SPEKTRUM

für Versicherungsrecht (SpV)

Arbeitsgemeinschaft Versicherungsrecht im DAV

Ausgabe 1
Februar 2018

www.spektrum-versicherungsrecht.de
www.davvers.de

Inhalt

Editorial

Sehr geehrte Leser des Spektrum für Versicherungsrecht,

der erste Monat des Jahres 2018 liegt schon hinter uns, die erste Veranstaltung in diesem Jahr, die die Arbeitsgemeinschaft zu Fortbildungszwecken und der Möglichkeit des fachlichen Gedankenaustauschs anbietet, am 17. Februar 2018 in Obernai/Elsaß vor uns.

Am 22. und 23. Juni 2018 wollen wir uns in Baden-Baden zur Fachtagung treffen, die auf Referentenseite ausschließlich von den Mitgliedern des IV. Zivilsenats des Bundesgerichtshofs gestaltet wird. Wir freuen uns darauf, dass wir erneut Gastgeber dieser exklusiven Fortbildungsveranstaltung sein dürfen.

Heute darf ich Sie auch davon in Kenntnis setzen, dass aufgrund der persönlichen Unterstützung des Verlegers, Herrn Dr. Hans-Dieter Beck, dankenswerter Weise auch in diesem Jahr für unsere Mitglieder die Möglichkeit besteht, zu ermäßigten Teilnehmerpreisen an den inhaltlich spannend gestalteten und mit hochkarätigen Referenten besetzten Seminaren der MWV Münchener Wirtschaftsseminare teilzunehmen. Diese Seminare finden regelmäßig an einem Wochentag statt, so dass auch zahlreiche Sachbearbeiter der Assekuranz hieran teilnehmen und die Möglichkeit zum Gedankenaustausch und zum Kennenlernen besteht. Die Mitglieder der Arbeitsgemeinschaft erhalten von mir in den nächsten Tagen per Email eine Nachricht, der ein besonderes Anmeldeformular für die die MWV-Seminare beigefügt ist, die in München, Köln und Hamburg stattfinden.

Im Jahr 2008 ist das reformierte VVG in Kraft getreten, Anlass für die Arbeitsgemeinschaft, den diesjährigen Versicherungsrechtstag unter dem Titel „10 Jahre VVG-Reform – Auswirkungen auf die Praxis“ durchzuführen. Der Versicherungsrechtstag findet am 28. und 29. September 2018 im Arabella Carlton Hotel in Nürnberg statt, wir hoffen auf rege Beteiligung. Nähere Einzelheiten hierzu kann ich zu einem späteren Zeitpunkt mitteilen.

Besondere Aufmerksamkeit wird der Bereich der Berufsunfähigkeitsversicherung erfahren; in Hinblick auf den Umstand, dass die Leistungsverweigerung des Versicherers bei Eintritt des Versicherungsfalls den betroffenen Versicherungsnehmer vor existentielle Probleme stellen kann, bedarf es wohl in stärkerem Maße als bisher der Aufklärung und größerer publizistischer Präsenz als bisher, um den vertragsschließenden Versicherungsnehmer in spe über seine Pflichten bei Abschluss eines Vertrages zu unterrichten.

Ich wünsche Ihnen im Namen aller Mitglieder des Geschäftsführenden Ausschusses der Arbeitsgemeinschaft Versicherungsrecht ein spannendes und erfolgreiches Jahr 2018.

Berlin, im Februar 2018

Monika Maria Risch
Rechtsanwältin u. Fachanwältin f. Versicherungsrecht

Die Musterbedingungen des GDV für die Cyberrisiko-Versicherung*

Im April 2017 hat der Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) seine unverbindlichen Musterbedingungen für die Cyberrisiko-Versicherung bekannt gegeben. Die Veröffentlichung war von den Marktteilnehmern mit Spannung erwartet worden. Der GDV hat mit der Entwicklung der Musterbedingungen für die Cyberrisiko-Versicherung auf ein gesteigertes Marktbedürfnis reagiert, insbesondere für den Bereich kleiner und mittelständischer Unternehmen. Am Markt bereits bestehende Versicherungskonzepte konzentrierten sich nämlich in erster Linie auf den industriellen Bereich. Hinzu kommt, dass sich der Markt für Cyberversicherungen insgesamt durch ein sehr heterogenes Angebot kennzeichnet. Die Unterschiede sind vielfältig und zeigen sich sowohl im Aufbau, wie etwa auch in Bezug auf die Beschreibung des versicherten Risikos, den Versicherungsfall, Ausschlüsse und einzelne Leistungsbausteine.[1]

