Swiss Re
Institute

Medienmitteilung

Neue *sigma*-Studie von Swiss Re: Trotz ihrer Komplexität können Versicherer und Unternehmen Cyber-Risiken bewältigen; offizielle Eröffnung des Swiss Re Institute

- Die möglichen Kosten von Cyber-Angriffen steigen rasant; Cyber-Sicherheit und Cyber-Widerstandsfähigkeit werden für Unternehmen immer wichtiger
- Der Markt für Cyber-Versicherungen entwickelt sich rasch weiter, doch der Deckungsumfang ist noch relativ gering
- Produkt- und Prozessinnovationen sowie Big Data und Smart Analytics werden die Entwicklung von verbesserten Cyber-Versicherungslösungen unterstützen
- Regierungen können eine wichtige Rolle bei der Stärkung der Cyber-Widerstandsfähigkeit spielen
- Dies ist die erste Studie des Swiss Re Institute, das heute offiziell eröffnet wird

Zürich, 1. März 2017 – Cyber-Risiken stellen für Unternehmen eine wachsende Bedrohung dar, zumal die jüngsten Angriffe zeigen, dass die Kosten im Fall eines Cyber-Angriffs die Schäden im Zusammenhang mit verlorenen oder beschädigten Daten deutlich übersteigen können. Laut der neuesten *sigma*-Studie von Swiss Re, «Cyber: Bewältigung eines komplexen Risikos», müssen Unternehmen noch viel mehr tun, um die Cyber-Sicherheit in ihre Risikomanagementstrategie zu integrieren. Initiativen zur Stärkung der Cyber-Widerstandsfähigkeit gibt es bereits. Der Markt speziell für Cyber-Versicherungen entwickelt sich zwar rasant weiter, doch der Deckungsumfang im Verhältnis zur möglichen Exposition ist bislang noch relativ gering. Produkt- und Prozessinnovationen sowie moderne Analysetechnologien werden die Entwicklung verbesserter Cyber-Versicherungslösungen unterstützen und die Grenzen der Versicherbarkeit wie auch den Deckungsumfang erweitern. Letztlich bleiben jedoch einige Cyber-Risiken, vor allem solche im Zusammenhang mit extremen, katastrophalen Schadenereignissen möglicherweise unversicherbar.

Gross angelegte Cyber-Angriffe aus der jüngsten Vergangenheit zeigen vermehrt, dass die Kosten, die durch Lücken in der Cyber-Sicherheit entstehen, weit über die Schäden im Zusammenhang mit verlorenen oder beschädigten Daten hinausgehen. Unternehmen müssen nun auch die möglichen Schäden an Reputation, Sachwerten oder geistigem Eigentum sowie Unterbrechungen des Geschäftsbetriebs einkalkulieren.

Der zunehmende Umfang und das wachsende Ausmass potenzieller Kosten durch Cyber-Vorfälle sind eine Folge der sich kontinuierlich

Darren Pain, Zürich
Telefon +41 43 285 2504

Kurt Karl, Armonk
Telefon +1 914 828 8686

Jonathan Anchen, Bangalore
Telefon +91 80 4900 2650

Investor Relations, Zürich
Telefon +41 43 285 4444

Swiss Re AG
Mythenquai 50/60
Postfach
CH-8022 Zürich

Telefon +41 43 285 2121
Fax +41 43 285 2999

www.swissre.com
@SwissRe

weiterentwickelnden Cyber-Risikolandschaft, die von drei wichtigen Faktoren geprägt wird:

- Steigende Geschwindigkeit und zunehmendes Ausmass des digitalen Wandels
- Zunahme der Schwachstellen durch Hyperkonnektivität angesichts der rasanten Verbreitung von beispielsweise internetfähigen Geräten und Cloud-Computing
- Weiterentwicklung von Hackern, die sich der möglichen wirtschaftlichen Vorteile erfolgreicher Cyber-Angriffe bewusst sind

Trotz des erhöhten Bewusstseins in Bezug auf die Gefahren sind Unternehmen in der Regel schlecht auf die Bewältigung von Cyber-Risiken vorbereitet. Relativ wenige Unternehmen haben Cyber-Sicherheitslösungen fest in ihre Risikomanagementstrategie integriert. Angesichts der bevorstehenden neuen Gesetzgebung in vielen Ländern, unter der die Unternehmen zur Umsetzung höherer Datenschutzmassnahmen gezwungen werden, könnte sich die Regulierung als Katalysator für einen Wandel erweisen. In der Folge «müssen Unternehmen – grosse wie kleine – mehr in ihre Cyber-Sicherheitsarchitektur investieren, um ein solides Risikomanagement vor und nach einem Schaden zu entwickeln», erklärt Kurt Karl, Chefökonom bei Swiss Re.

