Bundesverband Deutscher Versicherungs-Makler e.V.

PRESSE-INFORMATION

Essen, den 30. September 2024

Cyber-Versicherung – beherrschen die Versicherer das Risiko?

Cyberrisiken - die Evolution der Cyber-Bedrohungslandschaft

Die Cyber-Bedrohungslandschaft entwickelt sich auch in 2023/2024 kontinuierlich weiter. Cyberangriffe werden zunehmend gefährlicher, da die Techniken, mit denen Angreifer in Systeme eindringen, immer ausgefeilter werden. Gleichzeitig nimmt auch die Häufigkeit derartiger Angriffe immer noch zu.

Ransomware hält sich bereits seit einigen Jahren prominent an der Spitze der Bedrohungen – nicht zuletzt aufgrund ihrer hohen Erfolgsquote und relativ geringen Kosten in der Durchführung. Diese Form von Malware verschlüsselt die Daten von Unternehmen und im Anschluss fordern kriminelle Organisationen Lösegeld für deren Freigabe. Neben der reinen Verschlüsselung von Daten und Unterbrechung des Geschäftsbetriebes drohen die Angreifer auch damit, vertrauliche Informationen zu veröffentlichen. Sog. Ransomware as a Service (RaaS) Plattformen ermöglichen es mittlerweile zudem auch weniger technisch versierten Kriminellen Ransomware-Angriffe durchzuführen.

In den letzten Monaten haben aber auch Supply-Chain-Angriffe, bei denen Angreifer nicht direkt das Hauptziel, sondern die Lieferkette eines Unternehmens angreifen, an Bedeutung zugenommen, da die Abhängigkeit der Unternehmen von Drittanbietern (Software oder Dienstleistungen) ständig steigt. Für Versicherer birgt diese Art von Angriff ein hohes Kumulrisiko, da ein und derselbe Angriff potenziell eine Vielzahl von Unternehmen gleichzeitig betreffen kann.

Die Angriffsformen Phishing und Social Engineering sind nicht neu, werden aber immer raffinierter und damit gefährlicher. Zunehmend personalisierte Phishing-Mails oder täuschend echt klingende Anrufe mithilfe von KI-generierten Stimmen (sog. Vishing – Voice Phishing) sollen Mitarbeiter dazu bringen, Gelder zu überweisen, vertrauliche Informationen preiszugeben oder Malware zu installieren.

Angesichts dieser Entwicklungen ist es für Organisationen (und auch uns Versicherungsmakler) unerlässlich, ihre Cyber-Sicherheitsstrategien kontinuierlich auf die sich verändernde Bedrohungslandschaft anzupassen. Die Arbeit darf nie aufhören. die Cyber-Versicherung ist dabei ein wichtiges Instrument im Risikomanagement-Baukasten der Unternehmen, da die Versicherer aus den Schäden viel über erfolgreiche Prävention gelernt haben und dieses Wissen jetzt auch den Versicherungskunden zur Verfügung gestellt wird.

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

Die Tatsache, dass dennoch mehr als 80% der Unternehmen weltweit davon ausgehen, nicht ausreichend gegen digitale Bedrohungen geschützt zu sein[1], ist daher gleichermaßen erstaunlich wie erschreckend und ein Aufruf an die Cyber-Versicherungsbranche durch gut zugängliche, sowie transparente und verständliche Versicherungslösungen weiter Abhilfe zu schaffen.

Haben die Versicherer das Risiko im Griff

Das Cyber-Risiko und der Bedarf zu dessen Absicherung bleiben also hoch und trotz des bereits beträchtlichen Marktwachstums der vergangenen Jahre wird die Nachfrage nach Cyber-Versicherung weiterhin steigen. Aktuell wird der deutsche Cybermarkt dabei auf ein Prämienvolumen von etwa 550 Mio. Euro geschätzt. Wir schätzen, dass sich das Prämienvolumen noch mindestens verdreifacht.

