IT-Security

Für den Ernstfall eine Cyberversicherung

Angriffe auf IT-Systeme gehören inzwischen zu den grossen Risiken, gerade auch für kleinere und mittlere Unternehmen. Laut Umfrage des Markt- und Sozialforschungsinstituts gfs-zürich wurde bereits jedes vierte KMU in der Schweiz Opfer einer Cyberattacke. Ein Fall für die Versicherungswirtschaft? Auch der Schweizerische Kaderverband (SKV) mischt neu in diesem Geschäft mit. SKV-Geschäftsführer Marc Gerosa sagt, was Sache ist.

Interview: Roger Strässle

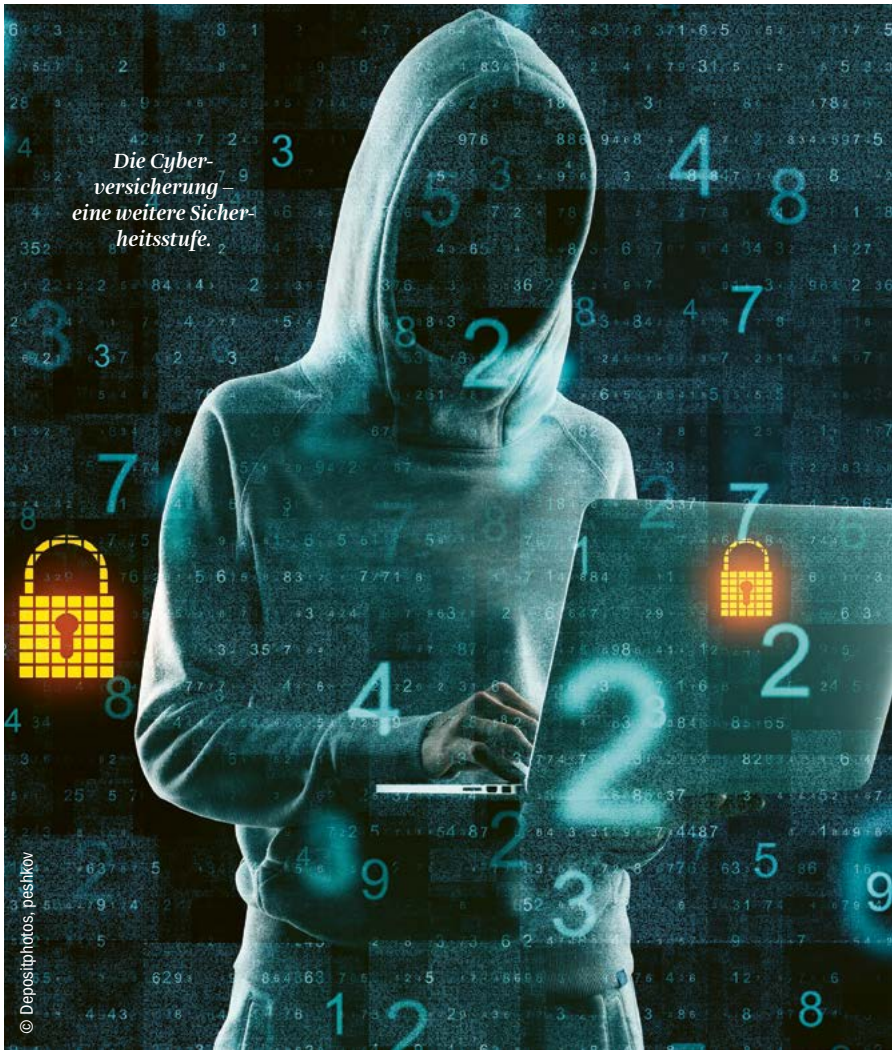
Der Schweizerische Kaderverband bietet neu eine Cyberversicherung an. Weshalb kommen Sie erst jetzt mit einer solchen Lösung?

MARC GEROSA: Wir beschäftigen uns schon länger mit dem Thema und haben mit diversen Versicherungsunternehmen Gespräche geführt. Gerade kleinere Unternehmen – also unsere Klientel – haben bis anhin mit einem Abschluss einer solchen Police gezögert.

