Bewertung von Cyber-Risiken

Ralf Haftmann,
Senior Underwriter,
DUAL

In einem Zeitalter der zunehmenden Digitalisierung der Gesellschaft und des stetigen Umgangs mit Medien der Informationstechnologie rückt aus Sicht der Versicherungswirtschaft die Handhabbarkeit der daraus resultierenden Risiken in den Vordergrund. Gleichzeitig gehen mit der Übernahme dieser neuartigen Gefahren aufgrund noch immer geringer Erfahrungswerte Herausforderungen in Bezug auf deren Beurteilung einher. Nachfolgend wird beschrieben, wie die Bewertung solcher Cyber-Risiken erfolgen kann, welche Kriterien zur Risikoermittlung maßgeblich sind und welche Herausforderungen mit dem Underwriting von Cyber-Risiken verbunden sind.

Ein Cyber-Risiko wird sowohl vergangenheits- als auch zukunftsorientiert betrachtet. Die Cyber-relevante Vorschadensituation eines Versicherungsnehmers liefert in der retrospektiven Betrachtung für eine erste Risikoeinschätzung wichtige Erkenntnisse. Hierbei muss ein Schaden allerdings nicht zwangsläufig negativ auszulegen sein; vielmehr kommt es darauf an, wie das Unternehmen in einem Schadenfall reagiert hat, welche Rückschlüsse es gezogen hat und welche Maßnahmen getroffen wurden. Prospektiv gesehen sind für das Underwriting aber auch die zukünftige Ausrichtung des Unternehmens, abzusehende Entwicklungen in der IT und potenzielle Gesetzesänderungen von maßgeblichem Interesse, um beurteilen zu können, welche Risiken dem Unternehmen in der Zukunft drohen können. In praktischer Hinsicht reduzieren momentan Einjahresverträge die Problematik einer zu weitgehenden und oft nicht zu erfüllenden Zukunftsbetrachtung. Die Versicherungswirtschaft ist gegenwärtig auch noch nicht in der Lage in entscheidendem Maße zukunftsorientiert zu agieren. Branchentypisch erfolgt ein Großteil der Risikobetrachtung in der Retrospektive. Durch das sich stetig ändernde Cyber-Risiko wird sich dies nun vermehrt in die prospektive Perspektive verschieben.

Als wichtige Kriterien bei der Bewertung eines Cyber-Risikos gelten die Betriebsbeschreibung und die Branche, in der das zu beurteilende Unternehmen tätig ist. Hieraus lässt sich in erster Instanz ableiten, wie attraktiv der Versicherungsnehmer für potenzielle Angreifer sein kann. In dem Zusammenhang kann sich eine Unternehmens-/Branchenklassifizierung anbieten, anhand derer die Branche bzw. die Tätigkeit des Unternehmens eingestuft und mit anderen Unternehmen verglichen werden kann. Allerdings ist die Festlegung auf ein wesentliches Bewertungskriterium wie die Tätigkeit/Branche des Unternehmens nicht ausreichend; vielmehr ist die Berücksichtigung verschiedener Merkmale entscheidend. Weitere Punkte, die ein erstes Bild des Unternehmens aufzeigen, sind z.B. die Rechtsform, Webseite, Jahresumsatz und Anzahl der Mitarbeiter. Dies sind Punkte, die als Grundlage für die Prüfung eines (nicht nur expliziten Cyber-) Risikos angesehen werden.

Neben diesen eher strukturellen Eigenschaften eines Unternehmens sind zur Beurteilung des Cyber-Risikos aber vor allem auch die technischen und organisatorischen Aspekte der IT-Sicherheit von entscheidender Bedeutung, welche letztlich auch die Qualität des IT-Risikomanagements widerspiegeln. Demnach stellt sich die Frage, inwiefern die Sicherheit des IT-Systems als kritisch einzustufen ist, was sich anhand der Abhängigkeit des Unternehmens von Daten und Internet, Art und Anzahl gespeicherter Daten, Komplexität der eigenen IT und entsprechender Schutzmaßnahmen beurteilen lässt. In erster Linie geht es um die grundsätzliche Sicherheit der Informationssysteme. Hierunter fallen z.B. alle Maßnahmen und Prozesse zum Krisen-, Reaktions-, Benachrichtigungs-, und Kontinuitätsmanagement sowie umgesetzte Sicherheitsrichtlinien und -standards. Zudem sind entsprechende Überwachungs- und Schutzmaßnahmen sowie konkrete Bestandteile der IT-Sicherheit von Bedeutung, wie z.B. Firewalls, Anti-Virus-Software, Angriffserkennungssysteme sowie regelmäßige Updates und Backups. Auch die Themen Netzwerk- und Datensicherheit sowie etwaige Verschlüsselungen und Authentifizierungen spielen in diesem Bereich eine wichtige Rolle. Im Rahmen der Abhängigkeit von Informationssystemen ist auch die maximale Ausfallzeit, bis Umsatzeinbußen zu erwarten sind, maßgeblich, was vor allem auf den Baustein der Cyber-Betriebsunterbrechung (BU) abzielt.

