

Cyberschutz für beratende Berufe - Steuerberater, Rechtsanwälte und Wirtschaftsprüfer im Fokus



HDI Versicherung AG, Gebäude in Hannover

© HDI/ Thomas Bach

Steuerdaten von Kunden, Prozessakten oder Unternehmensinterna - die Rechner von Steuerberatern, Wirtschaftsprüfern und Rechtsanwälten beherbergen eine Vielzahl sensibler Informationen. Daten, die auch für Cyberkriminelle von hohem Interesse sind. Aber nicht nur der Diebstahl von Kundendaten ist eine Gefahr für Kanzleien. Auch selbst können sie zum Ziel von Erpressungen werden, zum Beispiel durch den Einsatz von Ransomware, die Daten des Unternehmens verschlüsselt, so dass sie nicht mehr genutzt werden können.

Spätestens seit den Cyber-Angriffen ‚WannaCry‘ und ‚Petya‘ ist klar: Cyberkriminalität geht alle an. Nach rund 46.000 Cyberangriffen 2015 weist die Kriminalstatistik des BKA für 2016 knapp 83.000 Fälle aus. Das ist fast eine Verdoppelung. Die Dunkelziffer dürfte allerdings noch wesentlich höher liegen. „Viele Betroffene merken entweder gar nicht, dass ihre Daten gestohlen wurden, oder werden erst viel später darauf aufmerksam, wenn diese Daten missbraucht werden“, erklärt Dr. Karl Bialek, Leiter Produktmanagement Vermögensschaden-Haftpflicht der HDI Versicherung. Viele scheuten sich außerdem davor, Anzeige zu erstatten. Schließlich möchte sich keiner nachsagen lassen, Daten wären bei ihm nicht sicher.

Technische Sicherungen sind nur Basisschutz

Die aktuellen Angriffe zeigen auch wieder, wie Kriminelle inzwischen vorgehen und wie wichtig regelmäßige Updates und Patches sind. Firewall, Virens Scanner und regelmäßige Softwareupdates sind zur Absicherung der IT inzwischen auch bei den meisten kleineren Unternehmen und Selbstständigen selbstverständlich. Kommt dazu noch ein spezielles Angriffserkennungssystem,

ist ein solider Grundschutz erreicht. Insbesondere kleine Unternehmen konzentrieren sich in Sachen IT-Sicherheit jedoch oft ausschließlich auf diese technische Sicherung ihrer IT-Systeme.

Einen hundertprozentigen Schutz kann jedoch auch die beste Technik nicht bieten. Denn trotz aller Vorkehrungen bleibt immer die Schwachstelle Mensch. So können Computer befallen werden, wenn ein Nutzer eine infizierte Datei herunterlädt, eine verseuchte Website besucht oder den harmlos aussehenden Dateianhang einer E-Mail öffnet. Die Folgen können verheerend sein. Denn neben dem Diebstahl von Daten, die von Kriminellen missbraucht werden können, kann Ransomware wichtige Dateien des Computers verschlüsseln. Die sollen dann angeblich nach Zahlung eines Lösegelds wieder freigegeben werden. Karl Bialek warnt jedoch: "Es ist keineswegs gewährleistet, dass auch nach einer Lösegeldzahlung die Dateien tatsächlich wieder entschlüsselt werden." IT-Experten und Polizei raten daher, auf keinen Fall zu bezahlen sondern Anzeige zu erstatten. Existenziell wichtig ist auch für diesen Fall, dass ein aktuelles und sicheres Backup aller wichtigen Daten existiert.

Kanzleien im Visier

Wer annimmt, dass nur große Unternehmen Ziele der Cyber-Kriminellen sind, liegt falsch. Denn wo Großunternehmen ganze Abteilungen von IT-Experten für ihre System-Sicherheit einsetzen, ist bei Kanzleien meist der externe IT-Fachmann am Zug, der nur bei Bedarf geordert wird. Jeder, der mit sensiblen Daten arbeitet, muss jedoch immer damit rechnen, ins Visier von Kriminellen zu geraten. Kanzleien sehen sich somit einem nicht zu unterschätzenden Risiko gegenüber.

Auch über die möglichen Folgen eines Cyberangriffs sind sich viele nicht klar. Mögliche direkte Kosten zum Beispiel für die Wiederherstellung von Daten sind zwar den meisten präsent. Bei einem Cyberangriff drohende wirtschaftliche oder rechtliche Folgen werden aber oft nicht berücksichtigt. Das ist die Erfahrung, die die Berater von HDI häufig bei ihren Kundenterminen machen. "Die wirtschaftlichen Konsequenzen zum Beispiel eines Betriebsstillstands oder schadensersatzrechtliche Folgen eines Hackerangriffs, der ermöglicht wird, weil die technischen Schutzvorrichtungen einmal nicht greifen, werden von vielen unterschätzt. Ganz zu schweigen von möglichen Imageschäden", weiß HDI Vermögensschaden-Haftpflichtexperte Bialek.

Restrisiko versichern

Bei diesem Restrisiko greift die Cyber-Versicherung. Sie springt ein, wenn trotz aktueller technischer Schutzmaßnahmen ein entsprechender Schaden entstanden ist. "Speziell für Selbstständige wie Rechtsanwälte, Wirtschaftsprüfer und Steuerberater haben wir deshalb unseren Cyber-Versicherungsschutz Cyberrisk angepasst", ergänzt der HDI Experte. Der Schutz ist als Zusatzdeckung zur Berufshaftpflicht konzipiert und springt sowohl bei Drittschäden ein, als auch bei Eigenschäden. Damit sind also Datenschäden, die einem Dritten entstehen oder Datenschutzverletzungen genauso versichert, wie der eigene Datenverlust oder die Kosten einer Betriebsunterbrechung.



Karl Bialek

© HDI Versicherung AG

Pressekontakt:

Andreas Ahrenbeck
Telefon: +49 511 645-4746
Fax: +49 511 645-4504
E-Mail: andreas.ahrenbeck@hdi.de

Unternehmen

HDI Versicherung AG
HDI-Platz 1
30659 Hannover

Internet: www.hdi.de

Über HDI Versicherung AG

Die HDI Versicherung AG bietet Sachversicherungslösungen für Privat- und Firmenkunden. Dabei reicht die Angebotspalette von Kfz-Versicherungen über private Haftpflicht- und Hausratversicherungen bis hin zu Komplettlösungen für kleine und mittlere Unternehmen sowie speziellen, berufsbezogenen Lösungen für Freie Berufe.

Die HDI Versicherung AG gehört zur Talanx-Gruppe. Talanx ist mit Prämieinnahmen in Höhe von rund 32 Milliarden Euro in 2015 und rund 22.000 Mitarbeiterinnen und Mitarbeitern eine der großen europäischen Versicherungsgruppen. Die Talanx AG ist an der Frankfurter Börse im MDAX sowie an den Börsen in Hannover und Warschau gelistet (ISIN: DE000TLX1005, WKN: TLX100, polnisches Handelskürzel: TNX).