Management von Cyber-Risiken – eine unmögliche Aufgabe?

Martin Kreuzer

Cyber-Bedrohungen sind eines der größten Risiken des 21. Jahrhunderts. Der digitale Wandel hat unsere globale Wirtschaft voll im Griff. Die zunehmende Nutzung modernster Technologien verspricht dabei unglaubliche Fortschritte, schafft aber auch potenzielle, neue Angriffspunkte und eine neue Risikolandschaft. Somit verändern sich auch die Bedrohungslagen stetig. Damit aus dieser Unsicherheit ein Risiko wird, dass hinreichend zu managen ist, braucht es einen breiten Schulterschluss von Unternehmen, Regierungen und Versicherungswirtschaft.

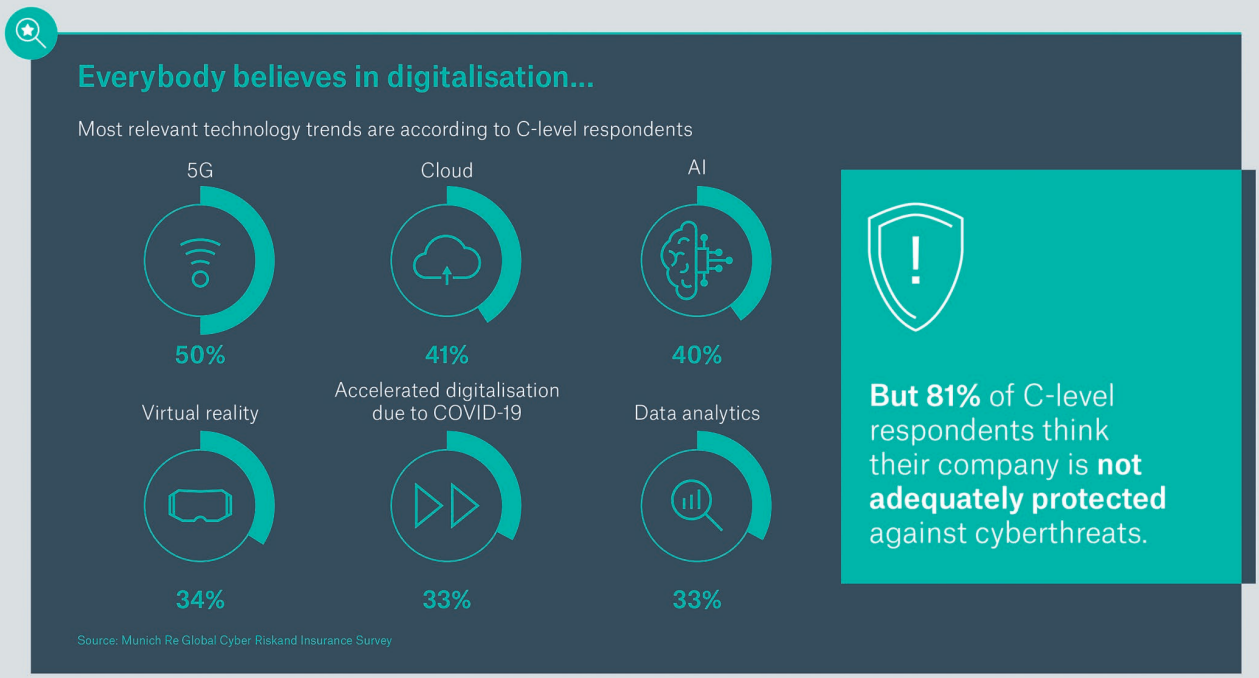
Cyberangriffe auf Regierungen, Unternehmen aller Branchen sowie kritische Infrastrukturen haben ihr disruptives Potenzial längst unter Beweis gestellt. Jeden Tag erleben wir neue Beispiele für schädliche Cyberangriffe. Die Notwendigkeit, unsere digitale Infrastruktur zu schützen, liegt auf der Hand. Aber wie dies erreicht werden kann, bleibt eine tägliche Herausforderung für alle Beteiligten. Die Versicherer dürfen nicht unterschätzen, wie bedeutend die Bewältigung dieser Herausforderung ist.

