Cyberversicherungen

Sechs Tipps für die richtige Umsetzung in der Kundenberatung

Cybersicherheit zählt im Zeitalter der Digitalisierung zu den wichtigsten Zukunftsthemen. Aber was bedeutet das konkret für Vermittler? Wie sollen sie das Thema Cyber bei ihren Kunden positionieren? Eine Handlungsanweisung in sechs Schritten erläutert der IT-Risiko-Manager und selbständiger VdS-Fachberater für Cybersicherheit, Nikolaus Stapels, in seinem Gastbeitrag.

Die Aufgabe des Vermittlers sollte zunächst vor allem sein, die eigenen Kunden für das Thema Cybersicherheit zu sensibilisieren und sie als Risikocoach zu beraten. Der Identifikation, Analyse und Bewertung von Risiken folgt dann die Absicherung, zunächst durch präventive Maßnahmen wie Richtlinien, Technik und Mitarbeitersensibilisierung. Erst im nächsten Schritt geht es darum, die Restrisiken mit Hilfe von Versicherungslösungen abzusichern.

Aber was bedeutet das konkret für die Beratungssituation beim Kunden?

Obwohl sich immer mehr Unternehmer bewusst sind, dass es keinen hundertprozentigen Schutz gegen Hackerangriffe oder einen Datenverlust gibt, beschäftigen sich die meisten erst mit dem Thema Cyberversicherung, wenn es zu spät ist oder der Schaden schon entstanden ist – mit schwerwiegenden Folgen: eine durchschnittliche Schadenhöhe im sechsstelligen Bereich bei Kleinunternehmen treibt viele Unternehmen in den Konkurs.

Genau bei diesem Szenario muss der Vermittler ansetzen: der Kunde soll sich nicht erst melden, wenn ein Schaden entstanden ist, sondern der Berater muss ihn bereits im Vorfeld darüber informieren, dass es eine Lösung gibt, um sein Unternehmen zu schützen.

Die folgenden Tipps für die vertriebspraktische Umsetzung sollen Vermittler bei der Platzierung des Themas bei ihren Kunden unterstützen und – falls nicht vorhanden – auch ihr eigenes Verständnis für die IT-fachlichen-Hintergründe schärfen.

Tipp 1: Aufklären

Zeigen Sie Ihrem Kunden, dass – im Gegensatz zur Annahme vieler – auch sein Unternehmen

durchaus interessant für Hacker ist. Denn: In vielen Fällen sind es Zufallstreffer der Hacker. Es werden Trojaner verschickt und jemand im Unternehmen installiert diesen unwissentlich. Die wesentlichen Fragen, die Sie mit Ihrem Kunden klären müssen, sind, "Wie groß ist die Abhängigkeit der IT für den Geschäftsbetrieb?" und "Kann der Betrieb, wenn alle Daten von jetzt auf gleich weg sind, normal weiterfunktionieren?".

Tipp 2: Firewall und Virenschutz – unverzichtbar aber nicht unfehlbar

Technische Schutzmaßnahmen hat heutzutage jedes Unternehmen implementiert. Firewall oder Virenscanner sind auf jeden Fall unverzichtbar, aber es bleibt ein Restrisiko bestehen. Wenn Hersteller solcher Lösungen damit werben, dass 99 Prozent der Viren erkannt werden, klingt das erst einmal sehr gut. Wenn man aber weiß, dass es Studien zufolge pro Tag circa 400.000 neue Viren, Trojaner und Würmer gibt, dann bedeutet das im Umkehrschluss, dass Virenprogramme in Unternehmen 4.000 Viren, Trojaner und Würmer pro Tag nicht erkennen und diese sich teilweise ungehindert im System ausbreiten können.

Tipp 3: Datensicherungen und Cloud

Das Beste, was Unternehmen machen können, um diesem Restrisiko vorzubeugen, ist es, eine Datensicherung zu erstellen – und das machen die meisten Unternehmen auch. Dabei gilt es aber, einige Punkte zu beachten: Die Datensicherungen dürfen beispielsweise nicht ausschließlich im Unternehmen gelagert werden, denn im Brandfall wären dann sowohl die Daten als auch die Datensicherung weg. Aus diesem Grund ist es sinnvoll, die Datensicherung außerhalb des Unternehmens zu lagern. Hierfür greifen viele auf die günstige Möglichkeit der Speicherung der Datensicherung in einer Cloud zurück. Wichtig ist es in diesem Zusammenhang, einen guten Cloud-Standort zu wählen, am besten einen Server in Deutschland.

