VERSICHERUNGEN ASSURANCES INSOS

Schweizer Firmen unterschätzen Cyber-Risiken

Digitale Technologien, Geräte und Medien eröffnen uns ungeahnte Möglichkeiten. Gleichzeitig werden aber auch Cyber-Angriffe immer komplexer, raffinierter und häufiger. Schweizer Unternehmen gehören in ihren je-weiligen Branchen oft zu den Weltmarktführern. Doch der Erfolg hat auch eine Schattenseite. Er ruft Kriminelle auf den Plan. Die damit verbundenen Cyber-Risiken sind aber nie nur die Angelegenheit der IT-Abteilung, obschon dieser Bereich technisch in der Verantwortung steht und somit eine führende Rolle spielt. Das Risiko Management einer Unternehmung benötigt ein profundes Verständnis über die konstante Weiterentwicklung der möglichen Risiken, aber auch über die Instrumente und Techniken, diesen Ereignissen entgegen zu treten. Die Akteure im Bereich Cyber-Kriminalität und deren Absichten sind nämlich äusserst vielseitig. Einerseits wollen sie die „Opfer" schädigen bzw. im Markt zurückbinden oder sich andererseits mittels Erpressungen (z.B. Fall Genfer Kantonalbank von Anfang 2015) finanziell bereichern.

Was versteht man unter Cyber-Risiken?

Cyber-Angriffe können für Unternehmen drastische Konsequenzen nach sich ziehen, wie etwa finanzieller Verlust (Betriebsunterbruch, Datenwiederherstellung), Störung der Geschäftsabläufe oder Reputations-Schäden. Als Cyber-Kriminalität gilt jedes Verbrechen, das mit Hilfe eines Computers, Netzwerks oder Hardwaregeräts extern oder intern begangen wird. Solche Verbrechen können auf nur einem Computer oder an mehreren Orten gleichzeitig erfolgen.

Was versteht man unter Cyber-Versicherungen?

Cyber-Versicherungen decken vielfältige Eigen- und Drittschäden, die Unternehmen als Opfer von Cyber-Kriminalität selbst erleiden oder für die sie von ihren Kunden (z.B. durch ungenügende Firewalls) haftbar gemacht werden.

Uns wird das nicht passieren…

Eine Studie (Clarity on Cyber Security) des Beratungsunternehmens KPMG zeigt nun, dass den Schweizer Unternehmen allein im letzten Jahr durch Cyber-Kriminalität ein Schaden von rund 200 Millionen Franken entstanden ist.

Bei Angriffen sind oft die Mitarbeiter einer Firma die grösste Schwachstelle. Mittels sogenannter Phishing-Attacken versuchen Cyberkriminelle die Gutgläubigkeit der Angestellten auszunützen. Über gefälschte Websi-tes, E-Mails oder Kurznachrichten werden sie aufgefordert, ihre persönlichen Daten preiszugeben. Dadurch ge-lingt es den Verbrechern, sich Zugang zu den Computersystemen der Firmen zu verschaffen, wo sie dann teil-weise enormen Schaden anrichten.

Cyber-Kriminalität hat naturgemäss eine starke technische Komponente. Dennoch entsteht ein Grossteil der erfolgreichen Cyber-Angriffe unter Ausnutzung menschlicher Fehler. Jegliche Arten von Unternehmen und Organisationen, die in der Öffentlichkeit stehen, tragen ein Risiko, nicht nur Finanzdienstleister, öffentliche Institutionen wie Bund und Kantone oder bekannte Marken (Coca-Cola, Apple, Ebay etc.). Gemäss KPMG sind Firmen vielfach bei Angriffen auf Web Server Software am verwundbarsten. Umfragen zufolge waren bereits über 70 Prozent der grösseren Unternehmen in der einen oder anderen Art von Cyber-Angriffen betroffen. Problema-tisch ist die Tatsache, dass Angriffe meist sehr lange nicht entdeckt werden. Im Durchschnitt bemerken Firmen Cyber-Angriffe während rund 200 Tagen nicht.

Haben sich die Kriminellen also einmal eine Art digitales Einfallstor in eine Firma geschaffen, so können sie dieses oft ungehindert hunderte von Malen nutzen. Dabei nehmen Anzahl, Komplexität und Professionalität der Angriffe zu, da die Angreifer stets mit neuester Technologie aufwarten.
Je nach Abhängigkeit von der IT kann die Unternehmenstätigkeit mit allen Konsequenzen die damit verbunden sind, komplett zum Stillstand gebracht werden. Cyber-Sicherheit sollte daher Chefsache sein. Gegen Cyber-Angriffe kann man sich in einem gewissen Rahmen durchaus verteidigen, wenn man sich den möglichen Gefahren bewusst ist. Die Beauftragten für Informatiksicherheit im Unternehmen sollten daher entsprechend aus-gebildet sein und gegen die sich verändernden Bedrohungen à jour bleiben.