Die Risiken steigen stark

Generell nehmen die Abhängigkeiten von digitalen Geschäftsmodellen exponentiell zu und damit auch die Angriffspunkte, um ein potenzielles Opfer eines Cyberangriffs zu werden. Um nur einige Zahlen zu nennen: Cybersecurity Ventures prognostiziert, dass es bis zum Jahr 2022 rund sechs Milliarden Internetnutzer und bis zum Jahr 2030 mehr als 7,5 Milliarden Internetnutzer geben wird (vgl. Cybersecurity Ventures: https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/). Die Zahl der vernetzten Geräte wird voraussichtlich von 27 Milliarden Geräten im Jahr 2017 auf 125 Milliarden im Jahr 2030 ansteigen (vgl. IHS Markit: https://cdn.ihs.com/www/pdf/IoT_ebook.pdf). In praktisch jedem Sektor werden diese Geräte, selbstlernende Roboter und automatisierte Prozesse eine Vielzahl von Daten erzeugen, sammeln und analysieren und für mehr Effizienz und höhere Produktivität sorgen. Gleichzeitig werden immer mehr unternehmenskritische digitale Ressourcen und Prozesse entstehen, die Cyberangriffen ausgesetzt sein werden. Dies gilt insbesondere für Betriebstechnologien, die im industriellen Umfeld oder im Bereich der kritischen Infrastrukturen eingesetzt werden.

Die Ergebnisse einer globalen Munich Re Cyber Umfrage offenbaren die Risiken der Digitalisierung: Während aus Sicht der Manager 5G, Cloud Computing und Künstliche Intelligenz die Top-Technologien der weiteren Digitalisierung sind, glauben 81 % der weltweit befragten Führungskräfte, dass ihr Unternehmen nicht ausreichend gegen Cyberbedrohungen geschützt sei (siehe ▶ Abb. 01).

Abb. 01. Schutz vor Cyber-Bedrohungen



Quelle: Munich Re

Erhebliches Schadenpotenzial, uneinheitliches Risikobewusstsein

Eine adäquate Prävention ist der Schlüssel, um die verschiedenen Schwachstellen zu verringern. Es ist keine Überraschung, dass nicht nur die Gefährdungen und Angriffsflächen zunehmen, sondern auch die Ausnutzung von Schwachstellen, insbesondere wenn es kein angemessenes Cyber-Risikomanagement gibt. Dies zeigt sich vor allem in den der weltweiten Kosten für Cyberkriminalität. Die Schätzung von Cybersecurity Ventures, dass diese bis zum Jahr 2025 jährlich 10,5 Billionen US-Dollar erreichen werden, liegen zwar am oberen Ende der Bandbreite unterschiedlicher Schätzungen (vgl. Cybersecurity Ventures: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/). Allein in Deutschland steigen die wirtschaftlichen Auswirkungen von Cyberkriminalität stark an: Die jüngste Studie des Bitkom vom August 2021 schätzt die jährliche Schadenshöhe in Deutschland aktuell bereits auf 223 Milliarden Euro – mehr als doppelt so viel wie 2018/19 (vgl. Bitkom: https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr).

Niemand kann die wirtschaftlichen Auswirkungen globaler Cyberattacken genau messen – aber eines ist klar: Die Auswirkungen von Ransomware, Betriebsunterbrechungen, Spionage, Sabotage, Datendiebstahl und damit verbundene Schäden durch Cyberattacken kosten Unternehmen Millionen und werden immer bedeutender.

