



Cyber-Schutz für KMU

Kam der Einbrecher früher persönlich ins Unternehmen, heißen die kriminellen Bedrohungen heute immer öfter Ransomware, Phishing oder Data Breach. Versicherungen schützen kleine wie große Unternehmen davor.

VON CARINA JAHN
UND SUSANNE KOWATSCH

► **Cyber Crime boomt.** Hackerangriffe haben zu jeder Tages- und Nachtzeit Saison. Dafür braucht es keine eingeschlagenen Fenster, keine aufgebrochenen Türen. Hacker sitzen in der Regel zum Tatzeitpunkt zu Hause vor ihrem Laptop. Mit Computertechnologie, die immer größere Bereiche erfasst, dem Wachstum des elektronischen Handels sowie dem Einsatz von Clouds, der die Verwundbarkeit von Systemen erhöht, steigen auch die Gefahren von Cyber-Attacken. Angriffe

auf Großunternehmen wie Sony, Yahoo oder FACC wurden medial verfolgt und gerieten so ins Visier der Öffentlichkeit. Von Hacking-Fällen gegenüber kleinen und mittleren Unternehmen hört man dagegen kaum.

Doch der Anschein, Cyber-Kriminalität betrifft nur die Großen, trügt. „Je kleiner das Unternehmen, desto geringer die Sicherheitsstandards und desto anfälliger ist man in der Folge“, weiß Norbert Jagerhofer, Versicherungsmakler und Berater in Versicherungsangelegenheiten. Die Dunkelziffer ist dementsprechend hoch. Bislang werden nur die wenigsten Fälle zur Anzeige gebracht. „Oft ist es falsche

Scham“, so Jagerhofer, „obwohl man eigentlich mit internationalen Konzernen in guter Gesellschaft ist. Manche Geschäftsführer denken auch deshalb nicht daran, weil sie im Vordergrund die Krisenbewältigung sehen. Und viele haben Angst, damit in die Medien zu geraten.“

Lösegeldforderungen und Betriebsunterbrechung

Die Angriffe sind äußerst vielfältig und können in den unterschiedlichsten Szenarien auftreten. Stark verbreitet ist die gezielte Erpressung durch Ransomware. „Bei einer derartigen Attacke werden die elektronischen Daten des Unter-

Foto: alphasprint - Thinkstock.com

„Je kleiner das Unternehmen, desto geringer die Sicherheitsstandards und umso anfälliger sind sie“, weiß Versicherungsmakler Norbert Jägerhofer



nehmens mittels einer Schadsoftware verschlüsselt und nur gegen Bezahlung einer Lösegeldforderung, meist in der Internet-Währung Bitcoin, wieder freigegeben“, weiß Cyber-Versicherungsexpertin Kerstin Keltner von Koban Südvers. Folglich kann es zu einer Betriebsunterbrechung und hohen Kosten kommen. Auch Phishing-Attacken, bei denen Passwörter oder Zugangsdaten abgefischt werden, Umleitungen von Zahlungsströmen oder Datendiebstahl (Data Breach) zählen zu den typischen Risikoszenarien. Laut KPMG-Studie gaben 72 Prozent der 236 befragten österreichischen Unternehmen an, in den letzten zwölf Monaten Opfer von Cyber-Angriffen geworden zu sein, mehr als die Hälfte von ihnen litten in Folge unter einer Unterbrechung der Geschäftsprozesse.

„Wir wurden von der Digitalisierung sozusagen überrannt, viele Dienste haben wir bereits genutzt, bevor wir uns Gedanken darüber gemacht haben, welche Folgen die Nutzung hat“, bekommt Keltner öfters zu hören, sie ergänzt: „Dies müssen Unternehmer nun nachholen. Am besten kombiniert man die Thematik Cyber Crime mit dem Datenschutz und schult die Mitarbeiter eingehend über den professionellen Umgang mit den neuen Medien und über die Herausgabe von Informationen unter Nutzung dieser Medien.“

Was die Versicherung verlangt

Hundertprozentige Sicherheit bei Technik und dem Faktor Mensch lässt sich jedoch nie erreichen. Deshalb lautet das Gebot der Stunde, das Restrisiko zu versichern. Immer mehr Versicherungsunternehmen haben dieses wachsende Segment entdeckt und Produkte

entwickelt. „Es ist eine boomende Versicherungssparte, für die Versicherer ein Hoffungsmarkt. Allerdings gibt es teils auch Probleme für die Versicherer beim Underwriting, weil man derzeit noch kaum Erfahrungswerte hat“, so Rechtsanwalt Thomas Böhm, Partner bei CMS, der sich auf Versicherungsrecht spezialisiert hat und Unternehmen zu Cyber-Risiken berät.

