte-Umfang entstehen, deren Analyse kaum mehr möglich ist. Zudem erschließt sich der Sinn einer solch umfangreichen Speicherung auch nicht und widerspricht dem Nachhaltigkeitsgedanken.

Wenn überhaupt eine Speicherung in Erwägung gezogen wird, sollte sich die Speicherfrist an den Fristen des § 5 Abs. 2 von drei Monaten bzw. 12 Monaten bei vermutetem Angriff orientieren. Hierzu ist auch im aktuellen Jahresbericht des BSI vermerkt, dass entsprechenden Angriffen lediglich ein „… wochenlanges Ausbreiten in internen Netzwerken vorangehen kann …". Zudem ist eine Trennung der Daten in personenbezogene und nicht personenbezogene Daten technisch sehr aufwändig und ggf. nicht leistbar.

§ 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastruktur

Die Versicherungswirtschaft begrüßt einen Austausch bzgl. Sicherheitsvorfällen und Angriffsrisiken und erachtet einen sektorenübergreifenden Informationsaustausch zwischen Wirtschaft und den Behörden als sinnvoll. Die Versicherungswirtschaft hat bereits vor zehn Jahren erfolgreich das Krisenreaktionszentrum für IT-Sicherheit der deutschen Versicherungswirtschaft (LKRZV) als zentrale Meldestelle etabliert. Diese gut etablierten Kanäle sollten aber nicht durch zentrale Krisenkommunikationssysteme ausgehebelt werden. Daher begrüßen wir die Streichung einer solchen Einrichtung gegenüber den vorherigen Referentenentwürfen.

Es ist nicht nachvollziehbar, warum das BSI während einer erheblichen Störung die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen sollte, da die unternehmensinterne Krisenbewältigung unbedingt Vorrang haben sollte. Wie soll der Schutz der Unternehmensinteressen und der hochsensiblen Unternehmensinformationen gewährleistet werden und wie ist dies mit den Grundsätzen der DSGVO vereinbar (Abs. 4a)?

Die Versicherungswirtschaft fordert daher eine ersatzlose Streichung des § 8b Abs. 4a BSIG-E.

§ 9b Untersagung des Einsatzes kritischer Komponenten

Nach § 9b BSIG-E sind Betreiber Kritischer Infrastrukturen verpflichtet, dem BMI den Einsatz kritischer Komponenten anzuzeigen (Abs. 1) und nur kritische Komponenten von Herstellern einzusetzen, die eine Garantieerklärung der Vertrauenswürdigkeit über die gesamte Lieferkette hinweg abgeben (Abs. 2). Während dieser Prüfung durch das BMI, die innerhalb eines Monats erfolgen soll, ist der Einsatz der kritischen Komponenten nicht gestattet (Abs.3).

Des Weiteren kann das BMI den Einsatz einer kritischen Komponente untersagen (Abs. 3). Seitens der Versicherungswirtschaft ist nicht erkennbar, weshalb das BMI und nicht das BSI, als die nationale Behörde für die Cybersicherheitszertifizierung, die zudem vor dem Hintergrund dieses Gesetzesentwurfes in ihrer Kompetenz gestärkt wird, für eine derartige Anzeigepflicht und Überprüfung der kritischen Komponenten zuständig sein soll. Neben bestehenden Anzeige- und Meldepflichten gegenüber der BaFin und dem BSI soll nun mit dem BMI ein weiterer Akteur hinzukommen. Diesem bürokratischen Mehraufwand steht kein erkennbarer Mehrwert gegenüber.

Daneben geben wir zu bedenken, dass gerade bei global hergestellten und komplexen Hard-, Software- und Elektronik-Produkten die Lieferketten bzw. Produktionsketten in ihren einzelnen Bestandteilen nicht immer in Gänze zurückverfolgbar sind. Die Abgabe einer Garantieerklärung über die gesamte Lieferkette ist daher teilweise gar nicht erst möglich. Auch bleibt ungewiss, ob die Hersteller im Übrigen überhaupt eine solche Garantieerklärung abgeben würden. Bereits in dem geltenden Aufsichtsrechtsrahmen bestehen für Versicherungsunternehmen hohe Anforderungen bzgl. der Beschaffung, Vertragsverhandlungen und Überprüfung der Hersteller/Dienstleister. Insbesondere mit großen Anbietern erweist sich die vertragliche Absicherung dieser Anforderungen in der Praxis bereits als sehr aufwendig. Problematisch wird dies dann, wenn keine Ausweichmöglichkeit zu einem anderen Anbieter besteht. Den Unternehmen bleibt dann nur die Möglichkeit, auf die Innovationskraft zu verzichten und mithin den technologischen Anschluss im globalen Markt zu verpassen. Auch ist zu befürchten, dass die in einigen Bereichen bereits bestehende Konzentration auf einige wenige Anbieter noch zunimmt. Die nun vorgeschlagenen Anforderungen würden diese Problematik insgesamt verschärfen und zu signifikanten zusätzlichen Aufwänden für die Versicherungsunternehmen führen.