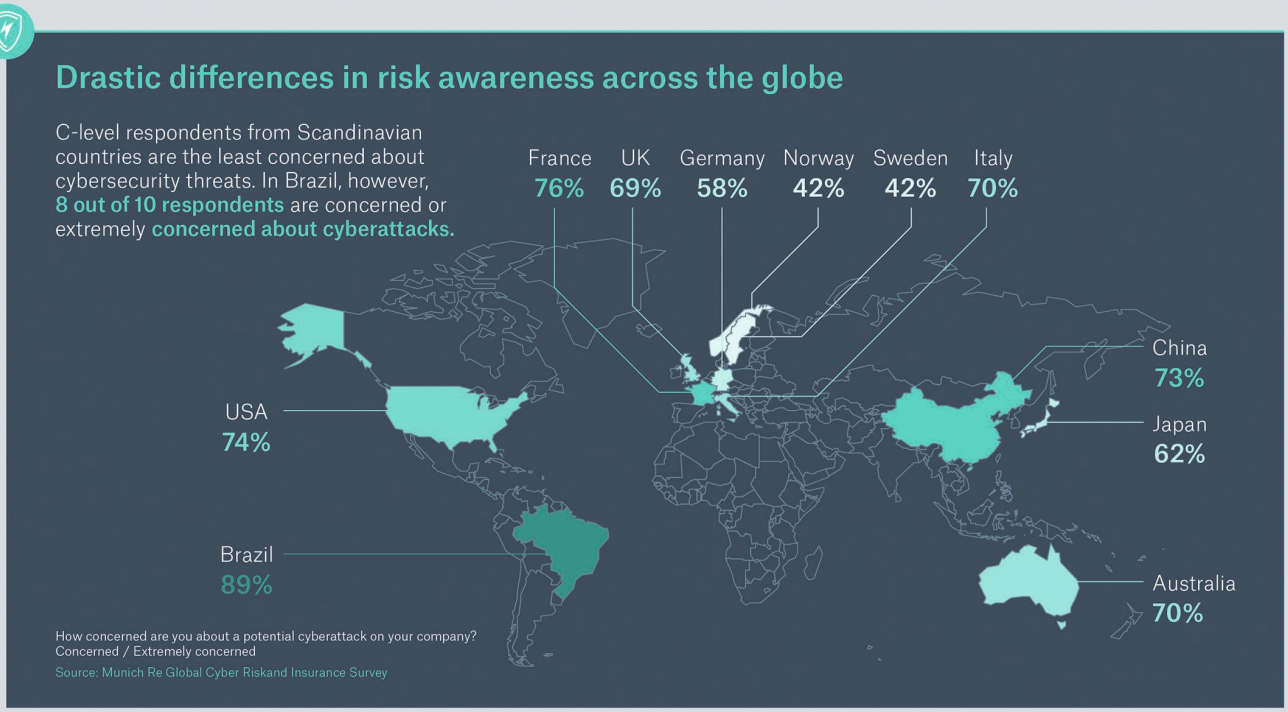
Dennoch gibt es weltweit drastische Unterschiede im Bewusstsein für Cyberrisiken (siehe ▶ Abb. 02). Insbesondere die skandinavischen Märkte scheinen am entspanntesten zu sein: Während nur etwa 40 % der befragten Führungskräfte wegen eines potenziell erfolgreichen Cyberangriffs auf ihr Unternehmen besorgt sind, trifft dies auf 62 bis 76 % ihrer Kollegen in den übrigen europäischen und nordamerikanischen Märkten sowie in Australien und den asiatische Hightech-Märkten wie Japan und die industrialisierten Teile Chinas zu. Die lateinamerikanischen Märkte führen die Liste an, wobei Brasilien die meisten besorgten Befragten aufweist.