Aber, wichtiger Hinweis: das Unternehmen bleibt für die Einhaltung der datenschutzrechtlichen Bestimmungen weiterhin verantwortlich. Dies gilt auch nach dem 25. Mai 2018, wenn die EU-Datenschutzgrundverordnung in Kraft tritt. Datenschutz kann nicht in eine Cloud outgesourct werden. Sollte es zu einer Datenschutzverletzung kommen, weil die Cloud gehackt wurde, dann haftet das Unternehmen. Diese Tatsache ist vielen Unternehmen nicht bekannt, deshalb muss der Berater auf diese Punkte im Gespräch hinweisen.

Tipp 4: Darstellung möglicher Schadenssummen

Neben dem reinen Hinweis auf mögliche Konsequenzen ist es wichtig, die möglichen Kosten, die im Schadenfall auf den Kunden zukommen, auch konkreter beziffern zu können, denn viele sind sich gar nicht bewusst, wie hoch ein Cyberschaden überhaupt ausfallen kann.

Wie allerdings diese Kosten im Einzelnen zu berechnen sind, wissen einer Untersuchung zufolge 86 Prozent der Vermittler selbst nicht und benötigen daher entsprechende Unterstützung. Das Cyber-Summen-Tool – eine Software, die auf Basis umfassender Schadenauswertungen Algorithmen entwickelt hat, um realistische Versicherungssummen zu berechnen – bietet hier eine Lösung und eignet sich darüber hinaus als vertriebsunterstützendes Beratungstool zur Visualisierung der Risiken.

Tipp 5: IT-Experten einbinden

Binden Sie einen IT-verantwortlichen Mitarbeiter des Unternehmens in das Beratungsgespräch mit Ihrem Geschäftskunden zum Thema Cybersicherheit ein. Scheuen Sie nicht das Gespräch mit dem IT-Fachmann, Sie müssen selbst kein IT-Experte sein, um zu Cyberpolicen beraten zu können, aber Sie sollten die Risiken kennen und darstellen können. Gemeinsam mit dem Fachmann können Sie Ihrem Kunden aufzeigen, was bereits für die IT-Sicherheit im Unternehmen gemacht wird, dass es aber keinen 100prozentigen Schutz geben kann. Ihr Ziel ist es, dieses Restrisiko über eine Cyberpolice abzusichern.

Tipp 6: Assistance-Leistungen ansprechen

Nicht nur vielen Kunden ist das Thema Cyberversicherung fremd, auch viele Berater betreten mit der Beratung von Cyber-Risiken und der Vermarktung von Cyberpolicen Neuland. Vermittler sollten sich daher das notwendige Wissen zur kompetenten Beratung aneignen und sich in diesem zukunftsträchtigen Themenfeld weiterbilden. Setzen Sie dann in der Vermarktung beim Kunden das erworbene Know-how ein, sensibilisieren Sie ihn für Risiken, Konsequenzen und die zur Verfügung stehenden Lösungen. Erklären Sie die wichtigsten Vorteile der Absicherung und vor allem auch die Assistance-Leistungen, die Sie mit anbieten, aber gehen Sie nicht zu sehr in die Tiefe des Produktes.

Fakt ist: Eine Cyberversicherung verhindert keinen Angriff, macht die finanziellen Folgen aber überschaubar.

Nutzen Sie das Thema Cyber als Anlass für ein Beratungsgespräch mit Ihrem Kunden. Wenn Sie ihm aufzeigen können, dass Sie das Thema kompetent beraten und auf Einwände eingehen können, steigt das Abschlusspotenzial ungemein.

Über den Autor:

Nikolaus Stapels ist zertifizierter IT-Risk Manager und selbständiger VdS-Fachberater für Cyber-Security mit langjähriger Erfahrung im Versicherungsvertrieb. Für Versicherungsvermittler bietet der Cyber-Experte **zertifizierte Weiterbildungen und entwickelt beratungs- und vertriebsunterstützende Softwaretools**.