«Auch Versicherer sind mit Cyberthema gefordert». Die Digitalisierung macht die Welt nicht nur einfacher, sondern schafft auch neue, komplexe Risiken. Unternehmen tun gut daran, ihre IT-Risiken genau zu prüfen. Cyberversicherungen sind nur ein Teil der Lösung.

INTERVIEW: THOMAS BERNER

Cyber-Risiken entwickeln sich zu einem Top-Thema in der Unternehmensführung. Hacker-Angriffe auf staatsnahe und private Unternehmen nehmen auch in der Schweiz zu. Hingegen scheint es erst seit kurzer Zeit adäquate Deckungen gegen solche Risiken zu geben, meint etwa Rolf Th. Jufer. Er ist Mitglied der Geschäftsleitung der Funk Insurance Brokers AG und seit 2013 als Leiter von Marketing und Vertrieb für die Bereiche Marktentwicklung, Markenpositionierung, Neukundengewinnung und das Funk RiskLab verantwortlich.

Herr Jufer, weshalb muss Cyber Security für KMU grundsätzlich ein Thema sein?

Rolf Th. Jufer: Industrie 4.0, Digitalisierung oder IoT - das sind Begriffe, die eine neue Epoche für die Gesellschaft und Wirtschaft angestossen haben und so auch den Unternehmensalltag massgeblich prägen oder aber ganz bestimmt prägen werden. Es geht einerseits darum, die Chancen dieser Entwicklung optimal zu nutzen und sich andererseits als Unternehmen auch den Risiken der dynamisch voranschreitenden Vernetzung von Mensch, Maschine und Prozessen zu stellen. Das heisst, regelmässig die Robustheit der eigenen Unternehmung zu prüfen, Mitarbeitende regelmässig zu sensibilisieren, die IT-Sicherheit permanent zu optimieren sowie sich im Rahmen des Cyber-Risikomanagements regelmässig ein Bild über das Cyber-Restrisiko zu machen. Dieses Restrisiko ist dann zu bewerten und gegebenenfalls im Versicherungsmarkt zu platzieren.

Was sind derzeit die grössten Cyber-Risiken aus Sicht der Versicherer?

Versicherer sind mit dem Cyberthema aktiv gefordert. Wie bei vielen neuen Risiken fehlen gute statistische Grundlagen über Schadenshäufigkeit und Schadenswahrscheinlichkeit. Bei Cyberschäden im Unternehmensbereich besteht in vielen Ländern noch keine Meldepflicht und so ist die Dunkelziffer dieser Schäden enorm hoch. In diesem Umfeld die richtige Preis- und Reservepolitik zu betreiben, fordert die Erst- und Rückversicherer enorm.

Gemäss verschiedenen Studien sind KMU sich zwar der Risiken bewusst, tun aber zu wenig zu ihrem Schutz. Inwiefern deckt sich dies mit Ihren Beobachtungen?

Wir sensibilisieren Unternehmen seit rund fünf Jahren zum Thema Cyber-Risiken und können die Studienresultate bestätigen. Seit Ende des letzten Jahres können wir jedoch eine deutliche Verhaltensänderung der Unternehmen feststellen. Nicht mehr nur Unternehmen aus der Finanz- und Versicherungsindustrie fragen aktiv nach Deckungsmöglichkeiten gegen Cyber-Risiken, sondern auch KMU jeder Grösse wollen konkret wissen, wie Cyber-Risiken im Versicherungsmarkt abgedeckt werden können. Der Kauf von Cyberversicherungslösungen durch Unternehmen hat markant zugenommen.

Mit welchen Partnern arbeiten Sie als Versicherungsbroker zusammen und weshalb?

Wichtig ist für Unternehmen, dass sie das Cyberthema, wie schon gesagt, ganzheitlich angehen. Eine Versicherungslösung alleine ist kein robustes Cyberkonzept. Daher arbeiten wir im Bereich IT-Sicherheit und Datenschutz mit bewährten Partnern zusammen: InfoGuard ist ein Spezialist für Cyber-Security. Die Anwaltskanzlei MME hat sich auf Datenschutz und IT-Recht spezialisiert. Der holistische Ansatz hilft unseren Kunden auch, sichtbar bessere Konditionen im Versicherungsmarkt zu erhalten. Was die Versicherungspartner betrifft, so sind wir als unabhängiger Versicherungsbroker unseren Kunden verpflichtet, im Markt nach der individuell besten Lösung, unter Berücksichtigung des besten Leistungs- und Preisverhältnisses, zu suchen. Aufgrund der eher dürftigen Angebote im Markt Schweiz haben wir vor einem Jahr mit Funk CyberSecure einen eigenen Deckungsrahmen definiert, den wir nun mit ausgewählten Versicherern in der Schweiz umsetzen. Die Versicherungsgesellschaft, welche am schnellsten auf unser Wording reagiert hat, war ein global führender und sehr erfolgreicher US-Industrieversicherer. Wir stehen aktuell mit weiteren Versicherungsunternehmen in Verhandlung.