Wie man Cyberrisiken managt

Cyberrisiken stellen Unternehmen, Regierungen und die Versicherungsbranche vor neue und einzigartige Herausforderungen. Daher muss das Cyber-Risikomanagement den individuellen Anforderungen mit einem risikobasierten Ansatz gerecht werden. Das bedeutet, dass die Cybersicherheitsmaßnahmen das individuelle Risikoprofil jeder Organisation widerspiegeln müssen, einschließlich der zugrunde liegenden Bedrohungen und Schwachstellen sowie der Maßnahmen zur Risikominderung. Wichtig ist, dass es sich hierbei nicht um ein singuläres Projekt oder eine einmalige Evaluierung handelt, sondern um einen fortlaufenden Prozess, der tief in der DNA einer Organisation verankert sein sollte. Der erste Schritt ist eine fortlaufende Cyber-Risikobewertung mit einer Analyse der Auswirkungen auf das Geschäft und einer Definition der eigenen Risikobereitschaft. Auf dieser Grundlage sollten weitere Überlegungen, Prioritäten, Reaktionspläne und Investitionen das Managementsystem für die Informationssicherheit prägen.

Das Informationssicherheits-Risikomanagement ist ein Schlüsselaspekt für den Umgang mit Bedrohungen und steht im Einklang mit regionalen und internationalen Gesetzen und Vorschriften wie der GDPR (https://gdpr.eu/), der NIS-Richtlinie (https://www.enisa.europa.eu/topics/nis-directive) sowie vielen Informationssicherheitsstandards und -rahmenwerken wie der ISO 27001 (https://www.iso.org/isoiec-27001-information-security.html), dem internationalen Standard für Informationssicherheitsmanagement, und CIS Controls für die Cyberabwehr.

Abb. 02: Drastische Unterschiede im Risikobewusstsein



Quelle: Munich Re

Die fortlaufende Identifizierung, Analyse, Bewertung und Überwachung von Cyber-Risiken führt zu Entscheidungen darüber, wie mit den Risiken umzugehen ist. Dazu gibt es in der Regel vier Optionen:

- Verringerung der Wahrscheinlichkeit und der Auswirkungen eines Cyber-Ereignisses durch die Implementierung von Cyber-Sicherheitskontrollen
- Akzeptieren des Risikos im Rahmen der festgelegten Risikobereitschaft
- Vermeidung des Risikos durch Beendigung oder Änderung der ursächlichen Aktivität
- Übertragung des Risikos durch Outsourcing oder Abschluss einer Versicherung

Die Rolle der Cyberversicherung

Cyber-Versicherer haben bereits bewiesen, dass sie Teil der Lösung sein können, wenn es darum geht, die Widerstandsfähigkeit und Reaktionsfähigkeit in allen Branchen zu verbessern. Die sich schnell verändernde digitale Landschaft kann es allerdings erschweren, Risiken zu identifizieren und zu quantifizieren.

Aus versicherungstechnischer Sicht gibt es dabei wesentliche Unterschiede zwischen Cyberrisiken und herkömmlichen Risiken. Historische Daten, wie sie beispielsweise bei der Berechnung künftiger Naturgefahren nützlich sind, sagen nicht viel über künftige Cyber-Ereignisse aus. Daten von vor mehr als zehn Jahren, als es etwas wie Cloud Computing noch nicht gab, sind bei der Bewertung von Risiken für heutige Technologien wenig hilfreich. Versicherer und Rückversicherer müssen trotzdem die sich im Zuge dieser rasanten technologischen Fortschritte ständig weiterentwickelnden Risiken erkennen und modellieren. Wer sich hier allein auf Versicherungsfachwissen stützt, wird schnell an seine Grenzen stoßen. Stattdessen sollte es das Ziel aller Beteiligten sein, über die gesamte Wertschöpfungskette hinweg zusammenzuarbeiten und möglichst viel Transparenz zu schaffen. IT-Spezialisten, Behörden, Wissenschaft und Forschung können dazu beitragen, das Bewusstsein für die Risiken zu schärfen und ihre Expertise in die Entwicklung geeigneter Cyber-Deckungen und damit verbundener Dienstleistungen einzubringen.

