Versicherungswirtschaft

Magazin für Führungskräfte und Entscheider

73. Jahrgang | JANUAR 2018 | 19,– €

ISSN 0042-4358 | E 6945

Bedrohliche Verführung

Wie künstliche Intelligenz einer ganzen Branche den Kopf verdreht

INTERVIEW

Christoph Schmallenbach über den Generali-Umbau

RISIKOMARKT HEILWESEN

Haftpflichtversicherer denken um

SCHARF GESCHALTET

Die Folgen des BRSG für Vermittler

Auf dem Stand der Technik

Ein Marktüberblick zu den Sicherheitsobliegenheiten in der Cyber-Versicherung

Von Dirk-Carsten Günther und Nazan Ider

Im April 2017 veröffentlichte der GDV Musterbedingungen zur Cyberversicherung. Zielgruppe sind Unternehmen mit einem Umsatz bis 50 Mio. Euro. Diese Musterbedingungen sind der Ausgangspunkt für einen Vergleich der gegenwärtig noch heterogenen Bedingungswerke auf dem Markt. Der Vergleich ist beschränkt auf eine der wichtigsten Regelungen in einer Cyber-Versicherung - und zwar die vor Eintritt des Versicherungsfalls durch den Versicherungsnehmer zu erfüllenden Sicherheitsobliegenheiten i.S.d. § 28 Abs. 1 VVG.

Grundsätzlich können die Obliegenheiten in die Kategorien Datensicherung, Zugriffssicherung, aktuellen technischen Stand der Systeme, Schutz gegen Schadsoftware und weitere Obliegenheiten unterteilt werden. Während der GDV vorgibt, mindestens einen wöchentlichen Sicherungsprozess durchzuführen, gibt es innerhalb dieses Vergleichs nur zwei Versicherer, die ebenfalls diese Vorgabe machen. Andere Wordings sehen eine tägliche Datensicherung vor. Zu beachten ist, dass der zeitliche Intervall, in dem die Datensicherungen durchgeführt werden sollten, sich nach dem des Unternehmens zu richten hat. Die Obliegenheit ist entsprechend anzupassen.

Des Weiteren sehen die GDV-Musterbedingungen und auch die Bedingungen verschiedener Versicherer vor, die Datensicherungsmedien physisch von den gesicherten Systemen zu trennen. Sind Backup-Systeme mit ihren Zielsystemen verbunden, können sie möglicherweise nachträglich vom betroffenen System verändert werden und es besteht die Gefahr, dass sie bei einem Angriff ebenfalls zu Schaden kommen.

HINDERNIS FÜR DEN HACKER

Auf erste Sicht ist erstaunlich, dass 6 von den 13 betrachteten Bedingungswerken keine Obliegenheiten oder Verhaltensregeln für den Versicherungsnehmer für dessen Datensicherung bestimmen, was gerade bei einem Kumulereignis enorme negative Auswirkungen für diese Cyber-Versicherer haben kann, da dann nur noch die allgemeinen subjektiven Risikobegrenzungen mit ihren hohen Nachweisanforderungen - insb. §§ 23, 26 VVG (Gefahrerhöhung), § 81 Abs. 2 VVG (grob fahrlässige Herbeiführung des Versicherungsfalls), § 82 VVG (Verletzung der Schadenminderungsobliegenheit) zurückgegriffen werden kann.

> „Etwa die Hälfte der betrachteten Versicherer formuliert keine Obliegenheit zur Zugangssicherung, was sich aus geringen Entschädigungslimits oder veralteten Wordings erklären dürfte."