Kann sich jedes Unternehmen versichern lassen? „Die Versicherer verlangen konkrete Mindeststandards“, so Böhm, „sowohl technische als auch Compliance und Handhabung betreffend, sie sind von der Versicherung genau definiert.“ Seine IT veraltet und damit unsicher zu belassen, die Mitarbeiter nicht zu schulen und ausschließlich Geld in eine Versicherungspolize zu investieren funktioniert also nicht. Erfüllt das Unternehmen die Mindestanforderungen in einem Punkt nicht, kann die Versicherung entweder eine höhere Prämie verlangen oder das betreffende Risiko vom Versicherungsschutz ausschließen oder gar die Deckung verweigern.

Je nach Zielgruppe, insbesondere Unternehmensgröße, fordern die Versicherer Unterschiedliches als Voraussetzung. So verlangen etwa Wiener Städtische sowie Donau Versicherung als Grundvoraussetzungen für eine Annahme eine Firewall, Antivirenprogramm sowie Back-ups mindestens wöchentlich. Das sollte hoffentlich auch ein Kleinunternehmen schaffen. Der Forderungskatalog des Spezialversicherers Hiscox ist deutlich detaillierter, und fordert beispielsweise zusätzlich ein abgestuftes Rechtekonzept mit administrativen Kennungen ausschließlich für IT-Verantwortliche. Die HDI wiederum nennt auch eine gewisse Umsatzgröße als Voraussetzung.

„Die Mindeststandards stets auf dem neuesten Stand zu halten ist eine verbreitete vertragliche Obliegenheit“, ergänzt Böhm. Tut man dies nicht und ein Schaden tritt ein, kann die Versicherung ihre Leistung kürzen oder eventuell ganz verweigern. Es sei denn, es liegt kein Verschulden beim versicherten Unternehmen vor.



„Die Cyber-Versicherung kombiniert Haftpflichtversicherung und Eigenschadenversicherung“, schildert Cyber-Versicherungsexpertin Kerstin Keltner von Koban Südvers

Wie aufwendig der Abschluss einer Cyber-Versicherung ist, hängt maßgeblich von der Unternehmensgröße sowie dem technischen Standard ab. Bei der Risikoerfassung kleiner und mittlerer Unternehmen genügt oft die positive Bewertung eines ausgearbeiteten Fragebogens. Bei größeren Unternehmen arbeiten Versicherer häufig mit externen Dienstleistern zusammen, die vor Ort das Risiko überprüfen.

Übrigens: Zum Einstieg lässt sich der eigene IT-Sicherheitsstatus auch über einen Selbsttest im Internet unter www.vds-quick-check.de überprüfen.

Bausteinprinzip

„Die Cyber-Versicherung kombiniert zwei Versicherungstypen: die Haftpflichtversicherung und die Eigenschadenversicherung. Sie ist nach dem sogenannten Bausteinprinzip aufgebaut, so dass der Versicherungsnehmer die Zusammensetzung der einzelnen Deckungsmodule frei und auf seine individuelle Risikolage zugeschnitten auswählen kann“, erklärt Keltner von Koban Südvers.

1. Die eigenen Schäden betreffen Krisenmanagement, Lösegelder, Betriebsunterbrechung und vieles mehr.
2. Die Haftpflicht bietet Schutz vor Drittschäden in Folge von Cyber-Attacken aufgrund von Verletzungen betreffend Datenschutz, Vertraulichkeitsverpflichtung oder Netzwerksicherheit.
3. Eine optimale Ergänzung zur Cyber-Deckung ist die Vertrauensschadenversicherung, die Schutz bei Cyber-Betrugsfällen wie etwa Phishing bietet.