Für Erst- und Rückversicherer ist die Fähigkeit, Risiken zu verstehen und zu quantifizieren, von entscheidender Bedeutung, um nachhaltige Versicherungslösungen anzubieten und die Kapazitäten bereitzustellen und Prämien bezahlbar zu halten. Das Cyber-Risiko ist jedoch aufgrund der Komplexität von Geräten, Software und Systemen sowie der Möglichkeiten für unlautere Handlungen schwer zu verstehen. Um nur einige Beispiele für Fragen zu nennen, die Cyber-Versicherer berücksichtigen müssen:

- Wie groß sind die Risiken für ein bestimmtes versichertes Unternehmen?
- Wie sieht die Bedrohungslage aus?
- Wer ist ein Ziel und was könnte ein „Kollateralschaden“ sein?
- Wie hoch entwickelt ist die Risiko- und Sicherheitskultur des Versicherten?
- Wie gefährdet ist die Umsatzgenerierung?
- Könnten sich diese Probleme aggregieren und vervielfachen?

Und die vielleicht wichtigste Frage von allen ist: Wer ist verantwortlich und haftet, wenn etwas schief geht? Die ausgeklügelten Wertschöpfungsketten im IoT-Bereich (Internet der Dinge) machen die Übertragung von Haftungen zwischen Lieferanten so komplex, dass sie oft nicht wissen, wie die Verantwortung in der Kette mit ihren unterschiedlichen Regulierungsansätzen verteilt ist. Um potenzielle Risiken klarer zu erkennen, müssen wir die branchenübergreifende Zusammenarbeit verstärken, die bisher zwar einige Erfolge gezeigt hat, aber immer noch verbessert werden kann.

Ein Ausblick

Die Dynamik der oben genannten Veränderungen sowie die zunehmende Häufigkeit und Schwere von Cybervorfällen werden sich in einer steigenden Nachfrage nach Cyberversicherungen niederschlagen. Munich Re geht davon aus, dass der globale Cyber-Versicherungsmarkt bis zum Jahr 2025 einen Wert von rund 20 Mrd. USD erreichen wird.

Vor allem kleine und mittelständische Unternehmen werden überproportional von Cybervorfällen betroffen sein und damit die Nachfrage antreiben. Das Gesundheitswesen, freiberufliche Dienstleistungen, der Einzelhandel, die verarbeitende Industrie, Regierungsbehörden (einschließlich Bildungseinrichtungen) sowie Finanzdienstleistungen werden die am stärksten gefährdeten Branchen sein. Daher wird ein großer Teil der Nachfrage nach Cyber-Versicherungen höchstwahrscheinlich auch weiterhin aus diesen Branchen kommen. Neben dieser Nachfrage durch Unternehmen rechnet Munich Re auch mit einem Wachstum bei Cyberversicherungen für Privatpersonen und Familien.

Während der Datenschutz bereits weitgehend geregelt ist, ist die Welt der vernetzten Geräte und des Internets der Dinge noch immer unterreguliert. Aufgrund der Bedeutung dieses Aspekts unterstützt Munich Re die entsprechende Regulierung zusammen mit einem Klassifizierungsschema, das dem Risikoinhaber einen Überblick über die Cybersicherheitsmerkmale eines Geräts verschafft. Das übergeordnete Ziel ist es, Kunden dabei zu helfen, die Qualität ihrer vernetzten Geräte oder Cybersicherheitsdienste in Zukunft besser einschätzen zu können.

Unterdessen werden insbesondere Ransomware-Angriffe immer häufiger und sorgen für zunehmende Schäden. Die Versicherungsunternehmen bemühen sich um eine sorgfältigere und disziplinierte Herangehensweise an das, was sie versichern, und möchten besser verstehen, was ihre Kunden tun. Insgesamt führen die Entwicklungen im Moment zu angespannten Marktbedingungen. Versicherungsunternehmen könnten die Deckung für eine gewisse Zeit zurückfahren oder zurückziehen oder die Prämien für risikoreichere Aspekte erhöhen, beispielsweise für die Deckung von IoT-Netzwerken.

