Identifikation und Bewertung von Cyber-Risiken

Das Thema Cyberkriminalität gewinnt an Bedeutung, doch Makler zeigen sich bis dato eher zurückhaltend. Wichtig für das Beratungsgespräch ist zu wissen, welche Bedrohungen es gibt und welche Auswirkungen diese haben. Welche Fragen im Kundengespräch aufkommen können und wie Vermittler damit umgehen sollten, zeigt dieser Leitfaden.

Innerhalb von weniger als fünf Jahren haben sich Cyber-Risiken-Versicherungen auch im deutschsprachigen Raum zu einer eigenen Produktklasse entwickelt. Dies liegt nicht daran, dass etablierte Versicherungslösungen seit jeher Lücken aufweisen. Vielmehr ist es der Tatsache geschuldet, dass die rasante technologische Entwicklung nicht nur einzelne Arbeitsprozesse, sondern auch ganze Geschäftsmodelle verändert oder entstehen lässt, deren Risiken in der Vergangenheit schlichtweg nicht da waren. Spätestens seit „Snowden" haben die Medien nicht nur die Vorteile von Social Networks, Cloud, Big Data, Industrie 4.0, vernetztem Fahren und Home-Automatisierung im Blick. Befeuert durch immer wieder neue „Datenskandale" ändert sich die Risikowahrnehmung und in Folge auch die Toleranz von Nutzern und schließlich die gesetzlichen Rahmenbedingungen.

Man sollte also meinen, dass Versicherern Cyber-Risiken-Versicherungen nur so aus der Hand gerissen werden. Auch wenn gerade im vergangenen Jahr sowohl Angebotsanfragen als auch Versicherungsabschlüsse deutlich gestiegen sind, ist dem (noch) nicht so. Die Gründe dafür liegen sowohl für Vermittler als auch für ihre Kunden in der Komplexität der Cyber-Risiken und der Neuartigkeit dieser Produktklasse. Waren für Vermittler bislang wirtschaftliche, rechtliche und Branchenkenntnisse ausreichend, um Risiken und deren Transfer mit ihren Kunden zu besprechen, benötigen sie für die Beratung zu Cyber-Risiken und deren Versicherung nun auch noch ein Mindest-Know-how in Sachen Informations- und Kommunikationstechnologie (IKT).

Damit stellt sich für viele Vermittler die Frage: „Wie bringe ich meinen Kunden das Thema ‚Cyber' näher, ohne gleich am ersten Kunden-Einwand zu scheitern?". Vorweg gestellt gilt: Ohne die Aneignung zumindest eines Basis-IKT-Wissens kann kein Vermittler seiner Aufgabe gerecht werden. Hier empfiehlt sich gegebenenfalls die Einschaltung von Spezialmaklern, die schon über entsprechendes Fachwissen verfügen. Darüber hinaus gilt es, den richtigen Einstieg zu finden. Die folgenden Situationen können zum Beispiel im Kundengespräch auftreten:

Gesprächssituation

Da das Thema „Cyber" auf der Tagesordnung des Jahresgesprächs steht, zieht der Geschäftsführer des Kundenunternehmens seinen IT-Leiter zum Gespräch mit dem Vermittler dazu. Die Wahrscheinlichkeit, dass der IT-Leiter eine ihm von außen „aufgezwungene" Diskussion über IT-Sicherheit und mögliche Schäden als Angriff auf sein Revier wahrnimmt, ist groß.

Don'ts für den Vermittler im Gespräch mit dem Kunden und seinem IT-Leiter

- Zählen Sie keine theoretischen Schadenszenarien auf.
- Erklären Sie nicht, wo mögliche IT-Sicherheitsdefizite in seinem Unternehmen liegen.
- Lassen Sie sich nicht auf ein IT-fachliches Kräftemessen ein, das Sie nicht gewinnen können.

Dos

- Bereiten Sie sich anhand von tatsächlichen Fällen aus der Branche des Kunden oder zu ähnlichen Geschäftsmodellen vor. Im Zweifelsfall kann Ihnen der Underwriter Ihres Versicherers diese zur Verfügung stellen. Nutzen Sie die vorbereiteten Beispiele.
- Nennen Sie Beispiele, in denen Unternehmen auch ohne eigene Versäumnisse Opfer von Cyber-Vorfällen wurden.
- Bitten Sie gegebenenfalls den Cyber-Fachmann des Versicherers oder seines Forensikers zu dem Gespräch hinzu oder vereinbaren Sie einen optionalen „Telefonjokertermin".

Kundenfrage: „Welche Cyber-Risiken habe ich denn?"

