Stellungnahme

des Gesamtverbandes der Deutschen Versicherungswirtschaft

zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

- Referentenentwurf vom 4. November 2014 -

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: +32 2 28247-39
ID-Nummer 6437280268-55

Ansprechpartner:
Dr. Axel Wehling
Fred Chiachiarella

E-Mail: a.wehling@gdv.de
f.chiachiarella@gdv.de

www.gdv.de

Inhaltsübersicht

Zusammenfassung
Der Verband begrüßt, dass die Bundesregierung mit dem vorgelegten Entwurf einen wichtigen Schritt in Richtung IT-Sicherheit und vor allem Rechtssicherheit gehen möchte.

Hierbei wurden bereits die Vorschläge der Branchen zum Referentenentwurf des IT-Sicherheitsgesetzes aus dem Jahr 2013 mit in den neuen Entwurf aufgenommen. Dies gilt insbesondere für die Stärkung des kooperativen Ansatzes und die Stärkung der sogenannten Single Point of Contacts (SPOCs) der Branchen.

Änderungen sollten noch im Bereich der Meldepflichten erfolgen. So sollten die Meldungen, die keine Nennung des betroffenen Betreibers benötigen, eher anonymisiert als nur pseudonymisiert und sicher über die SPOCs erfolgen.

Insbesondere muss sichergestellt werden, dass durch mögliche Spezialgesetzgebung keine dezentralen Meldestrukturen geschaffen werden, die die Möglichkeiten der schnellen und fachkundigen Analyse und unverzügliche Weiterleitung an das Bundesamt stark beeinträchtigen würden.

1. Einleitung

Der Gesamtverband der Deutschen Versicherungswirtschaft begrüßt die Schwerpunktsetzung auf IT-Sicherheit in der Digitalen Agenda und die Fortführung der Initiative der Bundesregierung, mit dem Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) nicht nur IT-Sicherheit, sondern vor allem auch Rechtssicherheit zu schaffen.

Die Versicherungswirtschaft ist einer der Wirtschaftszweige, der mit als erster die Digitalisierung aufgegriffen und vorangetrieben hat. Sie ist nicht nur Nutzer neuer Informations- und Kommunikationstechnologien, sondern auch Impulsgeber für Innovationen und Stärkung der Informationsgesellschaft. Die verantwortungsvolle Verarbeitung umfangreicher und oft sensibler Daten ist daher die Basis eines erfolgreichen Versicherungsgeschäfts, IT- und Datensicherheit sind für die Versicherungswirtschaft Kernanliegen.

Zum jetzt vorliegenden Referentenentwurf (Stand: 4. November 2014) möchten wir wie folgt Stellung nehmen:

2. Änderungen zum Entwurf der letzten Legislaturperiode

Aus Sicht der Versicherungswirtschaft ist es erfreulich, dass die Vorschläge und Kritikpunkte der Wirtschaft zum Referentenentwurf aus dem Jahr 2013 aufgenommen wurden. Hierbei sind vor allem die folgenden Punkte hervorzuheben:

2.1. § 8a Abs. 1, 3 BSIG

Absatz 1:
Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der Stand der Technik zu berücksichtigen. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

Absatz 3:
Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und, soweit erforderlich, im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.

Der Nachweis der Vorkehrungen aus Absatz 1 („angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse“) gemäß Absatz 3 wird im neuen Entwurf weiter gefasst, was den betroffenen Unternehmen den erforderlichen Gestaltungsrahmen und verantwortliche Umsetzung ermöglicht und daher zu begrüßen ist.

Allerdings wird in Absatz 3, Sätze 3 und 4 die Übermittlung der gesamten Prüfungsunterlagen, für den Fall der Entdeckung von Sicherheitsmängeln bei der Aufstellung der Nachweise, nicht auf signifikante Sicherheitsmängel beschränkt. Dies hat der Verband bereits in seiner letzten Stellungnahme angemerkt.

2.2. § 8a Abs. 2 BSIG

Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten.

