«Quantencomputing ist noch *Zukunftsmusik*»

Ivo Heeb, Expert Underwriter im Bereich Cyber der Allianz Commercial, erklärt, warum Ransomware-Attacken niemals aufhören, Quantencomputing Anlass zur Sorge gibt und Datenschutz ein Thema der Cyberversicherung ist.

INTERVIEW: SANDRA WILLMEROTH

MIRJAM HAGEN

Zur Person

Ivo Heeb ist bei der Allianz Commercial in der Schweiz als Expert Underwriter für den Bereich Cyber & Technology verantwortlich. Er startete seine berufliche Laufbahn bei der Zurich im Bereich Financial Lines und verfügt über mehr als dreissig Jahre Berufserfahrung in der Versicherungsbranche. Nach einer Zwischenstation bei der ACE Group als Financial-Lines-Manager erfolgte 2009 der Wechsel zur Allianz Global Corporate & Specialty (AGCS).

Warum werden immer mehr kleine und mittlere Unternehmen Opfer von Cyberattacken?
Die grössten Schweizer Unternehmen haben in den letzten fünf Jahren sehr grosse Fortschritte im Bereich IT-Security gemacht. Sie tun, was möglich ist, um ihre IT-Infrastruktur zu schützen, und entsprechend schwer ist es für Cyberkriminelle, da überhaupt noch reinzukommen. Das hat dazu geführt, dass sich kriminelle Hackerbanden zunehmend auf das mittelständische Segment spezialisieren, weil dort bekannte Angriffspunkte oft nicht gepatcht sind und Sicherheitslücken nicht geschlossen werden. Man kann relativ einfach im Internet scannen, welche Firmen bestimmte Schwachstellen aufweisen. Man muss als Unternehmen also weder berühmt noch international bekannt sein, um in den Fokus von Cyberkriminellen zu geraten.

Im Cyberresilienz-Bericht der Allianz Commercial ist zu lesen, dass Ransomware-Attacken zurückgegangen sind. Ist es Zeit für eine Entwarnung?
Ransomware-Attacken sind zwar weniger geworden, aber sie werden niemals aufhören. Denn aufseiten der Angreifer hat sich da eine sehr gut funktionierende, arbeitsteilige Industrie entwickelt. Alle Elemente, die für eine Ransomware-Attacke notwendig sind, kann man ganz einfach im Darknet als Dienstleistung buchen. Es ist ein kriminelles Universum geworden, das sehr, sehr lukrativ ist und ein überschaubare Risiko hat, entlarvt zu werden, weil eine transnationale Verfolgung schwierig ist.

Auch das mobile Arbeiten bietet leichte Angriffsflächen für Hacker. Wie können Unternehmen ihre Systeme schützen?
Sie sollten ihren Mitarbeitenden für den Zugriff auf ihr Netz von extern die entsprechende Technologie in die Hand geben, beispielsweise eine Multifaktor-Authentifizierung und idealerweise auch von der Firma ständig auf dem neusten Stand gehaltene, sichere Geräte. Und mobiles Arbeiten setzt voraus, dass man die Leute entsprechend schult, sodass sie unterwegs vielleicht nicht jeden WLAN-Hotspot nutzen. Diese Sensibilisierung ist wirklich das A und O. Die Mitarbeiterinnen und Mitarbeiter müssen wissen, dass man nicht einfach so auf Links klickt und dass man keine Attachments öffnet, wenn man den Absender nicht kennt.

«Man muss nicht international bekannt sein, um in den Fokus von Cyberkriminellen zu geraten.»

«Aber das kostet ja alles so viel Zeit und Geld», höre ich da viele Unternehmer klagen. Wie viel darf ausreichender Cyberschutz ein Unternehmen kosten?
Da gibt es keine Faustregel, das sind Überlegungen, die jedes Unternehmen im Rahmen seines Risikomanagements anstellen muss. Da wird entschieden, welche Risiken das Unternehmen bei sich behält, welche Risiken mit entsprechenden Massnahmen reduziert werden und welche man auf den Versicherer überträgt. Leider sind im KMU-Bereich viele Firmen noch nicht so weit und fällen solche Entscheide eher aus dem Bauch heraus.

Was unter Umständen teuer werden kann?
Prävention lohnt sich extrem. Wir haben im Rahmen unserer Cyberresilienz-Studie festgestellt, dass Unternehmen, die auf Cyberangriffe vorbereitet sind und einen Angriff frühzeitig erkennen, um den Faktor 1000 profitieren. So gesehen beläuft sich ein Schadenfall nur auf 2000 Franken anstatt auf 2 Millionen Franken. Und dafür muss man nicht überall das Neueste und Beste haben, aber ein guter Grundschutz, der kostet nun mal was. Diese Investition ist wichtig und notwendig und auch eine Voraussetzung dafür, dass ein Unternehmen überhaupt eine Cyberversicherung abschliessen kann. Wenn gewisse Massnahmen im Unternehmen nicht umgesetzt werden, dürfte es schwer sein, einen Versicherer zu finden.

Warum sind die Prämien für einen Versicherungsschutz in den letzten Jahren so stark gestiegen?
Das Geschäft der Versicherer basiert auf sehr vielen Daten, und die gab es anfangs zu Cyberangriffen nicht. Obwohl es eigentlich schon länger Cyberschadenfälle gab, waren diese in den Systemen der Versicherungsgesellschaften nicht als solche gekennzeichnet. Darum war die Risikokalkulation zu Beginn eher ein Schuss ins Blaue. Man wusste nicht wahnsinnig viel über diese Risiken. Als dann relativ schnell viele und auch teure Schadenfälle auftraten, führte das zu einer ersten Korrektur und damit zu steigenden Prämien und steigenden Anforderungen an die Versicherungsnehmer.