Welche Versicherungsprodukte in Sachen Cyber-Risiken werden derzeit am meisten nachgefragt und von wem?

Die Cyber-Risk-Versicherung wird am meisten nachgefragt. Die Erweiterung von bestehenden Versicherungen wie z.B. Sach-, EDV-, Vertrauensschaden- und Haftpflichtversicherungen ist zwar punktuell möglich, doch weitaus am besten eignet sich die Cyber-Risk-Versicherung für die heutigen Cyber-Risiken. Grosse Nachfrage besteht vor allem im Finanzdienstleistungs- und Versicherungssektor, gefolgt vom Fertigungssektor, Arzneimittel- und Life-Science-Sektor und dem übrigem Dienstleistungssektor.

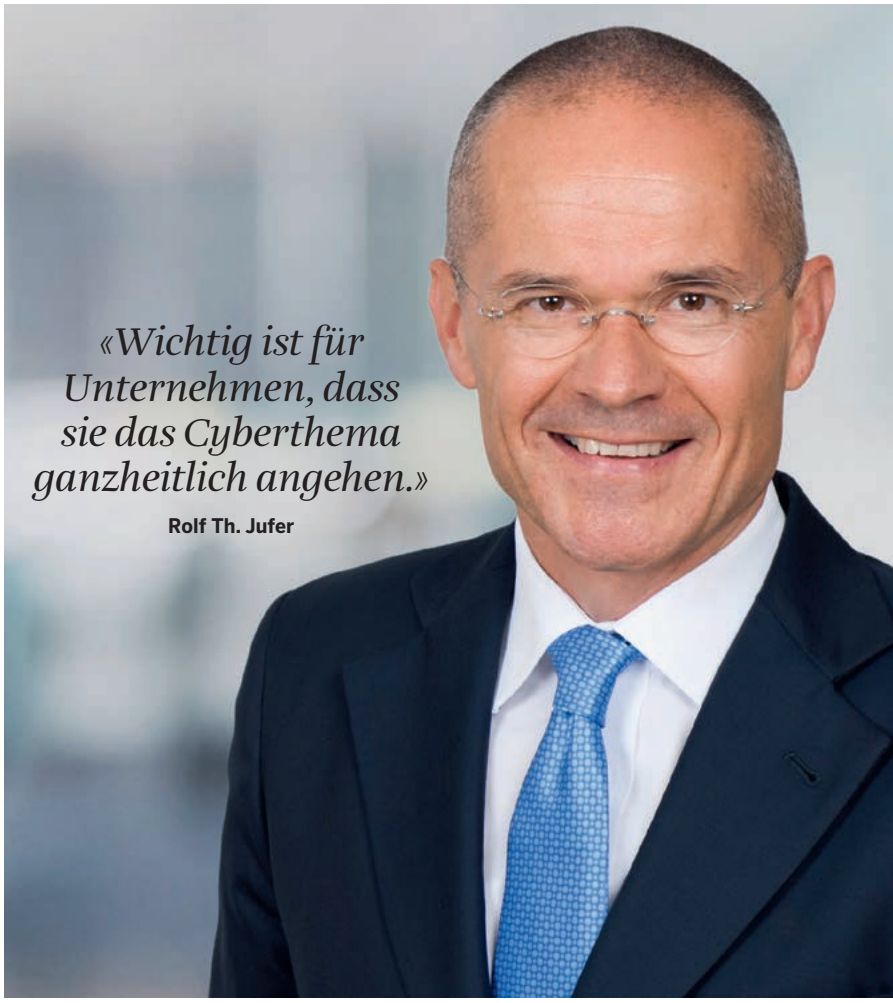
Welche Arten von Cyber-Risiken lassen sich denn auf welche Arten versichern?

Es gibt zahlreiche Arten von Cyber-Risiken. Die Realität zeigt auf, dass sich das organisierte Verbrechen ins Internet verschoben hat und Unternehmen häufig und intensiv von «Cyber-Angriffen» bedroht werden. Auf dem Vormarsch sind neuere Erpressungsformen (Ransomware, DDoS-Attacken), aber auch bekannte Angriffe wie gezieltes Hacking, Trojaner, Phising, Datenbeschädigung, Datendiebstahl, Spionage, etc.).

Wie bereits erwähnt, eignet sich für die Abdeckung der Cyber-Restrisiken eine spezifische Cyber-Risk-Versicherung. Letztere deckt sowohl Schäden, welche der Versicherte einem Dritten verursacht (Drittschäden), als auch Schäden, welche beim Versicherten selbst entstehen (Eigenschäden).

