NACHGEFRAGT

«NUR DIE WENIGSTEN SIND UMFASSEND GEWAPPNET»

Tom Kessler über Unterschiede in der Handhabung von Cyber-Risiken, Vorgehen zu deren Minimierung sowie die Versicherbarkeit von Cyberangriffen.

INTERVIEW WERNER RÜEDI

Wie sind Unternehmen gegen Cyber-Risiken gewappnet?
Tom Kessler: Wir sehen zwar ein zunehmendes Bedürfnis von Unternehmen, sich mit einem professionellen Partner zu der Cyber-Risiko-Landschaft auszutauschen, aber gemäss den Umfrageresultaten unseres «Cyber Risk Survey Reports 2016» fühlt sich das Management dennoch erst bei 14 Prozent der Unternehmen für die betrieblichen Cyber-Risiken verantwortlich. Zu oft werden Cyber-Risiken immer noch als reines IT-Thema angeschaut, ohne die organisatorischen Risiken im Betrieb sowie deren finanziellen Auswirkungen miteinzubeziehen. Ich vermute daher umfassend gegen Cyber-Risiken gewappnet sind heute erst die wenigsten Unternehmen.

Gibt es Unterschiede nach Branchen?
Ja. Unternehmen aus der Finanz- und Telekommunikationsbranche oder dem eCommerce zum Beispiel zeigen ein grosses Interesse und setzen sich aktiv mit ihren Cyber-Risiken auseinander. Aber auch die Gesundheitsbranche und die öffentliche Hand nehmen die Risiken überdurchschnittlich ernst.

Woher rühren diese Unterschiede?
Dies hat sicherlich damit zu tun, wie sehr ein Unternehmen Cyber-Risiken ausgesetzt ist und was bei einem Schaden bzw. Ausfall der IT-Infrastruktur auf dem Spiel steht. Zudem gab es beispielsweise im Gesundheitswesen bereits einige prominente Fälle, die fast zu einer Katastrophe geführt hätten. Das hat die Sensibilität in der Branche sicher noch erhöht.

Welches Vorgehen empfehlen Sie Unternehmen, um Risiken zu minimieren?
Das kann unterschiedlich sein, da verschiedene Branchen auch unterschiedlichen Cyber-Risiken ausgesetzt sind. Zudem ist jedes Unternehmen unterschiedlich technisch geschützt sowie organisatorisch aufgebaut und lebt gemäss einer eigenen Risiko- und Versicherungspolitik. Aber ein Unternehmen sollte die Cyber-Risiken, denen es ausgesetzt ist, kennen und sich deren finanziellen Auswirkungen bewusst sein. Deshalb empfehlen wir allen, die betriebsinternen Worst-Case-Szenarien bezüglich der Cyber-Risiken zu analysieren und die wichtigsten Daten sowie Prozesse mit Priorität technisch zu schützen. Das Restrisiko kann dann wo sinnvoll mittels einer Cyber-Versicherung auf den Versicherungsmarkt transferiert werden.

Tom Kessler ist Mitglied der Geschäftsleitung von Kessler & Co AG

Die Dimensionen einer Cyberattacke können gigantisch sein. Lässt sich überhaupt alles versichern?
Das Ausmass eines Cyberangriffs lässt sich heutzutage mehrheitlich versichern, trotz den möglicherweise grossen finanziellen Auswirkungen. Die klassische Cyber-Versicherung als Vermögensschadenversicherung bietet ein breites Spektrum an Deckungsmöglichkeiten. Dazu zählen einerseits sogenannte Eigenschäden, also zum Beispiel Aufwendungen für ein funktionierendes Krisenmanagement sowie den entgangenen Gewinn bzw. die Verlustvergrösserung in Folge eines Netzwerkunterbruchs. Andererseits sind die Bezahlung von berechtigten Schadenersatzansprüchen sowie Abwehrkosten bei unberechtigten Ansprüchen ebenfalls Bestandteile einer umfassenden Lösung. Hier lassen sich auch Unterschiede im internationalen Vergleich feststellen. Während in den USA Auswirkungen aufgrund von Datenschutzverletzungen als hohes Risiko wahrgenommen und versichert werden, beschäftigen Unternehmen in Europa mehrheitlich die finanziellen Konsequenzen eines Netzwerkunterbruchs.

Wie berechnen Versicherer und Broker eigentlich Prämien zu Cyberversicherungen?
Die Berechnung von Cyber-Risiken ist für Versicherer noch eine Herausforderung, da es sich um vergleichsweise neuartige Risiken handelt, die zusätzlich einem stetigen technischen und rechtlichen Wandel unterstellt sind. Gleichzeitig existieren neue Formen von Kumulrisiken, wie die steigende Vernetzung von Unternehmen, der potenzielle Ausfall von IT-Dienstleistern mit hohem Marktanteil oder Viren, die länderübergreifend auftreten. Damit Versicherer Cyber-Risiken identifizieren und richtig bewerten können, sind Informationen zum Tätigkeitsbereich sowie der Struktur des Unternehmens, zum Branchenumfeld, zur geografischen Ausrichtung sowie zur IT-Infrastruktur notwendig. Ob ein Unternehmen als risikobehaftet wahrgenommen wird, hängt ebenfalls stark von dessen Risk Management ab. Von hoher Bedeutung ist dabei die Frage eines vorliegenden Business Continuity Plans, die implementierten Sicherheitsmassnahmen oder das Vertragsmanagement mit Outsourcing-Partnern.

Bild: zvg