Die sich stetig weiterentwickelnde Bedrohungslage stellt aber auch die Cyber-Versicherer vor eine große Herausforderung, denn sie sind gezwungen, ihren Prozess der Risikoeinschätzung und -bewertung ebenfalls kontinuierlich auf die veränderten Angriffsvektoren anzupassen. Sie haben sich dementsprechend spezialisierte Abteilungen und Underwriter aufgebaut. Kunden werden wegen der ständig wechselnden Bedrohungslagen also von Jahr zu Jahr mit mehr und neuen Fragen und Anforderungen für den Abschluss oder die Verlängerung ihrer Cyber-Versicherung zu kämpfen haben. Viele schätzen aber auch den Input der Versicherungen für die Weiterentwicklung ihrer IT-Sicherheit. Einige Anbieter gehen ferner einen anderen Weg und finden – im Rahmen eines sog. „Outside Scans“ – selbst heraus, wie es um die IT-Sicherheit ihrer Kunden bestellt ist. Durch die über das Internet öffentlich zugänglichen Datenpunkte einer Unternehmens-IT ziehen die Versicherer dann Rückschlüsse über das IT-Sicherheitsniveau im gesamten Netzwerk eines Unternehmens. Die Breite der Informationen, die die Versicherer zur IT-Sicherheit der Kunden erhalten, nimmt also ebenfalls zu. Auch die Rückmeldungen der Versicherer zu den Ergebnissen dieser Scans stellt eine wichtige Rückmeldung für die Kunden zur Verbesserung ihrer IT-Sicherheit dar.

Um die Herausforderungen der Cyber-Bedrohungslandschaft effektiv zu bewältigen sind zudem Partnerschaften zwischen Versicherern und IT-Sicherheitsunternehmen etabliert. So tragen präventive Dienstleistungen, wie z. B. Sicherheitsbewertungen, Schulungen für Mitarbeiter oder Unterstützung bei der Entwicklung von Notfallplänen dazu bei, das Risiko von Cyber-Angriffen zu senken. Cyber-Versicherungen beinhalten auch integrierte Incident-Response-Services durch Dienstleister, die im Falle eines Cyber-Angriffs bei der forensischen Untersuchung, der Wiederherstellung von Daten bis hin zur Verhandlungsführung mit Erpressern unterstützen.

[1] Munich Re Global Cyber Risk and Insurance Survey 2024

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

Bei der versicherungsnehmenden Wirtschaft hat nicht zuletzt das auch durch medienpräsente Großschäden gestiegene Risikobewusstsein dafür gesorgt, dass bereits vermehrt Fokus auf erforderliche IT-sicherheitstechnische Schutzmaßnahmen gelegt wird. War diese intrinsische Motivation bisher nicht ausreichend, um die notwendigen Maßnahmen umzusetzen, so kommt zukünftig noch extrinsische Motivation für Unternehmen hinzu: neue gesetzliche Regelungen, wie etwa die erwartete Umsetzung der NIS 2– Richtlinie. Diese zwingt etwa 30.000 betroffene Unternehmen in Deutschland dazu, Maßnahmen zur Gewährleistung eines adäquaten Cyberschutzes umzusetzen und nimmt auch insbesondere das Lieferketten-Risiko in den Fokus – für die Verletzung dieser Pflichten haften die Unternehmensorgane persönlich.

Es gibt noch immer Schadenszenarien, für die Versicherer keine (ausreichende) Deckung am Markt anbieten, auch dies ein Beispiel, dass die Versicherungswirtschaft ihre Risiken aktiv managed. Ein Beispiel hierfür sind indirekte Schäden beispielsweise durch Reputationsverlust nach einem Cyber-Angriff. Auch die Deckung von Supply-Chain-Risiken ist oft nur begrenzt gegeben, da die Abhängigkeit von Dritten, sowie das IT-Sicherheitslevel dieser für den Versicherer nur schwer zu quantifizieren ist.

