Underwriting bei Cyber: „Die Risikofaktoren sind extrem dynamisch“

25. August 2025 Beitrag bearbeiten

Bildquelle: Daniel Roberts auf Pixabay

Im Bereich des Cyber-Schadenmanagements greifen bewährte Mechanismen des klassischen Versicherungsgeschäfts nicht, schreiben die Codecentric-Fachleute Marc Lenze und Kaan Soyyigit im Gastbeitrag für VWheute. Insbesondere die Risikobewertung berge Herausforderungen, denen sich das Underwriting stellen muss. Eine Bewertungsmatrix, Cyber-Sicherheitsschulungen sowie externe Expertise geben Underwritern an die Hand, was sie dafür benötigen.

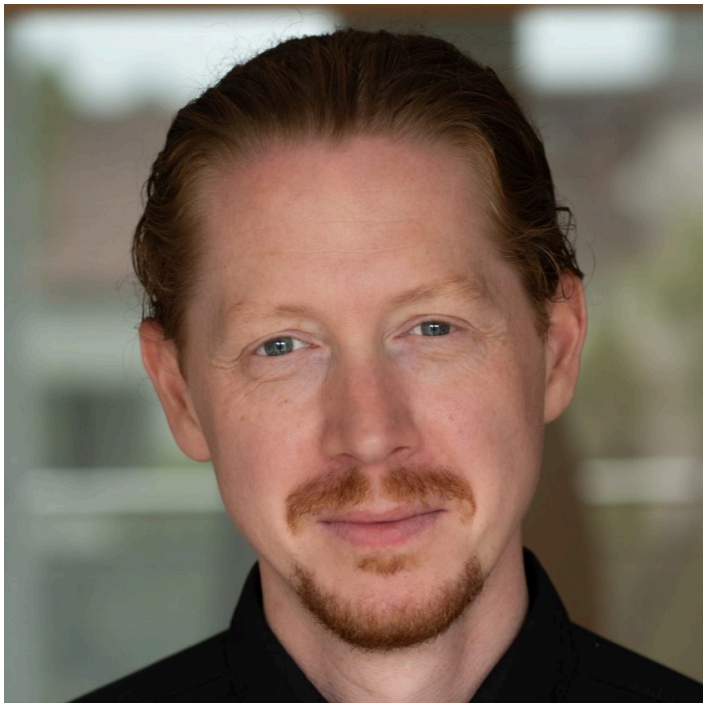
Die Risikobewertung im traditionellen Versicherungsgeschäft wie Sach-, Haftpflicht- oder Transportversicherungen und die darauf basierende Berechnung von Beiträgen sowie die Ausgestaltung von Policen und Verträgen basieren in der Regel auf zwei Säulen: jahrzehntelangen historischen Daten und verlässlichen statistischen Modellen. Risiken wie Feuer, Sturm oder Einbruch sind zwar im Einzelfall unvorhersehbar, in der Masse aber kalkulierbar.

Dabei verstehen Versicherungsunternehmen die Kausalitäten, können Risikofaktoren klar benennen und deren Eintrittswahrscheinlichkeit mit hoher Präzision berechnen. Underwriter haben so die Möglichkeit, anhand von Bauplänen, Sicherheitszertifikaten und Bilanzen eine ausreichend genaue Risikoeinschätzung vorzunehmen. Die Risikolandschaft

ist weitgehend statisch, verändert sich nur langsam und kann entsprechend gut angepasst werden.

Die neue Realität im Cyberraum: Dynamik, Komplexität und ein unsichtbarer Gegner

Das Cyber-Schadenmanagement bricht radikal mit diesen Prinzipien. Hier sehen sich Versicherer und Kunden nicht mit mehr oder minder statistischen Wahrscheinlichkeiten konfrontiert, sondern mit intelligenten Gegenspielern, die sich permanent und schnell anpassen: den Angreifern. Die Risikofaktoren sind extrem dynamisch.



Marc Lenze, Business Development Lead IT-Security bei Codecentric. Bildquelle: Unternehmen

Zusätzlich fehlt im Bereich der Cyberversicherungen eine ausreichende historische Datengrundlage. Während Brandschutzversicherungen beispielsweise auf eine Datenhistorie von 100 Jahren zurückgreifen können, gibt es für Cyberbedrohungen gerade einmal seit rund 10 Jahren relevante Aufzeichnungen, die aber heute schon mit hoher Wahrscheinlichkeit nicht mehr ausreichend relevant sind. Denn die Bedrohungslage im Bereich Cyberangriffe steigt und verändert sich kontinuierlich sowie schnell.

Hinzu kommt die extreme technische Komplexität, die für das klassische Underwriting eine erhebliche Herausforderung darstellt. Um die IT-Sicherheits-Reife eines Unternehmens wirklich beurteilen zu können, reicht ein Standardfragebogen nicht aus. Vielmehr sind hier tiefgreifendes technisches Fachwissen und Erfahrung erforderlich, was bei Underwritern nicht vorausgesetzt werden kann. Denn die Bewertung von Cyberrisiken ist eine völlig neue Disziplin, die auch eine neue Art von Expertise erfordert. Ein einfaches „Anpassen“ traditioneller Prozesse reicht nicht aus, um sich im Cyber-Schadenmanagement nachhaltig aufzustellen.