Swiss Quality Broker AG
Etzelstrasse 27
8808 Pfäffikon
T. +41 58 508 08 17
info@sqbroker.ch

Advantis Versicherungsberatung AG
Buckhauserstrasse 17
8048 Zürich
T. +41 43 311 86 13
nicola.bonsignore@advantis-ic.com

Ihre mögliche Cyber Bedrohung

Die Akteure und deren Absichten können im Bereich Cyber Crime äusserst vielseitig sein. Darunter fallen u.a.:

- **Fahrlässige Mitarbeiter**, z.B. in den Bereichen Datenpannen, Hardwareverlust, Malware oder Phishing
- **Unredliche Mitarbeiter**, z.B. mittels physischem Diebstahl oder Entwendung von Daten (z.B. im Kündigungsfall)
- **Externe Personen,** z.B. mittels „Hacktivismus", krimineller Vereinigungen oder ausländischer Regierungen
- **Ihre Subunternehmer**, welche grundsätzlich den gleichen Risiken ausgesetzt sind, wie Sie als Auftraggeber

5-Punkte Checklisten für Unternehmungen für die Cyber Vorbereitung:

- **Verantwortlichkeiten definieren:** Die Verantwortung gegenüber der Unternehmensleitung in Bezug auf IT-Sicherheit und Cyber-Risiken festlegen und bestimmen welche Informationen benötigt werden um Entscheidungen rechtzeitig fällen zu können.

- **Die eigenen Cyber-Risiken verstehen:** Verstehen, welche Informationen wirklich entscheidend und welche Risiken relevant sind sowie sich bewusst sein wie stark man diesen gegenüber tatsächlich ausgesetzt ist.

- **Aktive Entscheidungsrolle spielen:** Risikofähigkeit innerhalb der Unternehmung festlegen und diese auf allen Stufen kommunizieren. Sicherstellen, dass die gewählten Ressourcen wirkungsvoll zum Einsatz kommen.

- **Ausfallplan erstellen:** Wie wissen Sie, dass Sie angegriffen worden sind? Was wollen Sie dann machen? Haben Sie vernünftige Vorbereitungen getroffen?

- **Strategische Prioritäten anstreben:** Stellen Sie sicher, dass die Risikominimierung trotzdem Wachstum zulässt, dass Risikokontrollen nicht den Fortschritt einschränken und dass Sie genügend Flexibilität bewahren um trotzdem auf Chancen und Möglichkeiten reagieren zu können.

Die Versicherungsmöglichkeit von Cyber Risiken im Vergleich

	Sach / EDVA	Betriebs-Haft	Berufs-Haft	K&R	Crime	Cyber
DRITTSCHÄDEN						
Ansprüche infolge Datenschutzverletzung	X	●	X	X	X	✓
Ansprüche infolge Persönlichkeitsrechtverletzung (nach einem Datenverlust	X	X	●	X	X	✓
Ansprüche infolge Verletzung geistigen Eigentums	X	X	●	X	X	✓
Ansprüche infolge Übermittlung von Malware auf Drittsysteme	X	X	●	X	X	✓
EIGENSCHÄDEN						
Kosten für IT-Forensik (Berater)	X	X	X	X	X	✓
Kosten für PR-Berater	X	X	X	X	X	✓
Kosten für Rechtsberatung (nicht Anspruchsabwehr im Haftpflichtfall)	X	X	X	X	X	✓
Kosten für die Benachrichtigung der Betroffenen nach einem Datenverlust	X	X	X	X	X	✓
Kosten für Wiederherstellung von Daten nach einem Hackerangriff	●	X	X	X	●	✓
Kosten für Betriebsunterbruch (entgangener Gewinn/Mehrkosten)	X / ●	X	X	X	X	✓
Erpressung/Bedrohung	X	X	X	✓	X	✓
Belohnung für Hinweise, die zur Ergreifung des Erpressers führen	X	X	X	✓	X	✓

✓ versicherbar X nicht versicherbar ● Einschluss tw. möglich

Fazit

Mängel bei der Cyber-Sicherheit wurden bisher oft auf die fehlenden finanziellen und personellen Ressourcen zurückgeführt. Glücklicherweise wird Cyber-Sicherheit heute in zunehmendem Masse weniger als simples Technologieproblem als vielmehr als effektives Geschäftsrisiko betrachtet. Die Assekuranz hat deshalb die Thematik der Cyber-Risiken aufgegriffen. Umfassende und überraschend preisgünstige Deckungen werden angeboten. Noch im Jahre 2014 hat eine von „Corporate Trust" durchgeführte Studie aufgezeigt, dass lediglich 15,6 Prozent der Befragten den Abschluss einer Cyber-Versicherung für wichtig erachten. Bereits ein Jahr später (2015) würde dieses Resultat – nicht zuletzt wegen den wöchentlich eintreffenden Nachrichten über Cyber-Angriffe - wohl ganz anders aussehen. Einen 100%-igen Schutz gegen Cyber-Risiken gibt es aber leider nie.

Swiss Quality Broker AG
Etzelstrasse 27
8808 Pfäffikon
T. +41 58 508 08 17
info@sqbroker.ch

Advantis Versicherungsberatung AG
Buckhauserstrasse 17
8048 Zürich
T. +41 43 311 86 13
nicola.bonsignore@advantis-ic.com