```
{
<cyber~Angriffe>
[3 von 10
Unternehmen].sind
bereits betroffen$

[Kein.Risiko?]
67 % halten das
Cyber-Risiko für
das eigene Unternehmen
für gering
}

```

Halbwissen beim Kunden und Berater vermeiden

NIKOLAUS STAPELS
Selbstständiger VdS-Fachberater für Cyber-Security

Das Beratungsfeld Cyber stellt neue Anforderungen an Kundenansprache und Know-how, Aus- und Weiterbildung sind daher enorm wichtig und Grundlage für den Vertriebserfolg.
Bei Cyber-Angriffen und Cyber-Kriminalität denken die meisten an den „klassischen" Hacker, der abends alleine vor dem Rechner sitzt und gezielt nach einem Opfer sucht. Die Realität sieht anders aus: Viele Unternehmen werden zufällig ausgewählt, und es kann jedes Unternehmen treffen, vom kleinen Handwerksbetrieb bis zum DAX-Unternehmen. Eine Cyber-Versicherung alleine wird einen Schaden nicht verhindern, die finanziellen Folgen können damit aber überschaubarer werden.
Die Aufgabe des Vermittlers besteht nicht darin, ein Informationssicherheitsmanagement beim Kunden zu implementieren, aber er muss den Kunden darüber aufklären, dass Hacker auf unterschiedlichsten Wegen in ein Unternehmen eindringen können und dass es wichtig ist, Vorkehrungen zu treffen, um dies zu verhindern.
Die Fragebögen der Versicherer geben durch Risikofragen erste Hinweise zu notwendigen Standards, unter anderem wird empfohlen: Datensicherung mindestens alle zwei bis drei Tage, eine Lagerung der Datensicherung auch außerhalb des Unternehmens, Einbringen und regelmäßiges Update von Firewall und Antivirenprogramm sowie ein regelmäßiges Update des Betriebssystems.
Aufgrund der Neuartigkeit des Produkts und des damit verbundenen Know-hows scheuen viele Vermittler noch das Thema und kommen ihrer Aufklärungs- und Beratungsfunktion gegenüber ihren Kunden nicht, nicht richtig oder nur zögerlich nach.
Aber welches Wissen wird konkret benötigt? Um im Bereich Cyber-Sicherheit erfolgreich zu beraten und zu verkaufen, sollten Vermittler folgende Themen kennen und beim Kunden ansprechen können: Wie gehen Cyber-Kriminelle vor? Was passiert, wenn Daten gestohlen werden (Auswirkungen der DSGVO)? Was gilt es bei einer Cloudnutzung zu beachten? Wie wird eine Versicherungssumme ermittelt? Welche Gefahren gibt es für Unternehmen?
Neben dem Produktwissen sollte der Berater dem Kunden auch erläutern, welche Assistance-Leistungen dieser im Schadensfall über die reine Geldzahlung hinaus erhält. Jene kann der „normale" IT-Dienstleister vor Ort in der Regel nicht gewährleisten. Viele Versicherer arbeiten deshalb mit international tätigen Unternehmen zusammen, die innerhalb kürzester Zeit beim betroffenen Unternehmen vor Ort eine Lösung suchen.
Aktuell sprechen viele Berater das Thema Cyber mit Halbwissen beim Kunden an. Erfahrungsgemäß braucht der Kunde dann nur ein oder zwei Argumente (Vorwände) zu nennen, die viele Berater nicht entkräften können, und das Thema ist vom Tisch. Schade, denn gerade Cyber als brandaktuelles Thema eignet sich hervorragend als Anlass für ein Beratungsgespräch und öffnet die Türen, um andere Themen anzusprechen. Kompetente Beratung zu den Risiken 4.0 setzt neben Versicherungsexpertise und Risikomanagement-Know-how auch IT-fachliches Cyber-Grundwissen voraus. Diese Wissenskombination macht für die meisten Vermittler ein „Neulernen" notwendig, um das sie sich über entsprechende Weiterbildung bemühen müssen. Daher die Empfehlung: Machen Sie sich fit, damit Cyber auch für Sie zu einer vertrieblichen Erfolgsstory wird.

Nikolaus Stapels (38) ist selbstständiger VdS-Fachberater für Cyber-Security und unterstützt Versicherer und Vermittler bei der vertrieblichen Umsetzungspraxis für Cyber-Produkte durch Aus- und Weiterbildung sowie die Entwicklung beratungs- und vertriebsunterstützender Software.

