Versicherungen schützen vor Folgen von Hacker-Attacken

Cyber-Versicherungen. Hacker-Attacken können für Unternehmen schwere Folgen haben. Versicherungen schützen. Doch was muss ein derartiger Vertrag leisten? Ein Leitfaden.

Sicherheit der IT-Systeme hat für Unternehmen große Bedeutung. [AFP]

Die im Mai in Kraft tretende Datenschutzgrundverordnung macht die Situation für Unternehmen nicht gerade einfach: Unternehmen treffen eine Reihe an Datenschutz-Verpflichtungen – sollte es trotzdem zu einer Hacker-Attacke kommen, sind die Folgen oft desaströs: Betroffene Dateninhaber sind zu verständigen, sie haben weiters einen Anspruch auf materiellen sowie immateriellen Schadenersatz, wenn ihre Daten durch ein intern oder extern verursachtes Leck publik werden und direkt in Geld messbare Schäden eingetreten sind oder die Daten-Inhaber durch das Bekanntwerden bloßgestellt wurden.

Baukasten-System

Die Versicherungswirtschaft hat dieses Problem erkannt und bietet daher spezielle Cyber-Versicherungen an – nicht zuletzt stufen laut einer Allianz-Umfrage Unternehmen in Europa Cyber-Risiken als die zweitgrößte Bedrohung für Unternehmen ein, noch vor politischen Einflüssen oder Verwerfungen auf den Märkten.

Doch welche Versicherung passt zu welchem Unternehmen? Antworten auf diese Frage hat Rechtsanwalt Thomas Böhm, Partner bei der Kanzlei CMS Reich-Rohrwig Hainz in Wien. „Grundsätzlich werden derartige Versicherungen als Bündelversicherungen angeboten. Das bedeutet, dass sie aus einer Grunddeckung und Zusatz-Paketen bestehen, es handelt sich also um eine Art Baukasten-System“, erklärt der Jurist.

„Ich würde jedem Unternehmen raten, zunächst eine genaue Risikoanalyse durchzuführen.“

Thomas Böhm
Rechtsanwalt

In der Grunddeckung leisten Cyber-Versicherungen die Deckung des Schadens des Unternehmens an sich – „häufig wird dies mit einer Haftpflicht kombiniert, falls das betroffene Unternehmen Schadenersatzansprüchen von Außenstehenden ausgesetzt ist“, erklärt Böhm: „Ein Beispiel: Ein E-Mail mit einer Schadsoftware verlässt ein Unternehmen und es kommt in einem anderen Unternehmen dadurch zu einem Schaden. Die Versicherung deckt daher nicht nur den Schaden im eigenen Unternehmen, sondern auch berechtigte Schadenersatzforderungen des anderen Unternehmens bzw. die Kosten, diese Ansprüche abzuwehren (Anwaltskosten, Prozesskosten etc., Anm).“

Neben der Grunddeckung decken diese Versicherungsverträge aber auch noch zusätzliche Risiken ab. Diese müssen Unternehmen einzeln wählen. „Darunter fallen beispielsweise die Versicherung gegen Betriebsunterbrechungen“, erklärt der Rechtsanwalt: Hacker oder andere Cyber-Kriminelle können alle Server im Unternehmen zum Stillstand bringen, das bedeutet, dass das Unternehmen bis zur Behebung des Schadens handlungsunfähig ist – jede Stunde Betriebsunterbrechung führt zu hohen Verlusten. Ein weiteres Modul im Cyber-Versicherungs-Baukasten können etwa die Kosten für Krisen-PR sein – nicht zuletzt werden Cyber-Attacken oft von Medien mit besonderem Interesse verfolgt – es schadet daher mitunter nicht, dass für solche Krisen per Versicherung ein Etat zur Verfügung steht, um eine ausgewogene Berichterstattung über den Fall zu erreichen. „Krisen-Management und anwaltliche Kosten sind hier ebenfalls Kostenpositionen, die nach einer Hacker-Attacke anfallen können und die beim Abschluss der Versicherung mitbedacht werden können“, sagt Böhm. Viele Versicherungen haben mittlerweile eigene Krisen-Hotlines eingerichtet, die betroffenen Unternehmen Hilfe durch Experten anbieten.

Ein Problem, das Unternehmen bei Cyber-Attacken haben, ist, dass die Täter im Vergleich zu anderen Angriffen auf das Unternehmen meist sehr schwer auszuforschen sind oder es auch sein kann, dass die heimische Justiz bzw. Kriminalpolizei für die Ausforschung der international agierenden Täter gar nicht zuständig sein muss. Das bedeutet, dass eine Schadloshaltung am wahren Täter meist ausscheidet und eine Cyber-Versicherung die einzige Möglichkeit ist, einen Ersatz für die anfallenden Schäden zu erlangen.

Regress-Zahlungen drohen

In vielen Fällen sind die Täter aber keine verborgen agierenden Computer-Genies, die irgendwo auf der Welt in einem dunklen Kämmerchen sitzen und wahllos Unternehmen attackieren. Häufig gehen die Attacken etwa von Mitarbeitern oder Konkurrenten aus. Sollte die Versicherung die Schäden gedeckt haben, müssen die Täter damit rechnen, dass sich die Versicherung an ihnen schadlos halten und geleisteten Schadenersatz einfordern wird.

Der passende Vertrag

Doch wie sollen Unternehmen die Verträge hinsichtlich der Deckungssummen und zu versichernden Risiken dimensionieren? Böhm: „Ich würde jedem Unternehmen raten, zunächst einmal eine Risiko-Analyse durchzuführen. Auf dieser Basis sollte man dann mit Versicherern in Kontakt treten. Bei den Deckungssummen würde ich dazu raten, diese im Zweifel eher höher als niedriger zu wählen. Am Markt werden heute Versicherungen mit einer Deckungssumme von bis zu 500 Millionen Euro angeboten.“

Die Auswahl, welche einzelnen Zusatz-Module bei einer Cyber-Versicherung gewählt werden, hängt laut Böhm sehr von den Risiken ab, mit denen das Unternehmen zu tun hat. Ein einfaches Produktionsunternehmen hat eine komplett andere Risiko-Struktur als etwa ein Gesundheits-Institut, in dem sensible Patientendaten verarbeitet werden. Und: „Man muss regelmäßig überprüfen, ob sich Risiken geändert haben und die Deckung entsprechend anpassen“, so Böhm. [Michael Sazel]

AUF EINEN BLICK

Versicherungsschutz. Die Schäden nach Angriffen auf die unternehmenseigene IT oder Schäden bei anderen Unternehmen oder Privaten, die durch Datenlecks entstehen, können rasch große Ausmaße annehmen und für Unternehmen existenzbedrohend sein. Sei es, weil der Betrieb nach einem Angriff stillsteht oder weil sich Privatpersonen, deren Daten in die Öffentlichkeit gelangt sind, zusammenschließen und Sammelklagen durchführen. Cyber-Versicherungen decken diese Schäden ab. Der Versicherungsschutz besteht aus einem Basispaket und Zusatz-Modulen.