Cyberrisiken richtig transferieren

Know-how Eine systematische Einbindung von Cyberrisiken in den Risikomanagement-Prozess ist entscheidend für den Firmenerfolg. Dabei kann die Übertragung von Cyberrisiken auf eine Versicherungsgesellschaft eine wichtige Rolle spielen.

Von Manuel Pachlatko

Cyberrisiken sind heutzutage allgegenwärtig. Gemäss Allianz Risk Barometer 2022 (siehe auch Seite 32ff) stellen sie für Unternehmen sogar das grösste Geschäftsrisiko in diesem Jahr dar, gefolgt vom Risiko einer Betriebsunterbrechung, die wiederum durch einen Cybervorfall ausgelöst werden kann. Es erstaunt daher nicht, dass die Abschätzung und Absicherung von Cyberrisiken – im Fachjargon Informationssicherheitsrisiken genannt – mittlerweile weit oben auf der Prioritätenliste der Geschäftsleitungen stehen.

Cybervorfälle stellen vor allem darum ein grosses Risiko dar, da die Mehrheit der Unternehmen zunehmend von digitalen Abläufen abhängig ist. Als Folge haben Ransomware-Angriffe, die Ausnutzung von Softwareschwachstellen oder Insider-Bedrohungen oft eine verheerende Auswirkung für Firmen. Böswillige Attacken machen gemäss dem weltweit grösten Versicherungsmakler Marsh unterdessen etwa 80 Prozent der Cyber-Vorfälle aus. Gemäss Comparitech haben Schweizer Firmen, die im Jahr 2022 von Cyber-Kriminalität betroffen waren, rund 700 Millionen Schweizer Franken verloren. Es muss ausserdem mit einer hohen Dunkelziffer gerechnet werden. Die weltweiten Schäden beliefen sich im gleichen Jahr auf etwa 300 Milliarden Schweizer Franken.

Die Verwundbarkeit von Firmen ist branchenunabhängig und hängt nicht von der Unternehmensgrösse ab. Gemäss einer Studie des Forschungsinstituts GFS-Zürich war bereits jedes dritte Schweizer KMU von einer Cyberattacke betroffen (siehe auch Seite 48). Neben der traditionellen IT bleiben auch komplexe Maschinensteuerungssysteme nicht verschont. Ein hundertprozentiger Schutz vor Cybervorfällen ist nicht zu bewerkstelligen. Jedes Unternehmen kann Opfer werden. Die ausschlaggebende Frage lautet also nicht, ob es ein Unternehmen trifft, sondern in welchem Ausmass.

Cyberrisiko-Management

Um die Frage nach einem möglichen Schadensausmass beantworten zu können, ist ein angemessenes und funktionierendes Cyberrisiko-Management zu etablieren. Zu diesem Zweck werden zunächst die relevanten Bedrohungen identifiziert, die durch höhere Gewalt, technisches Versagen, organisatorische Mängel und fahrlässiges oder vorsätzliches Handeln verursacht werden können. Der überwiegende Teil der Vorfälle kann durch Business Resilience bewältigt werden. Hingegen ist es notwendig, die Szenarien herauszuarbeiten, die eine besondere Behandlung erfordern.

Bei den sogenannten Katastrophenereignissen handelt es sich um Vorfälle, die

MINDESTANFORDERUNGEN VON VERSICHERUNGEN AN IHRE KUNDEN

Quelle: in Anlehnung an «Top Cybersecurity Controls» von Marsh, 2022

Die Mindestanforderungen, die von der global agierenden Versicherungswirtschaft gefordert werden, befassen sich mit diesen zwölf Kernthemen.

dem Unternehmen nachhaltigen Schaden zufügen können. Als Kennzahlen hierfür werden die Recovery Time Objective (RTO) und die Recovery Point Objective (RPO) herangezogen. Die RTO ist die maximale Zeitspanne, die für die Wiederherstellung der IT- und Geschäftsaktivitäten nach einem Vorfall festgelegt wird. RPO definiert diesen Wert in Bezug auf die Datenverlusttoleranz. Bei Überschreitung der festgelegten Werte wird typischerweise von einer Katastrophe gesprochen, die eine gesonderte Handhabung erfordert.

Die Feststellung der potenziellen Schadensauswirkungen erfolgt in der Regel unter der Leitung des Chief Information Security Officer (CISO) oder der IT-Abteilung. Das ist insofern sinnvoll, da diese Verantwortlichen beurteilen können, welche Systeme am kritischsten für den Betrieb sind und welche Vorkehrungen gegen potenzielle Störungen getroffen wurden. Gleichwohl ist die fachübergreifende Einbindung der Finanz-, Personal- und Rechtsabteilung in diesem Zusammenhang zu berücksichtigen.

Die Versicherung stellt somit das letzte Glied im Cyberrisiko-Management dar, wenn trotz aller Schutzmassnahmen ein Katastrophenfall eintritt. So lassen sich selbst die ermittelten und bleibenden Restrisiken möglichst beherrschen.

Midestanforderungen einer Cyberversicherung

Mit der Festlegung der Katastrophenszenarien und der damit verbundenen Restrisiken ist eine Grundlage für die Überprüfung der Versicherbarkeit erarbeitet worden. Sind versicherbare Risiken gegeben, gilt es, die strengen Anforderungen der Versicherer zu erfüllen. Die Mindestanforderungen, die von der global agierenden Versicherungswirtschaft gefordert werden, befassen sich mit den zwölf Kernthemen, die in der Grafik auf der gegenüberliegenden Seite aufgeführt sind.