Der Verband befürwortet explizit den hier festgeschriebenen gemeinsamen, kooperativen und verantwortlichen Ansatz, der bereits in den letzten Jahren aktiv im Umsetzungsplan KRITIS (UP KRITIS) - auch mit seinen Branchenarbeitskreisen als „etablierte Kooperationsplattform“[1] - erfolgreich installiert wurde. Nach Inkrafttreten der Regelung kommt es

[1] Referentenentwurf zum IT-Sicherheitsgesetz, S. 36, 3. Absatz

natürlich darauf an, wie genau das Verfahren ausgestaltet wird und dass die Betreiber Kritischer Infrastrukturen wirklich ein Mitspracherecht bei den brancheneigenen Standards haben werden. Der Verband wird sich in diesen Prozess konstruktiv und zielorientiert einbringen.

2.3. § 8b Abs. 5 BSIG

Zusätzlich zu den Kontaktstellen nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame Ansprechstelle benennen. Wurde eine solche benannt, erfolgt der Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt nach Absatz 2 Nummer 4 und nach Absatz 4 Satz 1 über die gemeinsame Ansprechstelle.

Der Verband begrüßt ausdrücklich die durch diese Regelung vorgenommene, effiziente Stärkung der sogenannten Single Point of Contacts (SPOCs), die neben den Kontaktstellen der Betreiber benannt werden können. Dies wird zu einer verkürzten Kommunikation zwischen den Branchen und dem Bundesamt führen und damit insbesondere auch zu schnelleren Reaktionszeiten in Krisenfällen. Aber auch für kleine Versicherungsunternehmen, die von den Reglungen nicht betroffen sind, ist ein solcher Branchenansprechpartner als Bindeglied zu den zuständigen Behörden sinnvoll.

Bereits im Jahr 2010 wurde von der Versicherungswirtschaft das Krisenreaktionszentrum für IT-Sicherheit der deutschen Versicherungswirtschaft GmbH (LKRZV) gegründet. Es erfüllt bereits jetzt die Forderung der Bundesregierung und ihrer Bundesbehörden, im IT-Krisenfall die Reaktions- und Kommunikationsfähigkeit innerhalb der Branche und mit den zuständigen Behörden sicherzustellen. Das LKRZV gilt in der Versicherungswirtschaft und bei den Bundesbehörden als kompetenter Ansprechpartner, wenn es um IT-Sicherheit geht und arbeitet bereits von Beginn an aktiv in den Gremien des UP KRITIS mit.

In Satz zwei dieses Absatzes wird betont, dass insbesondere die pseudonymisierten Meldungen über den SPOC zu erfolgen haben. Dies ist zu begrüßen.

Eine Beschränkung auf § 8b Absatz 4 Satz 1 ist an dieser Stelle jedoch nicht sinnvoll. Aus Gründen der Rechtsklarheit sollte sich die Formulierung auf den gesamten § 8b Absatz 4 beziehen, um zu verdeutlichen, dass die SPOCs die Meldungen ebenso wie die Kontaktstellen der Betreiber übernehmen können.

2.4. § 8 c Abs. 1 BSIG

Die §§ 8a und 8b finden keine Anwendung auf Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

Diese Regelung stellt sicher, dass insbesondere kleinere Unternehmen durch Administrationskosten und Kosten für den Nachweis der technischen und organisatorischen Vorkehrungen nach § 8a I, III BSIG nicht unverhältnismäßig belastet werden. Auch diese Regelung wird daher ausdrücklich begrüßt. Schließlich ist festzustellen, dass auch die nicht betroffenen Versicherungsunternehmen selbstverständlich höchste Anforderungen an ihre IT-Sicherheit erfüllen.