Können Sie das noch genauer erläutern?

Ansprüche Dritter können entstehen, wenn der Versicherte durch Sicherheitsmängel in seinem System Daten von Dritten beschädigt oder zerstört oder deren Geschäftstätigkeit beeinträchtigt oder unterbricht. Ebenso kann der Verlust von vertraulichen Daten Dritter oder deren unerlaubter Veröffentlichung zu Ansprüchen führen. Die Versicherung deckt die Abwehr unbegründeter sowie die Übernahme begründete Schadenersatzansprüche Dritter. Im Eigenschadenbereich wird die Wiederherstellung des IT-Systems, mit den durch einen Cyberangriff beschädigten, blockierten oder zerstörten Daten, Programmen und Netzwerken, bezahlt. Bei einem Betriebsunterbruch z.B. nach einem Denial-of-Service-Angriff werden der Ertragsausfall sowie die weiteren Kosten, welche zur Fortführung der Betriebsaktivitäten erforderlich sind, gedeckt. Auch die Erpressungszahlungen sowie diverse Kosten wie diejenigen für die Beauftragung eines professionellen Krisenmanagers, von spezialisierten Computer-Forensikern, PR-Experten und von Fachanwälten fallen unter die Versicherungsdeckung. Im Weiteren ist es möglich, den Cyber-Diebstahl (Geldabgang nach einem Cyber-Angriff) zu versichern.



Welche weiteren Schäden sind noch zu erwähnen, und wie hoch sind Selbstbehalte, Prämien etc.?

Als Voraussetzung für ein versichertes Ereignis in einer Cyber-Risk-Versicherung ist die Informationssicherheitsverletzung notwendig. Darunter können u.a. die Netzwerksicherheitsverletzung, Zerstörung, Beschädigung etc. des Computer-Systems oder von Teilen davon, Daten- und Vertraulichkeitsverletzung, Verletzung von Benachrichtigungspflichten sowie rechtswidrige Kommunikation fallen. Die Selbstbehalte sind je nach Risiko und Branche des Versicherten unterschiedlich und belaufen sich in der Regel auf zwischen CHF 5 000 und CHF 500 000. Dies gilt ebenso für die Prämien, welche in der Regel zwischen zwei Promille und ein Prozent der Versicherungssumme betragen.

Zum Schluss: Was können KMU tun, um ihr Cyber-Risikomanagement zu verbessern?

Zuerst sollten sich KMU fragen, ob die eigenen IT-Kapazitäten überhaupt ausreichen, um eine zeitgemässe, technische IT-Sicherheit zu gewährleisten, oder ob deren Auslagerung an spezialisierte Anbieter sinnvoller ist. Dies kann z.B. anhand der Zeit von der Veröffentlichung von Sicherheitsupdates bis zu deren Installation auf der eigenen Umgebung festgestellt werden. Dabei gilt es zu beachten, das Cyberkriminelle nach ungefähr einer Woche dazu in der Lage sind, Sicherheitslücken, die die Updates zu schliessen suchen, auszumachen und zu nutzen. Ebenso wie die KMU versuchen auch organisierte Cyberkriminelle effizient zu wirtschaften. Wieso also komplexe und zeitaufwendige Codes (Exploits etc.) schreiben, wenn doch der schwächste Punkt jeder IT-Abwehr der Mensch ist? In diesem Kontext gilt es die eigenen Mitarbeitenden hinsichtlich IT-Sicherheit regelmässig zu schulen, um ihr Bewusstsein für potenzielle Angriffe zu schärfen und das Risiko dadurch zu minimieren. KMU müssen sich ausserdem bewusst werden, dass es trotz aller präventiven Massnahmen keine 100 %-ige Sicherheit gibt. Erfahrungsgemäss gibt es immer wieder Mitarbeitende, die trotz aller Warnungen verdächtige Mails samt Anhängen öffnen. Ferner ist insbesondere bei gezielten Cyberangriffen (z.B. Social Engineering) eine Abwehr so gut wie unmöglich. Deshalb sollte auch der Notfall im Rahmen des Business Continuity Managements (z.B. IT-Systemausfall, verursacht durch eine Ransomware) und des Krisenmanagements (z.B. Diebstahl von sensiblen Kundendaten) vorbereitet und geübt werden. Als letzten Schritt in der ganzheitlichen Behandlung der Cyber-Risiken im Rahmen des Risikomanagements sollten KMU eine auf die eigenen Bedürfnisse angepasste Versicherungslösung evaluieren, um den Unternehmenswert zu schützen und Schäden und Kosten im Falle eines Cyberangriffs transferiert zu haben.