Darüber hinaus wird das Monitoring von Cyber-Kumulszenarien eine zentrale Aufgabe für die gesamte Versicherungsbranche bleiben. Ein ebenfalls weiterhin wichtiges Thema für Versicherer und ihre Kunden wird es sein, „stille" Cyber-Deckungen aus ihrem Portfolio herauszulösen und weitgehend in eine konkrete Deckung zu überführen. Munich Re geht davon aus, dass sich diese Aufgaben fortsetzen müssen, um ausreichend Transprarenz zu schaffen.

Es gibt eine Reihe von extremen Risiken, welche die Versicherungswirtschaft nicht alleine tragen kann. Eine breite Diskussion über den Umgang mit den Themen, in denen die Versicherbarkeit über die Belastbarkeit unserer Branche hinausgeht, ist daher unumgänglich. Dazu gehören derzeit Netzausfälle, die die Stromversorgung oder Internet- und Telekommunikationsverbindungen unterbrechen. Solche Szenarien und die damit verbundenen Kosten sollten von Staat und Unternehmen gemeinsam getragen werden, zum Beispiel in Form von Pool-Lösungen.

Die Versicherungswirtschaft ist bereit, die beschriebenen Herausforderungen zu meistern und gemeinsam Resilienz und mehr Sicherheit zu erreichen. Mit der Erfahrung im Risikomanagement, dem Risikotransfer und einem breiten Netz von Vor- und Nachsorgeleistungen sind Cyberrisiken für die Versicherungswirtschaft keine unmögliche Aufgabe.

1. Munich Re verfügt über ein Team von über 130 Experten, die Cyber-Lösungen für die gesamte Wertschöpfungskette entwickeln – von der Risikoanalyse über die Prävention bis hin zum Risikotransfer. Darüber hinaus verfügt sie über ein stetig wachsendes Netzwerk von externen Experten und Partnern, die Dienstleistungen vor und nach einem Cyberangriff anbieten.

2. Die Absicherung von Cyber-Risiken ist nach wie vor eines der wichtigsten strategischen Wachstumsfelder und Tätigkeitsbereiche von Munich Re. Mit einem Marktanteil von etwas mehr als 10 % am weltweiten Cyberversicherungsmarkt ist Munich Re der führende Versicherer.

Literatur

Cybersecurity Ventures
IBM
HIS Markit
Bitkom
Munich Re

Autor
Martin Kreuzer
Senior Risk Manager Cyber Risks,
Munich Re

IMPRESSUM

Herausgeber:
Gesellschaft für Risikomanagement und Regulierung e.V.
Schwarzwaldstraße 42
D-60528 Frankfurt am Main
VR 14261 Amtsgericht Frankfurt am Main
info@ firm.fm, www.firm.fm

Verantwortlich für den Inhalt:
Frank Romeike,
RiskNET GmbH, Gesellschaft für Risikomanagement und Regulierung e.V.

Layout:
Uta Rometsch, Stuttgart

Bildnachweise:
Adobe Stock – stock.adobe.com

© Das Urheberrecht liegt bei den jeweiligen Autoren und Autorinnen sowie bei der Gesellschaft für Risikomanagement und Regulierung e.V., Frankfurt am Main 2021.
Die Artikel geben die Meinung der Autoren wieder und stellen nicht notwendigerweise den Standpunkt der Gesellschaft für Risikomanagement und Regulierung e.V. dar.
Vervielfältigung und Verbreitung, auch auszugsweise, mit Quellenangabe gestattet.

FIRM
Frankfurter Institut für
Risikomanagement und Regulierung

Gesellschaft für Risikomanagement und Regulierung e. V.
Schwarzwaldstraße 42
60528 Frankfurt am Main | Germany
Tel.: +49 (0) 69 87 40 20 00 | Fax: +49 (0) 69 87 40 20 09
info@firm.fm | www.firm.fm