Die GDV-Musterbedingungen bezwecken, Anbietern als auch Kunden als Orientierungshilfe zu dienen und dabei zur Entwicklung des noch jungen Marktes der Cyberversicherungen beizutragen.[2] Als echte Multi-Line Police konzipiert, bündelt die Cyberrisiko-Versicherung Elemente aus den klassischen Sparten der Haftpflicht- und Sachversicherung, respektive der Technischen Versicherung, in einem Produkt.

I. Aufbau und Struktur der Cyberrisiko-Versicherung

Entsprechend der neuen Struktur der Verbandsbedingungen sind die Musterbedingungen in zwei Teile gegliedert. Teil A besteht aus vier Abschnitten und enthält die spezifischen Bestimmungen zur Ausgestaltung des Versicherungsschutzes in der Cyberrisiko-Versicherung. Hervorzuheben ist dabei der gewählte modulare Ansatz.[3] So sehen die Musterbedingungen insbesondere jeweils separate Bausteine für Kostenpositionen vor und nach Eintritt des Versicherungsfalls, Drittschäden und Eigenschäden vor. Dies eröffnet im Einzelfall flexible Gestaltungsmöglichkeiten. So könnte das Produkt je nach Bedarf etwa auch ohne Drittschaden-Komponente oder Betriebsunterbrechung angeboten werden. Desgleichen können etwaige Anpassungen und Nachjustierungen einfacher im Rahmen der einzelnen Leistungsbausteine vorgenommen werden.

Eine hervorgehobene Stellung im Rahmen des modularen Konzepts nimmt der in Abschnitt A1 geregelte Basis-Baustein ein, da er die allgemeinen, für sämtliche Bausteine geltenden Regelungen vor die Klammer zieht. Im Einzelnen enthält der Basis-Baustein Regelungen zum sachlichen, persönlichen und räumlichen Anwendungsbereich der Musterbedingungen, zum Versicherungsfall und zu den versicherten Zeiträumen, zu den Obliegenheiten sowie den generellen Ausschlüssen.

Teil B der Musterbedingungen für die Cyberrisiko-Versicherung enthält die im Wesentlichen VVG-basierten allgemeinen Bestimmungen über Rechte und Pflichten der Parteien (Beitragszahlung, Kündigung, Gefahrerhöhung, etc.).

II. Versichertes Risiko

Zum versicherten Risiko im Rahmen der Cyberrisiko-Versicherung gehören Vermögensschäden und Kostenpositionen, die durch eine Informationssicherheitsverletzung verursacht worden sind. An dieser Stelle zeigen sich bereits Unterschiede zu anderen Marktbedingungen. Bisweilen wird der Gegenstand der Versicherung für sämtliche Bausteine separat definiert; teilweise werden auch unterschiedliche Termini zur Beschreibung des versicherten Risikos verwendet („Netzwerksicherheitsverletzung“ oder „Datenrechtsverletzung“, etc.).

1. Informationssicherheitsverletzung

Ausgehend von den Schutzzielen der Informationssicherheit wird der Begriff der Informationssicherheitsverletzung in A1-2.1 AVB-Cyber definiert als eine Beeinträchtigung der Verfügbarkeit, Vertraulichkeit, Integrität elektronischer Daten oder informationsverarbeitender Systeme, die der Versicherungsnehmer zur Ausübung seiner beruflichen Tätigkeit nutzt. Da es ausschließlich auf die Nutzung der Systeme zu beruflichen Zwecken ankommt, fällt sowohl die Nutzung privater Geräte zu beruflichen Zwecken („byod“= bring your own device), als auch die Verarbeitung auf Systemen externer Dienstleister in den Deckungsbereich. Was den Einsatz externer Dienstleister betrifft, so ergeben sich versicherungstechnisch angesichts der potentiellen Kumul-Last allerdings gewisse Schwierigkeiten, denn bei einem Aus-

---

* Der Autor ist Rechtsreferendar und wissenschaftlicher Mitarbeiter am Lehrstuhl für Bürgerliches Recht, Handels- und Gesellschaftsrecht, Privatversicherungsrecht und Internationales Privatrecht an der Freien Universität Berlin bei *Prof. Dr. Christian Armbrüster*. Der Autor hat an der Erarbeitung der Musterbedingungen für die Cyberrisiko-Versicherung als Mitglied der Projektgruppe „Cyberversicherung“ beim Gesamtverband der Deutschen Versicherungswirtschaft e.V. mitgewirkt.