Hinsichtlich der Art von Daten stehen vor allem Kredit-/EC-Karteninformationen, Sozialversicherungsnummern, Steuer-, Finanz- und Bonitätsdaten sowie weitere besondere personenbezogene Daten (z B. die Gesundheit von Kunden betreffend) im Mittelpunkt. Von entscheidender Bedeutung sind neben Art und Umfang der im Unternehmen gespeicherten, verarbeiteten und übertragenen vertraulichen Daten auch der Umgang mit diesen. In diesem Zusammenhang ist häufig von Interesse, ob Daten an Dritte weitergegeben bzw. im Auftrag Dritter verarbeitet werden, sie stets verschlüsselt sind, grundsätzliche Zugriffskontrollen bestehen und ob die Mitarbeiter im Umgang mit den Daten geschult sind. Entscheidend ist hierbei auch, ob das jeweilige Unternehmen über eine geprüfte Datenschutzrichtlinie verfügt, anhand derer Dritte den Umgang mit Daten nachvollziehen können.

Mithilfe dieser Kriterien kann neben der maßgeblichen technisch-objektiven Informationssicherheit auch der eher subjektive Aspekt des Verhaltens und der Einstellung des Unternehmens hinsichtlich der Daten-, aber auch hinsichtlich der grundsätzlichen IT-Sicherheit ermittelt werden. In diesen

Bereich fallen außerdem Regelungen von Verantwortlichkeiten für die Informationssicherheit, die Einhaltung aufgesetzter Standards und Richtlinien sowie Vorgaben für Mitarbeiter z.B. in Bezug auf Datensicherheit und mobile Endgeräte.

Mit diesen oftmals im Rahmen eines Cyber-Fragebogens ermittelten Aspekten werden die grundsätzliche Versicherbarkeit sowie etwaige Zu- oder Abschläge auf die Grundprämie bestimmt. Die Risikoerfassung über einen Fragebogen kann somit den ersten Schritt zur Bewertung eines Cyber-Risikos darstellen. Hierbei geht es insbesondere darum, das Unternehmen anhand verschiedener Parameter (Branche, Umsatz, Tätigkeit, Anzahl an Daten, Geräten, Mitarbeitern etc.) zu beurteilen und möglichst anhand einer entsprechenden Klassifizierung mit den Gegebenheiten der sich herauskristallisierenden Klasse abzugleichen. Hierbei kann sich ausgehend von den objektiven Erkenntnissen auch ein subjektives Gesamtbild des Unternehmens hinsichtlich dessen Risikoeinstellung ergeben.

Je nach Komplexität eines Risikos kann als weiterer Schritt die Analyse durch technische Sachverständige im Rahmen einer Risikobegehung erfolgen. Eine solche kann vor allem Sinn ergeben, um das BU-Risiko zu verstehen sowie einen besseren subjektiven Eindruck hinsichtlich der Risikoeinstellung des Unternehmens gewinnen zu können. Hier ist aber vor allem das Verhältnis zwischen diesem zusätzlichen Aufwand und der letztlich zu erzielenden Prämie entscheidend.

Ein weiterer Schritt im Rahmen eines Underwriting-Prozesses ist die Besprechung und Bewertung des Risikos im Team. In diesem Zusammenhang ist die Zusammenstellung des Underwriting-Teams aus Spezialisten verschiedenster Sparten (Haftpflicht-, Sach- und Technische Versicherung) und einem entsprechenden IT-Experten von entscheidender Bedeutung, um so dem vielschichtigen Cyber-Risiko gerecht werden zu können. Zu nennen sind hier im Eigenschadenbereich vor allem die klassische Sach-BU-Versicherung, aber auch im speziellen die Software- und Elektronik-BU-Versicherung. Für den Baustein der Fremdschadendeckung können auch die klassischen Formen der Haftpflichtversicherung – insbesondere im Zusammenhang mit möglichen Ansprüchen Dritter und Datenschutzverletzungen – hilfreich sein, um das Cyber-Risiko in seinem vollen Umfang zu verstehen. Hier werden vor allem Erfahrungswerte aus der Haftpflichtversicherung speziell für IT-Unternehmen verwendet. Zurückzugreifen ist auch auf Erfahrungen aus der Vertrauensschadenversicherung im Zusammenhang mit dem Risiko eigener Mitarbeiter, aber auch krimineller Dritter (in der erweiterten Deckungsform). Hieraus wird deutlich, dass Erkenntnisse und Erfahrungen aus anderen Sparten, in denen zum Teil bereits ein Cyber-Risiko enthalten ist, durchaus bei der Bewertung von Cyber-Risiken hilfreich sein können. So kann ein vergleichbarer oder ähnlicher Versicherungsumfang hinsichtlich versicherter Gefahren, Schäden oder Kosten bestehen.

