

DIE VERSICHERUNG VON CYBER-RISIKEN

Thomas Böhm, Partner und Experte im Versicherungsrecht bei CMS in Wien, über die Möglichkeiten und Grenzen von Cyber-Risk-Versicherungen. Eines ist jedenfalls klar: Auch die besten Präventivmaßnahmen bieten keinen hundertprozentigen Schutz.

Die Errungenschaften unserer hochtechnisierten Welt zeigen ihre Schattenseiten und rücken das Thema Cyber Risk stärker in den Fokus. Typische Bedrohungen durch Cyber-Kriminalität sind Datendiebstahl und Datenschutzverletzungen, Diebstahl geistigen Eigentums, virtuelle Erpressung oder Denial-of-Service Attacks (DoS).

Wie Studien, bei denen Cyber Security-Experten von österreichischen Unternehmen befragt wurden, belegen, wurden 72 Prozent der österreichischen Unternehmen in den letzten 12 Monaten Opfer von Cyberangriffen, Computersabotage, digitaler Erpressung oder einer anderen Form von Cyberkriminalität. In der Folge litt rund die Hälfte davon auch an einer Unterbrechung der Geschäftsprozesse. Und auch kleine Unternehmen werden als Ziel immer beliebter: 66 Prozent der



Einige Versicherungen übernehmen auch Lösegeldzahlungen bei DoS-Fällen.

österreichischen KMU waren in den vergangenen Jahren betroffen. Tendenz steigend. Österreichische Unternehmen erleiden jedes Jahr Schäden in Millionenhöhe. Das Center for Strategic & International Studies (CSIS) schätzt die Schäden durch Cyber-Kriminalität auf rund 600 Milliarden USD weltweit. Und die Gefahr von Cyber-Angriffen wächst. Versicherungsunternehmen bestätigen, dass Cyber-Risiken zu den Top-Risiken für Unternehmen im Jahr 2018 zählen.

DARAUF KOMMT ES AN

Der Aufbau eines gezielten Cyber-Risikomanagements ist für jedes Unternehmen unverzichtbar. Eine Cyber-Risk-Versicherung kann ein sinnvoller Baustein sein, denn eines ist klar: Auch die besten Präventivmaßnahmen bieten keinen hundertprozentigen Schutz. Restrisiken bleiben immer. Ziel der Cyber-Risk-Versicherung ist die bestmögliche Absicherung des Unternehmens gegen diese Risiken.

Schwierigkeiten bereitet die Erfassung des Risikos durch das Versicherungsunternehmen. Bei KMUs genügt dazu vielleicht ein von der Versicherung ausgearbeiteter Fragebogen. Bei größeren Unternehmen kann es für die Versicherung erforderlich sein, mit (externen) Experten vor Ort die Risiken von allen Seiten zu prüfen. IT-Mindeststandards sind oft Voraussetzung für eine Deckung. Die Risikoprüfung mündet zuweilen im Vorschlag bestimmter technischer Lösungen und Produkte, die umzusetzen sind, um Risiken zu minimieren. Erst nach Ermittlung des Restrisikos kommt es zum Abschluss des Vertrags. Werden die Mindeststandards nicht erfüllt, kann das zu einer erhöhten Prämie, zum Ausschluss bestimmter Risiken von der Deckung oder schlimmstenfalls zur Weigerung der Versicherung führen, den Vertrag abzuschließen.

WAS EINE CYBER-RISK-VERSICHERUNG KANN

Die Versicherungsprodukte umfassen üblicherweise eine Grunddeckung, in der die Versicherung Versicherungsschutz für Eigenschäden des versicherten Unternehmens und Haftpflichtversicherungsschutz für Drittschäden übernimmt. Versichert werden beispielsweise die

Wiederherstellungskosten, die Kosten für forensische Untersuchungen zur Ermittlung der Ursache und Bestätigung des Versicherungsfalls, Benachrichtigungen von Betroffenen und Datenschutzbehörden oder Öffentlichkeitsarbeit im Krisenfall (PR-Beratung). Im Haftpflichtteil umfasst der Versicherungsschutz die Erfüllung begründeter und die Abwehr unbegründeter Haftungsansprüche inklusive der damit verbundenen Kosten. Die Haftpflicht kann beispielsweise durch eine Verletzung der Vertraulichkeit elektronischer Daten Dritter, die sich im Verfügungsbereich der Versicherten befinden, ausgelöst werden. Die Grunddeckung kann nach dem Baukasten-Prinzip um individuelle Deckungsvarianten erweitert werden. Das Angebot ist vielfältig. Die Notwendigkeit solcher Zusatzprodukte hängt stark vom Einzelfall ab. Die meisten Anbieter versichern optional unter anderem

Betriebsunterbrechungsschäden. Es gibt auch Versicherungen, die die Übernahme von Lösegeldzahlungen bei DoS-Fällen zusagen. Die Regelung des Versicherungsfalls ist unterschiedlich. Im Haftpflichtversicherungselement kommt üblicherweise das »Claims-Made-Prinzip« zur Anwendung. Als Versicherungsfall gilt dann die erstmalige schriftliche Erhebung eines Haftpflichtanspruchs gegenüber dem Versicherungsnehmer. In der Eigenschadenversicherung ist mit dem nach den jeweiligen Bedingungen definierten Schaden auch der Versicherungsfall eingetreten. Aufgrund der schwer abschätzbaren Schäden einer Cyber-Attacke sollte die Einschätzung der Deckungssummen großzügig erfolgen. Derzeit sind Deckungssummen bis zu 500 Millionen Euro möglich. Der Trend geht in Richtung noch höherer Deckungssummen.

WAS EINE VERSICHERUNG NICHT KANN

Kein Versicherungsschutz besteht im Cyber-Haftpflichtfall in aller Regel dann, wenn die Ansprüche des Dritten auf vorsätzlicher Schadenverursachung oder wissentlichen Abweichen von Gesetz, Vorschrift oder Anweisungen des Auftraggebers beruhen. In der Eigenschadenversicherung wird die Deckung ebenfalls bei vorsätzlicher Schadensherbeiführung ausgeschlossen. Darüber hinaus kommt es auf die konkreten Versicherungsbedingungen an.

Allerdings ist das Cyber-Risiko sehr dynamisch. Eine Cyber-Versicherung sollte daher regelmäßig überprüft werden und erforderlichenfalls in Zusammenarbeit mit dem Versicherungsunternehmen im Hinblick auf eine geänderte Risikolage angepasst werden, um Deckungslücken zu vermeiden.