Die vielen Hackerangriffe auf Schweizer Unternehmen sowie das steigende Bedürfnis im Markt zeigen uns, dass auch wir eine solche Versicherung für unsere Mitglieder anbieten müssen, da wir diese vollumfänglich unterstützen wollen. Zusammen mit der Basler Versicherung haben wir das nun attraktiv umgesetzt. Wir sind klar der Ansicht, dass heutzutage jedes Kleinunternehmen eine Cyberversicherung haben sollte, um damit gegen den Worst Case gewappnet zu sein. Denn schon manch ein Kleinunternehmen hat sich von einem Cyberangriff nicht mehr erholt.

Welche Vorteile bieten Sie gegenüber anderen Mitbewerbern?

Bei der Cyberlösung des SKV handelt es sich um ein umfangreiches Leistungspaket. Mit unserem modularen Produkt



Die Cyberversicherung – eine weitere Sicherheitsstufe.

© Depositphotos, peshkov

können die SKV-Mitglieder aus drei auf sich aufbauenden Paketen den für sie passenden Schutz auswählen.

Wir haben den Vorteil, dass wir als Verband den Mitgliedern eine Prämienreduktion anbieten können.

Das revidierte Datenschutzgesetz der Schweiz, das voraussichtlich 2022 in Kraft treten wird, nimmt die Unternehmen stärker in die Pflicht. Wer seine Hausaufgaben nicht gemacht hat, schliesst eine Cyberversicherung ab und das Problem ist gelöst.

Selbstverständlich sind gewisse Kosten im Rahmen von Datenschutzverletzungen in der Cyberversicherung berücksichtigt. Es wäre jedoch ein falsches Zeichen, wenn eine Versicherungslösung die Umsetzung der Datenschutzgesetze kompensieren würde. Der Schutz von Daten ist Teil des Risikomanagementprozesses, den jedes Unternehmen aus eigenem Interesse an die Hand nehmen sollte.

Was, wenn ein Mitarbeiter mutwillig Firmendaten verkauft?

Unsere Lösung berücksichtigt nicht nur kriminelle Ursachen (Cyber Crime) sondern auch fahrlässiges oder vorsätzliches Verhalten von Mitarbeitenden.

Nimmt der SKV eine Firma genau unter die Lupe, bevor er mit ihr eine Cyberversicherung abschliesst?

Wir prüfen das Risiko im Rahmen des Online-Abschluss-Prozesses mittels Fragebogen, den das Unternehmen ausfüllen muss. Fallen die Antworten positiv aus, erhält das KMU relativ schnell einen Versicherungsabschluss. Stellen wir aber fest, dass minimale Sicherheitsaspekte wie zum Beispiel Passwortschutz oder Firewall fehlen, prüfen wir das Risiko vertieft. Allenfalls kommen unsere Fachleute zum Schluss, dass wir das Unternehmen nicht versichern können. Wir erwarten von unseren Mitgliedern, dass sie gewisse Vorkehrungen treffen, um gegen Hackerangriffe gerüstet zu sein.

Betonen möchte ich noch Folgendes: Macht ein Unternehmen falsche Angaben, kann die Versicherung im Schadenfall Leistungen ablehnen.

Wäre es nicht sinnvoller, wenn ein Unternehmen, bevor es bei einer Versicherung anklopft, ein Cyber-Security-Konzept umsetzt?

Ein Cyber-Security-Konzept erachte ich für jedes Unternehmen als sehr wichtig. Damit ist zum Beispiel klar festgelegt, dass alle Sicherheits-Updates der Software immer gemacht und somit Sicherheitslücken geschlossen werden. Nur wenn solch grundlegende Sicherheitsstufen im Betrieb klar geregelt sind, ist eine Cyberversicherung als weiterer Schutz sinnvoll.

Der SKV schreibt, bei erfolgreichem Hackerangriff unterstütze ein Team von Experten das betroffene Unternehmen. Was heisst das konkret?

Haben die Hacker zugeschlagen, sind unter Umständen verschiedene Disziplinen gefragt, um die Normalität eines Betriebs wieder herzustellen. Das bedingt ein Expertennetzwerk, das schnell funktioniert: forensische Untersuchungen, Fernwartung und so weiter. Trifft der Worst Case ein, braucht es vielleicht auch Fachleute, die bezüglich Reputationsschaden ein KMU beraten: Wie verhält man sich gegenüber Kunden, den Medien und anderen Anspruchsgruppen. Das alles bietet unsere Versicherungslösung.

Man kann die Versicherung jederzeit über die 24-Stunden-Hotline kontaktieren, denn im Ernstfall muss es rasch gehen. Selbstverständlich kann eine Firma auch die eigenen, vertrauten IT-Spezialisten in Absprache mit der Versicherung miteinbeziehen.

