ıalität: Vorsicht vor Schlupflöchern bei Cybercrime-Versicherungen

12.05.2020 | Kunde: Seipt & Partner | Ressort: Österreich / Wirtschaft / Finanzen / Recht / Versicherung | Ankündigung

Cybercrimeversicherungen, also die Absicherung vor Attacken aus dem Internet, boomen auch in Österreich. Die Angst ist berechtigt, stieg doch laut der neuen Kriminalstatistik des Bundeskriminalamts 2019 die Internetkriminalität um 45 Prozent im Vergleich zum Vorjahr. Das Problem: Beinahe täglich denken sich Hacker neue Bedrohungen aus, die viele Versicherungen als Schlupfloch nützen, um im Schadensfall nicht zu zahlen. Und auch die Gefahr von Bedienungsfehlern durch Mitarbeiter (Stichwort Homeoffice) sollte von Versicherungen abgedeckt werden. Daher sind eine kontinuierliche Anpassung der bestehenden Versicherungs-Polizzen und das „aufrüsten" auf einen 360-Grad Versicherungsschutz unabdingbar.

Honorarfreies Fotomaterial, Copyright siehe Dateinamen, unter: FOTOLINK

Wien, 12. Mai 2020. Das jüngste Datenleck des Wirtschafts-und Finanzministeriums, bei dem die persönlichen Daten von mehr als einer Million Bürger öffentlich einsehbar waren, macht es deutlich: Unzählige Institutionen oder Unternehmen sind von IT-Sicherheitslücken oder Hackerattacken bedroht. Laut der Kriminalstatistik 2019 des Bundeskriminalamts explodierte die Internetkriminalität um 45 Prozent. Auch Cybercrime-Delikte im engeren Sinn haben zugenommen. Hier stiegen etwa in Wien die Anzeigen wegen „Betrügerischen Datenverarbeitungsmissbrauchs" (etwa bei bargeldlosen Zahlungen mittels NFC-Funktion) um + 372,2 % oder wegen Erpressungen um + 23,6 %. Die Versicherungsbranche reagiert darauf mit einem ganzen Bündel unterschiedlicher Angebote. Der Haken: Da sich die Art und Weise der Cyberattacken täglich ändert, decken viele dieser Polizzen neuartige Bedrohungsszenarien nicht ab. „Bei vielen Cyberversicherungsprodukten handelt es sich um Polizzen mit zahnlosen Deckungen. Die Versicherungen finden im Ernstfall häufig einen Ausschlussgrund und zahlen nicht. Wirklich sinnvoll sind vollwertige ‚Crime-Deckungen`, die möglichst breit Gefahren abdecken. Das betrifft z.B. auch ‚Vertrauensschäden` oder die Mitversicherung der groben Fahrlässigkeit von Mitarbeitern", erklärt **Benedikt Seipt** von Seipt & Partner aus Wien, mit mehr als 6000 Kunden einer der führenden Versicherungsmakler Österreichs.

Wann eine Cyber-Versicherung Sinn macht

Hackerangriffe haben heute viel weitreichende Auswirkungen als noch vor wenigen Jahren. Durch die fortschreitende Digitalisierung der Unternehmen steigt die Abhängigkeit von Technik, IT oder dem elektronischen Zahlungsverkehr. Kommt es in diesen sensiblen Bereichen zu einem Cyberangriff droht der Betriebsstillstand, im schlimmsten Fall sogar der Konkurs. „Derzeit findet eine Sensibilisierung in diesem Bereich statt. Datensicherheit muss als Teil des unternehmerischen Risikomanagements gesehen und somit zur Chefsache erklärt werden. Natürlich sollte eine Notwendigkeit

einer solchen Absicherung individuell -von Fall zu Fall -überprüft werden", so Seipt. Ist z.B. ein mittelständisches Unternehmen mehrere Tage lang nicht in der Lage, den Geschäftsbetrieb oder die Produktion aufrecht zu erhalten, kann ein Cyberangriff die Existenz bedrohen. Dies gilt auch bei Verstößen gegen die DSGVO oder bei Verletzungen des Copyrights und von Lizenzen.

Zweites Sicherheitsnetz für KMUs

Cyberversicherungen lohnen sich aber nicht nur für große Unternehmen, sondern auch für den typischen Klein-und Mittelbetrieb. „Oftmals passieren Fehler durch menschliches Versagen. Das typische ‚Totschlag-Argument`, man hätte sowieso eine IT-Abteilung, greift hier nicht. Das wäre so, als würde man bei einem Brand den Brandschutzbeauftragten zum Löschen rufen", erklärt Seipt. Hier ist die Cybercrime-Versicherung eine gute Ergänzung zu klassischen IT-Sicherheitsmaßnahmen. „Diese ist sozusagen ein zweites Sicherheitsnetz bei gezielten Angriffen und stellt den präventiven Assistance-Gedanken, aber vor allem die hochprofessionelle Schadenbegleitung durch teils äußerst preisintensive Forensiker in den Mittelpunkt", so der Versicherungsprofi.

360 Grad-Schutz schließt die Schlupflöcher der Versicherungen

Es gibt unzählige Versicherungen, die z.B. gegen Viren schützen. Einen echten 360-Grad-Schutz, der gegen alle Eventualitäten absichert, findet man nur beim Spezialanbieter. Unternehmer sind daher gut beraten, mit speziellen Versicherungspaketen alle Eventualitäten abzusichern. Doch diese Angebote sind dünn gesät. Seipt: „Durch unsere Inhouse-Risikoanalyse können wir für jedes Unternehmen ein individuelles Angebot schnüren. Meines Wissens sind wir die einzigen Anbieter in Österreich, die so ein 360-Grad-Paket anbieten können, das einerseits zukunftssicher ist und gleichzeitig alle Cybergefahren abdeckt." Anders ausgedrückt: Die Versicherungsbedingungen werden flexibel gestaltet. Der Deckungsschutz hält Schritt mit der sich täglich ändernden Gefahrenlage. „Durch eine sogenannte ‚Bestklausel` kommen unsere Versicherungsnehmer in den Genuss einer tagesaktuellen Deckungsvariante", betont Seipt. Der Schutz umfasst weiters auch Verstöße gegen die Geheimhaltungspflicht und den dadurch entgangenen Gewinn, Bußgelder von Datenschutzbehörden, Lösegelder und vieles mehr. Seipt weiter: „Gerade mit Blick auf einen möglichen Betriebsstillstand sollte das für jeden CEO Anlass genug sein, eine Versicherung mit dieser digitalen Vertrauensschadendeckung in das Risikomanagement einfließen zu lassen."

Die Experten von Seipt & Partner stehen für Interviews zur Verfügung!

Über Seipt & Partner

Seipt & Partner Versicherungsmakler GmbH ist ein unabhängig agierendes Unternehmen mit Hauptsitz in Wien. 1995 von Benedikt Seipt gegründet, gehört Seipt & Partner zu den führenden, österreichischen Versicherungsmaklern im Sachversicherungsbereich. Derzeit vertrauen 6250 Kunden mit mehr als 21.000 Verträgen auf die Expertise des Unternehmens mit 22 Mitarbeitern.

www.seipt.at