Mögliche beispielhafte Antworten für den Vermittler im Gespräch (je nach Geschäftsmodell des Kunden können Sie bereits im Vorfeld etwaige Risikoschwerpunkte identifizieren):

Von Thomas Pache, Manager Professional Indemnity Financial Lines bei AIG Europe Limited

- Handelt es sich um ein Unternehmen mit einer großen Anzahl von Endkunden?
  Schon allein die Benachrichtigungskosten können sich leicht zu größeren Summen addieren.
- Ist das Unternehmen international tätig?
  Die rechtliche Beratung über die jeweiligen nationalen Pflichten in mehreren Ländern führt wegen der Einschaltung lokaler Fachleute leicht zu einem höheren fünfstelligen Betrag.
- Werden Kreditkartendaten verarbeitet?
  Das vertragliche PCI-Reglement sieht empfindliche (vertragliche) „Strafgebühren" vor.
- Ist die Logistik oder die Produktion hochautomatisiert?
  Eine Betriebsunterbrechung könnte zum Beispiel durch Veränderung/Vernichtung der Logistikdaten oder einen DDoS-Angriff eintreten.
- Allein die Feststellung, ob unberechtigte Zugriffe von außen oder von innen erfolgten, ist mit einigem forensischen Aufwand und damit auch mit Kosten verbunden.

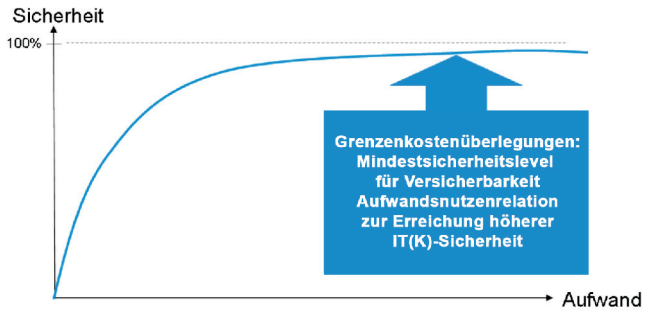
Kundenfrage: „Ich gehe doch davon aus, dass alle meine Risiken versichert sind – oder wurde ich in der Vergangenheit falsch beraten?"

Mögliche Antwort: Da Sie Ihr Unternehmen am besten in- und auswendig kennen, benötige ich zunächst die aus Ihrer Sicht denkbaren Cyber-Schadenszenarien, damit ich sie gegen Ihre aktuelle Deckung prüfen kann. Nahezu sämtliche Kosten für IT-Forensik, Rechtsberatung, PR- und Krisenmanagement sind im Zweifelsfall nicht gedeckt. Ähnlich verhält es sich mit der sogenannten „sachschadenlosen Betriebsunterbrechung".

Kundenfrage: „Unsere IT ist sicher. Warum sollte ich dann überhaupt eine Cyber-Risiken-Versicherung abschließen?"

Mögliche Antwort: Wie bei allen Versicherungen sind auch Cyber-Risiken-Versicherungen nur in dem Bereich sinnvoll, wo zusätzliche Investitionen in die IT-Sicherheit (zum Beispiel Einstellung eines zusätzlichen Mitarbeiters) keinen nennenswerten Sicherheitszuwachs mehr erbringen. Aus Sicht der Versicherer muss die Informationssicherheit ein Mindestniveau überschreiten, um Versicherungsschutz anbieten zu können.

Aufwand und Nutzen müssen stimmen



Quelle: AIG

Kundenfrage: „Was deckt denn eine Cyber-Risiken-Versicherung überhaupt?"

Mögliche Antwort:

- Schadenersatzleistungen: Ähnlich einer Betriebshaftpflichtversicherung besteht Versicherungsschutz für die Abwehr und gegebenenfalls Befriedigung von Schadenersatzansprüchen Dritter. Im Zusammenhang mit Kreditkarten bieten einige Versicherer Schutz für vertragliche Ansprüche.
- Kostenentschädigungen: Es besteht Versicherungsschutz für Kosten, die infolge eines sich realisierenden Cyber-Risikos entstehen, wie zum Beispiel Kosten einer Datenwiedererfassung.
- Betriebsunterbrechungsleistungen: Ähnlich einer Feuerbetriebsunterbrechung besteht Versicherungsschutz für entgangene Gewinne und weiterlaufende Kosten einer Betriebsunterbrechung. Allerdings ist hierfür kein Sachschaden erforderlich. Es reicht ein sich realisierendes Cyber-Risiko.
- Service-/Assistanceleistungen: Anders als bei üblichen Versicherungslösungen greifen Cyber-Risiken-Versicherungen in der Regel schon bei einer vermuteten Informationssicherheitsverletzung. Das bedeutet, dass der Versicherte schon während der Gefährdung von erfahrenden Fachleuten aus den Bereichen Recht, Forensik, PR und Krisenmanagement unterstützt wird.

Idealerweise bereitet sich der Vermittler auf das Kundengespräch so vor, dass er bereits beim Erstgespräch eine grobe Vorstellung von den möglichen Kosten einer solchen Cyber-Risiken-Versicherung geben kann. Eine Reihe von Versicherern kann hierzu eine grobe Indikation an die Hand geben, ohne dass schon ein vollständiger Fragebogen ausgefüllt werden muss. ■