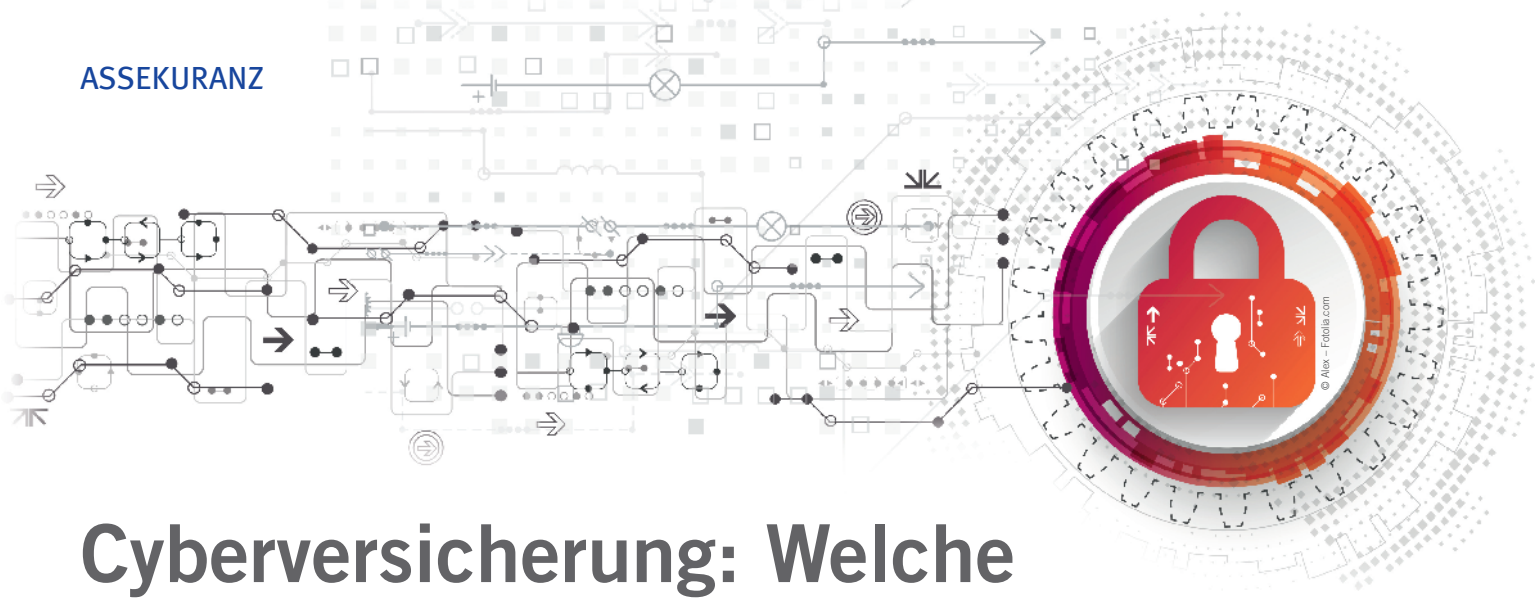

Cyberversicherung: Welche Deckungssummen sind realistisch?

Wenn auch in aller Munde, ist die Cyberversicherung immer noch echtes Neuland für viele Versicherungsmakler. Die Abschätzung der Risiken, die Erfassung von Daten sowie die Ermittlung von Deckungssummen stellen dabei besondere Herausforderungen dar. Deshalb sollten Makler bei der Beratung auf ganz bestimmte Aspekte achten.

Die Cyberversicherung hat sich in den vergangenen Jahren zu einer stark wachsenden Versicherungssparte entwickelt – fast wöchentlich steigen Gesellschaften mit eigenen Cyberversicherungsprodukten in den Markt ein. Neben der konstant wachsenden Anzahl an Cybervorfällen hat vor allem die positive Marktentwicklung beim Abschluss von Cyberpolicen in den USA und UK den deutschen Markt nachhaltig beeinflusst. Im Prinzip war es nur eine Frage weniger Monate, bis etablierte Versicherer hierzulande ein eigenes Produkt auf den Markt bringen würden. Darüber hinaus schafft die zunehmende Digitalisierung der Gesellschaft und in der Industrie ein neues Risikofeld – Rahmenbedingungen, mit denen Assekuranzen und Vermittler umgehen müssen.

KPMG, eines der wirtschaftsstärksten Wirtschaftsprüfungsunternehmen weltweit, schätzt das Prämienvolumen im Jahr 2017 auf 90 bis 100 Mio. Euro. Allerdings führt das zügige Wachstum dazu, dass auf der Bedingungsseite ein recht unübersichtliches Durcheinander der Wordings und Klauseln vorherrscht. Das ist natürlich für alle Beteiligten, vor allem jedoch für Makler und Versicherungsvermittler, eine extrem anspruchsvolle Situation. Ein Marktvergleich der zahlreichen Bedingungswerke war lange kompliziert und der Ruf nach einer Vereinheitlichung verständlicherweise groß. Im April hat der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) die langersehnten Musterbedingungen zur Cyberversicherung veröffentlicht. Ein erster Schritt zu mehr Verständlichkeit. Dennoch wirft die wachsende junge Sparte der Cyberversicherung nach wie vor viele Fragen auf. Vermittler sind irritiert, wenn es darum geht, die passende Versicherungssumme festzulegen. Auch ist selten klar, welche Bereiche unter den Cyberschutz fallen und entsprechend versichert werden müssen. Das fängt bei der IT-Infrastruktur an und geht bis hin zu Cyberdrittschäden.

> Auf der Bedingungsseite herrscht ein Durcheinander der Wordings und Klauseln. Das ist für alle Beteiligten, vor allem jedoch für Makler und Versicherungsvermittler, eine extrem anspruchsvolle Situation.