Allerdings ist die Frage, ob, wie und zu welchen Konditionen ein Unternehmen im Falle eines erfolgreichen Cyberangriffs versichert ist, von existenzieller Bedeutung für die Profitabilität und Zukunftsfähigkeit der Cyber-Versicherungssparte einerseits und für die Absicherung von Unternehmen gegen die Folgen von Cyberangriffen andererseits.

Zwischen Hoffnung und Realität: Die Grenzen aktueller Cyberversicherungen

So weiß jedes Unternehmen, das Opfer eines Cyberangriffs geworden ist, welche Folgen nicht ausreichende IT-Sicherheit mit sich bringen kann: Produktionsstillstand, Ausfälle im Vertrieb oder beim Kundenservice, Datenverlust oder Reputationsschäden, um nur einige zu nennen. Im schlimmsten Fall führen Cyberangriffe sogar in die Insolvenz.

Im Ernstfall „gerettet“ zu werden, ist für viele Unternehmen die Hauptmotivation zum Abschluss einer Cyberversicherung. In der Realität kann allerdings kein Versicherer garantieren, dass ein betroffenes Unternehmen einen Angriff bzw. dessen Folgen übersteht. Auch, wenn es vielen Unternehmen offenbar nicht bewusst ist: Eine Cyberversicherung ist kein Allheilmittel für die eigene IT-Sicherheit.

Der Abschluss einer Cyberversicherung beginnt mit der Risikobewertung. Sie bildet die Basis für die Versicherungspolice. Doch das Risiko wird meist mit einem rudimentären bzw. lückenhaften Fragebogen bewertet, den die Unternehmen mit dem Underwriter ausfüllen. IT-Sicherheitsexperten sind dabei in der Regel nicht anwesend. Diese Art der Risikobewertung führt schnell zu einer unpräzisen und unrealistischen Einschätzung.

Zwar erhalten Unternehmen damit in der Regel den gewünschten Versicherungsschutz, zahlen aber oftmals einen unangemessenen Versicherungsbeitrag oder wiegen sich durch die nicht korrekte Risikobewertung fälschlicherweise in Sicherheit. Hier liegt der Kern des Problems: Es wird ein schwer kalkulierbares wirtschaftliches Risiko versichert. Damit kann es schnell zu Unter- oder Überversicherungen kommen.

Deshalb mündet ein Cyberangriff trotz Versicherungsschutz für viele Unternehmen in der Nachverhandlung mit dem Versicherer. Denn die in der Regel sehr allgemein gehaltene Risikobewertung lässt nicht selten erheblichen Interpretationsspielraum auf beiden Seiten zu. Oft finden sich beide Parteien nach einem Angriff schnell in einem Einigungsverfahren vor Gericht wieder oder einigen sich außergerichtlich. Danach wird das Versicherungsverhältnis in vielen Fällen aufgelöst, was für beide Seiten unbefriedigend ist. Aber nicht nur bei den Versicherungsnehmern klaffen Erwartungshaltung und Realität in puncto Cyberversicherung in hohem Maße auseinander. Viele Versicherer beobachten steigende Schadenskosten und eine sinkende Profitabilität – in einem Markt, der eigentlich enormes Wachstumspotenzial verspricht.

Schwierige Risikokalkulierbarkeit

In der Regel führen beim Versicherer die Underwriter die Risikobewertung durch, aber nur wenige können auf langjährige Erfahrungen und die erforderliche Expertise im Bereich IT-Security zurückgreifen. Hinzu kommt, dass die Risiken der Unternehmen sehr unterschiedlich sind. Diese fehlende Vergleichbarkeit führt dazu, dass viele Cyberversicherungs-Policen entweder zu hoch oder zu niedrig angesetzt sind. Mit der

steigenden Anzahl an Cyberangriffen nimmt auch die Anzahl der Unternehmen zu, die Versicherungsleistungen in Anspruch nehmen. Das verstärkt die Unkalkulierbarkeit des Risikos für die Versicherer zusätzlich.

Was können Versicherer tun, um den Wachstumsmarkt Cyberversicherung wirtschaftlich sinnvoll zu bedienen?

Kaan Soyyigit, Market Lead Insurance bei Codecentric. Bildquelle: Unternehmen

Die Lösung all dieser Herausforderungen liegt großteils im Underwriting-Prozess selbst. Eine solide Basis ist nötig, auf welcher die Underwriter Cyberrisiken von Unternehmen bestmöglich bewerten können. Die allgemeine „Forensic Readiness“ ist sowohl für das Underwriting als auch das anfragende Unternehmen von entscheidender Bedeutung. Denn die Beantwortung der Frage „Wie gut ist das Unternehmen auf einen möglichen Angriff vorbereitet?“ steht in direkter Korrelation zu den möglichen späteren Kosten.