Zu Rückversicherungen ist festzustellen, dass diese der Risikobewältigung einzelner Versicherungsunternehmen dienen und daher per se nicht als Kritische Infrastruktur angesehen werden können. In der Versicherungsbranche sind nur Erstversicherungen als kritisch anzusehen, da diese den direkten Kontakt zu den Verbrauchern haben, was bei Rückversicherern nicht der Fall ist. Dies gilt umso mehr, wenn die Rückversicherer keinen Hauptsitz in Deutschland haben.

3. Artikel 1: Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

3.1. § 8b Abs. 4 BSIG

Betreiber Kritischer Infrastrukturen haben bedeutende Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der von ihnen betriebenen Kritischen Infrastrukturen führen können, über die Kontaktstelle unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur geführt hat.

Der Verband begrüßt, dass mit „bedeutende Störungen“ nun eine Formulierung gefunden wurde, die zusammen mit der höchstrichterlichen Rechtsprechung zu § 100 I TKG eine klare und rechtssichere Grundlage für das weitere Verfahren darstellen kann.

Der Verband befürwortet außerdem, dass die Meldepflicht nunmehr in mehreren Stufen erfolgen soll und dass „Die Nennung des Betreibers […] nur dann erforderlich [ist], wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur geführt hat.“ Jedoch ist laut Gesetzesbegründung vorgesehen, dass diese pseudonymisiert und nicht anonymisiert erfolgen soll. Wenn von einer Pseudonymisierung nicht abgewichen werden kann, muss durch ein geeignetes Verfahren sichergestellt werden, dass die Pseudoidentität von den Branchenansprechpartnern so gewählt wird, dass ein Rückschluss auf das meldende Unternehmen nicht möglich ist. Hier wäre es essentiell, dass die Meldungen soweit wie möglich anonym erfolgen, da vor allem ein nationales Lagebild erstellt werden soll.

Das System für die Meldungen soll laut Gesetzesbegründungen wie folgt ablaufen: „Es beginnt mit der verschlüsselten Versendung der Meldung des betroffenen Betreibers an die gemeinsame Ansprechstelle. Der gemeinsamen Ansprechstelle ist die Identität des Meldenden bekannt, aber durch die Verschlüsselung kann er den Inhalt der Meldung nicht einsehen. In einem nächsten Schritt entfernt die gemeinsame Ansprechstelle die Identität des Betreibers und fügt eine Pseudoidentität - etwa im Sinne eines Kennzeichens - ein. Danach erfolgt der Versand der weiterhin verschlüsselten Meldung an das Bundesamt, das mithilfe eines entsprechenden Schlüssels Zugriff auf den Meldeinhalt erlangt. Eine potentiell notwendige Kommunikation zwischen den Teilnehmern erfolgt auf dem umgekehrten Weg und damit ebenfalls über die gemeinsame Ansprechstelle. Der gesamte Übermittlungsprozess muss vom Ablauf her nachvollziehbar und auch auditierbar sein.“[2]

Aus Sicht des Verbandes ist es weiterhin notwendig und bisher auch geübte Praxis, dass das LKRZV als gemeinsame Ansprechstelle den Inhalt der Meldung kennt, um ggf. eine brancheninterne Betroffenheit z. B. durch mehrere vergleichbare Warnmeldung aus verschiedenen Unternehmen schnell erkennen zu können und dem Bundesamt eine entsprechende Einschätzung mitzugeben.

[2] Referentenentwurf zum IT-Sicherheitsgesetz, S. 41-42

Gleichzeitig kann das LKRZV so branchenspezifische Warnungen an seine Mitglieder verschicken, um unabhängig von der Analyse des Bundesamtes bereits im Vorfeld die IT-Sicherheit der Branche zu stärken.

3.2. § § 8c Abs. 2, 3 BSIG

§ 8c Abs. 2 BSIG
§ 8a findet keine Anwendung auf Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen sowie auf Betreiber von Telematikinfrastrukturen nach § 291a des Sozialgesetzbuchs Fünftes Buch. Entsprechendes gilt für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes, Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes für den Geltungsbereich der Genehmigung sowie sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften vergleichbare oder weitergehende Anforderungen im Sinne von § 8a erfüllen müssen.

