Versicherungsforen-**Themendossier**
Nr. 3/2021

Daten als Treiber:

Wie Versicherer mit dem »Öl des 21. Jahrhunderts« umgehen

Auszug

Cyberrisiken profitabel versichern –

Wie können Versicherer diese Herausforderung meistern

Versicherungsforen-**Themendossier**

Eine Publikation der

Versicherungsforen Leipzig

Cyberrisiken profitabel versichern – Wie können Versicherer diese Herausforderung meistern?

Das rasante Wachstum und die zunehmende Komplexität von Cyberkriminalität stellen weltweit eine große Herausforderung für die Versicherungsbranche dar. Schnell haben sich Cyberkriminelle auch die Situation während der Corona-Krise zunutze gemacht, um Unternehmen und öffentliche Einrichtungen mit Phishing-Mails, DDoS-Attacken und Ransomware anzugreifen.[1] Diese gefährliche Dynamik verleiht dem Markt für Cyberrisiken einen signifikanten Schub. Die Munich Re schätzt daher, dass der Markt weit über das bisher prognostizierte Volumen von 20 Milliarden US-Dollar im Jahr 2025 wachsen könnte. Daraus ergeben sich für Versicherer zwei grundsätzliche Fragen: Wie können sie ein profitables Cyber-Geschäft etablieren und welche Herausforderungen sind auf dem Weg dahin zu bewältigen?

Barrieren für zuverlässige Vorhersagemodelle

Obwohl der Bedarf an Schutz vor Cyberkriminalität deutlich steigt, gehen viele Versicherer diese Risikosparte noch sehr zögerlich an. Die Vorsicht rührt daher, dass Cyberrisiken sich nach herkömmlicher Auffassung deutlich von anderen Risiken unterscheiden, und daher schwierig zu versichern sind. Hier die wesentlichen Hürden aus Sicht der Versicherer:

Mangel an historischen Daten

Die Versicherungsbranche hat sich langsam entwickelt und einen riesigen Bestand an historischen Daten aufgebaut, mit denen sie Vorhersagen für die Zukunft treffen kann. Da die versicherungsmathematischen Modelle immer detaillierter geworden sind, haben sich auch die Underwriting-Entscheidungen verbessert und spiegeln eine immer realistischere Risikoeinschätzung wider. Im Gegensatz dazu sind Cyberattacken eine neue Art der Bedrohung, für die noch keine ausreichenden versicherungsmathematischen Daten vorliegen. Darüber hinaus verändern sich die Angriffsmethoden so schnell, dass die bisher gesammelten Daten schnell ihre Relevanz verlieren.

Breite Angriffsfläche von Cyberattacken

Cyberrisiko ist kein bloßes IT-Risiko, sondern ein unternehmensweites Risiko. Der Einsatz von 5G und die damit erzielte Konnektivität – etwa in Industrie 4.0-Umgebungen oder Lieferketten – führen dazu, dass Cyberrisiken sowohl Personen als auch Prozesse und Technologie betreffen. Dies macht es deutlich komplexer, Risiken und Abhängigkeiten zu verstehen.

Konfrontation mit einem aktiven Gegner

Hinter Cyberkriminalität stecken oft eigene Mitarbeiter oder ein Netzwerk von Cyberkriminellen im Untergrund. Ihre Motivation und Verhaltensmuster sind bei weitem undurchsichtiger als beispielsweise bei einer Person, die einen Diebstahl oder Betrug begeht.

---

1 BKA (2020): Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeSonderauswertungCorona2019.html

Potenzial für ein globales Kumulrisiko

Ein großer Cyberangriff könnte zu erheblichen individuellen Verlusten in allen Märkten führen. Bisher hat es noch keinen Cyberangriff gegeben, der groß genug war, um ein Rating-Ereignis zu werden, aber das Potenzial ist vorhanden. Viele Underwriter schätzen das systemische Risikopotenzial von Cyberattacken nicht richtig ein.

Bewertung von Risiken durch Cybercrime: Technologie als Startpunkt

Das Tempo, in dem sich Cybercrime entwickelt, erfordert Strategien, die über die üblichen versicherungsmathematischen Modelle hinausgehen. Ein Ansatz ist das IT-zentrierte Modell, das Profile der Cybersicherheit von Unternehmen erstellt, um sie dann mit den branchenweit besten Praktiken zu vergleichen. In einem detaillierten „Cyber Health Check" werden dabei Sicherheitssoftware, Verschlüsselungstools und andere Elemente der Cybersicherheit auf Unternehmensebene untersucht.