Matrix zur Risikobewertung etablieren:
Ohne Cybersecurity-Expertise geht es nicht

Eine Bewertungsmatrix bildet die solide Grundlage für die Ermittlung des IT-Sicherheits-Risiko-Score der anfragenden Unternehmen durch das Underwriting. Bei der Erstellung der Matrix gilt es, alle relevanten Themenbereiche zu betrachten. Dazu zählen beispielsweise Back-up & Wiederherstellung, Cloud-Sicherheit, Datenbank-Management, Notfallmanagement, Schwachstellen- & Patchmanagement, Identity & Access Management. Doch damit kennen sich die Underwriter in der Regel nicht aus. Deswegen ist es sinnvoll, sich für die Erstellung der Bewertungsmatrix fachliche Expertise und Unterstützung zu holen, beispielsweise bei IT-Dienstleistern, die über langjährige Erfahrungen in den Bereichen Cyberangriffe und Cyberabwehr verfügen.

Ist die Bewertungsmatrix erst einmal erstellt, sollte sie regelmäßig aktualisiert werden, um mit den Entwicklungen aufseiten der Angreifer mitzuhalten. Außerdem sollten die Underwriter regelmäßig in Sachen Cybersecurity geschult werden, um das nötige Grundverständnis für IT-Sicherheitsrisiken und ihre Bewertung zu haben. So entsteht im Underwriting Schritt für Schritt mehr Verständnis sowohl für die Funktionsweise der Matrix als auch das in ihr enthaltene fachliche Wissen.

Um nicht nur in der Theorie, sondern auch im praktischen Einsatz beim Kunden zu bestehen, ist es sinnvoll, dass der Sicherheitsexperte vom IT-Dienstleister den Underwriter – zumindest anfangs oder in besonders anspruchsvollen Fällen – bei Gesprächen zur Risikobewertung begleitet. Denn die zu bewertenden Unternehmen unterscheiden sich voneinander und ihre Infrastrukturen können sehr komplex sein. Expertise ist hier das A und O. Nur so sind Versicherer in der Lage, Risiken qualifiziert einzuschätzen. Damit sinkt ihr finanzielles Risiko und das Geschäftsmodell „Cyberversicherung“ ist erfolgreich für beide Seiten – Versicherung und Kunde.

Prävention zum Selbstschutz der Unternehmen

Zwar scheint die Bewertungsmatrix auf den ersten Blick vor allem das Risiko aufseiten der Versicherer zu minimieren, doch dieser Eindruck täuscht. Eine gute Risikobewertung durch das Underwriting zahlt auch auf die IT-Sicherheit der Unternehmen ein. Für viele Unternehmen ist die allgemeine Bedrohungslage sehr undurchsichtig. Die Idee, sich gegen einen Cyberangriff zu versichern, ist daher naheliegend und sinnvoll. Doch das reicht nicht aus.

Jedes Unternehmen muss verstehen, wo seine individuellen Cyberrisiken liegen, und sich mit passenden Maßnahmen im Rahmen eines Threat Informed Defense-Ansatzes – hier wird auf die individuelle Bedrohungslage und die entsprechende Absicherung eines Unternehmens fokussiert – vor Angriffen schützen. Das passiert allerdings aufgrund von Personal-, Zeit- und Budgetmangel oft nicht oder nicht in ausreichendem Maße.

Deswegen profitieren Unternehmen von einem fachlich gut aufgestellten Underwriter. Er zeigt ihnen im Rahmen der Risikobewertung, wo welche IT-Security-Präventionsmaßnahmen unmittelbar notwendig und sinnvoll sind. Vielleicht erhalten Unternehmen auf diesem Wege im ersten Schritt keinen Versicherungsschutz, sondern eher einen Aufgabenkatalog, der für den Erwerb des Schutzes erfüllt werden muss. Mittelfristig erhöht diese Vorgehensweise aber ihr Schutzniveau, weil Awareness und Akzeptanz für präventive IT-Sicherheitsmaßnahmen deutlich zunehmen. Setzen sie die erforderlichen Maßnahmen um, sind sie entsprechend abgesichert und bekommen ihre Cyberversicherung unter Umständen sogar günstiger.

Fazit

Sowohl für Unternehmen als auch für Versicherer hat ein fachlich und prozessual gut aufgestelltes Underwriting für Cyberversicherungen enorme Vorteile. Für Versicherer ist es vor allem wirtschaftlich wichtig und von Vorteil, in die Cyberkompetenz ihrer Underwriter und eine realistische Risikobewertung mittels Bewertungsmatrix zu investieren. Die versicherten Unternehmen profitieren von einem höheren Schutzniveau, weil sie ihre individuellen Risiken erkennen, zielgerichteter präventiv absichern und im Falle eines Falles über ihre Cyberversicherung richtig abgesichert sind. Eine Win-win-Situation für beide Seiten entsteht: zufriedene Versicherer und Versicherungsnehmer.

Autoren: Marc Lenze, Business Development Lead IT-Security; Kaan Soyyigit, Market Lead Insurance; beide bei Codecentric

---