§ 8c Abs. 3 BSIG
§ 8b Absätze 3 bis 5 finden keine Anwendung auf Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen sowie auf Betreiber von Telematikinfrastrukturen nach § 291a des Sozialgesetzbuchs Fünftes Buch. Entsprechendes gilt für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes sowie sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften vergleichbare oder weitergehende Anforderungen im Sinne von § 8b Absätze 3 bis 5 erfüllen müssen.

Nach den hier vorliegenden Normen besteht damit die Möglichkeit, Spezialregelungen zu schaffen, die das gesamte etablierte und gut funktionierende bidirektionale Warn- und Meldesystem zwischen dem Bundesamt und den SPOCs, das in den §§ 8a und 8b Abs. 3 bis 5 BSIG ausgeführt wird, aushebeln würde.

Der Verband hat bereits in seiner Stellungnahme zum Referentenentwurf aus dem Jahr 2013 hervorgehoben, dass der Erhalt bewährter Warn- und Meldewege notwendig ist. Bei der Krisenkommunikation ist es besonders wichtig, dass diese direkt, schnell und zielgerichtet zwischen Experten erfolgt. Gewonnene Erkenntnisse müssen gerade bei relevanten IT-Sicherheitsvorfällen schnellstmöglich ausgetauscht werden, um drohenden Schäden erfolgreich entgegenwirken zu können.

Die Versicherungswirtschaft verfügt mit dem LKRZV bereits über eine sichere und bewährte zentrale Kommunikationsinfrastruktur mit dem Bundesamt. Hinzu kommt, dass das Bundesamt auch in der Vergangenheit immer wieder unter Beweis gestellt hat, dass es über die fachliche und technische Kompetenz verfügt, Meldungen schnell einzuordnen, die notwendigen Schritte zum Schutz aller Kritischen Infrastrukturen einzuleiten und gegebenenfalls den betroffenen Unternehmen und Branchen über das LKRZV Hilfe anzubieten.

Hier dezentrale Meldestrukturen für die Versicherungsunternehmen über die Aufsichtsbehörde BaFin (zum Bundesamt) einzuführen, würde nicht nur den Alarmierungsweg unnötig verlängern und damit den Schaden möglicherweise vergrößern, sondern auch verhindern, dass Sicherheitswarnungen branchenübergreifend und schnellstmöglich versandt werden können. Dem Anspruch des IT-Sicherheitsgesetzes, die IT-Sicherheitslage für ganz Deutschland zu verbessern, würde diese Regelung nicht gerecht werden.

Es würde außerdem dazu führen, dass die Aufsicht über die Kritischen Infrastrukturen in verschiedene Aufsichtsbereiche (bspw. Bundesamt für Verkehr oder das Bundesamt für Ernährung und Landwirtschaft) zerfasert und damit einen erheblichen Bedeutungsverlust erleiden würde. Ein einheitliches Lagebild - welches in § 8 Abs. 2 Nr. 3 BSIG als Aufgabe des Bundesamtes explizit genannt wurde - und schnelle Reaktionen, die allen KRITIS-Branchen zugutekommen, wären so praktisch unmöglich.

Der Verband plädiert daher für die ersatzlose Streichung in beiden Absätzen ab „sowie“ („…sowie sonstige Betreiber Kritischer Infrastrukturen, die aufgrund von Rechtsvorschriften vergleichbare oder weitergehende Anforderungen im Sinne von § 8b Absätze 3 bis 5 erfüllen müssen….“).

Alternativ besteht die Möglichkeit, dass Aufsichtsbehörden die Informationen über Vorfälle aus den entsprechenden Branchen über das Bundesamt erhalten. Damit werden das Bundesamt sowie die Kritischen Infrastrukturen über ihre „Branchen-SPOCs“ zu einem effizienten und möglichst unbürokratischen Verfahren beitragen. So kann auch das Interesse der Betreiber Kritischer Infrastrukturen, einen einzigen und schnellen Warn- und Meldeweg zu einer kompetenten Behörde zu haben, mit dem Interesse der Aufsichtsbehörden, Informationen zu erhalten, in Einklang gebracht werden.