1 *Pawig-Sander*, VW 6/2017, 55.

2 *Graß/Pache*, PHi 2017, 122, 124.

3 *Graß/Pache*, PHi 2017, 122, 125.

fall, respektive einer Störung oder Unterbrechung der Dienstleistung, sind potentiell sämtliche Kunden des Dienstleisters durch ein einziges Schadenereignis betroffen. Zur Risikobegrenzung sind Angriffe auf einen Cloud-Dienstleister, die zu einem Ausfall, einer Störung oder Unterbrechung der Dienstleistung führen, deshalb prinzipiell vom Versicherungsschutz ausgenommen. Versichert bleiben sollen allerdings (zielgerichtete) Angriffe auf den Versicherungsnehmer beim Cloud-Dienstleister. Konkret bedeutet das: Wird z.B. der Zugang des VN beim Dienstleister gehackt und Daten gelöscht, verschlüsselt oder anderweitig verändert, besteht grundsätzlich Versicherungsschutz im Umfang der einzelnen versicherten Leistungsbausteine; bezieht sich der Angriff dagegen auf den Cloud-Anbieter und führt zu dessen vollständigem Ausfall, besteht keine Deckung.

Aus der Regelung in A1-2.4 AVB-Cyber ergibt sich, dass der Eintritt der Informationssicherheitsverletzung durch eines der dort benannten Ereignisse eintreten muss. Anders als die meisten Anbieterwordings werden die Ursachen allerdings abstrakt und nicht ausgehend von konkreten Angriffsszenarien (wie z.B. Denial-of-Service-Attacken, Cyber-Erpressung, etc.) beschrieben. Dies eröffnet Auslegungsspielräume, die zu Gunsten einer möglichst umfassenden Berücksichtigung auch neuer Risikoszenarien bewusst in Kauf genommen wurden.

2. Vermögensschaden

In Abgrenzung zu Personen-, Sach- und daraus resultierenden sog. Vermögensfolgeschäden entspricht die Definition in A1-3 AVB-Cyber im Wesentlichen der gängigen versicherungsrechtlichen Terminologie reiner Vermögensschäden. Wichtig ist die Klarstellung, dass elektronische Daten keine Sache i.S. der Bedingungen sind. Dies gilt unabhängig von ihrer Verkörperung auf einem physischen Datenträger. Hervorzuheben ist auch der Hinweis, dass der Verlust von elektronischen Daten als Folge des Abhandenkommens von Sachen als Vermögensschaden versichert bleibt. Gemeint ist damit der Verlust von Daten aus dem Abhandenkommen von Hardware i.S. einer Verletzung der Verfügbarkeit, nicht dagegen die Kosten für den Neuerwerb verlorener Hardware. Denkbar ist auch der Ersatz von Kosten zur Erfüllung gesetzlicher Benachrichtigungspflichten, wenn aufgrund eines Datenträgerverlustes damit zu rechnen ist, dass sensible Daten Dritten zur Kenntnis gelangen.

III. Einheitlicher Versicherungsfall

Dem Versicherungsfall liegt das Manifestationsprinzip zu Grunde. Die Anbindung des Versicherungsfalls an die Manifestation des Schadens ermöglicht – anders als die Schadenereignistheorie – eine eindeutige zeitliche Zuordnung des Versicherungsfalls. Oftmals lässt sich nämlich der genaue Zeitpunkt des Eintritts einer Informationssicherheitsverletzung nicht beweissicher feststellen, der Eintritt eines Schadens dagegen schon. Eine genaue zeitliche Zuordnung ist allerdings gerade im Hinblick auf die Erfüllung vertraglicher Obliegenheiten sowie zur Gewährleistung einer rechtzeitigen Einbindung des Versicherers in das Schadenmanagement entscheidend.