Die Obliegenheiten zur Zugriffssicherung sehen laut GDV-Empfehlungen Maßnahmen zur Sicherung der Zugänge zu betrieblichen Daten, Programmen und Systemen vor: Individuelle Zugänge mit Passwort für jeden Nutzer und Administrator stellen durch die Notwendigkeit, dass für den Zugang zu jedem System eine Benutzerkennung und ein Passwort benötigt wird, bei einem Angriff ein Hindernis für den Hacker dar. Mithilfe dieser Maßnahme werden individuelle Zugriffsrechte für jeden Account definiert um somit nachvollziehen zu können, welche Angriffs- oder schadenrelevanten Tätigkeiten zu welchem Zeitpunkt von welchem Nutzer durchgeführt wurden, zumal in nicht seltenen Fällen ein Angriff nicht von außen, sondern durch einen Mitarbeiter des Versicherungsnehmers erfolgt. Zudem sind technisch erzwungene Mindestanforderungen an Passwörter erforderlich. Der GDV empfiehlt individuelle Zugänge für alle Nutzer und der Sicherung dieser Zugänge durch ausreichend komplexe Passwörter. Die Vorgabe der Passwortsicherheit findet sich nur in einem der untersuchten Bedingungswerke wieder.

Andere Versicherer formulieren die Anforderungen an die Zugangssicherung eher hinsichtlich des Einsatzes von Sicherheits- oder Verschlüsselungstechnologien. Im Zeitalter der Digitalisierung mit seiner Verschmelzung zwischen privaten

und betrieblichen Belangen und Entwicklungen wie „Bring your own device" sind einige dieser Obliegenheiten für den Versicherungsnehmer nur schwer umzusetzen. Etwa die Hälfte der betrachteten Versicherer formuliert keine Obliegenheit zur Zugangssicherung, was sich aus geringen Entschädigungslimits oder veralteten Wordings erklären dürfte.

Die Regelungen zum aktuellen Stand der Systeme sehen eine regelmäßige und zeitnahe Installation von Sicherheitsupdates vor. Schadprogramme nutzen bereits bekannte Sicherheitslücken von Softwares aus, für die es Updates gibt, Unternehmen diese jedoch nicht installiert haben. Aus diesen Gründen wird vom GDV empfohlen, ein Patch-Management-Verfahren einzuführen. Ein funktionierendes Patch-Management ist zwingend, da eine Schutzsoftware nutzlos ist, wenn sie nicht auf dem aktuellsten Stand ist. Im Gesamtvergleich haben nur 3 von 12 Versicherern ein Patch-Management oder eine ähnliche Regelung namentlich benannt.

DISKUSSION UM DEFINITION

Von besonderer Bedeutung ist Frage nach dem in den verschiedenen Wordings oft verwendeten Begriff des „Stand der Technik". Der Begriff lässt erheblichen Interpretationsspielraum offen und wird unter anderem auch vom IT-Sicherheitsgesetz, dem Telemediengesetz und der Europäischen Datenschutzgrundverordnung gefordert. Es werden vom Gesetzgeber keine Kriterien zur Bestimmung genannt.

Ausgehend vom gewollten Zweck der Gesetzgebung werden mit dem „Stand der Technik" ein hohes Sicherheitsniveau und hoher Datenschutz mittels fortschrittlicher Verfahren angestrebt. Es besteht ein 3-Stufen-Verhältnis zwischen

Subjektive Risikobegrenzung: Sechs von dreizehn betrachteten Bedingungswerken bestimmen keine Verhaltensregeln bei der Datensicherung für Versicherungsnehmer.

FOTO: FOTOLIA/FRSTUDIO

den allgemein anerkannten Regeln der Technik, dem Stand der Technik und dem Stand der Wissenschaft und Technik. Die unterste Stufe bilden hierbei die anerkannten Regeln der Technik, die sich auf eine Mehrheitsauffassung und eine allgemeine Anerkennung bestimmter Verfahren stützt, wohingegen der Stand der Technik sich umschreiben lässt als die Gesamtheit der neuesten Erkenntnisse berücksichtigenden technischen Standards, die eine optimale Gefahrsteuerung gewährleisten und deren praktische Eignung durch eine erfolgreiche Erprobung unter den üblichen Betriebsbedingungen bei gleichen oder gleichartigen technologischen Verhältnissen nachgewiesen ist oder jedenfalls soweit gesichert erscheint, dass ihre Anwendung dem Betreiber kein unzumutbares Kostenrisiko auferlegt.