Dazu wird so gut wie immer auf Assistance im Schadenfall gesetzt. Die Generali etwa betont bei ihrem Produkt, das sich in erster Linie an Kleinunter-

Cyber-Versicherungen für Unternehmen: Aktuelle Produkte im Überblick

Versicherung	Produktname	Voraussetzungen für Annahme durch Versicherer	Wichtigste Deckungselemente	Prämienhöhe
Allianz	Allianz Business & Allianz Cyber Schutz	Voraussetzungen laut auszufüllendem Fragebogen	Computerschaden-Versicherung, Notfall-IT-Assistance, Schutz bei Datenschutz-, Vertraulichkeitsverletzungen, Cyber-Attacken. Haftpflichtansprüchen, Betriebsunterbrechung; für forensische Dienstleistungen und Krisenkommunikation; Vertrauensschaden etc.	abhängig von Versicherungssumme
Donau Versicherung (VIG)	Cyberschutz	Firewall, Antivirenprogramm, Back-ups mindestens wöchentlich	Datenschutzverletzungen, -verlust, -beschädigung und -diebstahl, Betriebsunterbrechung, Verletzung der Geheimhaltungspflicht, Medienhaftpflicht, Gefährdung der Netzwerksicherheit, Cyber-Erpressung, Krisen- und PR-Management	abhängig von Branche, Versicherungssumme, Selbstbehalt, Umfang
Generali	Elektronik Pauschalversicherung inkl. Cyber-Deckung	Fragebogen und Erst-Check durch das automatisierte Tool. Bei etwaigen Schwachstellen hilft das Generali-IT-Assistance-Team; positive Beurteilung	1. monatliche Schwachstellenanalyse durch ein automatisiertes Tool. 2. 24/7-Hilfestellung durch Generali-IT-Assistance. 3. Versicherungsschutz: Elektronik Pauschal- plus Mitversicherung von Datenverlust und -wiederherstellung, Betriebsunterbrechung	umfassendste Deckung inklusive Zusatzmodule ab ca. 1.000 Euro Jahresprämie ²
HDI	Cyber+	gewisse Umsatzgröße sowie Erfüllung aktueller IT-Sicherheitsstandards	Haftpflicht, Eigenschäden, 24-Stunden-Hotline, Forensik, Datenschutzverfahren, Überwachungsdienstleistungen, Wiederherstellung, Vertrauensschäden, Betriebsunterbrechung, Cloud-Dienstleistungen, Datenschutz-Verfahrens-Rechtsschutz etc.	einzelfallabhängig
Hiscox	Hiscox CyberClear	umfassende IT-Schutzmaßnahmen ³	Deckung von Schäden durch Netzwerksicherheits-Datenrechtsverletzung, Bedienfehler, Cyber-Erpressung. Eigenschädenschutz, Betriebsunterbrechung, Haftpflichtversicherung, div. Serviceleistungen etc.	von 825 € bei Jahresumsatz von 2,5 Mio. € (Vers.summe 250.000 €), bis zu Prämie von 3.125 € für 10 Mio. € Jahresumsatz (Vers.summe 2 Mio.)
Markel Deutschland ¹	Markel Pro Cyber	Antiviren-Scanner, Firewall und Back-ups	Mitversicherung von Bedienfehlern, Sicherheitsanalyse und -verbesserungen nach Schadenfall, Betriebsunterbrechung, Vertragsstrafen bis 250.000 Euro, Abwehrkosten in Bezug auf behördliche Verfahren etc.	Einstiegsprämie: nur Cyber-Eigenschadendeckung 199,50 € netto, alle Bausteine ab 380,00 € netto
Uniqa	Cyberversicherung	Risikofragebogen ausgefüllt und positiv bewertet sowie ²	Wiederherstellung der gespeicherten Daten nach missbräuchlichem Zugriff von außen, Betriebsunterbrechung. Befriedigung/Abwehr von Schadenersatzforderungen, Vorbeugekosten Imageverlust nach Datendiebstahl etc.	max. € 435,70 brutto/Jahr (nicht umsatzabhängig), abhängig vom versicherten Vertragszustand ⁴
Wiener Städtische	Cyber Protect	Firewall, Antivirenprogramm, Back-ups mindestens wöchentlich	Datenschutzverletzungen, -verlust, -beschädigung, -diebstahl, Betriebsunterbrechung, Verletzung der Geheimhaltungs-, Medienhaftpflicht, Gefährdung der Netzwerksicherheit, Cyber-Erpressung, Krisen- und PR-Management etc.	Prämie abhängig von Branche, Versicherungssumme, Selbstbehalt sowie Versicherungsumfang
XL Catlin	XL Catlin Cyber – Cyberschaden-Versicherung	positive Prüfung eines unterschriebenen Cyber-Fragebogens	Ansprüche Dritter bei Verstößen gegen Datenschutzgesetze, wegen unberechtigter Datenverbreitung, Schäden aufgrund von Netzwerkangriffen oder Datenmissbrauch durch Dritte	erst für mittelständische und große Unternehmen ab einem Umsatz von ca. 25 Mio. Euro

