WILHELM

RECHTSANWÄLTE

Christian Drave, LL.M. Versicherungspraxis, Juni 2015

Emerging Risks

Cyberrisiken als Herausforderungen für das Risikomanagement

1. EINFÜHRUNG

Als sogenannte „neue Risiken“ stellen Cyberrisiken Risikomanagement und Versicherungseinkauf der Unternehmen vor besondere Herausforderungen. Diese Herausforderungen betreffen Risikobewertung, -vermeidung und -transfer gleichermaßen. Möglichkeiten und Probleme im Umgang mit Cyberrisiken und ihrer Versicherung sind im Folgenden dargestellt.

2. SCHADENPOTENTIALE UND RISIKOANALYSE

Cyberrisiken sind nicht einheitlich definiert. Zum Risikomanagement eines Unternehmens gehört jedoch der Umgang mit sämtlichen relevanten Risiken, unabhängig von der Art oder Qualifikation der Risiken.

Das Risikomanagement erfordert im ersten Schritt, dass der Versicherungsnehmer die Risiken identifiziert, die im Unternehmen bestehen. Im Anschluss daran ist das Schadenpotential festzustellen: Wie hoch ist die Eintrittswahrscheinlichkeit und die mögliche Schadenhöhe? Bei dieser Bewertung ergeben sich für Cyberrisiken und -schäden Besonderheiten.

2.1 Potentiale für Eigenschäden und Haftpflichtschäden

Cyberrisiken führen vor allem zu Vermögensschäden. Dabei sind zwei Arten von Schäden zu differenzieren: Eigenschäden und Haftpflichtschäden, also Drittschäden. Eigenschäden des Versicherungsnehmers durch Cyberrisiken liegen beispielsweise im Verlust

von geistigem Eigentum, etwa durch den gezielten Diebstahl von Produkt- oder Entwicklungsinformationen.

Erhebliche praktische Relevanz haben Betriebsunterbrechungsschäden. Sie können schnell existenzgefährdendes Ausmaß erreichen – unabhängig davon, ob beispielsweise ein Stahlwerk außer Funktion gesetzt wird oder ein Onlinehändler seinen Vertrieb nach einer Hackerattacke für Tage nicht betreiben kann.

Schäden durch Cyberrisiken können auch am Vermögen Dritter eintreten (Drittschäden/Haftpflichtschäden). Das können Vertragspartner des eigenen Unternehmens sein, wie beispielsweise ein Abnehmer oder der jeweilige Partner in der Lieferkette, mit dem ein Datenaustausch besteht. Zunehmende Outsourcing-Tendenzen vergrößern die Zahl der Vertragspartner.

Aus Sicht des Risikomanagements stellen sich verschiedene Fragen: Ist eine Analyse und Optimierung der eigenen IT-Sicherheit ausreichend? Oder muss das Unternehmen, etwa durch entsprechende Vertragsgestaltungen, dafür sorgen, dass seine externen Dienstleister ebenfalls nach adäquaten Standards arbeiten? Wo bestehen zudem Risiken, Dritte zu schädigen und damit einen Haftpflichtanspruch zu verursachen?

2.2 Risikoanalyse

Die Risikoanalyse hat zu berücksichtigen, dass sich das rechtliche Umfeld im Bereich der IT-Sicherheit national wie international verändert. Entsprechend verändern sich die Risiken für die Unternehmen und die Anforderungen an ihre Sicherheitsstrukturen.

Beispielsweise will die Bundesregierung mit dem gegenwärtig vorliegenden Entwurf des neuen IT-Sicherheitsgesetzes Anforderungen an die Unternehmen in Sachen Datensicherheit verschärfen. Der Entwurf sieht umfassende Auskunfts-, Dokumentations- und Berichtspflichten und eine Zusammenarbeit mit der zuständigen Behörde (Bundesamt für Sicherheit in der Informationstechnik, BSI) vor.

Vergleichbares gilt international. In den USA soll das sogenannte Cybersicherheitsgesetz eine Zusammenarbeit zwischen US-Unternehmen und Regierung beim Kampf gegen Cybergefahren ermöglichen. Interessant ist die Gesetzesinitiative vor allem unter dem Gesichtspunkt drohender Haftpflichtschäden. Das Gesetz soll unter anderem Unternehmen, die mit den Behörden zusammenarbeiten und Informationen über Cybergefahren austauschen, vor Klagen Dritter wie etwa Kunden oder Aktionären schützen.

