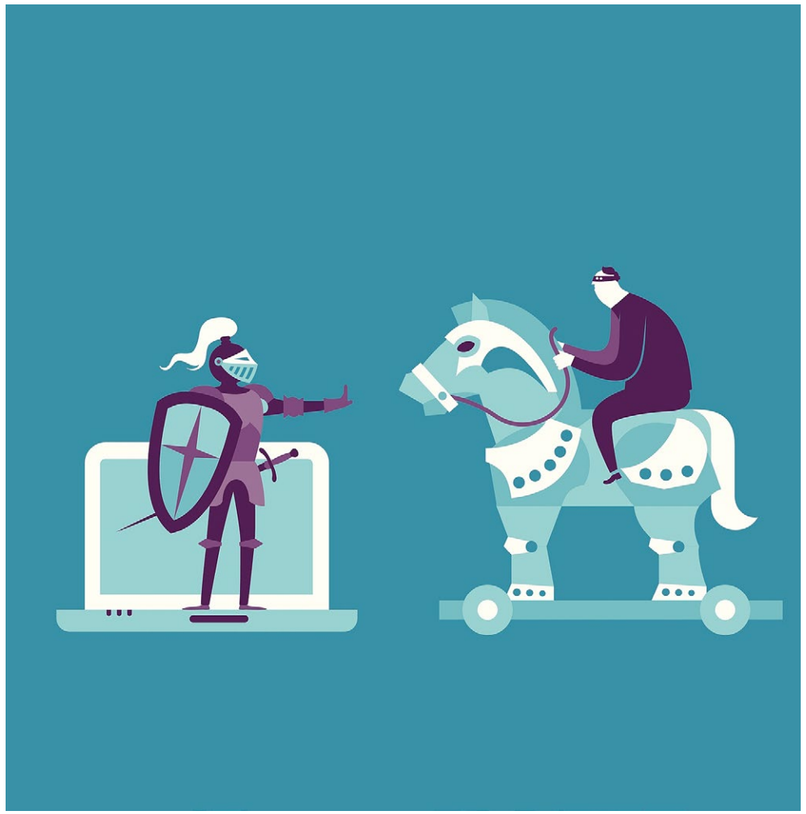
Policen fürs Netz

Die Versicherung von Cyber-Risiken ist für Unternehmen nötiger denn je. Die Assekuranz ist gefordert, langfristig ausgerichtete Lösungen für aktuelle und künftige Risiken zu bieten.

VON NADINE JANSER



Versicherungsschutz für Cyber-Crime ist gefragt. Gezeichnet werden solche Risiken indes nur zurückhaltend.

Bild: iStock

Die Digitalisierung mit der zunehmenden Vernetzung und den Möglichkeiten, riesige Datenmengen zu verarbeiten, bietet ungeahnte Chancen. Doch auch die Risiken sind gross: Störungen bzw. Sabotage an IT-Systemen, Datenverlust durch kriminelle Handlungen wie Hacker-Angriffe oder auch einfach durch menschliches bzw. technisches Versagen zählen heute zu den grössten Risiken von Unternehmen. So überrascht es nicht, dass die OECD in «The cyber insurance market: Responding to a risk with few boundaries» die Investition von Unternehmen für 2018 in entsprechende Sicherheitsmassnahmen auf rund 93 Milliarden US-Dollar schätzt. Und dies zu Recht, denn in den kommenden fünf Jahren werden gemäss dem aktuellsten «WEF-Report» die Kosten für Schäden aus Cyber-Angriffen auf rund acht Billionen US-Dollar ansteigen.

Vor diesem Hintergrund beschränken sich die Unternehmen nicht mehr nur auf präventive Massnahmen, sondern gehen vermehrt zu einem Risikotransfer über. Schätzungsweise platziert schon heute weltweit jedes dritte Grossunternehmen eine Cyber-Versicherung (OECD); angetrieben von eigenen Schadenerfahrungen, Medienberichten über Vorfälle sowie von rechtlichen und technologischen Entwicklungen. Dies führt in der Versicherungsindustrie zu einem grossen globalen Wachstum im Bereich Cyber-Versicherungen. Haben Unternehmen in Europa 2016 rund 300 Millionen US-Dollar investiert, dürften es bis Ende 2018 gemäss Munich Re schon gegen 900 Millionen US-Dollar sein. Dabei positioniert sich der Schweizer Markt neben Frankreich, Deutschland und Italien als Vorreiter innerhalb von Kontinentaleuropa.