1) Modulares Cyber-Produkt mit sechs Bausteinen zu Cyber-Eigenschadendeckung, Cyber-Betriebsunterbrechung, Cyber-Erpressung, Cyber-Zahlungsmittel (ins. Kreditkarten), Cyber-Vertrauensschaden und Cyber-Haftpflicht; 2) Haupt-Zielgruppe sind KMUs bis zu 10 Mitarbeiter; versicherbar sind KMUs bis zu 50 PCs. 3) Durchgängiger Virenschutz, Firewall-Strukturen an allen Netzübergängen, abgestuftes Rechtekonzept mit administrativen Kennungen nur für IT-Verantwortliche, mind. tägliche Datensicherung auf separierten Systemen oder Datenträgern; 4) Voraussetzung sind eine Technikversicherung, Betriebsunterbrechungs- und Betriebshaftpflichtversicherung bei Uniqa

nehmen bis zehn Mitarbeitern richtet, ihren Fokus auf Prävention und aktive Unterstützung. Eine monatliche Schwachstellenanalyse ist ebenso drin wie eine 24-Stunden-Assistance durch IT-Experten. Letzteres bieten faktisch alle Versicherer, schließlich kann ein fachmännischer Umgang mit dem Schaden auch die Folgekosten senken.

Kosten für forensische Dienstleistungen – um das Verbrechen aufzuklären – sind ebenfalls häufig dabei. So ist es im Fall eines Angriffs von enormer Bedeutung, nicht irrtümlich die Spuren der Täter zu beseitigen. Einfach den Stecker zu ziehen sei keine adäquate Abwehrmaßnahme, so Keltner von Koban Südvers und präzisiert: „Grundsätzlich lautet die Regel: Nicht online-

basierte Systeme heruntergefahren werden, um eine Ausweitung der Attacke auf Back-up-Systeme zu verhindern. Online-basierte Systeme dürfen dagegen nicht heruntergefahren werden.“

Und selbst die Kosten für fachmännische Krisen-PR werden häufig bis zu einer gewissen Höhe gedeckt.

Was kostet's?

Die Prämien für Cyber-Versicherungen variieren je nach Umsatz, Versicherungssumme und Deckungsbausteinen. Welche Bausteine Sinn machen, hängt stark vom konkreten Unternehmen ab. Die Einstiegsprämie reicht in etwa von 199,50 Euro alleine für die Cyber-Eigenschadendeckung bei Markel

Deutschland. Die Uniqa bepreist ihre Cyberversicherung mit maximal 435,70 Euro brutto pro Jahr, allerdings muss man dafür zusätzlich auch eine Technik-, Betriebsunterbrechungs- und Betriebshaftpflichtversicherung in ihrem Haus abschließen. Das Produkt der Generali, das alleine abgeschlossen werden kann, kostet in seiner umfassendsten Deckung inklusive aller Zusatzmodule ab etwa 1.000 Euro jährlich.

Und noch ein Preisbeispiel für größere Unternehmen: Bei einem Jahresumsatz von 2,5 Millionen Euro (Versicherungssumme 250.000 Euro) nennt Hiscox eine Prämie von 825 Euro, bei zehn Millionen Jahresumsatz (Versicherungssumme zwei Millionen) sind es 3.125 Euro an Jahresprämie.