▶ Neuerungen werden teils als Standard, teils als optionale Bausteine präsentiert. Klauseln wie jene zur Betriebsunterbrechung durch Bedienungsfehler, die noch vor einiger Zeit als exotisch galten, sind zum Muss avanciert. Auch die Deckungssummen und Risikoausschlüsse sind in Bewegung – im Einklang mit der IT-Landschaft selbst, die ständig neue Risiken hervorbringt.

Erschwerend kommt hinzu, dass der Begriff „Cyber-Versicherung" in Deutschland nicht inhaltlich geschützt ist. Viele Versicherer nutzen ihn auch für Zusatzpolicen, die gar keinen umfassenden Schutz vor Cyber-Risiken bieten. Die GDV-Musterbedingungen hatten nun bereits zur Folge, dass mehrere Versicherer ihre Cyber-Tarife entsprechend angepasst haben. Von Standards wie in anderen Versicherungssparten ist die Branche aber immer noch weit entfernt.

WAS BRAUCHT DER PRIVATKUNDE?

Um in diesem Dickicht die passenden Angebote für ihre Kunden herauszufiltern, sollten Makler die wichtigsten Risikoblöcke in der Cyber-Sparte in den Blick nehmen. Bei Privatpersonen sind das in der Regel: Identitätsdiebstahl, also die missbräuchliche Nutzung personenbezogener Daten wie Anschriften oder Kreditkartennummern, Vermögensschäden, Schäden an Hard- oder Software sowie Schadensersatzansprüche Dritter. Der Verlust der Arbeitsfähigkeit gehört ebenfalls zu den Cyber-Risiken von Privatpersonen, wenn auch in geringerem Umfang als bei Unternehmen. „All diese Risiken abzusichern ist sinnvoll", urteilt Spezialmakler Erichsen. Welche Angebote und Einzelbausteine sich konkret für welchen Kunden eignen, hänge

stark von den persönlichen Voraussetzungen und den Leistungen der Tarife ab. Insofern lassen sich auch die Kosten kaum vorab einschätzen.

Mit vielen Cyber-Policen können sich Privatkunden beispielsweise explizit gegen finanzielle Verluste beim Online-Shopping absichern und bekommen über den Versicherer psychologische Beratung, wenn sie Opfer von Cyber-Mobbing geworden sind. Ob diese Bausteine ein Must-have sind oder nur ein Nice-to-have, das hängt vom Umfeld und den Aktivitäten der Versicherungsnehmer ab. Die Kosten der Basisschutz-Policen variieren je nach Anbieter, beginnen aber bei circa fünf Euro pro Monat, also rund 60 Euro pro Jahr.

Das Potenzial für Makler ist im Privatkundenbereich enorm: Im vergangenen Jahr war in Deutschland gerade einmal 1 Prozent aller Haushalte dezidiert gegen Cyber-Risiken versichert, zeigt eine Umfrage des Marktforschungsinstituts YouGov von September 2017. Zugleich könnte sich jeder fünfte Befragte vorstellen, eine entsprechende Versicherung abzuschließen. „Sinnvoll ist es, Kunden mit Tipps zum richtigen Umgang mit Cyber-Risiken anzusprechen, zum Beispiel zum Umgang mit riskanten Mails“, sagt Studienautor Christoph Müller. „Dabei sollte die Ansprache passend zur Zielgruppe gewählt werden.“ Die Umfrage habe etwa ergeben, dass junge Besserverdiener, die am ehesten eine Cyber-Versicherung abschließen würden, den telefonischen Direktvertrieb bevorzugten.

[Die Schäden]

Kosten für Aufklärung und Datenwiederherstellung
59 %

Unterbrechung des Betriebsablaufs
43 %

Reputationsschaden
14 %

Diebstahl von Kreditkartendaten
11 %

Diebstahl unternehmenseigener Daten oder Betriebsgeheimnisse
8 %

WAS BRAUCHT DER GEWERBEKUNDE?

Trotz des Potenzials im Privatkundenbereich: Bislang richten sich die meisten Cyber-Versicherungen an Unternehmen. Wie Privatkunden sollten sich auch kleine und mittelgroße Firmen gegen Identitätsdiebstahl absichern, gegen Hard- und Software- sowie Vermögensschäden und gegen Haftpflichtschäden im digitalen Bereich. Zusätzlich ist eine Absicherung von Betriebsunterbrechungen für Unternehmen ein zentraler Punkt. ▶