Eine mögliche nachträgliche Untersagung durch den Entzug der Vertrauenswürdigkeit und die damit verbundenen Rückbauverpflichtungen von bereits eingesetzten IT-Produkten sorgt für erhebliche Unsicherheit und könnte im Extremfall eine Bedrohung der unternehmerischen Existenz darstellen. Faktisch würde dies bedeuten, dass erhebliche Rückstellungen gebildet werden müssten, um einen eventuell angeordneten Rückbau zu bewerkstelligen. Daher bedarf es dringend einer Korrektur und Klarstellung des Gesetzgebers. Klare Verantwortlichkeiten, Ausstiegsszenarien und ausreichende Übergangsfristen müssen Rechtssicherheit garantieren, da es sonst zu erheblichen negativen Auswirkungen auf die Geschäftsprozesse der Versicherungsunternehmen kommen könnte.

Ebenfalls berücksichtigt der Entwurf nicht, dass unsichere technische Produkte auch im Nachgang durch das Ergreifen zusätzlicher organisatorischer und technischer Maßnahmen nachjustiert werden können. Insofern sollten vorrangig zu ergreifende mildere Maßnahmen ermöglicht werden. Angesichts der aufgezeigten erheblichen Unsicherheiten, Konzentrationsrisiken und Mehraufwendungen sollte § 9b des BSIG-E in seiner jetzigen Form ersatzlos gestrichen werden.

§ 14 Bußgeldvorschriften

Mit § 14 Abs. 5 BSIG-E wird die Erhöhung des „maximalen Bußgeldes“ von 100.000 Euro auf neue Stufen des Bußgeldes von bis zu 2 Millionen Euro angehoben. Dabei richtet sich die neue Höhe des Bußgeldes nach den begangenen Ordnungswidrigkeiten, aufgelistet in § 14 Abs. 1 bis 4 BSIG-E.

Die in der alten Version des RefE formulierte Orientierung an den DSGVO-Bußgeldern wurde zwar erfreulicherweise in der aktuellen Version gestrichen, allerdings verweist nun § 14 Abs. 5 BSIG-E auf § 30 Abs. 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten. Der darin enthaltene Verweis hebt die Höhe des Bußgeldes in den Fällen nach § 14 Abs. 5 BSIG-E auf die zehnfache Höhe an. Damit ist indirekt eine Analogie zum DSGVO-Bußgeld nach wie vor enthalten, auch wenn die 20 Millionen Euro anders als die 4 % des weltweiten erzielten jährlichen Umsatzes nun die höchste Summe darstellt.

Der Verweis auf das Gesetz über Ordnungswidrigkeiten sollte daher ersatzlos gestrichen werden

§ 14 BSIG-E lässt zudem das Verhältnis zur DSGVO nach wie vor missen und schafft damit rechtliche Unklarheit bzgl. der zu leistenden Bußgelder. Hier ist es dringend erforderlich, sicher zu stellen, dass es nicht zu einer Doppelregulierung/-bestrafung durch DSGVO und IT-SIG 2.0 bzw. BSIG-E kommen wird (sobald personenbezogene Daten betroffen sind). Beispielsweise könnte ein Verstoß gegen § 8a Abs. 1 S. 1 BSIG zugleich einen Verstoß gegen Art. 32 DSGVO darstellen. In diesen Fällen könnte ein Unternehmen dem aktuellen RefE zufolge sowohl nach § 14 BSIG-E als auch nach Art. 83 DSGVO mit einem Bußgeld sanktioniert werden, obgleich die Bußgeldvorschrift der DSGVO in ihrem Anwendungsbereich abschließend ist. Statt wie bisher auf einen kooperativen/unterstützenden Ansatz zu setzen, folgt der derzeitige Entwurf einem bestrafenden Regulierungsansatz, der in seiner jetzigen Form zu kritisieren ist.

Der Gesetzgeber übersieht zudem, dass die Erhöhung der IT-Sicherheit ein wesentliches unternehmerisches Interesse der Verpflichteten darstellt und sie daher von sich aus ein primäres Interesse daran haben, Sicherheitsvorfälle gar nicht erst entstehen zu lassen. Dies gilt vor allem mit Blick auf bestehende vertragliche und außervertragliche Pflichten gegenüber den Versicherungskunden, der Wettbewerbssituation am Markt sowie der Verantwortung von Unternehmen gegenüber Aktionären und Investoren.

Fazit

Für die deutsche Versicherungswirtschaft ist eine möglichst hohe IT-Sicherheit ein essenzielles Gut. Wichtig ist dabei aber, dass bei der Erreichung dieses Ziels die

unternehmerische Freiheit und das eigenverantwortliche Handeln nicht unnötig eingeschränkt werden. Für eine wettbewerbsorientierte Zukunft ist die Balance zwischen Sicherheit und Innovationspotential von Bedeutung. Der vorliegende Einwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme geht in einigen Teilen über das notwendige Maß einer Regulierung im Bereich der Kritischen Infrastrukturen hinaus und verlässt den bisherigen Ansatz eines kooperativen Miteinanders von Staat und Wirtschaft.

Berlin, den 10.12.2020