3.4. § 8d BSIG

§ 8dAbs. 1 BSIG Das Bundesamt kann auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3 erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4 erteilen, wenn keine schutzwürdigen Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem entgegenstehen und durch die Auskunft keine Beeinträchtigung des Verfahrens oder sonstiger wesentlicher Sicherheitsinteressen zu erwarten ist.

§ 8d Abs. 2 BSIG Zugang zu den Akten des Bundesamtes in Angelegenheiten nach § 8a und § 8b wird nur Verfahrensbeteiligten gewährt.

Diese Regelung ist als Lex Specialis zum Informationsfreiheitsgesetz (IFG) anzusehen. Bei dem hier beschriebenen Verfahren ist jedoch sicherzustellen, dass auch pseudonymisierte Meldungen nicht an einen beliebig großen Empfängerkreis gegeben werden dürfen. Hierbei ist auch zu bedenken, dass bereits weitgehende Meldepflichten auch gegenüber den Betroffenen im Falle des Datenabflusses nach Bundesdatenschutzgesetz (BDSG) bestehen.

Berlin, den 12. November 2014

12.11.2014

Bundesministeriums des Innern
Alt-Moabit 101D
10559 Berlin

Anlage zur

Stellungnahme des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. zum IT-Sicherheitsgesetz, Referentenentwurf vom 4. November 2014

Hier: Kostenschätzung

In der Einladung zur Verbändeanhörung wurden wir gebeten, neben der Abgabe einer Stellungnahme, eine zahlenmäßige Schätzung zu den erwarteten jährlichen Meldefällen, den pro Meldung entstehenden Kosten sowie den erwarteten Kosten für die in § 8a Absatz 3 BSI-Gesetz (neu) vorgesehenen Audits zu übermitteln. Dies möchten wir im Folgenden tun:

Zu erwartende Anzahl jährlicher Meldefälle und pro Meldung entstehende Kosten

Zu der zu erwartenden Anzahl jährlicher Meldefälle und den Kosten pro Meldung hat der Bundesverband der Deutschen Industrie e.V. bereits eine Studie mit dem Titel „IT-Sicherheit in Deutschland - Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes“ vorgelegt. An den darin ermittelten Kosten werden wir uns orientieren.

Demnach sind pro Meldung Kosten in Höhe von 660 EUR zu erwarten. Diese Zahl wurde aus den Faktoren „Zeitaufwand pro Meldung“ (11 Stunden) und „Kosten je Zeiteinheit“ (60 EUR pro Stunde für einen ausgebildeten Informatiker) errechnet. Da mit den erhöhten Anforderungen auch ein erhöhter Bedarf an Fachpersonal (bspw. Forensiker und Rechtsanwälte) einhergeht, ist davon auszugehen, dass diese Kosten in Zukunft eher höher sein werden.

Weiterhin geht die Studie von ca. 50 Meldungen pro Jahr und Unternehmen aus. Laut der Studie beruht die Annahme „auf einer pragmatischen Schätzung, die aus der Beobachtung und Befragung der für die Behandlung von IT-Sicherheitsvorfällen eingesetzten Spezialisten basiert“[1]. Da laut Gesetzesbegründung dazu „insbesondere Fälle von Sicherheitslücken, Schadprogrammen und erfolgten, versuchten oder erfolgreich abgewehrten Angriffen auf die Sicherheit in der Informationstechnik sowie außergewöhnliche und unerwartete technische Defekte mit IT-Bezug (z. B. nach Softwareupdates oder ein Ausfall der Serverkühlung)“[2] zählen, ist von sehr viel höheren Zahlen auszugehen.