Abschließend gilt es Entscheidungen hinsichtlich einer etwaigen Risikozeichnung und einer entsprechenden Prämienkalkulation zu treffen. Wesentlichen Einfluss hierauf hat auch die jeweilige Vertragsgestaltung, welche als Mittel angesehen werden kann, um Risiken überhaupt als versicherbar darzustellen. Als maßgebliche Aspekte sind hier z.B. Selbstbehalte, Deckungssummenbegrenzungen und das zugrundeliegende Bedingungswerk zu nennen.

Die Problematik mangelnder Schadenerfahrung in der Bewertung von Cyber-Risiken führt vor allem zu Beginn bzw. mit Einführung eines Produkts zu einer übervorsichtigen Zeichnungspolitik. Der zumindest theoretischen Grenze der Versicherbarkeit aufgrund unzureichender Schätzbarkeit wird mit bereits ausreichend gewonnenen Erkenntnissen im Ausland (vor allem USA) begegnet, welche zumindest zum Teil auf den deutschen Markt übertragbar sind. Zudem sind mittlerweile auch in Deutschland durchaus Schadenerfahrungen vorhanden. Allerdings sollte in diesem Zusammenhang die unterschiedliche Risiko-Exponierung des deutschen und amerikanischen Marktes berücksichtigt werden. Während in den USA der Drittschaden im Vordergrund steht – insbesondere durch die Verletzung der

Geheimhaltung von personenbezogenen Daten –, liegt in Deutschland der Fokus vor allem auf den Eigenschäden.

Als eine der größten Herausforderungen beim Underwriting von Cyber-Risiken gilt das Änderungsrisiko. Die IT verändert sich stetig, wodurch laufend neue Risiken und Bedrohungsszenarien entstehen können. So werden auch Cyber-Kriminelle immer geschickter im Finden von Möglichkeiten, in die IT-Systeme einzudringen. Auch ist bei Vertragsabschluss die Entwicklung des Einzelrisikos nicht absehbar, sodass es von Seiten des Versicherers regelmäßig zu Neubewertungen kommen muss. Durch das Anspruchserhebungsverfahren und Einjahresverträge wird in der Praxis versucht, diesem Risiko entgegenzuwirken. Hierdurch wird die Cyber-Versicherung zu einem Shorttail-Produkt, sodass das Underwriting zeitnah auf Änderungen innerhalb des Risikos reagieren kann.

Möglicher Bewertungsansatz

Ausgehend von den vorgenannten Punkten kann ein möglicher Ansatz zur Bewertung und damit ein Underwriting-Prozess von Cyber-Risiken entwickelt werden. In erster Linie kann man – vor allem aus Praxis-Gesichtspunkten – von einer grundsätzlichen Versicherbarkeit ausgehen. Die zumindest theoretischen Grenzen der Versicherbarkeit liegen vor allem in der Schätzbarkeit aufgrund des hohen Änderungsrisikos und in der Unabhängigkeit aufgrund der anzunehmenden Korrelation von Cyber-Risiken. Eine in aktuarieller Hinsicht verwertbare Datenbasis – zur Realisierung einer Schätzung – können unterschiedliche Quellen liefern. Aus Studien und Publikationen können Informationen zu durchschnittlichen Schadenhöhen und -häufigkeiten entnommen werden. Zudem können andere etablierte Märkte (hier vor allem USA) entscheidende Auskünfte zu Schäden und Kosten geben, wobei zu beachten ist, dass diese an die Gegebenheiten des deutschen Marktes anzupassen sind. Relevant können auch Erfahrungen aus anderen Versicherungsprodukten (z.B. BU-, Elektronik-, Haftpflicht- und Vertrauensschadenversicherung) sein. Die Verarbeitung dieser Schadeninformationen zu einer entsprechenden Wahrscheinlichkeitsverteilung ist Aufgabe des Aktuars.

Bei der Beurteilung von Cyber-Risiken hat sich ein zweistufiges Bewertungsschema herauskristallisiert. Zunächst geht es um die Bewertung des Unternehmens im Sinne einer Unternehmensklassifizierung. Anschließend steht die Bewertung des individuellen IT-Risikomanagements des Unternehmens im Fokus.

