Die Cyber-Versicherung

Spezielle Versicherungen decken bei Cyber-Vorfällen sowohl Eigenschäden als auch Ansprüche Dritter ab. Wie das funktioniert und warum Unternehmen sich damit jetzt auseinandersetzen sollten, erläutert Oliver Delvos, Team-Leiter Cyber-Versicherungen bei AIG für den DACH-Raum.

Herr Delvos, warum sollten sich Unternehmen gerade heutzutage absichern?

Oliver Delvos: In Zeiten einer stetig voranschreitenden Digitalisierung, intelligenten Maschinen und der Einbindung ganzer Arbeitsabläufe in die Welt des IoT ist das Arbeiten im sogenannten Cyber-Raum schon lange nicht mehr nur Teil des privaten Alltags. Die Relevanz des Themas jedoch leitet sich für viele Unternehmen erst aus ihren unterschiedlichen Geschäftsmodellen ab. Was somit für hoch digitalisierte Geschäftsmodelle im Online-Versandhandel oder Banking selbstverständlich ist, wird für traditionelle Unternehmungen beispielsweise erst durch Digitalisierungsinitiativen oder etwa die neue EU-Datenschutzgrundverordnung auf die Tagesordnung gerufen. Wer hier unvorbereitet getroffen wird, verliert seine unternehmerischen Handlungsspielräume und fällt womöglich hinter dem Wettbewerb zurück.

Die Vernetzung der gesamten Unternehmensdaten über IT und sonstige Netzwerke bringt somit nicht nur Vorteile mit sich, sondern birgt auch Schwachpunkte, welche Kriminelle sich zunutze machen und so den Unternehmen großen wirtschaftlichen Schaden zufügen können.

Was sind die größten Cyber-Gefahren?

Die häufigsten Cyber-Vorfälle werden nach wie vor durch Schadprogramme generiert, die Unternehmensdaten verschlüsseln. Dabei ist das eigentliche Ziel meist die Forderung von Lösegeldern in Kryptowährungen. Insbesondere durch die zunehmende Komplexität der Lieferkette und dem hohen Grad der Vernetzung innerhalb der Unternehmen selbst kommt es in zunehmendem Maße zu einschneidenden Betriebsunterbrechungen, die zum Teil schwerwiegende finanzielle Folgen haben können – von Reputationsschäden ganz zu schweigen.

Und deshalb raten Sie zu Cyber-Versicherungen?

Im Mittelpunkt der Überlegung eines jeden Unternehmen sollte die Frage danach stehen, wie finanzielle Unwägbarkeiten und Katastrophenrisiken bestmöglich eingegrenzt werden können. Die Inanspruchnahme eines entsprechenden Versicherungsschutzes ermöglicht einen Risikotransfer für Vermögensschäden einer Organisation in die Bilanz des Versicherers beziehungsweise in den Versicherungsmarkt.

„Die tatsächliche Tragweite eines Cyber-Vorfalls wird vor allem von traditionellen Unternehmen nur selten in ihrem gesamten Umfang erkannt."

OLIVER DELVOS

Setzen produzierende Unternehmen bereits auf solche Versicherungen?

Wir nehmen hier eine große Unsicherheit wahr. Zu häufig fehlt es noch an Verständnis für die Komplexität und Dynamik, die mit der Cyber-Sicherheit und mit dem Einsatz von Versicherungen einhergehen. Der Markt in Europa ist vergleichsweise noch sehr jung – Unternehmen kaufen überhaupt erst seit ein bis zwei Jahren gezielt Cyber-Versicherungen.

Wie ist ihre Versicherungslösung aufgebaut?

CyberEdge 3.0 ist ein kombiniertes Produkt zur Absicherung von Eigenschäden, wie etwa zur Wiederherstellung von Daten und IT-Systemen. Weiterhin sichert sie Drittschäden und Haftungsansprüche ab. Das Produktportfolio besteht aus über 20 unterschiedlichen Versicherungsbausteinen, deren Deckung unter anderem Betriebsunterbrechungen durch Systemausfälle, Fehlbedienung, technische Probleme oder aufgrund eines Cyber-Angriffs auf externe IT-Dienstleister umfasst. Mit der Lösung sind Unternehmen zudem auf Vorfälle rund um das Thema Datenschutz vorbereitet.

Gleichwohl bietet eine solche Absicherung zusätzlichen Service durch die Unterstützung eines spezialisierten Partners aus dem Bereich Recht und IT. Dazu gehören etwa Service-Leistungen wie eine 24-Stunden-Hotline und der Zugang zu externen IT-Forensik-Experten.

Welche Parameter spielen für die Kosten der Versicherung eine Rolle?

Entscheidend ist die Auswertung der Maßnahmen, welche durch das Unternehmen bereits getroffen wurden und deren Implementierung. Fragen in diesem Zusammenhang können sein: Gibt es entsprechende Zertifizierungen? Werden die Vorfalls-Reaktions-Pläne regelmäßig getestet? Gibt es Schwachstellen-Scans?

Darüber hinaus muss geklärt werden, wie das Unternehmen patcht, ob regelmäßig Back-Ups erstellt werden und ob Mitarbeiter geschult werden. Auch sind die konsequente Einhaltung der DSGVO sowie ein umfassendes Firewall-Management entscheidend. *ld*

Bild: AIG