[1] Studie des Bundesverband der Deutschen Industrie e.V., „IT-Sicherheit in Deutschland - Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes“, Seite 32
[2] Referentenentwurf zum IT-Sicherheitsgesetz, Begründung zu § 8b BSI-G (neu), Seite 40

Nach § 8c Absatz 1 BSI-Gesetz (neu) und der darauf folgenden Rechtsverordnung sind die Unternehmen nicht betroffen, die „Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).“ darstellen. Ca. 63 % der Versicherungsunternehmen erfüllen diese Vorgaben nicht und sind daher vom neuen IT-Sicherheitsgesetz betroffen.

Aus den oben genannten Kriterien ergibt sich für die Versicherungswirtschaft folgendes Bild:

		Meldungen pro Jahr		
Gesamt VU	**betroffen***	**50**	**100**	**150**
KrankenV: 46	**32**	1.056.000 EUR	2.112.000 EUR	3.168.000 EUR
LebensV: 97	**76**	2.508.000 EUR	5.016.000 EUR	7.524.000 EUR
KompositV: 213	**115**	3.795.000 EUR	7.590.000 EUR	11.385.000 EUR
Gesamt: 356	**223**	**7.359.000 EUR**	**14.718.000 EUR**	**22.077.000 EUR**

Zu erwartende Kosten für die in § 8a Absatz 3 BSI-Gesetz (neu) vorgesehenen Audits:

Der Aufwand und damit die Kosten für eine Zertifizierung oder für ein Audit hängen stark vom Zertifizierungsverfahren, von den jeweiligen Gegebenheiten im Unternehmen und insbesondere dem gewählten Informationsverbund ab. Insofern können die folgenden Kosten nur ungefähre Schätzungen darstellen:

Zum Beispiel werden für eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz im Durchschnitt die folgenden Eckdaten angesetzt:

- 30 PT externer Prüfer für ein (Re-)Zertifizierungsaudit alle drei Jahre
- 2.500 EUR für das BSI-Zertifikat alle drei Jahre
- 11,5 PT externe Prüfer für die Überwachungsaudit in den Jahren dazwischen

Der jährliche Aufwand zur Vorbereitung eines solchen Audits kann bei einem größeren Verbund durchaus deutlich über 100 PT (intern und extern) liegen. Die Kosten können somit mit 100.000 EUR bis 200.000 EUR pro Jahr angegeben werden.

Die Vorbereitung einer Erstzertifizierung ist deutlich teurer. So werden hierfür Kosten für die Vorbereitung und Durchführung in Höhe von 500.000 EUR bis 1.000.000 EUR angesetzt.

Fazit

In der Gesetzbegründung ist ausgeführt, dass nur „die Einrichtung und Aufrechterhaltung entsprechender Meldewege“ zu Kosten führen würde. Es würden nur dann Mehrkosten entstehen, wenn „bislang noch kein hinreichendes Niveau an IT-Sicherheit bzw. keine entsprechenden Meldewege etabliert sind.“ Weitere Kosten entstünden „durch die Durchführung der vorgesehenen Sicherheitsaudits.“

* Ausweislich des Referentenentwurfs vom 4. November 2014, vorbehaltlich möglicher weiterer Regelungen, wie beispielsweise Rechtsverordnungen oder Verwaltungsakte.

Die Versicherungswirtschaft gehört zu den Vorreiterbranchen in Bezug auf die Sicherheit ihrer IT-Systeme und hat bereits heute im Wesentlichen die „angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse“ gemäß § 8a Absatz 1 BSI-Gesetz (neu) umgesetzt sowie auch die Meldewege durch das Krisenreaktionszentrum für IT-Sicherheit der deutschen Versicherungswirtschaft GmbH (LKRZV) sichergestellt.

Auch auf Basis der Kostenschätzung ist es immens wichtig, jetzt bei der Entwicklung von Branchenstandards darauf zu achten, dass diese sehr effizient und damit im Idealfall aufwandssenkend erfolgen können. Insbesondere sind Mehrfachmeldewege bzw. nicht einheitliche Meldestrukturen zu vermeiden.