Der Versicherungsfall gilt schließlich einheitlich für sämtliche Leistungsbausteine. In Abweichung dazu wird in der Praxis häufig für die Drittschaden-Komponente gesondert das claims-made-Prinzip als Versicherungsfall zu Grunde gelegt. Dies führt zu unterschiedlichen zeitlichen Anknüpfungen innerhalb der verschiedenen Leistungsbausteine und muss etwa im Hinblick auf Obliegenheiten, die in zeitlicher Hinsicht vom Eintritt des Versicherungsfalls abhängen (z.B. § 82 VVG), Beachtung finden.

IV. Vorrangigkeit der Cyberrisiko-Versicherung

Um eine möglichst frühzeitige Einbindung des Versicherers im Schadenfall zu gewährleisten, sehen die Musterbedingungen eine Vorrangigkeit der Cyberrisiko-Versicherung gegenüber anderen Versicherungen vor. Dies ist angesichts der weitreichenden Service-Elemente zur Gewährleistung eines effizienten Schadenmanagements zur Reduzierung von Ausfallzeiten auch erforderlich.

V. Ausschlüsse

Die allgemeinen, bausteinübergreifenden Ausschlüsse sind in A1-17 geregelt. Daneben sehen die einzelnen Leistungsbausteine besondere Ausschlüsse vor (A3-7; A4-1.2; A4-2.3). Marktseitig besteht sicherlich ein großes Bedürfnis für die Versicherung von Lösegeld-/Erpressungsforderungen angesichts der Betroffenheit der Unternehmen durch Ransomware. Letzteres ist vom Versicherungsschutz ausgeschlossen. Diese Entscheidung erfolgte allerdings noch in dem Bewusstsein, dass die Verlautbarung R 3/98 des Bundesamtes für das Versicherungswesen ein Verbot für die Bündelung der Lösegeld-/Produkterpressungsversicherung mit anderen Versicherungsprodukten vorsah. Das Bündelungsverbot hat die BaFin inzwischen in Bezug auf die Cyber-Versicherung aufgegeben.[4] Die übrigen darin geregelten Voraussetzungen für den Betrieb einer Lösegeldversicherung gelten allerdings fort.

Im Hinblick auf den Geldbußenkatalog der EU-Datenschutz-Grundverordnung dürfte marktseitig auch die Nachfrage nach einer Versicherung gegen Geldstrafen und Geldbußen steigen. Auch insoweit sehen die Musterbedingungen – ähnlich wie für das Verbandsmodell der D&O-Versicherung – einen Ausschluss vor. Zu berücksichtigen ist außerdem, dass vor dem Hintergrund ihres Sanktionszwecks gewichtige Gründe dafür sprechen, die Versicherung von Geldstrafen und Geldbußen

4 Vgl. die Mitteilung der BaFin vom 15.9.2017, abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichung-en/DE/Meldung/2017/meldung_170915_loesegeldversicherung.html.

als sittenwidrig einzustufen.[5] Verschiedene Marktbedingungen bieten hier Versicherungsschutz unter dem Vorbehalt der rechtlichen Zulässigkeit.

VI. Einzelne Leistungsbausteine

Die einzelnen Leistungsbausteine sind in den Abschnitten A2-A4 geregelt.

1. Service-/Kosten-Baustein

Abschnitt A2 regelt Kostenpositionen für den Zeitpunkt vor und nach Eintritt des Versicherungsfalls. Neben Forensik-Kosten zur Schadenfeststellung und damit zum Nachweis des Versicherungsfalls, enthält der Kosten-Baustein insbesondere das Angebot verschiedener Krisendienstleistungen (PR-Management, Benachrichtigungskosten, Call-Center-Leistungen), die dabei helfen sollen, ein effizientes Schadenmanagement zu gewährleisten, um so den Schaden möglichst gering zu halten. Sämtliche versicherte Dienstleistungen im Schadenfall knüpfen an ein enges Abstimmungsverhalten mit dem Versicherer an. Grund dafür ist, dass alle versicherten Kostenpositionen zum Zeitpunkt der Vertragsprüfung nicht prognostizierbar sind, da sie von der Art und dem Umfang des Cyber-Angriffs abhängen. Eine weitere Besonderheit des Kosten-Bausteins ist zudem der Ersatz vorgezogener Rettungskosten gem. A2-3 AVB-Cyber zur Vermeidung eines unmittelbar drohenden Schadens.

