

Geschäft mit der Cybergefahr



Fotocredits: Michael Stöckl | FUP Group

Michael Stöckl

Wozu Cybersecurity-Maßnahmen, wenn es ohnehin Versicherungen gibt? Experte Michael Stöckl im Interview.

Michael Stöckl ist Geschäftsführer der FUP Group GmbH und u. a. auf Cybersecurity-Versicherungen spezialisiert.

Ersetzt eine Cybersecurity-Versicherung Cybersecurity-Maßnahmen?

Michael Stöckl: Durch die strengeren Annahmekriterien der Versicherungswirtschaft und die Verknappung der Kapazitäten ist es heute unumgänglich geworden, dass der Versicherungsnehmer vor Installierung einer Cyber-Versicherung intern ein bestmögliches System zur Verhinderung von Cyber-Attacken installiert. Grundsätzlich ist – wie bei jeder anderen Versicherungssparte – eine Schadenszahlung im Versicherungsfall immer nur die zweitbeste Lösung, wenn der Eintritt eines Versicherungsfalles bereits im Vorfeld durch geeignete Maßnahmen vermieden hätte werden können.

Wie einfach ist es, an eine Cybersecurity-Versicherung zu kommen?

Wie bereits angesprochen, haben sich die Annahmekriterien wesentlich verschärft, es ist aber auch anzumerken, dass diese

im Wesentlichen auf hohe Versicherungssummen bzw. schadenskritische Deckungserfordernisse abzielen, d.h. Produkte in der Breite, z. B. für den Privatkundensektor, werden davon eher nicht betroffen sein.

Welche spezifischen Cyber-Risiken und -Szenarien decken Versicherungen ab? Welche wichtigen Ausschlüsse gibt es?

Dazu ist es einmal notwendig, relativ einfach die Funktion und Mechanismen einer Cyber-Versicherung zu erklären. Das Deckungskonzept ist ähnlich einer Sach-, Betriebsunterbrechungs- und Haftpflichtversicherung, kombiniert mit dem Einsatz einer professionellen „Eingreiftruppe“ unmittelbar nach dem Schadenseintritt. Für alle anfallenden Kosten ist eine Versicherungssumme vom Versicherungsnehmer frei wählbar, bis zu welcher dann Kosten übernommen werden. D.h. der Versicherungsnehmer wird auch dabei in die Pflicht genommen; zu geringe Deckungssummen können gravierende Deckungslücken schaffen.



Welche Anforderungen muss ich als Unternehmen erfüllen, um für eine Cybersecurity-Versicherung in Frage zu kommen? Was sind Voraussetzungen?

Ungeachtet der zwischenzeitlich umfangreichen Erfassungsfragebögen ist es meines Erachtens unumgänglich, im Vorfeld einen externen IT-Sicherheitsdienstleister zu beauftragen, das Unternehmen einem Penetrationstest zu unterziehen, um Schwachstellen im System aufzuzeigen.

Wie werden die Versicherungsprämien für Cybersecurity-Polizzen berechnet und welche Faktoren spielen dabei eine Rolle?

Im Vergleich zu bekannten Versicherungslösungen sind die Prämienaufwendungen für Cyber-Versicherungen relativ gering, obwohl das Bedrohungsszenario mittlerweile hinlänglich bekannt ist. Gravierende Faktoren sind jedenfalls die Qualität der bereits vorhandenen bzw. umgesetzten Abwehrmaßnahmen, die Größe und Exponiertheit des Risikos, sowie die notwendige Versicherungssumme.

Was ist im Ernstfall tatsächlich abgesichert?

Die Kosten des Krisenmanagements, der IT-Forensik sowie für die Wiederherstellung der IT, die Kosten von Anwälten und PR-Beratern, der durch den Cyber-Angriff verursachte Deckungsbeitragsverlust (Betriebsunterbrechungsschaden), sowie die Prüfung, Abwehr und Entschädigung im Falle von


Haftpflichtansprüchen Dritter. Zusätzlich können z. B. Erpressungsgelder oder Schäden durch Cyber-Diebstahl versichert werden. Die genaue Ausgestaltung der Versicherungslösung setzt einen umfassenden Risikodialog voraus und bedarf professioneller Beratung.

Welche Art von Unterstützung bieten Versicherungen im Falle eines Cyberangriffs? Wie schnell kann ich mit einer Reaktion rechnen?

Die bereits genannte Eingreiftruppe reagiert im Bedarfsfall äußerst schnell und ist nach Anforderung innerhalb von wenigen Stunden aktiv. Keinesfalls sollte im Angriffsfall durch unkoordiniertes Vorgehen der Schaden vergrößert werden. Diese Dienstleister sind Vollprofis und in der Lage, durch Verhandlung mit den Angreifern die Schadensaustragung zu koordinieren.

Welche Art von Unternehmen greift primär auf solche Versicherungen zu? Wie weit verbreitet sind Cybersecurity-Versicherungen in der Industrie?

Grundsätzlich ergibt sich der Bedarf einer Cyber-Versicherung für jeden PC, auf welchem Betriebsprogramme laufen und Daten abgespeichert werden. Oftmals richten Cyber-Attacken den meisten Schaden in Betrieben an, in denen man am wenigsten mit den Auswirkungen rechnet. Die Durchdringung des Marktes nimmt zwar aufgrund der Sensibilisierung laufend zu, dennoch hinken wir den internationalen Standards weit hinterher.



**“Oftmals richten
Cyber-Attacken dort
den meisten Schaden
an, wo am wenigsten
damit gerechnet wird.”**

Michael Stöckl
CEO, FUP Group GmbH