Dynamische Bedrohung und Versicherungsschutz: Aktuare im Kampf gegen Cyberrisiken

Die nahezu täglich nachzulesenden Berichte über Cyberangriffe auf unterschiedlichste Ziele zeigen, dass sowohl Unternehmen als auch die gesamte Gesellschaft mit einer dynamischen und stetig wachsenden Bedrohungslage konfrontiert sind. Insbesondere das Potenzial für systemische Cyberereignisse bzw. für Kumulereignisse, also für Ereignisse, die viele Versicherungsnehmer gleichzeitig betreffen, erfordert ein tiefgehendes und umfassendes Risikoverständnis, um den Versicherungsnehmern zuverlässigen Versicherungsschutz anzubieten. Die Entwicklung von unternehmensspezifischen, sogenannten Realistic Disaster Scenarios (RDS) ist eine Option, die Auswirkungen von sehr schweren, mit geringer Wahrscheinlichkeit eintretenden Cyberkatastrophen auf das Portefeuille eines Versicherungsunternehmens zu analysieren.

Seit Entwicklung der ersten Cyberpolice im Jahr 1999 durch Lloyd's hat sich der Cyber-Versicherungsmarkt beachtlich weiterentwickelt: Weltweit stieg die Cyberprämie 2023 auf 16,7 Milliarden USD und es wird weiterhin mit starkem Wachstum gerechnet. Auch im deutschen Versicherungsmarkt nimmt die Bedeutung stetig zu und mittlerweile gehört der Abschluss einer Cyberversicherung insbesondere bei größeren Unternehmen zur Regel. Zwar befindet sich die Cyberversicherung im deutschen Markt mit gebuchten Bruttobeiträgen in Höhe von 249 Mio. EUR 2022 im Vergleich zur gesamten Schaden- und Unfallversicherung mit gebuchten Bruttobeiträgen in Höhe von 79,3 Mrd. EUR immer noch auf einem geringeren Niveau, jedoch bleiben die Wachstumsraten im hohen zweistelligen Prozentbereich.

Die Profitabilität variiert bisher: Nachdem 2021 Gewinnerwartungen im deutschen Markt unerfüllt blieben (Schaden-Kosten-Quote: 123,7 %), konnte die Profitabilität 2022 nach einer Marktverhärtung deutlich verbessert werden (Schaden-Kosten-Quote: 77,7 %).[1]

Was ist in der Cyberversicherung versichert?

In der Cyberversicherung werden Informationssicherheitsverletzungen versichert, also Verletzungen der Integrität, der Vertraulichkeit oder der Verfügbarkeit von Daten. Die Versicherung umfasst typischerweise Eigenschäden, beispielsweise Schäden durch Betriebsunterbrechung oder aber Kosten für die Datenwiederherstellung, Drittschäden, beispielsweise Entschädigungsleistungen an Kunden wegen Datenverlust, und Kostenkomponenten bzw. Serviceleistungen, beispielsweise Kosten für IT-Forensiker zur Analyse und Schadensbegrenzung oder Anwaltskosten.

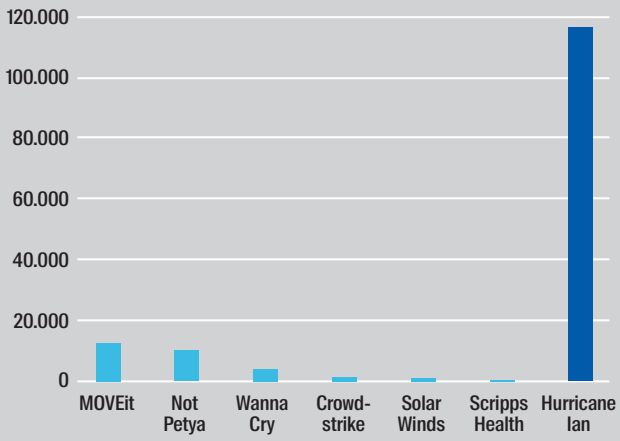
Durch die Vernetzung ist keine regionale Begrenzung für Schäden gegeben und das Kumulpotenzial ist somit im Vergleich zu anderen Sparten signifikant höher. Auch wenn die Versicherungswelt glücklicherweise bisher keine Cyberkatastrophen gesehen hat, so sind Szenarien mit weltweitem Ausmaß und systemischem Charakter denkbar.