Der Stand der Technik erlaubt im Gegensatz zu den allgemein anerkannten Regeln der Technik die schnellere Durchsetzung des technischen Fortschritts. Es wird auf eine allgemeine Anerkennung verzichtet, denn neue technische Fortschritte setzen sich langsam durch und werden erst am Ende dieses Prozesses allgemein anerkannt. Im Gegensatz zum Stand von Wissenschaft und Technik müssen die angewendeten Methoden nicht wissenschaftlich belegt sein, sondern die in der Praxis bislang erfolgreiche Anwendung ist ausreichend.

In Bezug auf das Cyberrisiko lässt sich daraus schließen, dass der Versicherungsnehmer grundsätzlich die aktuellsten Schutzmaßnahmen gegen Cyber-Angriffe verwenden muss, um dem Stand der Technik Genüge zu tun. Dabei ist der rasche technische Fortschritt zu beachten, der eine kontinuierliche Anpassung der Sicherheitsmaßnahmen und Vorkehrungen des Versicherungsnehmers erfordert. Was zu einem bestimmten Zeitpunkt als „Stand der Technik" gilt, kann alsbald aufgrund der innovationsbedingten Verschiebung und „Alterung" der Sicherheitsmaßnahme nur noch den „allgemein anerkannten Regeln der Technik" entsprechen. Zum Stand der Technik dürften insbesondere die Maßnahmen und Vorgaben des BSI gehören. Dabei kann es aber keinen Automatismus zu Lasten des Versicherungsnehmers geben. Bei einem kleineren Unternehmen können manche dieser Anforderungen aufgrund der Infrastruktur der IT nicht erfüllt werden. Hier ist jeweils im Einzelfall zu entscheiden, ob es bereits an der Verletzung des objektiven Tatbestands fehlt, z.B. bei fehlender Möglichkeit und/oder Zumutbarkeit oder erst an der subjektiven Seite des § 28 Abs. 2 VVG. Es gibt weitere vor dem Versicherungsfall zu erfüllende Obliegenheiten. Dies sind Obliegenheiten, die einen übergreifenden Zweck verfolgen, z.B. die Obliegenheit zur Einhaltung von gesetzlichen und behördlichen Sicherheitsvorschriften.

Diese Regelung ist aus der „klassischen" Rechtsprechung hinlänglich bekannt und bietet keine Besonderheiten. In der

Praxis der Cyber-Versicherung wird diese Obliegenheit nur selten eine Rolle spielen: So existieren zwar berufsgenossenschaftliche Vorschriften (DGUV, vormals BGV) und sind diese nach der Rechtsprechung behördliche Sicherheitsvorschriften; die DGUV-Vorschriften enthalten aber keine Vorgaben zur Cybersicherheit.

BUNDESAMT FÜR IT-SICHERHEIT SETZT HOHE STANDARDS

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet Mindeststandards für die Sicherheit der Informationstechnik der Bundesverwaltung auf der Grundlage des § 8 Abs. 1 BSIG. Die BSI-Standards sind Bestandteil der IT-Grundschutz-Methodik. Sie enthalten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen zu unterschiedlichen Aspekten der Informationssicherheit. Davon zu unterscheiden ist das Ziel der Technischen Richtlinien des BSI (BSI-TR) zur Verbreitung von angemessenen IT-Sicherheitsstandards. Diese technischen Richtlinien stellen keine behördliche Sicherheitsvorschrift dar, sondern haben nur Empfehlungscharakter. Sie ergänzen nur die technischen Prüfvorschriften des BSI und liefern Kriterien und Methoden für Konformitätsprüfungen sowohl der Interoperabilität von IT-Sicherheitskomponenten als auch der umgesetzten IT-Sicherheitsanforderungen.

Auch aus dem Datenschutzrecht sind keine gesetzlichen Sicherheitsvorschriften im Sinne der Cyber-Bedingungen herzuleiten. Das Bundesdatenschutzgesetz (BDSG) trifft unter anderem Regelungen für öffentliche und nicht-öffentliche Stellen, um personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen und dabei die „technischen und organisatorischen Maßnahmen" zu treffen, die erforderlich sind, um die Umsetzung der Ziele des Datenschutzes und der Datensicherheit zu gewährleisten (§ 9 BDSG). Aus § 9 BDSG lässt sich aber keine konkrete gesetzliche Verpflichtung zu einer bestimmten Maßnahme ableiten. Daran ändert auch die Datenschutzgrundverordnung nichts (vgl. Art. 5, 24, 25, 32 DS-GVO).

Mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) werden Betreiber kritischer Infrastrukturen verpflichtet, die für die Erbringung ihrer wichtigen Dienste erforderliche IT nach dem Stand der Technik angemessen abzusichern. Die Betreiber kritischer Infrastrukturen sind verpflichtet, IT-Sicherheit nach dem „Stand der Technik" umzusetzen und deren Einhaltung regelmäßig gegenüber dem BSI nachzuweisen (§ 8a BSIG). Ähnliches gilt für Telekommunikations- und Teledienstanbieter (§ 109 Abs. 1, 2 TKG bzw. § 13 Abs. 7 TMG) sowie für Energieversorgungsnetzbetreiber und Energieanlagenbetreiber (§ 11 Abs. 1a ,1b EnWG). Dass ein Versicherungsnehmer in einem dieser Fälle tätig ist, wird zum einen die große Ausnahme sein und zum anderen werden dann keine Muster-AVB, sondern individuelle Cyber-Versicherungslösungen Anwendung finden.

Die Regelungen der Gefahrerhöhung orientieren sich zumeist an den gesetzlichen Vorgaben aus den §§ 23 ff. VVG. Einige Versicherer definieren dabei den gefahrerheblichen Umstand nicht weiter, so wie es bei der Muster-AVB des GDV ist. Diese Regelungen sind nur deklaratorischer Art und bestimmen das, was sich schon unter den üblichen Auslegungsgrundätzen aus § 23 VVG ergibt. Es gibt es keine versicherungsrechtlichen Besonderheiten gegenüber der „klassischen" Sachversicherung. Würde man diese Regelungen als Verschärfung einer Gefahrerhöhung ansehen, wäre die Klausel unwirksam. Von den halbzwingenden Regelungen der Gefahrerhöhung kann außerhalb des Anwendungsbereiches eines sog. Großrisikos (§ 210 VVG) nicht zu Lasten des Versicherungsnehmer abgewichen werden (§ 32 VVG). Die Regelungen zu den Rechtsfolgen der Verletzung vertraglicher Obliegenheiten geben weitgehend den Gesetzestext, insb. den des § 28 VVG, unverändert wieder. Zum Teil wird gem. § 32 VVG zu Gunsten des Versicherungsnehmers abgewichen. Ein Versicherer verzichtet z.B. auf das Kündigungsrecht des § 28 Abs. 1 VVG.

GROSSE BANDBREITE AN REGELUNGEN

Die Marktanalyse ergibt eine sehr große Bandbreite bei den Regelungen über Obliegenheiten des Versicherungsnehmers vor Eintritt des Versicherungsfalls. Diese Regelungen dürften sich durch die Einführung der Muster-AVB des Gesamtverbandes der Deutschen Versicherungswirtschaft zukünftig annähern. Dies gilt jedoch nur für die Zielgruppe der Muster-AVB des GDV, also Mittelständler, Handwerksbetriebe bis hin künftig zu Privathaushalten. Im Industriebereich werden die Wordings einzelner Markteilnehmer auf Makler- und Versichererseite nur auf einzelne Regelungen der Muster-AVB zurückgreifen. Unabhängig davon, welche AVB verwendet werden, ist auf die Vereinbarung von in tatsächlicher (insbesondere technischer) und rechtlicher Hinsicht belastbaren Obliegenheiten größte Sorgfalt zu legen, da gerade bei Kumulereignissen und einer zunehmend höheren Versicherungsdichte ansonsten eine für den Versicherer nicht zu kalkulierende Gefahr besteht.

Prof. Dr. Dirk-Carsten Günther, Rechtsanwalt Bach Langheid Dallmayr, Professor am Institut für Versicherungswesen der TH Köln. **Nazan Ider,** Spezialistin Kompetenzstelle Cyber, Axa Konzern AG.