So können sich Firmen gegen Cyberattacken versichern

Viele Firmen wollen sich nach den Vorfällen mit Schadsoftware gegen Cyberattacken versichern lassen.

Alle reden über Cyber-Attacken. Kann ich meine Firma dagegen versichern?

Ja. Aber die bestehenden Versicherungen versichern nur gegen spezifische Einzelrisiken und die Deckungslimiten bei solchen Versicherungen sind sehr schnell erschöpft. Das liegt einerseits daran, dass Versicherungen gegen Cyber-Risiken erst seit kurzem existieren und sich noch kein Branchenstandard herausgebildet hat. Anderseits bestehen viele Ausschlussklauseln, welche solche Versicherungen für Firmen nur beschränkt attraktiv machen. In den Policen gibt es viele Stolpersteine, die Firmen berücksichtigen müssen.

Was sind Cyber-Risiken?

Cyber-Risiken sind potenzielle Risiken, die im Zusammenhang mit der Technologie oder mit Informationen eines Unternehmens stehen. "Darunter fallen so unterschiedliche Vorfälle wie Verluste durch Cyber-Kriminalität oder Cyber-Terrorismus, unbeabsichtigter oder versehentlicher Verlust von eignen oder fremden Daten, physischer Systemverlust sowie die Haftbarkeit für Online-Aktivitäten und Aussagen in E-Mails", sagt der Rechtsanwalt Nicolas Bracher, der als Fachmann auf diesem Gebiet gilt.

Sind Schäden durch Cyber-Attacken genau messbar?

Nicht immer. Und das hat Auswirkungen auf die Deckungslimite einer eventuellen Versicherung gegen Cyber-Risiken. Die Wiederherstellungskosten bei Datenverlusten, Lösegeldzahlungen bei Erpressungen, Bussen und Rechtskosten bei Datenschutzrechtsverletzungen sind messbar. Verluste durch Reputationsschäden oder Marktwertverluste sowie genaue Ertragsausfälle durch Betriebsunterbrüche sind schon viel schwieriger feststellbar und daher kaum von der Versicherung bei einem schwereren Schadensfall erstattbar.

Gibt es eine Versicherung in der Schweiz, die gegen alle Cyber-Risiken schützt?

Nein. Die bisher auf dem Markt verfügbaren Versicherungen etwa von Allianz, Axa Winterthur, HDI Global und Zürich bieten Versicherungsschutz gegen genau definierte Einzelrisiken. Das deckt nicht alle Cyber-Risiken ab, denen Firmen in den letzten Jahren ausgesetzt waren. Eine "Vollkasko"-Versicherung gegen Cyber-Attacken ist auch in Ländern, in denen solche Versicherungsmodelle länger bestehen, wie etwa den USA, nicht möglich. Dieses mangelnde Angebot führt dazu, dass die Nachfrage nach Cyber-Deckungen durch medial viel diskutierte Attacken ansteigt, "aber nach wie vor werden sehr wenige Deckungen auch gekauft", so der Leiter Unternehmensversicherung der Allianz Suisse, Bruno Spicher.

Was beinhalten die Versicherungen, die es momentan auf dem Markt gibt?

Die heute erhältlichen Policen beziehen sich primär auf Risiken im Zusammenhang mit Cyber-Kriminalität und Datenschutzrechtsverletzungen, schreibt Anwalt Nicolas Bracher im kürzlich erschienenen "Schulthess Manager Handbuch", das sich ausführlich mit dem Thema befasst. Sie bestehen meist aus verschiedenen Deckungsbausteinen und enthalten sowohl Elemente der Eigenschaden- als auch der Haftpflichtversicherung. Es kommt nicht selten vor, dass eine bestehende Versicherung einer Firma bereits einen Abschnitt zu Cyber-Risiken enthält. Die Kosten betragen je nach Police für KMU zwischen 10000 und 50000 Franken pro Jahr. Grosskonzerne zahlen weit mehr.

Ist meine Firma überhaupt gefährdet, Opfer einer Cyber-Attacke zu werden?
Es existieren seit längerem Cyber-Risiko-Tests und Self-Assessment-Tools. Online gratis zugänglich sind zudem Studien des Instituts für Versicherungswirtschaft IVW sowie der britischen Organisation AIRMIC, die Managern einen schnellen Einstieg in dieses Thema liefern und bei der Einschätzung der eigenen Gefährdung helfen können. Die Risikoprofile jeder Firma und jeder Branche unterscheiden sich teilweise deutlich. Laut einer Statistik von AIG Europe sind vor allem Finanzdienstleister und Telekommunikationsfirmen im Fokus von Cyber-Attacken. Grundsätzlich steigen die Gefahren aber bei all jenen Firmen, bei denen die Interaktion mit Kunden jederzeit online möglich ist, so der Versicherer AIG Europe.

Welche Arten von Kosten kommen auf attackierte Firmen zu?
Darunter fallen etwa Kosten zur Wiederherstellung von Daten bei Datenverlust, Ertragsausfälle durch Betriebsunterbrechungen, Erpressungszahlungen, aber auch die Haftbarkeit für Drittschäden bei Datenschutzrechtsverletzungen und Haftbarkeit für Schäden, die aus der Beeinträchtigung des berechtigten Zugangs von Kunden zu Daten resultieren.