Trotz der weiterhin dynamischen Bedrohungslage ist jedoch im Vergleich zu den vergangenen Jahren etwas mehr Ruhe in den Cyber-Versicherungsmarkt eingekehrt. Haben die Versicherer vor einigen Jahren noch versucht, die Folgen eines Ransomware-Angriffes in den Bedingungen stark zu begrenzen, so gehört dieses Phänomen inzwischen der Vergangenheit an. Zwar gibt es Anbieter, die den Markt aufgrund schlechter Schadenerfahrungen verlassen, es kommen jedoch auch neue Anbieter auf den Markt, sodass die Kapazitätsengpässe der vergangenen Erneuerungen überwunden zu sein scheinen. Auch die Anpassung des Kriegsausschlusses und dessen Ausweitung auf staatlich gesponserte Cyber-Operationen hat inzwischen in der Breite Einzug in den Policen gefunden, sodass aktuell keine größeren Wording-Anpassungen seitens der Versicherer zu erwarten sind. Der Versicherungsmarkt hat „Cyber gelernt“.

Inwiefern der erst kürzlich eingetretene IT-Flächenbrand nach dem Crowdstrike-Vorfall, bei dem ein fehlerhaftes Update in der Software des Anbieters die IT vieler Unternehmen für mehrere Stunden lahmlegte, auf der Bedingungsseite noch Konsequenzen hinsichtlich der in vielen Cyber-Policen mitversicherten Szenarien wie Fehlbedienung und/oder Technischer Probleme nach sich ziehen wird, bleibt dabei noch abzuwarten.

Die Versicherer sind also in der Lage Cyber-Risiken effektiv zu managen und Kumulgefahren zu minimieren. Analog der Vorgehensweise in der Feuerversicherung werden den Kunden zunehmend detaillierte Anforderungen zur Verbesserung der IT-Sicherheit gestellt und diese auch überwacht. Ferner wurden, insbesondere durch die Rückversicherer, Instrumente zur Kumulkontrolle entwickelt.

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

Bundesverband Deutscher Versicherungs-Makler e.V.

PRESSE-INFORMATION

Ausblick auf das Cyber-Renewal 01.25

Das diesjährige Cyber-Renewal wird grundsätzlich ruhiger ausfallen als die vergangenen Jahre. Dennoch bleibt die Sparte weiterhin dynamisch und das Augenmerk der Versicherer auf IT-Mindestanforderungen bleibt hoch. Kleinere Risiken können zu großen Teilen mit einem unveränderten Verlängerungsangebot rechnen, für die Verlängerung von größeren Risiken werden jedoch Verlängerungsfragebögen gefordert und – wo in den Vorjahren noch nicht zur Gänze durchgesetzt – sind vereinzelt weitere Auflagen oder noch Prämiensteigerungen zu erwarten.

Versicherungssummenerhöhungen: Kapazitäten im Cyber-Markt steigen grundsätzlich wieder, wenn auch abhängig von der Risikoqualität. Versicherer sind vereinzelt wieder bereit ihre Kapazitäten auf 10 Millionen Euro zu erhöhen.

Die Zukunft der Cyber-Versicherungen wird durch eine wachsende Komplexität der Risiken, technologische Fortschritte und sich verändernde regulatorische Anforderungen geprägt sein. Um wettbewerbsfähig zu bleiben und Ihr eigenes Risiko im Griff zu behalten, müssen Versicherer auch weiter in Technologien, Partnerschaften und innovative Produkte investieren, die nicht nur aktuelle, sondern auch zukünftige Cyber-Risiken effektiv abdecken. Proaktive Maßnahmen, flexible Anpassungen und eine enge Zusammenarbeit mit verschiedenen Dienstleistern werden entscheidend sein, um den Anforderungen des Marktes gerecht zu werden und das Vertrauen der Kunden zu gewinnen und zu halten.

Ansprechpartner:
Dr. Sven Erichsen, Finlex GmbH
Non-Executive Director
Telefon: 0049 15 16494 1213
E-Mail: sven.erichsen@finlex.de