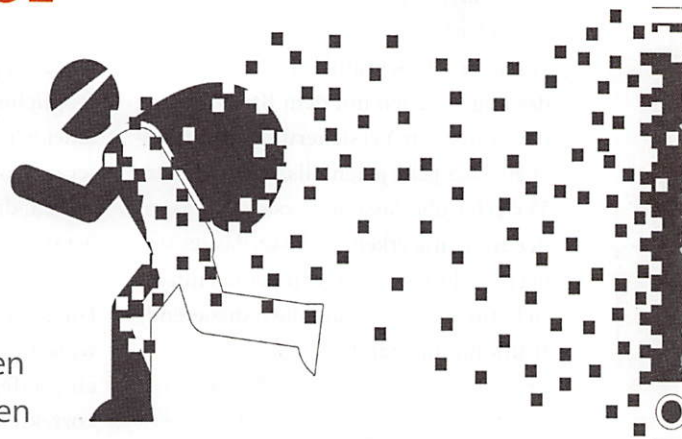


# Der Türöffner bei Gewerbekunden



Mit der Beratung von Cyber-Risiken und der Vermarktung von Cyber-Policen betreten Versicherungsvermittler oft Neuland. Neben Versicherungs-Know-how und dem Produktwissen sind hier auch IT-fachliches und technisches Wissen essenziell. Das fehlt aber vielen Vermittlern.

Viele Versicherer haben inzwischen Cyber-Policen auf den Markt gebracht. Ein Vertriebskonzept zum erfolgreichen Umgang mit dem Thema und Antworten auf die Frage, wie Kunden für diesen Markt erschlossen werden können, bleiben die Versicherer den Vermittlern aber meist schuldig. Vor diesem Hintergrund hat die UB1st-GmbH die Weiterbildung zum „Fachberater für Cyber-Risiken“ entwickelt. Bei dieser werden die Vermittler im komplexen Beratungsfeld „Cyber“ ausgebildet. Dabei steht nicht nur die Vermittlung von theoretischem Wissen im Vordergrund, sondern vor allem auch die vertriebspraktische Umsetzung in der Kundenberatung.

Ein völlig neues Softwaretool wird dabei eingesetzt, das die Ansprache beim Kunden akquisitorisch unterstützt, die Gefährdungslage beim Kunden ermittelt und Maßnahmen zur Risikominimierung vorschlägt. Kernstück ist aber die Ermittlung der ausreichenden Versicherungssumme.

Einer UB1st-Studie zufolge gaben 82 Prozent der befragten Berater an, dass sie sich nicht in der Lage sehen, eine angemessene Versicherungssumme zu ermitteln. In der Regel wird eine zu geringe Summe vorgeschlagen, oder die Höhe wird der Einschätzung des Kunden überlassen. Um für dieses Dilemma eine Lö-

sung zu entwickeln, hat die UB1st-GmbH auf Basis umfassender Schadenauswertungen Algorithmen entwickelt, um realistischer Versicherungssummen berechnen zu können.

## Reale Gefahr wird oft ignoriert

Tatsache ist, dass Industriespionage, Datenverluste, Verschlüsselungstrojaner (Ransomware) und Geheimnisverrat durch die eigenen Mitarbeiter in Unternehmen immer mehr zunehmen. Angenommen, in einem Unternehmen ist Feuer ausgebrochen und kein Mitarbeiter kümmert sich darum, der Brand wird einfach ignoriert und breitet sich langsam immer weiter aus. Was wie eine unmögliche Situation klingt, erleben Risikomanager und Cyber-Fachberater häufig, wenn sie mit Geschäftsführern oder Vorständen über das Thema „Cyber“

sprechen. Die Gefahr ist real, dennoch ignorieren viele Verantwortliche dies noch immer.