Wie lassen sich also nun Schritt für Schritt Deckungssummen für ein Risiko festlegen?

Die IT-Infrastruktur

Ein wesentlicher Bestandteil einer jeden Cyberversicherung ist die Wiederherstellung der IT-Infrastruktur und -sicherheit nach einem Cyberangriff, einem Hackereinbruch oder einer Infektion durch eine Schadsoftware. Vermittler können bereits im Kundengespräch eruieren, wie teuer die eingesetzten IT-Systeme generell sind und auf welche Höhe Kosten für die Wiederherstellung von Betriebssystemen, Datenbanken und Verwaltungssystemen durch die eigene IT-Abteilung oder einen externen Dienstleister geschätzt werden. Für mittelständische Betriebe erstrecken sich diese Instandsetzungskosten, die für die Feststellung des Schadens (IT-Forensik), die Installation von Programmen, Mehrkosten für Leihsysteme, neue Hard- und Softwarekomponenten sowie die Wiederherstellung von Datenbanken anfallen, auf bis zu 100.000 Euro. Weitaus höhere Summen fallen für Unternehmen mit teurem IT-Equipment wie Fertigungsstraßen und automatisierten Produktions-

maschinen an. Kosten, die im Rahmen einer fundierten Risikoanalyse realistisch skizziert werden können.

Datenverlust und Kreditkarten

Ein weiterer Kostenpunkt, den Versicherungsvermittler im Auge behalten müssen, sind Kosten für die Verletzung von Persönlichkeitsrechten. Dies gilt für alle Unternehmen, die personenbezogene Daten speichern und verarbeiten, also beispielsweise für Versicherungsmakler, Ärzteabrechnungsstellen, Ärzte, Rechtsanwälte und Steuerberater. Beziffern lässt sich die Summe laut aktuellem Stand mit bis zu 50 Euro pro Person, deren Rechte verletzt wurden, etwa durch einen Datendiebstahl. Doch woraus setzt sich dieser Wert eigentlich zusammen?

Im Falle eines Cyberdatenvorfalls ist der Versicherungsnehmer auf anwaltliche Beratung angewiesen, das gilt identisch für die betroffenen Personen. Aufwendig ist davon abgesehen die Zusammenarbeit mit PR-Beratern, zum Beispiel für die Erstellung von Informationsschreiben – diese fallen unter die Informationspflicht – und die Wiederherstellung des angeschlagenen Images. Weitere Kosten entstehen für Dienstleistungen wie die Überwachung von Identitätsdiebstählen. In Zahlen heißt das: Für ein medizinisches Zentrum mit 20.000 Patienten- und Mitarbeiterdaten sollten somit 1.000.000 Euro Versicherungssumme nur für diesen Bereich bereitgestellt werden.

Um die entsprechende Versicherungssumme für Versicherungsnehmer aus einer Branche mit digitalen Zahlungsmitteln wie Kreditkarten festzulegen, benötigt der Versicherungsmakler Informationen über die Anzahl der gespeicherten Kreditkarten. Die Entschädigungsleistung pro abhanden gekommener Kreditkarte kann vereinbarungsgemäß zwischen 10 und 20 Euro liegen. Ein Hotel mit 100.000 gespeicherten Kreditkarteninformationen müsste demnach für den Cyberschadenfall zwischen 1 und 2 Mio. Euro absichern.

Der Fall Betriebsunterbrechung

Ein Cyberangriff führt in der Regel immer auch zu einer Betriebsunterbrechung unterschiedlicher Zeitspannen, abhängig davon, wie stark das IT-System in Mitleidenschaft gezogen ist und wie lange Wiederherstellungsarbeiten andauern. Denn im heutigen Technologiezeitalter können kaum noch Bereiche der Wertschöpfungskette ohne IT-System bewältigt werden. Diese Betriebsunterbrechungsschäden sind für die betroffenen Unternehmen daher besonders fatal – Vermittler sollten mit dem Kunden mögliche Schadenszenarien konkret durchspielen. Um Ertragsausfälle und die Zahlung fortlaufender Kosten zu gewährleisten, entscheidet über die Festlegung der Versicherungssumme am Ende, wie viel Zeit für die Wiederherstellung der IT-Systeme im Höchstfallszenario benötigt wird. Ein Steuerberater, der für mehrere Wochen keinen Zugriff auf seine Steuerberatungssoftware mehr hat, sollte hier den entstehenden Ertragsausfall oder die Mehrkosten für die Bearbeitung durch andere Kanzleien mit einer entsprechenden Versicherungssumme absichern.

Diese Betriebsunterbrechungsschäden sind für die betroffenen Unternehmen besonders fatal – Vermittler sollten mit dem Kunden mögliche Schadenszenarien konkret durchspielen.

Ein Cyberdrittschaden

Auch im Fall eines Cyberdrittschadens, sprich wenn der Versicherungsnehmer einen Kunden oder sonstigen Dritten aufgrund einer Datenrechtsverletzung, eines Datenverlustes, einer Persönlichkeits- oder Markenrechtsverletzung schädigt oder gegen Geheimhaltungsvereinbarungen verstößt, greift die Haftpflicht im Rahmen des Versicherungspaketes, um Ansprüche – begründet oder nicht – befriedigen zu können. Als Orientierung kann der mittelständische Bereich dienen: Hier sind Versicherungssummen von 250.000 bis zu 1 Mio. Euro üblich.

Versicherungsmakler, die vorgenannte Punkte mit dem Versicherungsnehmer klären, sind in der Lage, eine gute Auswahl an geeigneten Versicherungssummen zu bestimmen und damit eine optimale Absicherung gegen Cyberschäden zu definieren. ■

Von Stephan Lindner, Head of Professional Lines bei Markel Deutschland