Das vielschichtige Cyber-Risiko kann nicht anhand eines einzelnen wesentlichen Bewertungskriteriums erfasst werden. Objektive Faktoren (Umsatz, Anzahl der Mitarbeiter etc.) vermitteln einen ersten Eindruck vom Risiko und können Auskünfte zu möglichen Schadenhöhen geben. Relevanter ist allerdings die Branche und konkrete Tätigkeit des Unternehmens. Hieraus lässt sich die Attraktivität für potenzielle Angreifer ableiten. Zur Analyse des Exposure ist auch eine differenzierte Risikobetrachtung innerhalb der Bausteine entscheidend. Im Eigenschadenbereich spielt vor allem der Baustein der BU eine entscheidende Rolle. Dieser kann aufgrund der vergleichbaren Ausprägung aus dem der Sach-BU entlehnt werden. Zu berücksichtigen ist hierbei vor allem die Abhängigkeit der Wertschöpfungskette von der IT, aber auch konkrete Überlegungen/Befragungen zu Ausfallzeiten und Ausweichmöglichkeiten. Im Fremdschadenbereich können Erfahrungen aus der Haftpflichtversicherung vor allem in Bezug auf IT-Unternehmen hilfreich sein. Speziell für den Bereich des Datenschutzes dienen vor allem Angaben zu Anzahl und Umgang der im Unternehmen gespeicherten Daten. Als risikoreich werden vor allem Daten im Zusammenhang mit Zahlungssystemen betrachtet.

Hieran anschließend kann eine Branchen-/Unternehmensklassifikation anhand der gesammelten Daten und Informationen erfolgen, welche mit den Spezifika der jeweiligen Branche, in die das Unternehmen einzustufen ist, abgeglichen werden. Cyber-Vorfälle aus der Vergangenheit machen deutlich, dass gewisse Branchen ein durchaus höheres Cyber-Risiko aufweisen und entsprechend auch in eine höhere Kategorie klassifiziert werden müssen. Hieraus wird die allgemeine Attraktivität des jeweiligen zu bewertenden Risikos für potenzielle Angreifer abgeleitet.

Im zweiten Schritt der Risikobewertung gilt es, das individuelle IT-Risikomanagement des Unternehmens zu betrachten. Dies erfolgt größtenteils über die objektive Erfassung im Rahmen eines Risikofragebogens. Entscheidend sind hier Informationen zur grundsätzlichen technischen und organisatorischen Sicherheit der IT sowie zum Umgang mit dem Datenschutz und mit branchenspezifischen und/oder gesetzlichen Richtlinien und Standards. Auch der Risikodialog mit der Geschäftsleitung und mit IT-Spezialisten bzw. eine Risikobegehung bei sehr komplexen Risiken kann Aufschluss über Haltung und Einstellung des Unternehmens zu sicherheitsrelevanten Aspekten im Rahmen der IT liefern.

Erfahrungsgemäß ist kein Unternehmen „immun" gegen das Cyber-Risiko. Im Grunde sind alle jederzeit angreifbar. Auch wenn sich ein Unternehmen aufgrund mangelnder Attraktivität für Angriffe von außen scheinbar sicher fühlt, können z.B. Fehler oder Bereicherungsabsichten von Mitarbeitern ein Cyber-Risiko hervorrufen. Dementsprechend kann die Analyse der IT-Sicherheit zwar als Maßstab zur Bewertung eines Risikos dienen, aber oftmals nicht das entscheidende Kriterium für die Zeichnung eines Risikos sein. Um dies abschließend zu beurteilen, ist ein Zusammenspiel aus objektiven Daten bezüglich des Risikos sowie subjektivem Empfinden und Erfahrungswerten (auch aus anderen Versicherungszweigen) des Underwriters nötig.

Bei grundsätzlich positiver Bewertung geht es letztlich darum, den Vertrag mitsamt Wording zu gestalten. In diesem Zusammenhang können bei Bedenken höhere Selbstbehalte, Deckungssummenbegrenzungen, explizite Ausschlüsse von Teilbereichen, besondere Vereinbarungen und vom Versicherungsnehmer zu erfüllende Obliegenheiten vereinbart werden.

Ob es sich beim beschriebenen Prozess bereits um adäquates Underwriting in der Praxis handelt, wird sich im Laufe der Zeit herausstellen. Speziell hierfür wird eine aussagekräftige Beurteilung weitere Schadenerfahrungen in den nächsten Jahren hilfreich sein. Bereits jetzt dürfte allerdings klar sein, dass sich das Underwriting stets den sich laufend ändernden Gegebenheiten der IT anpassen muss, um dauerhaft risikoadäquate Bewertungen vornehmen zu können. ■