Cyber-Versicherungen werden immer relevanter

Viele Unternehmen in Deutschland sind von Cyber-Attacken betroffen. Durch die größere Verbreitung von KI könnte die Gefahr solcher Angriffe sogar noch steigen. Die Bedingungen von Cyber-Versicherungen variieren jedoch erheblich.

58 Prozent: So hoch ist der Anteil der Unternehmen in Deutschland, die gemäß einer Umfrage des Versicherers Hiscox im Jahr 2023 Opfer einer Cyber-Attacke geworden sind. Dies waren zwölf Prozent mehr als im Vorjahr – Tendenz steigend. Die Absicherung gegen solche Angriffe wird daher für Unternehmen immer wichtiger. Denn nicht nur Cyber-Angriffe nehmen zu, auch die Methoden werden vor allem durch die Nutzung von Künstlicher Intel-ligenz (KI) immer ausgefeilter. Vor diesem Hintergrund rückt die Frage einer direk-ten oder indirekten Cyber-Versicherung für Unternehmen stärker in den Fokus. Für die Versicherungsbranche liegen hier große Potenziale – zum einen für Versi-cherer bei der Produktgestaltung, zum an-deren für Vermittler in der Beratung. Da-bei gilt es, auch die versicherungsrechtli-che Perspektive zu berücksichtigen.

Direkte und indirekte Cyber-Versicherungen

Viele Unternehmen haben seit Jahren Policen abgeschlossen, die ihre (techni-schen) Einrichtungen vor Schäden schüt-zen. Klassischerweise sind dies Sachver-sicherungen, aber auch so genannte tech-nische Versicherungen oder spezielle Elektronikversicherungen.

Auch wenn diese oft als Allgefahren-versicherung ausgeführt werden und so-mit einen weiteren Deckungsumfang aufweisen als zum Beispiel eine Feuer-oder Sachversicherung, die nur bei Schä-den aus bestimmten und vordefinierten Anlässen zahlt, so sind in der Regel Cy-ber-Angriffe nicht (vollständig) versi-chert. Eine klare Abgrenzung gibt es oft nicht, auch wenn sich große Versiche-rungsmärkte wie zum Beispiel Lloyd‘s of London für mehr Klarheit einsetzen und ihre Syndikate und damit die Versicherer aufgefordert haben, klar zu definieren, ob das Thema Cyber-Sicherheit abgedeckt ist oder nicht. Organisationen, die auf Nummer sicher gehen wollen, benötigen eine direkte oder reine Cyber-Versiche-rung, deren Versicherungsumfang Cy-ber-Kriminalität sicher abdeckt. Doch auch dort drohen Abstimmungspro-bleme und Fallstricke.

Die Bedingungswerke der Cyber-Ver-sicherungen variieren erheblich. Einige Anbieter schränken den Versicherungsge-genstand bereits bei der Beschreibung di-rekt wieder ein und bedienen sich zum Teil versteckter Ausschlüsse. Andere nut-zen einen Definitionsteil und grenzen den Deckungsumfang insbesondere von ande-ren Versicherungen wie der technischen Versicherung oder „Kidnap & Ransom“ ab. Eine Abgrenzung ist sinnvoll, da Dop-pelversicherungen im Schadensfall ähn-lich problematisch sein können wie eine echte Deckungslücke.

Vorzuziehen wäre – auch im Hinblick auf die Beweislast im Schadensfall oder vor Gericht – eine Einschränkung des Deckungsschutzes im Bereich der Aus-schlüsse. Deckt der Versicherer beispiels-weise nur Schäden durch „zielgerichtete Angriffe Dritter“ ab, bleiben wichtige Fragen offen. Weitere Fragen sind: Um-fasst der Versicherungsschutz auch Schä-den, die durch Schadsoftware entstehen und damit nicht nur zielgerichtet gegen das versicherte Unternehmen gerichtet sind, sondern oft gegen eine Vielzahl von Systemen und Unternehmen gleichzeitig? Wie ist das fahrlässige Fehlverhalten von eigenen Mitarbeitern einzuschätzen? Kann ein Mitarbeiter „Dritter“ im Sinne der Versicherungsbedingungen sein?

Cyber-Policen enthalten oft Aus-schlüsse für Programmierfehler. In die-sem Fall besteht kein Versicherungs-schutz, wenn etwa Entwicklungsfehler ei-nes Programms bei der Anwendung auf-treten und einen Systemausfall verursa-chen. Hier wäre dann die Lücke durch eine Elektronikversicherung zu schließen.

Kompakt

- Allgefahren- oder Technische Versicherungen decken Schäden durch Cyber-Angriffe oft gar nicht oder nur teilweise ab.
- Spezielle Cyber-Versicherungen bieten oft besseren Schutz – Deckungsumfang und Ausschlüsse sollten immer genau geprüft werden.
- Für den besten Schutz vor Cyber-Angriffen sollten Unternehmen verschiedene Sicherheitsmaßnahmen kombinieren.

Ebenfalls ausgeschlossen sind regelmäßig Schäden, die darauf beruhen, dass Programme nicht auf dem „aktuellen Stand der Technik“ sind. Wie schon in der Produkthaftpflichtversicherung ist auch für den Bereich der Cyber-Deckungen nicht geklärt, was unter dem Begriff „Stand der Technik“ zu verstehen ist – gerade in Bezug auf die sich ständig ändernden IT-Sicherheitsanforderungen. In der Praxis – und möglicherweise auch vertraglich – erfordert dieser Ausschluss daher, dass der Versicherungsnehmer aktuelle Sicherheitssoftware verwendet (Firewall, Antivirensoftware) und erkannte Sicherheitslücken in verwendeten Programmen über Updates oder „Patches“ schließt.

