Cyber-Risiken

die Evolution der Cyber-Bedrohungslandschaft und ihre Auswirkungen auf den Cyber-Versicherungsmarkt

Andrea Kotter, Vice President Cyber bei Finlex, beschreibt in ihrem Gastbeitrag die neuesten Entwicklungen in der Cyberversicherung sowie aktuelle Bedrohungen. Die ausgewiesene Cyberexpertin verfügt über viele Jahre Erfahrung als Underwriterin in der Rückversicherungsbranche.

Die Cyber-Bedrohungslandschaft entwickelt sich kontinuierlich weiter. Cyber-Angriffe werden zunehmend gefährlicher, die Techniken, mit denen Angreifer in Systeme eindringen, immer ausgefeilter. Gleichzeitig nimmt auch die Häufigkeit derartiger Angriffe zu. Insbesondere Bedrohungen wie Ransomware und Supply-Chain-Angriffe haben dabei an Bedeutung gewonnen.

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, woraufhin kriminelle Organisationen Lösegeld für deren Freigabe fordern. Zu den Betroffenen zählen dabei Unternehmen jeder Größe. Neben der reinen Verschlüsselung von Daten und Lahmlegung des Geschäftsbetriebes drohen die Angreifer auch damit, vertrauliche Informationen zu veröffentlichen. Plattformen für sogenannte Ransomware as a Service (RaaS)-Angebote ermöglichen es auch technisch ungeschulten Kriminellen, Ransomware-Angriffe durchzuführen, was die Bedrohung erhöht.

Auch Supply-Chain-Angriffe, bei denen Angreifer nicht direkt das Hauptziel, sondern die Lieferkette eines Unternehmens angreifen, gewinnen weiter an Bedeutung. Die Abhängigkeit der Unternehmen von Drittanbietern (Software oder Dienstleistungen) nimmt stetig zu, was das Risiko für Supply-Chain-Angriffe weiter erhöht. Für Versicherer birgt diese Art von Angriff ein hohes Kumulrisiko, da derselbe Angriff potenziell eine Vielzahl von Unternehmen gleichzeitig betreffen kann.

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

Andrea Kotter, Vice President Cyber bei Finlex

Angesichts dieser Entwicklungen ist es für Organisationen unerlässlich, ihre Cyber-Sicherheitsstrategien kontinuierlich auf die sich verändernde Bedrohungslandschaft anzupassen. Insbesondere Cyber-Risiken stehen als Auslöser für Betriebsunterbrechungen im Fokus des Risikomanagement von Unternehmen, wobei die Cyber-Versicherung ein wichtiges Instrument im Risikomanagement-Baukasten der Unternehmen darstellt.

Die Tatsache, dass laut einer Umfrage der Munich Re dennoch mehr als 80 Prozent der Unternehmen weltweit davon ausgehen, nicht ausreichend gegen digitale Bedrohungen geschützt zu sein, 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. Auch die Rolle der Versicherungswirtschaft, auf eine geeignete Prävention seitens der Versicherungsnehmer einzuwirken, ist dabei nicht zu vernachlässigen.

Auswirkungen auf den Cyber-Versicherungsmarkt

Das Cyber-Risiko und der Bedarf nach dessen Absicherung bleiben also hoch; und trotz des bereits beträchtlichen Marktwachstums der vergangenen Jahre wird die Nachfrage nach Cyber-Versicherungen weiterhin steigen. Aktuell wird der deutsche Cyber-Markt dabei auf ein Prämienvolumen von etwa 550 Millionen Euro geschätzt.

Die sich stetig weiterentwickelnde Bedrohungslage stellt dabei auch die Cyber-Versicherer vor eine große Herausforderung: Sie sind gezwungen, ihren Prozess der Risikoeinschätzung und -bewertung kontinuierlich auf die sich wandelnden Angriffsvektoren abzustimmen. Das sorgt nicht immer für Begeisterung bei den Kunden, die jedes Jahr mit neuen Fragen und Anforderungen für den Abschluss oder die Verlängerung ihrer Cyber-Versicherung konfrontiert werden. Einige Anbieter gehen deshalb bereits einen anderen Weg und finden – im Rahmen eines sogenannten „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 nachfolgend Rückschlüsse über das IT-Sicherheitsniveau des gesamten Unternehmens-Netzwerks.

Um die Herausforderungen der Cyber-Bedrohungslandschaft effektiv zu bewältigen, sind zudem Partnerschaften zwischen Versicherern und IT-Sicherheitsunternehmen unerlässlich. Präventive Dienstleistungen wie Sicherheitsbewertungen, Mitarbeiterschulungen und die Unterstützung bei der Entwicklung von Notfallplänen tragen dazu bei, das Risiko von Cyber-Angriffen zu senken. Zusätzlich bieten Cyber-Versicherungen integrierte Incident-Response-Services durch Dienstleister an, die im Falle eines Cyber-Angriffs bei der forensischen Untersuchung, der Datenwiederherstellung und sogar bei Verhandlungen mit Erpressern unterstützen.

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, 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“.

Trotzdem gibt es noch immer Schadenszenarien, für die keine (ausreichende) Deckung am Markt angeboten wird. 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 deren IT-Sicherheitslevel für den Versicherer nur schwer zu quantifizieren ist.

Ausblick und Fazit

Bei der versicherungsnehmenden Wirtschaft hat nicht zuletzt das durch medienpräsente Großschäden gestiegene Risikobewusstsein dafür gesorgt, dass vermehrt Fokus auf erforderliche IT-sicherheitstechnische Schutzmaßnahmen gelegt wird. War diese intrinsische Motivation bisher nicht ausreichend, um die notwendigen Maßnahmen umzusetzen, kommt zukünftig eine zusätzliche extrinsische Motivation für Unternehmen hinzu: neue gesetzliche Regelungen, wie die erwartete Umsetzung der NIS-2-Richtlinie. Diese verpflichtet etwa 30.000 betroffene Unternehmen in Deutschland, Maßnahmen zur Gewährleistung eines adäquaten Cyber-Schutzes umzusetzen und legt dabei besonderen Fokus auf das Lieferketten-Risiko, für dessen Pflichtverletzung die Unternehmensorgane persönlich haften.

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, müssen Versicherer 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 Stakeholdern werden entscheidend sein, um den Anforderungen des Marktes gerecht zu werden sowie das Vertrauen der Kunden zu gewinnen und zu halten.