Dieser Ansatz kann eine wichtige Rolle beim Underwriting von Cyber-Versicherungen spielen, stößt aber auch an Grenzen. Erstens kann er nicht in großem Umfang eingesetzt werden. Er erfordert eine Innenansicht eines Unternehmens, was für den Einsatz auf Portfolioebene zu zeit- und kostenintensiv ist. Zweitens ist das menschliche Verhalten ein kritischer Faktor, den dieser Ansatz nicht berücksichtigt. Die Lizensierung der neuesten Cybersicherheitssoftware ist zum Beispiel keine Garantie dafür, dass die Mitarbeiter diese Tools auch richtig einsetzen. Versicherer müssen nicht nur verstehen, was auf technologischer Ebene geschieht. Vielmehr muss sich der Versicherer ein möglichst vollständiges Bild davon machen, wie das Thema insgesamt in einem Unternehmen adressiert und die Prävention implementiert wird.

Der nächste Schritt: Risikomodellierung mit Verhaltensanalysen

Um Risiken durch Cyberangriffe adäquat einzuschätzen, können Versicherer Methoden der Verhaltensanalyse (Behavioral Analytics) einsetzen. Dabei werden reale Expositions- und Akkumulationsdaten aus zahlreichen Unternehmen in großem Umfang gesammelt. Im nächsten Schritt lassen sich dann mithilfe von Machine-Learning- und KI-Methoden Echtzeitanalysen der sich verändernden Cyberumgebung erstellen.

Diese Vorgehensweise ermöglicht nicht nur, ein Profil der Technologiekompetenz einer Organisation zu erstellen, sondern auch Daten über unternehmensweite Faktoren wie Prozesse, Personalrisiken und die potenzielle Attraktivität für Cyberkriminelle zu erheben. Entscheidend ist, dass hierbei auch externe Daten verwendet werden – öffentliche Daten genauso wie Open-Source-Daten und Drittanbieter-Daten.

Eine präzise Verhaltensanalyse versetzt Versicherer in die Lage, die oben angeführten Hindernisse für eine Risikobewertung von Cyberangriffen zu überwinden. Behavioral Analytics bietet entscheidende Vorteile:

Riesige Datenmengen erlauben ein passgenaues Underwriting

Echtzeitdaten sind nicht begrenzt, wie dies bei historischen Daten der Fall ist. Jede Person oder Organisation hinterlässt im Internet einen digitalen Fußabdruck, der Hinweise auf den aktuellen Zustand in punkto Cybersicherheit liefert. Zu wertvollen Anhaltspunkten zählen hier zum Beispiel die Fluktuation in IT-Sicherheitsteams, die Patching-Kadenz für Software und das Vorhandensein ungenutzter Dienste. Behavioral Analytics nutzt diese Hinweise, um ein leistungsstarkes Vorhersagemodell zu erstellen, das regelmäßig aktualisiert und getestet wird.

Modelle berücksichtigen die große Angriffsfläche von Cyberangriffen

Verhaltensmuster-Modelle sammeln Daten über das gesamte Ökosystem einer Orga-

nisation hinweg, einschließlich Technologie, Prozesse und Faktoren wie menschliche Fehler oder Vorsatz. Sie behandeln Cyberangriffe als ein unternehmensweites Risiko und nicht nur als Technologie-Risiko.

Der aktive Angreifer wird analysiert und modelliert

Die Analyse von kriminellem Verhalten ist eine zentrale Komponente der Verhaltensmodellierung. Nicht selten gehen Cyberangriffe von einem verärgerten Mitarbeiter im Unternehmen aus. Deshalb verwendet die Verhaltensanalyse zum Beispiel Daten aus Umfragen zur Mitarbeiterzufriedenheit oder Daten zur Gehaltsstruktur als Schlüsselindikatoren für Cyberschwachstellen.

Kumulative Exposition wird quantifiziert

Bei jedem Risiko liegt der Schlüssel zum Verständnis von Kumulation darin, die gemeinsamen Fehlerlinien zu finden und diese auf Portfolioebene zu managen. Für Cyberrisiken ist das nicht anders. Risikoindikatoren sind hier zum Beispiel die Abhängigkeit von einem gemeinsamen Dienstleister oder die Verwendung der gleichen Version einer bestimmten Art von Software. Durch den Einsatz von Behavioral Analytics ist es möglich, Tausende dieser digitalen Versionen von Fehlerlinien zu identifizieren und Monte-Carlo-Simulationen durchzuführen.