„Versicherer müssen mehr denn je sicherstellen, dass sie die dynamischen Entwicklungen in ihren Vertragswerken abbilden.“

So genannte Abstimmungsvorbehalte, die in einigen Bedingungswerken vorgeschrieben sind, können Schwierigkeiten in der Schadensregulierung verursachen. Das betroffene Unternehmen muss dabei mit dem Versicherer die von ihm beabsichtigten Maßnahmen im Vorfeld abstimmen, damit die Kosten später übernommen werden. Dies macht Sinn bei der Einschaltung von IT-Forensikern zwecks Schadensermittlung. Leider entstehen hier in der Praxis oft Probleme, da der Versicherungsnehmer gerne auf eigene oder bekannte externe Ressourcen bei der Schadensminderung zurückgreift, ohne dies mit dem Versicherer abzustimmen.

Cyber-Versicherungen und VVG verbesserungswürdig

Eine wesentliche rechtliche Frage ist auch, wie die Cyber-Versicherung zu den Regelungen des Versicherungsvertragsgesetzes (VVG) passt. Die Schadensregulierung in der Cyber-Versicherung betritt nicht nur bei den verwendeten Begrifflichkeiten und technischen Definitionen Neuland. Auch muss vielfach noch geklärt werden, wie die Regelungen des VVG auf diese Versicherung, die Risiken in den unterschiedlichsten Bereichen von Organisationen abdeckt, übertragen werden können. Das bisherige Verständnis von vorvertraglichen Anzeigepflichten und Gefahrerhöhungen oder auch von Auskunftspflichten muss gegebenenfalls vom Gesetzgeber angepasst werden. Oft ist es obligatorisch, vor einem Vertragsabschluss technische Fragebögen auszufüllen. Gerne werden auch Risikodialoge geführt, um das technische Risiko besser zu verstehen. Noch ist aber nicht klar, wie sich derartige Pflichten und Dialoge rechtssi-cher in das Geflecht der vorvertraglichen Anzeigepflichten einbinden lassen.

Weitere Unsicherheiten entstehen durch die Entwicklungen von KI. Die Europäische Union (EU) hat mit dem AI Act das weltweit erste Gesetz zur Regulierung von KI verabschiedet. Ziel der EU ist es, einen Rechtsrahmen vorzugeben, um die EU-Bürgerinnen und -Bürger zu schüt-zen. Zudem sollen die Möglichkeiten von KI in den Mitgliedstaaten der EU genutzt werden können. Diese Anforderungen spiegeln sich auch im Bereich von Cyber-Angriffen und deren Absicherung wider. Dabei spielen eben nicht nur Schutzmaß-nahmen für Hard- und Software, sondern auch Cyber-Versicherungen eine tragende Rolle. Diese sollen die finanziellen Konse-quenzen von Cyber-Angriffen überneh-men oder zumindest abmildern. Cyber-Kriminelle nutzen KI gezielt für Angriffe, etwa indem sie schädliche E-Mails (so ge-nannte Spear-Phishing-Mails) generieren, die Spamfilter durchbrechen. Die Nut-zung von ChatGPT kann die Gefahren von Cyber-Kriminalität auf ein neues Level heben, was wiederum Konsequenzen für Cyber-Versicherungen hätte.

Weitere Maßnahmen mit der Cyberversicherung kombinieren

Insgesamt sind Cyber-Angriffe von gesteigerter Professionalität, Geschwindigkeit und wachsender Anzahl geprägt. Kriminellen finden wertvolle Informationen über ihre Opfer immer schneller, Angriffe lassen sich immer kostengünstiger durchführen und Bots programmieren, wobei diese auch an die Security-Systeme der Firmen ange-passt werden. Mit Deep-Fake-Technologien wie Voice-Cloning oder automatisiertem Password-Guessing zielen Kriminelle immer häufiger auf wertvolle Daten.

Eine Versicherung muss daher so spezi-ell und dabei umfassend wie möglich sein. Für Organisationen stellt sich die Frage, ob alle betreffenden Bereiche mitversichert sind. Auch geht es um die Reichweite von Ausschlüssen in Fällen, in denen zum Beispiel Mitverschulden von Mitarbeitenden eine Rolle spielt. Zahlreiche Terminologien und Klauseln sind bisher jedoch noch unbestimmt und auslegungsbedürftig.

Vor allem beim Thema KI bleiben der-zeit noch Unsicherheiten. Es könnte aber gut sein, dass Versicherer etwa Prämien für ihre Policen danach bestimmen, wie risiko-behaftet ein Unternehmen selbst ist – also zum Beispiel wie viel KI es einsetzt oder wie es seine IT gegen den Einsatz von Schad-KI abgesichert hat. Präventiv wird es für Un-ternehmen darauf ankommen, verschie-dene Maßnahmen zu kombinieren: Auf-klärungsarbeit zur Reduzierung der Risi-ken durch menschliche Einfallstore, innovative Lösungen und Präventionsmaßnah-men aufseiten der Technik sowie eine aus-reichende Schadensabsicherung.

Auch wenn es bei der Cyber-Versicherung noch offene Fragen gibt: Um sich gegen finanzielle Auswirkungen und Belastungen, die ein Cyber-Angriff nach sich ziehen kann, zu schützen, führt kein Weg an einer passenden Versicherung vorbei. Versicherer müssen mehr denn je sicherstellen, dass sie die dynamischen Entwicklungen in ihren Vertragswerken abbilden. Vermittler wiederum können sich gerade vor dem Hintergrund dieser Dynamiken als fundierte Experten rund um Cyber-Risiken positionieren. ■

Verfasst von Udo Pickartz, Counsel mit Schwerpunkt Versicherungsrecht bei der Kanzlei Simmons & Simmons.