Bewältigung eines komplexen Risikos

Viele Unternehmen erwägen die Übertragung ihrer Cyber-Risiken auf Dritte, die diese besser absorbieren können. «Derzeit entwickelt sich ein spezieller Markt für Cyber-Versicherungen mit einer wachsenden Zahl von Versicherern, die sich in dieser Nischensparte weiter etablieren wollen», so Kurt Karl. Spezielle Cyber-Versicherungen bieten in der Regel einen grundlegenden Schutz vor Daten- und Netzwerkverletzungen sowie damit verbundenen Schäden mit Kapazitätsgrenzen auf dem Markt von aktuell rund 5 bis 100 Millionen USD. Einige bedeutende Cyber-Risiken bleiben jedoch weitgehend unversichert, und der bestehende Deckungsumfang ist im Vergleich zur möglichen Gesamtexposition der Unternehmen gering.

Ein wesentliches Hemmnis für die Entwicklung von Versicherungslösungen ist eng mit den naturgemässen Eigenschaften von Cyber-Risiken verbunden. Diese sind komplex und nur schwer zu quantifizieren, insbesondere angesichts des sich schnell verändernden technologischen Umfelds und des Mangels an historischen Daten zu Cyber-bedingte Schäden, aus denen Informationen über mögliche zukünftige Schäden abgeleitet werden können. In einem Versuch, die potenziellen Schäden von Cyber-Ereignissen abzuschätzen, experimentieren Versicherer und Risikoanalysten mit verschiedenen Ansätzen zur Modellierung von Cyber-Risiken, darunter deterministische Szenarioanalysen und probabilistische Modelle.

Die Erfahrung aus dem Umgang mit anderen Gefahren wie Naturkatastrophen lässt darauf hoffen, dass durch ein besseres Verständnis

der grundlegenden Risikofaktoren und die Verfügbarkeit umfangreicherer Daten zu Cyber-Schäden geeignetere Modelle entwickelt werden können.

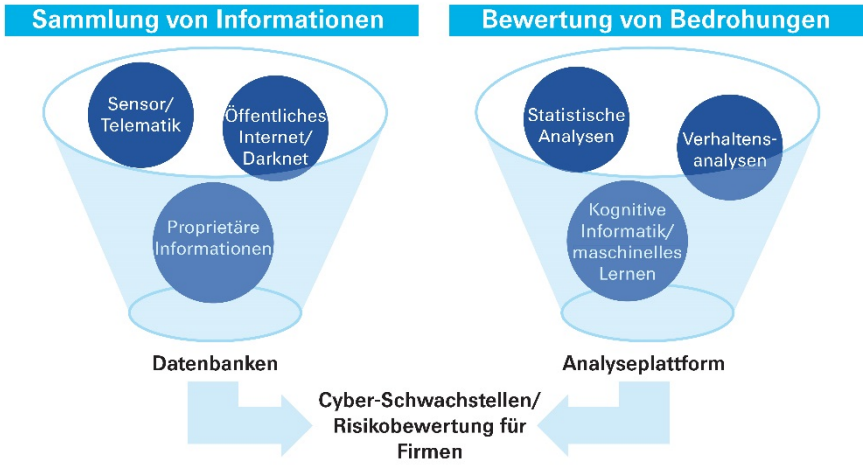
Produkt- und Prozessinnovationen

Bis dahin werden Produkt- und Prozessinnovationen im Versicherungswesen sowie andere Risikotransfermechanismen eine wichtige Rolle bei der Verbesserung des Cyber-Risikomanagements spielen. Ein wichtiger Faktor mit Einfluss auf das Innovationstempo wird die Erfassung und Analyse relevanter Daten und Informationen zur präzisen Bewertung von Cyber-Risiken sein. In der Branche gibt es ständige Entwicklungen zur verbesserten Erfassung und Verbreitung von Informationen. So haben zum Beispiel mehrere Risikoanalysten Datensysteme entwickelt, die Unternehmen einen standardisierten Ansatz zur Identifizierung, Quantifizierung und Meldung von Cyber-Risiken- an Versicherer ermöglichen.[1] In ähnlicher Weise setzt sich das CRO Forum für eine gemeinsame Sprache und allgemeine Rahmenbedingungen für Unternehmen zur Erfassung der wichtigsten Informationen über Cyber-Vorfälle und -Schwachstellen ein.

Die Versicherer wiederum treiben die Entwicklung von weniger komplexen und flexibleren Versicherungsprodukten voran. Dies beinhaltet die Entwicklung von Produkten speziell für kleine und mittlere Unternehmen, die versicherungstechnisch bislang benachteiligt waren und bei der Bewältigung von Cyber-Risiken oft weniger gut aufgestellt sind als grössere Unternehmen. Darüber hinaus erwägen einige (Rück-)Versicherer Partnerschaften mit Cyber-Sicherheitsfirmen und Anbietern von Datenanalysen, um Wissenslücken zu schliessen und ihren Kunden umfassendere bzw. zusätzliche Dienstleistungen bieten zu können. Moderne Analysetechnologien können die traditionellen Versicherungsinstrumente der (Rück-)Versicherer ergänzen und ihnen eine schnelle Reaktion auf die sich rasch verändernden zugrunde liegenden Risikofaktoren ermöglichen.