Die Gefahr ist menschengemacht, daher sind wesentliche Bestandteile der Analyse immer auf potenzielle Akteure und Verursacher ausgerichtet. Es gibt einerseits bösartige Angreifer wie ökonomisch getriebene Ransomware-Gruppen oder staatliche Akteure im Rahmen eines Cyberkriegs oder -angriffs. Andererseits sind aber auch Fehler wie Software Bugs, falsche Bedienung oder Konfiguration von Software oder misslungene Angriffe mögliche Auslöser.

Naturkatstrophen stellen derzeit für die Versicherungswirtschaft das mit Abstand größte Schadenpotenzial dar, jedoch ist im Vergleich zu bedenken, wie sich Cyberschäden zukünftig bei stärkerer Versicherungsdurchdringung und steigender Vernetzung entwickeln werden. Selbst im Vergleich volkswirtschaftlicher Schäden bestehen aber noch große Abstände.

1) https://www.gdv.de/gdv/medien/medieninformationen/cyberversicherer-kehren-in-die-gewinnzone-zurueck-markt-waechst-weiter--147652

Vergleich volkswirtschaftliche Schäden aus ausgewählten Cyberereignissen und maximaler versicherter Hurrikan-Schaden (Angaben in Mio. USD)



Quelle: eigene Darstellung

Was und wie können RDS beitragen?

Aufgrund der geringen Schadenerfahrung, insbesondere der bisher nicht existenten Schadenerfahrung für größere Kumule, stellen RDS eine adäquate Methode dar, um sich der Gefahr Cyber und ihrem Kumulpotenzial aus aktuariellem Blickwinkel zu nähern. Die schnelle Dynamik, bedingt durch sich anpassende Angriffsvektoren und eine sich wandelnde Produktlandschaft kann rasch in RDS eingebettet werden.

Das Konzept von RDS wurde 1994 insbesondere durch Lloyd's geprägt und wird bis heute als Methode für die Einschätzung von Akkumulationsrisiken (z.B. emerging risks, Naturkatastrophen-, Terror- oder Pandemierisiken) bei Versicherungsunternehmen verwendet.[2] Ziel ist ein detailliertes Narrativ von extremen Ereignissen zu entwickeln, die mit einer geringen, aber nicht zu vernachlässigenden Wahrscheinlichkeit eintreten können. Diese detaillierten Narrative ermöglichen eine Abschätzung des zugehörigen Schadens für das Versicherungsunternehmen. Dabei sollen die möglichen Ereignisse einerseits realistisch, andererseits individuell auf das jeweilige Risikoprofil des Versicherungsunternehmens zugeschnitten sein. Tatsächlich ist die Abschätzung der Eintrittswahrscheinlichkeit des Ereignisses außerordentlich relevant für die gesamte Risikoeinschätzung. Die relevanten Parameter sollen anhand einer realistischen Einschätzung konkretisiert und insbesondere gut begründet hergeleitet werden.

Der Einsatz von RDS bietet eine Vielzahl von Vorteilen in Versicherungsunternehmen, sie können für verschiedenste Anwendungsbereiche Unterstützung bieten. Einsatzmöglichkeiten der RDS-Methodik erstrecken sich von der Underwriting-Entscheidung (u. a. Risikoauswahl), über Pricing, Risikomanagement und Unternehmenssteuerung bis hin zur Quantifizierung der Risiko-Mitigation (z. B. Rückversicherung).