Cyberattacken werden in Zukunft genauso zum Unternehmensalltag gehören wie die IT-Infrastruktur selbst. Der Wunsch der Unternehmen sich gegen diese Risiken abzusichern, eröffnet den Versicherern ein immer größer werdendes Marktpotential, das sie nutzen sollten. Moderne Methoden wie Behavioral Analytics spielen eine Schlüsselrolle, wenn es darum geht, Cyberrisiken profitabel zu versichern. Dafür muss Cybercrime jedoch in einem größeren Kontext betrachtet werden. Die heutige Welt ist technologiegetrieben, schnelllebig, stark vernetzt und dreht sich um immaterielle Werte wie Daten, Reputation, Marken und geistiges Eigentum. Die Versicherungsbranche hat bisher mit diesen Veränderungen nicht Schritt gehalten und bietet keinen ausreichenden Schutz für neue Risken des 21. Jahrhunderts.

Autor

René Schoenauer
Director Product Marketing
EMEA
Guidewire

Impressum

Autor(en) des vorliegenden Themendossiers
Vincent Wolff-Marting et al.
T +49 341 98988-284
E vincent.wolff-marting@versicherungsforen.net

Feedback zum vorliegenden Themendossier
Wenn Sie uns Ihre Meinung mitteilen möchten, würde uns das sehr freuen. Vielleicht gibt es ja ein spezielles Thema, über das Sie im Themendossier einmal lesen möchten? Haben Sie weitere Fragen und Anregungen oder Anlass zur Kritik? In jedem Fall freuen wir uns über eine Nachricht von Ihnen.

Bitte senden Sie Ihre Kommentare an
Elisa Strey
T +49 341 98988-235
E elisa.strey@versicherungsforen.net

Abonnement des Versicherungsforen-Themendossiers
Aufgrund der Partnerschaft Ihres Unternehmens mit den Versicherungsforen Leipzig steht Ihnen das Abonnement des Versicherungsforen-Themendossiers unternehmensweit zur Verfügung! Gern können Sie deshalb weitere Empfänger aus Ihrem Haus registrieren lassen. Nutzen Sie dazu einfach unser Anmeldeformular unter www.versicherungsforen.net/abo_themendossier. Eine Übersicht über alle Partnerunternehmen finden Sie unter www.versicherungsforen.net/partner.

Abbestellen des Versicherungsforen-Themendossiers
Sie wollen das Themendossier in Zukunft nicht mehr empfangen? Senden Sie einfach eine E-Mail mit dem Betreff „unsubscribe Themendossier“ an kontakt@versicherungsforen.net.

Downloadbereich mit aktuellen Zahlen und Fakten zur Versicherungswirtschaft
Im Downloadbereich unter www.versicherungsforen.net/daten-fakten finden unsere Partner aktuelle Zahlen, Daten und Fakten zu verschiedenen versicherungswirtschaftlichen Themen. Diese werden fortwährend erweitert und regelmäßig aktualisiert. Aussagekräftige Charts sorgen für einen schnellen und detaillierten Überblick über relevante Branchenthemen. Sie möchten diese Informationen in Ihre Präsentationen einbinden? Dann stellen wir Ihnen die Zahlen, Daten und Fakten gern im neutralen Power-Point-Format zur Verfügung, das Sie mit einem Klick in das eigene Corporate Design überführen können.

Versicherungsforen-Newsletter
Wenn Sie regelmäßig per E-Mail über Aktualisierungen im Bereich „Wissen“ auf www.versicherungsforen.net, Veröffentlichungen, gegenwärtige Veranstaltungen sowie Nachrichten aus unserem Partnernetzwerk informiert werden möchten, können Sie sich auf www.versicherungsforen.net/newsletter anmelden. Diesen Service bieten wir auch für Nicht-Partnerunternehmen kostenfrei an.

Ein Unternehmen der LF Gruppe | Hainstraße 16 | 04109 Leipzig |
T +49 341 98988-0 | **F** +49 341 98988-9199 | **E** kontakt@versicherungsforen.net | **I** www.versicherungsforen.net
Geschäftsführung: Dipl.-Math. Justus Lücke, Dipl.-Winf. Jens Ringel | Amtsgericht Leipzig HRB 25803 | Ust.IdNr.: DE268226821