Die Risikoanalyse muss unternehmensbezogen erfolgen. Bei Unternehmen, die eine Vielzahl von Kundendaten, etwa Kreditkarteninformationen nutzen, liegt ein gravierendes Risiko im Verlust personenbezogener Daten. Das Unternehmen ist verpflichtet, die Behörde und vor allem sämtliche einzelnen Betroffenen über den Datenverlust zu informieren (vgl. § 42a BDSG). Dabei können Millionen von Datensätzen zu erheblichen Schäden führen. Anders liegt es bei der produzierenden Industrie. Dort steht möglicherweise der Ausfallschaden der IT-gesteuerten Fertigungsstraße im Fokus.

Die ermittelten Risiken sind nach Eintrittswahrscheinlichkeit und Schadenhöhe zu bewerten. Dabei kommt der Frage der wirtschaftlichen Auswirkung von Schadenszenarien eine erhebliche Bedeutung zu.

2.3 Risikoanalyse durch den Versicherer?

Aus Sicht des Versicherungsnehmers ist es sinnvoll, externe Spezialisten in die Risikoanalyse miteinzubeziehen, da Stresstests der IT (beispielsweise simulierte Hackerangriffe) von außerhalb des Systems und durch nicht mit dem System vertraute Personen erfolgen sollten.

Versicherer bieten im Zusammenhang mit dem Vertrieb von Cyberpolicen an, eine Risikoanalyse beim Versicherungsnehmer zu übernehmen. Die Versicherer arbeiten dabei in der Regel mit spezialisierten IT-Dienstleistern zusammen. Aus Sicht des Versicherungsnehmers ist zu berücksichtigen, dass häufig der gleiche Dienstleister nach einem Schadenfall im Auftrag des Versicherers den Schadennachweis sichert und dabei nicht vorrangig die Interessen des Versicherungsnehmers wahrnimmt. Das (ggf. zusätzliche) Hinzuziehen eigener externer Experten ist daher empfehlenswert.

3. RISIKOREDUKTION ODER RISIKOTRANSFER?

Im Anschluss an die Risikoanalyse ist zu klären, inwieweit und zu welchen Kosten Risiken vermieden bzw. reduziert oder aber an einen Risikoträger übertragen werden können bzw. vom Unternehmen selbst getragen werden.

Maßgeblich ist in diesem Zusammenhang, dass Cyberrisiken im Wesentlichen technische und organisatorische Risiken sind. Die Reduktion erfordert vor allem Investitionen in IT-Infrastruktur und Unternehmensorganisation (beispielsweise durch klare Prozesse und Datenschutzregelungen für die Mitarbeiter sowie eine konsequente Umsetzung und Kontrolle). Dies erfordert ein interdisziplinäres Risikomanagement in Zusammenar-

beit sämtlicher relevanter Kompetenzen (z.B. Risk Management, IT, Versicherung, Compliance, Controlling sowie Datenschutz). Je nach Risikoart gilt es dabei zu bewerten, welcher Umgang (z.B. Aufrüstung der IT-Infrastruktur, Restrukturierung interner Prozesse, Versicherung) mit dem einzelnen Risiko wirtschaftlich sinnvoll und technisch zielführend ist.

4. RISIKOTRANSFER DURCH VERSICHERUNG

Für die Risiken, die der Versicherungsnehmer nicht reduzieren oder selbst tragen will bzw. kann, stellt sich die Frage des Risikotransfers durch Versicherung.

4.1 Analyse des bestehenden Versicherungsschutzes

Im Einzelfall können Cyberrisiken bereits durch bestehende Versicherungsverträge gedeckt sein. Eine entsprechende Analyse muss unter Berücksichtigung der unternehmenseigenen Risiken und des individuell bestehenden Versicherungsprogramms erfolgen.

4.2 Ergänzung bestehender Policen vs. Einkauf einer Cyberpolice

Cyberrisiken, die nicht bereits durch bestehende Verträge gedeckt sind, kann der Versicherungsnehmer entweder durch die Ergänzung bestehender Policen oder den Einkauf separater Cyberversicherungen transferieren.