Selbstverständlich haben die meisten IT-Verantwortlichen und Unternehmensinhaber bereits von „Ransomware“, „Datendiebstählen“ oder „Fake President“ gehört – aber aktiv dagegen etwas unternommen noch nicht. Wenn ein Feuer ausbricht, wissen alle Mitarbeiter des Unternehmens, was zu tun ist. Wenn in einer Firma jedoch auf einmal 15 Rechner verschlüsselt werden, die Mitarbeiter nicht wissen, wie sie zu reagieren haben, und das Netzwerk zusammenbricht, dann herrscht im Unternehmen das absolute Chaos.

## Hohe Kosten, schlechte Reputation

Ein erfolgreicher Cyber-Angriff kann nicht nur die Reputation kosten, es entstehen auch Kosten für Rechtsberatung, Schadensersatz oder Benachrichtigung der Betroffenen. Durch den Abzug von Geschäftsgeheimnissen sowie andere Folgekosten des Angriffs werden immer mehr Firmen insolvent. Die Schadenbegleitkosten nach einem erfolgreichen Cyber-Angriff liegen oft im sechsstelligen Bereich. Daher empfiehlt es sich für Unternehmen, sich gegen diese Gefahr abzusichern. Eine Cyber-Versicherung kann zwar einen Schaden nicht verhin-

### Kompakt

- Viele Unternehmen wissen um Cyber-Risiken, handeln aber nicht dementsprechend.
- Versicherer bringen immer mehr Cyber-Policen auf den Markt. Das Produkt-Know-how fehlt aber oft.
- Die Weiterbildung „Fachberater für Cyber-Risiken“ soll diese Lücke schließen.



dern, die finanziellen Folgen jedoch beherrschbar machen.

Neben der realen Gefahr, Opfer eines Hackerangriffs zu werden, steigt auch der Regulierungsdruck. Die neue EU-Datenschutzverordnung wird ab Mai 2018 greifen und viele neue Pflichten mit sich bringen. So schreibt die ISO 9001 in der neuen Fassung ein Risikomanagement in Unternehmen vor. Viele Unternehmer oder Geschäftsführer sind sich aber nicht bewusst, dass sie privat und persönlich gegenüber den Kunden und Gesellschaftern voll haftbar gemacht werden können – ein GmbH-Mantel schützt in diesem Fall nicht vor solchen Ansprüchen. Dieses Manko erkennen immer mehr Firmen und schützen sich mit einer Cyber-Versicherung.

### Kunden sensibilisieren und als Coach beraten

Zur richtigen Kundenberatung gehört auch die eindeutige Klassifizierung der Kunden. Dabei gilt es, zwei Gruppen von Kunden zu unterscheiden:

- Kunden, die bereits selbst einen Cyber-Schaden hatten oder durch andere Unternehmen vom Umfang eines solchen Schadens Kenntnis haben. Diese sind sensibilisiert und schließen so eher eine Cyber-Versicherung ab.
- Kunden, die bisher noch keine Schäden hatten oder es noch nicht bemerkt haben. Bei diesen Kunden ist der Gedanke, ebenfalls Opfer eines Cyber-Angriffs zu werden, zu abstrakt – hier besteht dann dringender Aufklärungsbedarf seitens des Beraters!

Offen für den Austausch zum Thema „Cyber“ sind erfahrungsgemäß alle Gewerbetunden – gerade vor dem Hintergrund der aktuellen Hackerangriffe und der damit verbundenen Diskussion. Nachdem die Aufmerksamkeit geweckt wurde, ist es nun die Aufgabe des Vermittlers, Kunden zu sensibilisieren und als Risikocoach bestmöglich zu beraten.

Unternehmen investieren derzeit eher in präventive Maßnahmen wie Richtlinien, Technik und Mitarbeitersensibilisierung. Das ist natürlich eine gute Basis.

Die jüngsten Fälle und Studien beweisen jedoch, dass ein vollständiger Schutz, der nur auf Prävention aufgebaut ist, nicht möglich ist.