Der Risikoreifegrad wird anhand von Fragebogen oder von einem Risikodialog mit den Versicherern ermittelt. In einem nächsten Schritt soll mit einem Deckungskonzept der bestmögliche Versicherungsschutz konzipiert werden.

Typischerweise wird von den Versicherern folgender Leistungskatalog (nicht abschliessend) angeboten.

- **Eigenschäden:** Ertragsausfälle und Mehrkosten bei einer Betriebsunterbrechung, Kosten zur Wiederherstellung und Ersatzbeschaffung bei Datenverlust, Erpressungszahlungen oder versicherbare Bussen;
- **Haftpflichtschäden:** Deckung für Ansprüche von Dritten (Kunden und Unternehmen) oder Internet-Medienhaftpflicht;
- **Kosten:** Aufbau eines Callcenters, Strafzahlungen gegenüber Dritten oder Hardware Ersatzkosten.

Im Unterschied zu anderen Versicherungsprodukten übernimmt die Cyberversicherung nicht nur die Rolle des Schadenregulierers, sondern bietet auch Unterstützung im Krisenfall über einen fachlichen Triage-Service. Diese Dienstleistungen werden für gewöhnlich in drei Fachbereichen angeboten: technisch und organisatorisch (z. B. Forensik und Wiederherstellung), rechtlich (z. B. Meldepflichten) und im Bereich Kommunikation. Die anfallenden Kosten sind Teil des Versicherungsschutzes. Die Qualität der Dienstleister spielt dabei eine entscheidende Rolle.

Ausschlüsse und Kosten

In Versicherungspolicen finden sich neben den Klauseln zum Versicherungsschutz immer auch Ausschlüsse. Der Versicherer schliesst etwa vorsätzlich begangene Handlungen der geschäftsführenden Personen oder einen Zusammenbruch der kritischen Infrastruktur aus. Bei der Cyberversicherung handelt es sich um eine Vermögensschadenversicherung. Das bedeutet, Personen- und Sachschäden sind durch dieses Versicherungsprodukt nicht abgesichert.

Die Leistung wird durch eine Prämie kompensiert. Diese richtet sich nach dem Risikoprofil in Bezug auf Grösse, Risikoqualität und die vereinbarten Leistungen. Die Bandbreite reicht von einigen tausend Franken für KMU bis zu 15’000 bis 30’000 Franken pro Million Versicherungssumme für Grossunternehmen. Je nach Branche können Versicherer auch die Übernahme einer Police ablehnen, weil das Risiko zu hoch ist. Kritische Infrastrukturen fallen zunehmend in diese Kategorie.

Die zahlreichen Cyberangriffe der jüngsten Zeit haben zu einer starken Nachfrage nach Cyberversicherungen geführt. Das Versicherungsmodell wird allerdings mit jedem grossen (und versicherten) Schadenfall unrentabler. Die Versicherer müssen ihren Leistungskatalog daher laufend überarbeiten, um speziellen Risiken wie Ransomware, systemischen Bedrohungen und technischen Systemausfällen besser begegnen zu können. Die Professionalität der Täter nimmt dabei eine ebenso bedeutende Rolle ein.

Quo vadis Versicherungsmarkt?

Das Thema Cyberrisiken ist für die Assekuranz bei aller Aktualität immer noch relativ neu. Das Defizit der fehlenden historischen Daten muss durch eine rasche und systematische Auswertung der vorhandenen Schadensdaten reduziert werden. Darüber hinaus sind zu erwartende Entwicklungen zu berücksichtigen, um der tiefgreifenden und zugleich rasanten Entwicklung der Digitalisierung zu entsprechen. Erst auf dieser Grundlage lassen sich die Versicherungsparameter – Selbstbehalt, Versicherungssumme, Deckung und Prämie – sachgerecht ableiten.

Der Cyberversicherungsprozess, obgleich komplex und zeitaufwendig, hat oft den Vorteil, dass die Cybersicherheit gestärkt wird. Die Versicherer agieren in dieser Hinsicht als Partner, da sie in der Lage sind, Einsichten aus der Schadensperspektive zu vermitteln. Versicherer können auf diese Weise zu einem wirksameren Risikomanagement beitragen, wodurch solche unberechenbaren Risiken möglicherweise besser beherrschbar werden. ■

DER AUTOR

Bei seiner beruflichen Ausbildung hat **Manuel Pachlatko** den Fokus auf die Betriebswirtschaftslehre gelegt. Er studierte an der HWZ Betriebsökonomie mit der Vertiefung Banking & Finance im Bachelor und im Master mit Strategic Management. Zusätzlich ist er BSI-Sicherheitsbeauftragter und er hat den CAS Cyber Security und Information Risk Management absolviert. Beruflich hat es Manuel Pachlatko von Anfang an in die Versicherungsbranche gezogen. Früher war er bei Swiss Re und dann bei AIG im Underwriting tätig. Heute arbeitet er bei Kessler, einem führenden Schweizer Unternehmen für ganzheitliche Risiko-, Versicherungs- und Vorsorgeberatung, als Teamleiter Financial Lines und seit 2021 als Practice Leader Cyber Risk.