Voraussetzungen des Risikotransfers

Angesichts der zunehmenden Automatisierung, Vernetzung und Abhängigkeit von IT-Systemen bei gleichzeitiger Zunahme der Datenmengen gibt es heutzutage keine besonders gefährdeten Unternehmen mehr, welche ihre Cyber-Risiken versichern sollten. Vielmehr stellt sich die Frage, wie sie den Risikotransfer individuell erfolgreich gestalten können. Dazu sind zwei Voraussetzungen fundamental: Einerseits müssen die Unternehmen das Gefahrenpotenzial ihrer firmenspezifischen Cyber-Risiken kennen und mithilfe des Risk-Management-Prozesses (Identifikation, Analyse, Bewertung, Bewältigung) ihren Bedarf an Versicherung besser einschätzen. Andererseits ist der Versicherungsmarkt gefordert, langfristig ausgerichtete Lösungen für aktuelle und künftige Risiken zu bieten. Dazu gehört die transparente Darstellung des Deckungsumfangs (sogenannte stillschweigende Deckung bzw. silent cover) respektive der Deckungseinschränkungen in den bereits bestehenden Versicherungen. Spezifische Cyber-Versicherungen wiederum sollen insbesondere Risiken decken, die sich in die bestehenden Versicherungsportfolios nur schwer integrieren lassen. Zugleich sind sie zu vereinfachen.

Gerade bei Cyber-Versicherungen ist der Deckungsumfang nicht statisch, sondern in permanenter Entwicklung und Veränderung. Es ist daher durchaus möglich, dass die aktuell versicherbaren finanziellen Auswirkungen sowie die zur Verfügung gestellten Versicherungssummen aufgrund der Schadenentwicklungen der Versicherer schon in den kommenden Jahren nicht mehr transferierbar oder nur zu weit höheren Prämien verfügbar sind. Dies lässt den Rückschluss zu, dass die Versicherungsindustrie bereits heute Lösungen für Szenarien kreiert hat, bei deren Eintritt Unternehmen signifikante finanzielle Probleme erleiden.

Vier Kernthemen

Wie bei jedem Vertrag lohnt es sich auch hier, das Kleingedruckte genauer zu lesen. Aus über 250 begleiteten Gesprächen zwischen Unternehmen und Versicherern lassen sich folgende Kernthemen ableiten, die besonders beachtet werden sollten:

• Augenmerk auf das Krisenmanagement: Unternehmen sollten ein funktionsfähiges, umfassendes Krisenmanagement betreiben. Denn gemäss zahlreichen Studien verhält sich dessen Qualität umgekehrt proportional zum Gesamtschaden. Wichtig ist auch der Einbezug der Bedingungen der Versicherer hinsichtlich Pflichten im Schadenfall, die durchaus verhandelbar sind. Unter anderem gilt es zu klären, inwiefern ein Versicherer einem von einem Schaden betroffenen Unternehmen Autonomie bei der Schadenabwicklung gewährt. Da Versicherer in den Bereichen IT und Krisenkommunikation sowie in rechtlichen Fragen oft externe Partner zur Verfügung stellen, empfiehlt es sich vorgängig zu klären, welche Verpflichtungen Unternehmen dabei eingehen und wie die Zusammenarbeit im Schadenfall funktioniert.

