AGENTURORGANISATION

Schützen Sie Ihre Versicherungsagentur mit einer Versicherung vor Cyber-Risiken

von Johannes Behrends, Leiter der Abteilung für Cyber-Risiken, Aon Risk Solutions, Mühlheim

Die Cyber-Kriminalität hat in den letzten Jahren zugenommen. Hacker-Angriffe und Cyber-Attacken sind an der Tagesordnung. Auch Versicherungsvertreter stellen ein beliebtes Angriffsziel für Cyber-Attacken dar. Eine Cyber-Versicherung für Ihre Agentur ist daher zu empfehlen.

Die Bedrohungslage in der Versicherungsagentur

Hackerangriffe ...

Als Cyber-Risiko aus Sicht der Versicherungsbranche versteht man im Grundsatz das Risiko für Unternehmen, Opfer eines Hackerangriffs zu werden oder sensible Daten aufgrund von Fahrlässigkeit zu verlieren. Die Risiken sind vielfältig und folgenschwer.

Fahrlässig herbeigeführter Datenverlust durch einen Mitarbeiter

Fahrlässige Datenverluste können z. B. dadurch entstehen, dass einem Mitarbeiter der Agentur sein Diensthandy, Tablet oder Notebook verloren geht. Der potenzielle Finder hat Zugriff auf viele Informationen, schlimmstenfalls auf sämtliche Unternehmensdaten.

Zielgerichtete Angriffe auf Daten oder IT-Systeme

Bei einem Hackerangriff nutzen Angreifer nicht nur Sicherheitslücken im System aus. Sie nehmen auch immer öfter gezielten Einfluss auf die Mitarbeiter. Durch Social Engineering – die zwischenmenschliche Beeinflussung mit dem Ziel, unberechtigt an Informationen oder technische Infrastrukturen zu gelangen – schaffen es Hacker oft, schnell an ihr Ziel zu kommen.

... greifen Daten ab oder ...

Die meisten Hacker haben es auf die Daten der Agenturen abgesehen. Sie speichern zahlreiche sensible Informationen, angefangen bei Adressdaten bis hin zu Schadeninformationen oder Gesundheitsdaten. Ein Verlust dieser Daten kann für die Agentur verheerende Auswirkungen haben. Kriminelle können die erbeuteten Daten selbst nutzen, z. B. für Phishing- oder Spammails, oder sie verkaufen die Datensätze weiter.

Andere Hacker haben die vorsätzliche Löschung oder Beschädigung relevanter Daten oder Programme zum Ziel. Motive können Rache oder die Schädigung eines Mitbewerbers sein.

... legen Systeme lahm

Für Schäden sorgen auch die sogenannten DoS- (Denial of Service) oder DDoS-Attacken (Distributed Denial of Service). Dabei werden Systeme oder Dienste mit einer großen Zahl gleichzeitiger Anfragen überlastet, sodass sie ihren Dienst verweigern. Üblicherweise werden diese Angriffe auf Webseiten verübt. In jüngster Zeit ist immer öfter die Finanzbranche Opfer.

Schadsoftware ...

Für Aufsehen sorgte vor knapp einem Jahr der Cryptolocker „Locky". Die Ransomware infizierte in Deutschland zeitweise bis zu 5.000 Rechner pro Stunde. Sie verschlüsselte Daten auf den betroffenen Systemen und führte teilweise zu gravierenden Betriebsstörungen. Das Opfer bekam den Code zur Entschlüsselung nur gegen Zahlung eines Lösegeldes.

Beispiel

... legt Rechner lahm

Die FAZ berichtete kürzlich über einen Versicherungsvermittler, dessen Systeme von einer Ransomware infiziert wurden. Der Vermittler musste gleich für 15 betroffene Server zahlen.

Der aktuelle Schadenbericht des Versicherers American International Group (AIG), „Die Ursachen von Schadenfällen in der Cyber-Versicherung", zeigt: Die Schadenfälle in der Cyber-Versicherung nahmen drastisch zu. Registrierte AIG bei seinen Kunden im Jahr 2013 noch zwei versicherte Schadenfälle, so waren es im Jahr 2016 bereits 121. Ransomware ist mit 16 Prozent unter den AIG Schadenfällen die größte Bedrohung. Mit 23 Prozent waren Finanzdienstleister zudem die mit Abstand am stärksten betroffene Branche.

Cyber-Versicherung für Versicherungsvertreter

Diese Entwicklung zeigt: Sie sind gut beraten, wenn Sie nicht nur für Ihre Kunden, sondern auch für sich geeignete Schutzmaßnahmen ergreifen. Neben präventiven Maßnahmen sollten Sie auch den Abschluss einer Cyber-Versicherung in Betracht ziehen.