Im Prozess der Anwendung eines RDS gilt es, einige Vorteile nutzbar zu machen bzw. Besonderheiten zu beachten. In der Phase der Erstellung eines RDS ist die Individualisierung auf das eigene Unternehmen in adäquater Detailgenauigkeit und Tiefe die Grundlage für den späteren Umfang des Erkenntnisgewinns. Eine unternehmensübergreifende Zusammenarbeit bei der Erstellung ermöglicht auch spartenübergreifende Aussagen, die Szenarien können derart ausgestaltet werden, dass Schäden aus verschiedenen Sparten oder Versicherungsformen zur Schätzung beitragen. Diese umfassenden Szenarien sind häufig einfach in der Kommunikation auf einer höheren Detailebene und erlauben somit gute Abstimmung, bspw. zwischen Management und Fachabteilungen. Die vergleichsweise einfache Nachvollziehbarkeit der Methode ermöglicht zudem eine transparente Kommunikation und Zusammenarbeit. Katastrophenszenarien sollten in ihrer grundsätzlichen Ausgestaltung weitestgehend stabil bleiben. Dennoch bringen eine regelmäßige Wiederholung und Überprüfung möglicherweise neue Erkenntnisse, die andernfalls ausgeblieben wären.

Aufgrund dieser und weiterer Vorteile finden RDS auch bei der Analyse des Cyberrisikos Verwendung. Es gibt unter anderem prominente Beispiele von Lloyd's sowie das Cyber-Stress-Test-Szenario der EIOPA.

Eine besondere Herausforderung in der Sparte Cyber ist der große Abstand zwischen realen Ereignissen und den modellierten Katastrophen. Wie eingangs beschrieben, gibt es keine Schadenerfahrung für größere Kumule und damit können die Schätzungen nicht auf vergangenen Ereignissen beruhen. Von erhöhter Bedeutung für RDS im Segment Cyber ist zudem die oben beschriebene regelmäßige Wiederholung und Überprüfung der Schätzung. Durch die hohe Dynamik in der Gefahr Cyber neigen RDS hier zu einer höheren Änderungsrate als andere Sparten. Aufgrund der fehlenden Erfahrung und hohen Dynamik ist daher in Cyber die Auswahl von repräsentativen Szenarien nicht offensichtlich, die einerseits die Betroffenheit für individuelle Stakeholder bis hin zum gesamten Markt ermöglichen und damit alle für das Unternehmen entstehenden Risiken einschätzen lässt.

2) Lloyd's of London, UK; internationaler Versicherungsmarkt für Sach- und Rückversicherung

Dennoch haben sich im Markt ein paar wenige Szenarien als Standard herausgebildet, die bekanntesten Beispiele sind: Ransomware-Angriffe (Contagious Malware), der Ausfall von externen Service-Providern (z. B. Cloud-Infrastruktur) oder aber groß angelegte Datendiebstähle. Das Ransomware-Szenario reflektiert dabei hauptsächlich Schäden resultierend aus Betriebsunterbrechung, d. h. der Eigenschadenkomponente. Der Ausfall von externen Service-Providern berücksichtigt Haftungsrisiken einerseits für den Provider sowie andererseits für die ausfallende Partei beim Servicenehmer. Groß angelegte Datendiebstähle spiegeln das Schadenpotenzial in der Drittschadenkomponente der Cyberversicherung wider.

Ein weiteres, im EIOPA Stresstest enthaltenes Szenario ist Power Outage, also ein weitreichender Verlust der Energieversorgung. Allerdings ist dies in Überschneidung mit der Sachversicherung zu sehen, da hier Cybergefahren nur einen möglichen Auslöser unter vielen darstellen.

Neben der Einschätzung von Akkumulationsschäden eignen sich die Ansätze von RDS auch für die Entwicklung sowie die Validierung von Cybermodellen. Cybermodelle beruhen aufgrund der eingeschränkten Schadenhistorie nur für den sogenannten Frequenzbereich, d. h. für häufige Ereignisse, auf realen Schadendaten. Gerade im Bereich des Tails, also der sehr seltenen Ereignisse, handelt es sich auch in den Modellen meist um szenariobasierte Schätzungen, die mit davon unabhängig konstruierten RDS validiert werden können. Hierfür notwendig ist u. a. eine Einschätzung zur Wahrscheinlichkeit des Auftretens solcher Ereignisse. Da es sich aber um Extremereignisse ohne Historie handelt, ist dies mit hoher Modellunsicherheit verbunden und bringt stark ausgeprägte Sensitivitäten mit sich. Gleichzeitig muss berücksichtigt werden, dass die Frequenz eine zentrale Annahme im gesamten RDS ist. Insofern ist diese Annahme außerordentlich fundiert zu begründen.