• Stolpersteine bei der Betriebsunterbruchsdeckung: Cyber-Vorfälle können ein Unternehmen (vorübergehend) zum Stillstand bringen, entsprechend hoch fällt mitunter der finanzielle Schaden aus. Die Ursachen solcher Betriebsunterbrüche können vielfältig sein. Versicherbare bzw. versicherte Ereignisse umfassen Cyber-Angriffe, menschliches Versagen bis hin zu Hard- und Softwarefehlern. Dabei gehören zur IT-Infrastruktur der versicherten Unternehmen auch die ausgelagerten IT-Bereiche (inkl. Cloud-Dienstleistungen). Hingegen lässt sich die Wertschöpfungskette noch nicht vollständig abdecken. Ein Beispiel: Ein Cyber-Vorfall verursacht bei einem Lenkgetriebe-Hersteller einen Produktionsstopp, der bei einem europäischen Automobilzulieferer, der selber gar nicht angegriffen wurde, einen Betriebsunterbruch zur Folge hat. Den erlittenen Schaden könnte der Automobilzulieferer jedoch teilweise über die Mitversicherung von den durch ihn zu zahlenden Konventionalstrafen lösen. Ebenfalls gilt es ein Augenmerk auf die Berechnung möglicher Schäden durch Betriebsunterbruch zu legen. Diese können deutlich variieren, auch was den Bewertungszeitraum betrifft. Man nehme das Beispiel Sika: Das Unternehmen erzielte 2017 eine Umsatzsteigerung von 8,9 Prozent zum Vorjahr. Es wäre verheerend, würden bei einem Schadenfall lediglich die Umsätze von 2013 bis 2016 berücksichtigt. Gleiches gilt für die versicherten Kosten. Trägt der Versicherer beispielsweise lediglich die Kosten der Überstunden oder werden die Lohnkosten vollständig übernommen? In jedem Fall liegt der Schadennachweis beim Unternehmen.

• Versicherungsschutz für Cyber Crime: Zweifellos wäre der Vermögenstransfer aus Phishing-Angriffen sowie aus anderen Angriffsformen als Deckungselement in Cyber-Versicherungen prädestiniert. Der Versicherungsmarkt zeichnet solche Risiken jedoch nur zurückhaltend. In der Konsequenz sind nur Teilaspekte zu tiefen Limiten versichert. Aufgrund der Vielzahl solcher Fälle ist es daher sinnvoll, bei der Evaluation von Cyber-Versicherungen auch sogenannte Vertrauensschadenversicherungen mitzuberücksichtigen, die für solche Szenarien Deckung bieten. Dies kann die Auswahl an Versicherern einschränken.

• Handhabung von Vertragsausschlüssen und vertraglichen Verpflichtungen: Für die Unternehmen ist es zentral, die in den Policen definierten Ausschlüsse und Verpflichtungen kritisch zu hinterfragen. Ein Beispiel ist der sogenannte Vorsatzausschluss, in dem definiert wird, welche Arten vorsätzlichen Handelns durch das versicherte Unternehmen keinen Versicherungsschutz geniessen und inwiefern dem Unternehmen wie auch involvierten natürlichen Personen entsprechendes Verhalten zugerechnet werden kann. Ebenfalls sollten keine unterjährigen Verpflichtungen in Form von technischen Auflagen eingegangen werden. Denn Cyber-Versicherungen sehen meistens einjährige Vertragslaufzeiten vor, weshalb die Versicherer bereits eine kontinuierliche Risikoevaluation vornehmen können.

Aussichten

Die Entwicklung des Marktes im Bereich von Cyber-Versicherungen ist aufgrund des rasanten Fortschritts der Technologien und der damit verbundenen Risiken schwierig zu prognostizieren. Den Versicherern fehlt schlicht die nötige Langzeiterfahrung. Gleiches gilt für die Unternehmen, die mögliche Schadenereignisse nur beschränkt antizipieren können. Hinzu kommen gesetzliche Änderungen wie die Einführung der Europäischen Datenschutzgrundverordnung (EU-DSGVO) sowie die Revision des Schweizerischen Datenschutzgesetzes und deren Konsequenzen. Entsprechend bleibt ein kontinuierlicher Dialog zwischen Versicherern und Unternehmen zur Thematik unverzichtbar. ◆

Nadine Janser *ist Head Cyber Insurance bei der Kessler & Co AG*