2. Drittschaden-Baustein

Abschnitt A3 regelt den klassischen Haftpflichtversicherungsschutz für den Fall, dass der Versicherungsnehmer wegen einer Informationssicherheitsverletzung, die einen Vermögensschaden zur Folge hat, aufgrund gesetzlicher Haftpflichtbestimmungen privatrechtlichen Inhalts von einem Dritten auf Schadensersatz in Anspruch genommen wird. Vom Versicherungsschutz umfasst sind insbesondere auch Drittansprüche wegen Persönlichkeits- und Namensrechts-, Urheber- und Markenrechtsverletzungen. Fakultative Deckungserweiterungen bestehen für Vertragsstrafen wegen der Verletzung der PCI-Datensicherheitsstandards sowie in begrenztem Umfang für Folgeschäden aus dem Bereich der Vertragserfüllung. Beides im Umfang eines vertraglich fixierten Sublimits. Abwehrkosten werden nicht generell auf die Versicherungssumme angerechnet, sondern analog zur Betriebshaftpflichtversicherung ausschließlich bei Versicherungsfällen mit Auslandsbezug. Tendenziell weiter als die bisherige Marktpraxis gehen die AVB-Cyber im Hinblick auf das Produkt- und Leistungsrisiko, für das kein genereller Ausschluss vorgesehen ist.[6] Dies macht – angesichts des reinen Vermögensschadencharakters – insbesondere eine Abgrenzung zum erweiterten Produkthaftpflichtmodell erforderlich.

3. Eigenschaden-Baustein

Abschnitt A4 regelt den Versicherungsschutz für Eigenschäden des Versicherungsnehmers. Der Versicherungsschutz umfasst einerseits den Ertragsausfallschaden in Folge einer Betriebsunterbrechung, andererseits notwendige Aufwendungen zur Datenwiederherstellung. Eine Besonderheit besteht allerdings darin, dass im Schadensfall keine Berechnung des konkreten Unterbrechungsschadens erfolgt. Der Versicherer leistet in diesem Fall Entschädigung in Höhe eines vereinbarten Tagessatzes. Dies ermöglicht eine einfache und transparente Schadenregulierung.

VII. Risikomanagement und Versicherungsschutz

Ein effektives Risikomanagement kann die Wahrscheinlichkeit und das Ausmaß eines Schadens erheblich senken. Ein ausreichendes IT-Sicherheitsniveau ist deshalb Grundlage für die Gewährung weitreichenden Versicherungsschutzes. Zertifizierungen sowie die Verpflichtung zur Einhaltung technischer Standards können dabei eine maßgebliche Rolle spielen. Um den Erstversicherer bei der Bewertung des Risiko- und Schadenpotenzials zu unterstützen, hat der GDV zudem zusätzlich zu den Musterbedingungen einen unverbindlichen Muster-Fragebogen zur Risikoerfassung entwickelt.[7] Daneben spielen vertragliche Obliegenheiten eine entscheidende Rolle. Es reicht nämlich nicht aus, ein angemessenes Sicherheitsniveau bei Abschluss der Versicherung festzustellen. Vielmehr muss gewährleistet sein, dass der Versicherungsnehmer auch für die Dauer des Vertrags ein angemessenes IT-Sicherheitsniveau sicherstellt. Die in A1-16 AVB-Cyber im Einzelnen beschriebenen Obliegenheiten definieren das erforderliche Schutzniveau.

Dan Schilbach
Wissenschaftlicher Mitarbeiter
Freie Universität Berlin

5 *Armbrüster/Schilbach*, r+s 2016, 109, 112 ff.

6 Beachte aber: A1-17.6 (Fahrzeuge-Ausschluss) und A3-7.1 (Rückruf-Ausschluss).

7 http://www.gdv.de/wp-content/uploads/2017/08/Risikofragebogen_Cyber_August2017.pdf.

Impressum: „Spektrum für Versicherungsrecht" (SpV) erscheint viermal jährlich (i. d. R. in der Mitte des Quartals) als Beilage zur Zeitschrift „recht und schaden".
Schriftleitung (v. i. S. d. P.): RAin Isabell Knöpper, Kanzlei Dr. Eick & Partner, Anger 63, 99084 Erfurt,
Telefon: (0361) 57675-0, Telefax: (0361) 57675-20.
Verlag und Druck: Verlag C. H. Beck oHG (siehe Impressum der Zeitschrift „recht und schaden")