[1] Siehe zum Beispiel A. Russell, RMS Launches New Data Standard for Managing Cyber Insurance, rms.com, 19. Januar 2016, https://www.rms.com/newsroom/press-releases/press-detail/2016-01-19/rms-launches-new-data-standard-for-managing-cyber-insurance, und Verisk Cyber Exposure Data Standard and Preparer's Guide, air-worldwide.com, 2016, https://www.air-worldwide.com/Documentation/Cyber-Exposure-Data-Standard/air_cyber_exposure_data_schema_and_preparers__guide.htm

Abbildung 1: Smart Analytics als ergänzendes Versicherungsinstrument



Quelle: Swiss Re Economic Research & Consulting.

Eine weitere Möglichkeit zur Erhöhung der Versicherungskapazität von Cyber-Risiken stellt die Entwicklung von Anlageinstrumenten dar, die den Kapitalmarktinvestoren die Übernahme eines Teils des Risikos ermöglicht. Es gibt derzeit einige Initiativen zur Entwicklung von Versicherungsverbriefungen (sogenannte «insurance-linked securities», ILS), die operative Risiken wie Cyber-Gefahren abdecken. Der ILS-Markt für Cyber-Risiken steht noch am Anfang, könnte in der Zukunft aber wachsen.

Unterstützende Rolle von Regierungen

Um die Grenzen der Versicherbarkeit zu erweitern, müssen Unternehmen zusammen mit ihren Versicherern am Aufbau eines nachhaltigen Markts arbeiten. Auch Regierungen spielen eine wichtige Rolle bei der Stärkung der Cyber-Widerstandsfähigkeit. Dies umfasst auch Massnahmen zur Verbesserung der Erfassung und Verbreitung von Cyber-Informationen sowie die Verabschiedung von Gesetzen und Vorschriften zur Nutzung und zum Schutz des Cyberspace. Durch die Neugestaltung von Anreizen und die Steigerung des Bewusstseins für Cyber-Bedrohungen können Regierungen den privaten Sektor weiter in Richtung verbesserter marktorientierter Lösungen anstossen. Trotzdem könnte das mögliche Ausmass einiger Cyber-Schäden letztlich zu gross für den privaten (Rück-)Versicherungssektor sein. Dies gilt vor allem für Ereignisse mit Spitzenschäden, wie beispielsweise eine schwere Störung kritischer Infrastrukturen oder Netze, die zu erheblichen Kumulschäden führen könnten.

Swiss Re
Institute

Dies ist die erste *sigma*-Ausgabe, die unter dem Banner «Swiss Re Institute» veröffentlicht wird. Das Swiss Re Institute wird am 1. März 2017 offiziell eröffnet mit dem Ziel, die Position von Swiss Re als Vordenker in der Branche zu festigen und die zahlreichen Forschungs- und Öffentlichkeitsinitiativen des Unternehmens zu bündeln. Das Swiss Re Institute erstellt die Forschungsstudien von Swiss Re, einschliesslich *sigma*, der führenden Forschungspublikation der Versicherungsbranche.

Bemerkungen für die Redaktionen

Swiss Re
Die Swiss Re Gruppe ist ein führender Wholesale-Anbieter von Rückversicherung, Versicherung und anderen versicherungsbasierten Formen des Risikotransfers. Die von Swiss Re direkt oder über Broker betreuten internationalen Kunden sind Versicherungsgesellschaften, mittlere bis grosse Unternehmen und Kunden des öffentlichen Sektors. Swiss Re nutzt ihre Kapitalstärke, ihre Fachkompetenz und ihre Innovationsfähigkeit zur Entwicklung von Lösungen, die von Standardprodukten bis hin zu ausgeklügelten kundenspezifischen Versicherungsdeckungen für sämtliche Geschäftssparten reichen und das Eingehen von Risiken ermöglichen, was für Unternehmen und den allgemeinen Fortschritt von wesentlicher Bedeutung ist. Swiss Re wurde 1863 in Zürich gegründet und ist über ein Netz von Gruppengesellschaften und Vertretungen an rund 70 Standorten präsent. Das Unternehmen wird von Standard & Poor's mit «AA–», von Moody's mit «Aa3» und von A.M. Best mit «A+» bewertet. Die Namenaktien der Holdinggesellschaft für die Swiss Re Gruppe, Swiss Re AG, sind an der Schweizer Börse SIX Swiss Exchange gemäss International Reporting Standard kotiert und werden unter dem Tickersymbol SREN gehandelt. Für weitere Informationen zur Swiss Re Gruppe besuchen Sie unsere Website www.swissre.com oder folgen Sie uns auf Twitter @SwissRe.

So erhalten Sie diese *sigma*-Studie:
In elektronischer Form steht die *sigma*-Studie Nr. 1/2017, «Cyber: Bewältigung eines komplexen Risikos», in deutscher, englischer, französischer und spanischer Sprache auf der Website von Swiss Re bereit: www.swissre.com/sigma

Gedruckte Ausgaben von *sigma* Nr. 1/2017 sind jetzt ebenfalls auf Deutsch, Englisch, Französisch, und Spanisch erhältlich. Die Druckversionen in chinesischer und japanischer Sprache erscheinen demnächst. Bitte senden Sie Ihre Bestellung mit vollständiger Postanschrift an: sigma@swissre.com