Auch mit einer besseren IT-Sicherheit im Unternehmen werden Mitarbeiter immer noch ihre Tablets oder Handys verlieren. Unzufriedene Mitarbeiter werden auch künftig ihre Zugänge nutzen, um Schaden anzurichten oder sensible Daten zu entwenden und an Dritte zu veräußern. Schadprogramme der neuesten Generation nutzen Sicherheitslücken aus, bevor die Hersteller diese schließen können. Die Anschaffung hochwertiger Sicherheitstechnik wird mehr als Reaktion auf einen Angriff angeschafft, seltener als Prävention. Der VdS bezeichnet die Cyber-Risiken als die Brandgefahr des 21. Jahrhunderts. Die Wahrscheinlichkeit, gehackt zu werden, ist weitaus höher, als Opfer eines Brandschadens zu werden. Dennoch haben viele Unternehmen keine Cyber-Absicherung.

### Positionierung als Cyber-Experte

Um auch künftig unter den schwierigeren Marktgegebenheiten wachsen zu können, müssen Vermittler in wachstumsstarken Geschäftsfeldern der Versicherungsbranche kompetent und vertriebsorientiert aufgestellt sein. Eine Möglichkeit, sich vom Wettbewerb abzuheben, ist die Fokussierung auf die Cyber-Absicherung in Unternehmen.

Der wirtschaftliche Schaden im Bereich „Cyber“ beläuft sich in Deutschland laut einer Bitkom-Studie auf circa 51 Milliarden Euro im Jahr. Auf diese Gefahr müssen Unternehmen hingewiesen werden. Viele Berater sind sich jedoch nicht bewusst, dass sie in der Beraterhaftung stehen, wenn sie dieses Thema nicht beim Kunden ansprechen.

Der Grund, warum viele Vermittler das Thema „Cyber“ nicht oder nicht gerne ansprechen, ist, dass sie sich nicht in der Lage fühlen, auf Augenhöhe mit den IT-Verantwortlichen ihrer Gewerbetunden zu kommunizieren. Ihnen fehlt das notwendige IT-Wissen und damit oftmals

das Verständnis für die Gefahren, denen Unternehmen ausgesetzt sind. Im Umkehrschluss führt das dazu, dass es ihnen schwerfällt, im ersten Schritt Risiken zu identifizieren, zu analysieren und zu bewerten, um dann im zweiten Schritt die Restrisiken mittels Versicherungslösungen abzusichern.

### Kompetenter Partner sein

Aber umgehen können sie das Thema „Cyber“ über kurz oder lang auf keinen Fall. Daher müssen Vermittler lernen, Cyber-Risiken kompetent zu beraten. Eine Investition in Wissenserwerb zum Thema „Cyber“ zahlt sich auch im Vertriebs Erfolg aus. Der Vermittler fühlt sich sicher in seiner Rolle als Kompetenzträger in der Beratung von Risiken 4.0 und wird auch so vom Gewerbetunden wahrgenommen: als kompetenter Berater und Partner.

Ein probates Mittel zur Sensibilisierung von Gewerbetunden für das Thema „Cyber-Risiken“ sind neben individueller Ansprache vor allem Kundenveranstaltungen. Hier haben Vermittler die Gelegenheit, ihre Kunden zu informieren. Der Austausch zwischen Experten und Gewerbetreibenden ist gewinnbringend, sowohl für die Gewerbetunden als auch für die Positionierung des Vermittlers bei seinen Kunden.

Um an der viel prognostizierten Goldgräberstimmung „Cyber“ zu partizipieren, müssen sich Vermittler auf dieses neue Themenfeld einlassen. Ist die Tür beim Kunden erst einmal geöffnet, ergeben sich dann meist auch Chancen, andere Themen anzusprechen. Die Investition in Wissen lohnt sich also. Denn eines ist sicher: Cyber-Beratung ist kein Modetrend, der vorüberzieht. ■



**Autor:** Nikolaus Stapels ist IT-Risk-Manager und VdS-Fachberater für Cyber-Security und als solcher Trainer bei der UB1st-Gesellschaft für Beratungserfolg mbH ([www.ub1st-gmbh.de](http://www.ub1st-gmbh.de)).