Auch Mitarbeiter können ein Cyber-Risiko darstellen. Was heisst das für die Versicherung?
Das ist ein entscheidender Punkt. Hier müssen Firmen bei Abschluss einer Police alle Varianten versichern lassen. Problematisch wird es, wenn eine Versicherung nur Schäden aus strafbaren Handlungen von Mitarbeitern versichert. Das schliesst unlauteren Wettbewerb oder die Verletzung von Markenrechten durch Mitarbeiter im Digitalen aus. Ähnliche Einschränkungen ergeben sich, wenn nur vorsätzliche Handlungen von Mitarbeitenden gedeckt sind, nicht aber Schäden aus blossem Versehen, wenn etwa ein Mitarbeiter Hunderttausende Kundendaten versehentlich löscht oder öffentlich zugänglich macht.

Welche Verhaltenspflichten haben Firmen, die eine Cyber-Risiko-Versicherung abschliessen?
Sehr umfangreiche. Wichtige Pflichten bei der Versicherung von Cyber-Risiken sind etwa Sicherungspflichten wie das regelmässige Erstellen von Backups. "Die Rechtsfolgen einer Verletzung solcher Obliegenheiten variieren je nach Produkt und reichen von Leistungskürzungen bis zum gänzlichen Verlust des Anspruchs auf Versicherungsleistungen", so Anwalt Nicolas Bracher. Firmen müssen zudem regelmässig Sicherheitsmassnahmen wie Firewalls, Antivirensoftware aktuell halten.

Kann meine Cyber-Versicherung nur auf die Schweiz beschränkt werden?
Ja. Mit schwerwiegenden Folgen. Der örtliche Geltungsbereich einer Cyber-Versicherung sollte immer ausgeweitet werden, ansonsten müssen die Versicherten damit rechnen, dass ein Schaden, beispielsweise an Daten, die in einer Cloud gespeichert sind, davon überhaupt nicht gedeckt wird. Der örtliche Geltungsbereich Schweiz und Liechtenstein reicht bei Cyber-Versicherungen in keinem Fall!

Wie kann sich der Betrag, den ich von der Versicherung bekomme, verringern?
Beispielsweise durch Serienschadensklauseln. Solche Klauseln fassen mehrere Versicherungsfälle zu einem Versicherungsfall oder mehrere Schäden zu einem Schaden zusammen. Werden beispielsweise bei einem Hackerangriff die Kreditkartendaten von 1000 Kunden gestohlen, können die daraus resultierenden Drittschäden nur als ein Schaden und nicht als 1000 Schäden gelten, mit der Folge, dass die Deckungslimite nur einmal für alle Haftungsansprüche und nicht für jeden einzelnen Haftungsanspruch separat zur Anwendung kommt.

Was ist "Cyber Extortion"?
Darunter versteht man die Erpressung von Firmen durch eine Cyber-Attacke. Betroffene Firmen müssen einen Betrag bezahlen, damit die Attacken gegen die Firma aufhören oder sensible Daten wieder zugänglich gemacht werden.

Dürfen Lösegeldzahlungen bei Cyber-Erpressung überhaupt versichert werden?
Das ist noch nicht geklärt. Die Versicherung dieses Risikos könnte nämlich als sittenwidrig angesehen werden. Es besteht das Risiko, dass solche Policen zivilrechtlich nichtig sind. Im angelsächsischen Raum könnten solche Zahlungen zudem gegen Bestimmungen zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung verstossen.

Unsere Firma hat viele Dienste outgesourct. Was heisst das für die Cyber-Versicherung?
Es ist wichtig, dass geklärt wird, welche Mitarbeiter von Partnern Zugang zu den Systemen des Versicherten haben und welche sensiblen Daten bei Outsourcingfirmen gelagert werden. Ist das der Fall, besteht eine zusätzliche Risikoexposition, die von einer spezifischen Police abgedeckt werden muss. Vor allem bei Firmen, die mit vielen Partnern zusammenarbeiten und Daten outgesourct haben, kann es dazu kommen, dass Schäden nicht erstattet werden.

Gibt es einen Branchenstandard hinsichtlich der Versicherungsbedingungen bei Cyber-Risiken?
Nein, diese Versicherungen existieren erst seit so kurzer Zeit, dass sich noch keine verbindlichen Standards entwickelt haben, was für Kunden solcher Versicherungen mit einem gewissen Risiko verbunden ist.

Meine Versicherung schützt mich nur gegen "zielgerichtete Angriffe". Was heisst das?
Wenn eine Malware eine unbestimmte Zahl von Usern trifft und nicht nur gegen das Unternehmen gerichtet war, dort aber Schäden angerichtet hat, kann der Versicherungsschutz entfallen, da die Cyber-Attacke nicht zielgerichtet war. Auf solche Formulierungen ist bei Abschluss der Police genau achtzugeben.

Auf welche politischen Änderungen muss ich mich bezüglich dieser Versicherung vorbereiten?
Im Jahr 2018 kommt es zu einer Verschärfung des Datenschutzrechts in der Europäischen Union. In deren Rahmen werden umfangreiche Meldepflichten und einschneidende Sanktionen bei Datenschutzverletzungen durch Unternehmen eingeführt. Von dieser Entwicklung könnten auch viele Schweizer Firmen betroffen sein, so das "Schulthess Manager Handbuch 2017": "Im Rahmen einer geplanten Revision des schweizerischen Datenschutzgesetzes werden ähnliche Regeln in den kommenden Jahren mit grösster Wahrscheinlichkeit auch in der Schweiz eingeführt." Strengere Regularien könnten das Bedürfnis nach den Policen weiter steigen lassen.

Quelle: Schweizerische Handelszeitung