Neben der eigenen Entwicklung von RDS für Cyber in Versicherungsunternehmen besteht auch die Möglichkeit, diese von Drittanbietern einzukaufen. Die bekannten Anbieter für Cybermodellierung offerieren häufig neben der Berechnung des Gesamtrisikos auch die Möglichkeit, individuelle RDS zu modellieren. Hierbei kann der Anwender teilweise auch Einfluss auf die Szenariogestaltung oder die Parameter nehmen.

Die Schadenschätzung wird mittels Bottom-Up-Methodik ermittelt. Zuerst wird dazu der Schaden geschätzt, der bei den versicherten Unternehmen entsteht (ground-up). Danach muss dazu die Versicherungsstruktur bewertet werden: Welche Schäden werden durch den Versicherer getragen (Anwendung von Selbstbehalt und (Sub-)Limiten), welche werden weitergegeben (z. B. Rückversicherung)? Diese Bottom-up-Analyse ermöglicht die Verwendung der Methodik auch in der Zukunft, wenn die Deckungsfaktoren sich verändern oder weitere vom Schaden Betroffene (versicherbare Marktteilnehmer) ins Portfolio aufgenommen werden.

Generell eignet sich zur Evaluation auch die Hinzunahme von ökonomischen bzw. Markt-Schadenschätzungen für die gewählten RDS. Diese eröffnen weitere Plausibilisierung, Vergleiche der Zeichnungsstrategie mit dem generellen Markt und weitere interessante Management Informationen über eine Top-down-Analyse.

Fazit und Ausblick

Die inhärente Dynamik von Cyberrisiken macht es unerlässlich, sich mit möglichen, denkbaren, in der Zukunft auftretenden Szenarien zu beschäftigen. Schadenerfahrung, selbst wenn sie verfügbar wäre, veraltet schnell. Schon absehbare Entwicklungen sind ein Fortschreiten der Vernetzung, insbesondere auch weiter in den Bereich der Alltagsgegenstände, sowie eine weitere Standardisierung von genutzter Software. Damit gehen eine vergrößerte Angriffsfläche und ein größeres Kumulpotenzial einher. Die Versicherungswirtschaft ist vorbereitet, hier eine zentrale Rolle zu spielen, weitere Lösungen für Extremszenarien wie Public-Private-Partnerships oder Government-Backstops werden in vielen Ländern diskutiert.

Aktuare können hier mit ihrem besonders geschulten Blick auf Risiken einen wertvollen Beitrag leisten und diese Cybergefahr hinsichtlich Versicherbarkeit, Kumulpotenzial und Profitabilität für ein Versicherungsunternehmen untersuchen. Dies geschieht zumeist mit bekannten Methoden, die allerdings angepasst und adäquat eingesetzt werden müssen, um den Besonderheiten der Gefahr Cyber Rechnung zu tragen. Insbesondere bereitet den traditionellen aktuariellen Methoden der existierende Mangel an repräsentativer Schadenerfahrung Probleme.

Ein möglicher großer Einfluss auf der technologischen Seite ist die Entwicklung von künstlicher Intelligenz (KI). Auf der Angreiferseite kann KI genutzt werden, um großflächig automatisierte Angriffe zu ermöglichen. Gleichermaßen kann KI auf der Verteidigerseite eingesetzt werden, um automatisiert mögliche Angreifer zu entdecken und erfolgreich abzuwehren.

Insgesamt ist das Segment Cyber eine spannende Herausforderung für die aktuarielle Welt. Hier bietet sich die Möglichkeit, neue Methoden zu entwickeln und bewährte auf den Prüfstand zu stellen.