Kann man jetzt mit einer Konsolidierung der Prämien rechnen?
Ja, zum Teil sehen wir sogar Reduktionen auf der Prämienseite. Das ist bedingt durch den Markteintritt von vielen neuen Cyberversicherern, die von den stark gestiegenen Prämien angezogen wurden. Aber diese neuen Versicherer haben im Gegensatz zu den etablierten Gesellschaften auch die vielen Schadenfälle in der Vergangenheit nicht gesehen und bezahlt. Wie sich das in Zukunft weiterentwickelt, hängt sehr stark von der weiteren Schadenentwicklung ab. Und ich denke, der eine oder andere Versicherer wird auch Mühe haben, entsprechend Geschäfte zu generieren. Obwohl die Nachfrage nach Cyberversicherungen stark ist, gibt es am Ende vielleicht doch nicht Platz für jeden Versicherer, der in diese Branche einsteigen möchte.

1000
Um diesen **Faktor** in der Schadenhöhe profitieren Firmen, wenn sie einen Cyberangriff frühzeitig erkennen.

Welche neuen Risiken rollen mit der Entwicklung von künstlicher Intelligenz (KI) auf uns zu?
Das Rennen um die Antwort auf die Frage, ob die Angreifer oder die Cybersicherheitsbranche von den Entwicklungen der KI profitieren wird, ist offen. Beide Seiten sind extrem interessiert an den Möglichkeiten, die KI bietet, weil mit der KI gewaltige Effizienzsteigerungen möglich sind – sowohl auf der einen als auch auf der anderen Seite. Daher möchte ich die Technologie nicht verteufeln, zumal wir als Versicherungsgesellschaft davon profitieren werden. Aber man muss wachsam bleiben, was das für die weitere Schadenentwicklung und besonders für die Art der Angriffe, die wir sehen werden, zur Folge haben wird.

Sind die Folgen von Deepfakes über eine Cyberversicherung gedeckt?
Nein, denn viele der KI-generierten Betrugsversuche, wenn sich beispielsweise jemand als CEO ausgibt und eine Zahlungsanweisung verlangt, sind nicht Gegenstand einer Cyberversicherung, sondern fallen unter die Vertrauensschadenversicherung, die bei uns auch in einer anderen Versicherungssparte angesiedelt ist.

Ist eine solche Vertrauensschadenversicherung automatisch Bestandteil der Unternehmensversicherungen?
Nein, normalerweise nicht. Es handelt sich um einen separaten Baustein, der die Folgen eines Diebstahls oder einer Veruntreuung durch Mitarbeitende sowie eines Betrugs durch Dritte deckt. In diesem Bereich gab es jüngst sehr viele Fälle, wo es Betrügern gelungen ist, Geldströme umzuleiten, indem die Bankverbindung geändert wurde. Auch Betrügereien mit gefakter Stimme würden darunterfallen.

Was ist mit den Möglichkeiten, die das Quantencomputing dem Betrug eröffnen könnte, was rollt da auf uns zu?
Quantencomputing ist noch Zukunftsmusik, könnte aber einen echten Einfluss auf die Schadenbelastung haben, weil wir momentan davon ausgehen müssen, dass eine solche enorme Rechenpower es den Angreifern ermöglichen wird, selbst bestens geschützte Systeme auszuhebeln und Verschlüsselungen und Passwörter in kürzester Zeit zu knacken. Im Moment haben wir noch keine solchen Fälle gesehen. Aber wir müssen dranbleiben, denn das macht uns schon Sorgen.

Die Allianz Commercial publiziert jährlich den Cyberresilienz-Bericht. Was sind derzeit die überraschendsten Erkenntnisse?
Dass sich der Fokus tendenziell weg von den klassischen Cyberangriffen hin zu Datenschutzverletzungen verschoben hat. Diese hängen teilweise trotzdem mit Ransomware-Attacken zusammen, da die Angreifer die Daten nicht nur verschlüsseln, sondern sie meistens auch noch klauen, bevor sie sie verschlüsseln, und dann mit der Veröffentlichung derselben Daten drohen, wenn das Unternehmen nicht bezahlt. Das ist dann ein Fall für die Datenschutzkomponente einer Cyberversicherung.

Und was verstehen Sie unter «Non Attack Data Breaches»?
Dabei geht es nicht um Cyberattacken durch Hacker, sondern um Fälle, bei denen Firmen eine Datenschutzverletzung begangen haben und dafür eingeklagt werden. Man mag staunen, dass solches unter einer Cyberversicherung gedeckt ist – dem ist aber so. Cyberversicherungen sind so gesehen sehr umfangreiche Datenschutzverletzungsversicherungen, sogar losgelöst vom Medium. Denn selbst wenn ein Unternehmen seine ganzen Kundendaten in Papierform verlieren sollte, ist das ein Datenschutzvorfall, der unter den Deckungsumfang einer Cyberversicherung fallen kann.

«Viele KI-generierte Betrugsversuche sind nicht Gegenstand der Cyberversicherung.»

Aber es wird doch erst ein Thema, wenn jemand mit einer Klage droht, oder nicht?
Nein, denn grundsätzlich muss jede Datenschutzverletzung vom Unternehmen selbst angezeigt werden. Und wenn man das nicht tut, riskiert man eine Busse. Daher sind Datenschutzverletzungen auch ohne Kläger sehr ernst zu nehmen. Unternehmen sind in der Pflicht, die entsprechenden Bestimmungen einzuhalten.