«Schon manch ein Kleinunternehmen hat sich von einem Cyberangriff nicht mehr erholt.»

Was geschieht bei einem Fehlalarm?

Laufen in einem KMU eines Tages die Computer aus irgendwelchen Gründen nicht mehr und die Versicherung wird angerufen, weil eine Cyberattacke vermutet wird, so schalten sich rasch unsere Experten ein und schauen den Fall an. Stellt sich heraus, dass es kein Cyberangriff war, sondern irgendein technisches Problem, so entstehen für das KMU keine Kosten. Die Behebung eines allfälligen Schadens, welcher nicht mit einem Cybervorfall in Zusammenhang steht, ist jedoch nicht über die Cyberversicherung gedeckt.

Zahlt die Cyberversicherung auch, wenn das KMU fahrlässig gehandelt hat?

Hat das Unternehmen elementare Sorgfaltspflichten verletzt, kann es Leistungskürzungen geben. Wer grobfahrlässig handelt und zum Beispiel mehrmals Sicherheits-Updates wegklickt und als Folge davon erfolgreich von Hackern angegriffen wird, der kann nicht vollumfänglich die Versicherungsleistung in Anspruch nehmen. Auch wer zum Beispiel seinen USB-Stick mit sensiblen Kundendaten im Büro liegen lässt und die Türen nicht verriegelt, handelt grobfahrlässig. Klickt aber ein Mitarbeitender irrtümlich auf ein Phishing-Mail, ist das zwar fahrlässig, doch die Cyberversicherung deckt den entstandenen Schaden.

Nebst Schadenbehebung und Umsatzausfall kann man bei Ihnen auch

Über den SKV

Der Schweizerischen Kaderverband (SKV) wurde 1988 gegründet und ist ein Interessens- und Berufsverband für KMU, Selbstständige und Kaderpersonen.
Der SKV versteht sich als Ansprechpartner für sämtliche Versicherungs- und Vorsorgefragen.

> *www.kaderverband.ch*

Zur Person

Marc Gerosa ist Geschäftsführer des Schweizerischen Kaderverbandes (SKV).

Stellen wir fest, dass in einem Unternehmen minimale Sicherheitsaspekte fehlen, prüfen wir unser Versicherungsrisiko vertieft.

Cybererpressung versichern. Wie schnell bezahlt die Versicherung die geforderten Beträge an die Hacker?
Wenn Hacker alle Daten im Unternehmen verschlüsseln und das ganze System lahmlegen, raten wir grundsätzlich davon ab, Lösegeld zu bezahlen. Primär versuchen wir auf anderem Weg, das System des Versicherungsnehmers wieder zum Laufen zu bringen; zum Beispiel, die Daten via Back-up-System herzustellen. Nur als allerletzte Massnahme bezahlt die Versicherung Lösegeld.

Welchen Höchstbetrag kann ein KMU versichern?
Für Lösegeldzahlungen liegt die Obergrenze bei unserem Versicherungsmodell Top bei 50 000 Franken. Die versicherbare Obergrenze von Betriebs- und Ertragsausfall, für die Entfernung und Wiederherstellung des IT-Systems usw. liegt jedoch bei maximal je einer Million Franken.

In welcher Grössenordnung bewegen sich die Prämien?
Das hängt von verschiedenen Parametern wie Umsatz, Versicherungssumme und weiteren Faktoren ab. Im Durchschnitt kostet eine Jahresprämie für die Cyberversicherung um die 1500 Franken.

Wie sieht es mit dem Selbstbehalt aus?
Der Selbstbehalt ist frei wählbar. Er liegt zwischen 500 und 10 000 Franken – ausgenommen ist der Betriebsertragsausfall, bei welchem kein Selbstbehalt vorhanden ist.

Nach wie vielen Hackervorfällen wird einem KMU der Versicherungsvertrag gekündigt?
Das kann man nicht generell beantworten. Es kommt auf die individuellen Fälle an. Wiederholt sich ein Schadenfall, weil eine bestimmte Sicherheitslücke – obwohl bekannt – nicht geschlossen wurde, wird sich die Versicherung überlegen, dem Kunden den Vertrag zu verlängern, da er wesentliche Sicherheitsregeln und Sorgfaltspflichen nicht beachtet hat. ■

Hinweis: Mit dem Meldeformular des Nationalen Zentrums für Cybersicherheit können Cyberangriffe erfasst und gemeldet werden: www.report.ncsc.admin.ch