Cyber-Versicherungen bieten speziellen Schutz

Deckungslücken bei Absicherung in bestehenden Versicherungen

Cyber-Risiken können teilweise über übliche Versicherungen (Sach-, Haftpflicht oder Vertrauensschadenversicherung) abgedeckt sein. So können Betriebsunterbrechungsschäden zwar über die Sachversicherung abgesichert werden, in der Regel ist für den Versicherungsfall jedoch ein Sachschaden erforderlich. Der liegt bei einem Datenverlust oder Hackerangriff normalerweise nicht vor.

Um diese Deckungslücken zu schließen, wurden Cyber-Versicherungen entwickelt. Sie können

- an den Bedarf der Unternehmen angepasst werden,
- decken je nach Vereinbarung den Eigen- und Drittschaden und
- haben den Vorteil, dass sich das Unternehmen im Schadenfall nur an einen Versicherer wenden muss. Werden die Risiken hingegen über die bestehenden Industrieversicherungen versichert, muss mitunter jeder Versicherer über den Schaden informiert werden.

Grunddeckung der Cyber-Versicherungen

Schutz für bestimmte Dritt- und Eigenschäden

Die Versicherungsbedingungen der angebotenen Policen weichen teilweise stark voneinander ab. Es hat sich aber eine gewisse Grunddeckung herauskristallisiert: Es besteht Versicherungsschutz für Dritt- und Eigenschäden, die auf einer Informationssicherheitsverletzung beruhen.

Deckungsumfang einer Cyber-Versicherung

Versicherungsschutz für Eigenschaden	
Krisenmanagement-kosten	Der wichtigste Bestandteil der Cyber-Versicherung ist das Bereitstellen des Krisenmanagements. Die Versicherer gehen häufig Kooperationen mit Beratern wie IT-Forensikern, PR- und Rechtsberatern ein. Im Schadenfall wird so gewährleistet, dass den Versicherungsagenturen umgehend kompetente Hilfe zur Seite gestellt wird. Folgende Kosten werden erstattet: ■ Die Kosten für IT-Forensiker, die die Schadenursache und den Umfang klären sollen. ■ Die Kosten für Rechtsanwälte, die über einzuhaltende datenschutzrechtliche Regelungen beraten. ■ Die Kosten für PR-Berater, die dabei unterstützen, den Reputationsschaden gering zu halten.
Kosten für die Benachrichtigung der betroffenen Kunden	Allein durch die Portokosten für die Informationsbriefe an die betroffenen Kunden oder eine ganzseitige Anzeige in der Tagespresse entstehen schnell hohe Beträge.
Kosten der Wiederherstellung von Daten und Systemen	Im Schadenfall, etwa nach einem Hackerangriff, müssen Daten und Computersysteme repariert oder wieder hergestellt werden. Hierfür können erhebliche Kosten anfallen, die ebenfalls von den Versicherern erstattet werden.
Kosten für Betriebsunterbrechungsschäden	Kommt es durch einen Hackerangriff zu einer Betriebsunterbrechung, kann der durch die Unterbrechung verursachte Ertragsausfallschaden versichert werden.
Kosten für Erpressungsgeld	Werden Sie erpresst und etwa damit bedroht, dass sensible Daten veröffentlicht oder Systeme stillgelegt werden, wird gezahltes Erpressungsgeld erstattet. Selbst Belohnungen, die zur Ergreifung der Täter führen, können in die Versicherungsleistung eingeschlossen werden.
Versicherungsschutz für Drittschaden	
Schadenersatzansprüche aufgrund einer Verletzung der Vertraulichkeit	Auf der Drittschadenseite sind Ansprüche wegen Verletzung des Datenschutz-, des Persönlichkeitsrechts und der Verletzung geistiger Eigentumsrechte versichert. Auch wenn solche Ansprüche in vielen Branchen eher selten geltend gemacht werden, gibt es Fälle, in denen Ansprüche Dritter eher zu erwarten sind. Dies gilt z. B. für den Verlust von sensiblen Risikoinformationen oder Schadenfalldaten. Verliert ein Versicherungsvertreter solche Daten und gelangen sie an die Öffentlichkeit, ist es vorstellbar, dass Betroffene Schadenersatzansprüche geltend machen.
Schadenersatzansprüche aufgrund einer Netzwerksicherheitsverletzung	Übermittelt eine Agentur versehentlich Malware auf Systeme Dritter, z. B. bei einem Geschäftspartner, kann der dadurch bei dem Dritten entstandene Schaden ebenfalls mitversichert werden.

Der wichtigste Bestandteil der Cyber-Versicherung ist aber das Bereitstellen des Krisenmanagements. Gerade für kleinere oder mittelständische Agenturen, die oft nicht ausreichend auf den Krisenfall vorbereitet sind, stellt dieser Service einen enormen Vorteil dar.

FAZIT | Nehmen Sie Ihren eigenen Versicherungsschutz nicht auf die leichte Schulter. Sichern Sie Cyber-Risiken effektiv ab. Die Bedrohung durch Cyber-Risiken wird weiter zunehmen.

Für ausreichend Versicherungsschutz sorgen