Ob eine Deckungserweiterung oder eine separate Deckung sinnvoller ist, ist im Einzelfall von der Art des Risikos und den bereits vorliegenden Policen des Versicherungsnehmers abhängig. Liegt für ein Unternehmen beispielsweise der Risikoschwerpunkt auf Betriebsunterbrechungsschäden, so wird dieses Unternehmen eine Betriebsunterbrechungsversicherung halten. Hier kann es zielführend sein, mit dem Versicherer eine Erweiterung auf Cyberrisiken zu verhandeln – spielt es doch aus Sicht des Versicherungsnehmers im Ergebnis keine Rolle, ob der Betriebsunterbrechungsschaden auf einen Brand oder einen Hackerangriff (Verlust produktionsbezogener Daten) zurückgeht. Anders dürfte es beispielsweise bei Unternehmen aus dem Gesundheitswesen liegen, die mit einer Vielzahl sensibler Informationen umgehen (Verlust personenbezogener Daten).

4.3 Aspekte der Deckung

Am Markt verfügbare Cyberversicherungen unterscheiden sich hinsichtlich ihres Deckungsumfangs zum Teil erheblich.

4.3.1 Uneinheitliche Deckungsstandards

Für Versicherungsnehmer stellt eine besondere Herausforderung dar, dass der Markt der Cyberversicherung gegenwärtig keinen einheitlichen Deckungsstandard aufweist. Zwar unterscheiden Cyberdeckungen üblicherweise zwischen Eigenschaden- und Haftpflichtteilen sowie weiteren Leistungsbestandteilen der Deckung. Doch existieren keine einheitlichen Regelungen zu Versicherungsfall, Ausschlüssen und Obliegenheiten sowie den Folgen ihrer Verletzung. Während beispielsweise etliche Bedingungswerke dem Quotelungsprinzip des VVG folgen, sehen andere nach dem „Alles-oder-nichts-Prinzip“ als Sanktion für grob fahrlässige Obliegenheitsverletzungen völlige Leistungsfreiheit des Versicherers vor.

4.3.2 Abgrenzung der Versicherungsverträge

Um Deckungslücken und Doppelversicherung zu vermeiden, muss der Versicherungsnehmer neu einzukaufende Cyberversicherungspolicen gegenüber bestehenden Versicherungsverträgen abgrenzen. Es gilt dabei insbesondere, auf klare Definitionen von Versicherungsfall und Ausschlüssen zu achten, um sicherzustellen, wann welche Deckung greift. Es sind Ausschlüsse in Cyberpolicen zu vermeiden, die mit Ausschlüssen bestehender Industrieversicherungsverträge korrespondieren.

Auch sind Subsidiaritätsklauseln der Cyberpolice und der bestehenden Verträge zu prüfen und nach der einschlägigen Rechtsprechung zu bewerten, um festzustellen, welcher Versicherungsschutz möglicherweise nur nachrangig besteht.

4.3.3 Zusätzliche Leistungen

Cyberpolicen bieten Zusatzleistungen. Beispielsweise kann der Versicherer dem Versicherungsnehmer im Schadenfall IT-Forensiker zur System- oder Datenwiederherstellung bereitstellen oder aber Experten wie PR-Fachleute zum Krisenmanagement oder Rechtsanwälte zur Haftungsabwehr zur Seite stellen. Derartige Leistungsbestandteile machen regelmäßig einen großen Teil der Prämie aus. Aus Sicht des Versicherungsneh-

mers ist die Notwendigkeit zusätzlicher Leistungen vor dem Hintergrund der ihm bereits zur Verfügung stehenden Ressourcen und Dienstleister sorgfältig zu prüfen.

4.3.4 Nicht versicherbare Risiken

Im Versicherungseinkauf ist zu beachten, dass wesentliche Schadenpotentiale im Zusammenhang mit Cyberrisiken (derzeit) nicht versicherbar sind.

4.3.4.1 Reputationsschäden und Verlust geistigen Eigentums

Cyberschäden können zu gravierenden Reputationsverlusten führen. Derartige Schäden sind wirtschaftlich schwer darstellbar und gelten als nicht versicherbar. Dasselbe gilt für den Verlust geistigen Eigentums.

4.3.4.2 Bußgelder?

Zu relevanten Cyberrisiken zählt das Risiko, dass dem versicherten Unternehmen infolge eines schwerwiegenden Verstoßes gegen Datenschutzvorschriften eine Geldbuße auferlegt wird. Geldbußen können nach dem BDSG bis zu EUR 300.000,00 betragen, bei einer möglichen Gewinnabschöpfung mehr. Die Bedeutung dieses Risikos dürfte zunehmen. Die geplante EU-Datenschutzgrundverordnung zielt auf Bußgelder ab, die um ein Vielfaches höher ausfallen können.

Cyberdeckungen schließen regelmäßig Bußgelder vom Versicherungsschutz ausdrücklich aus. Die Versicherungswirtschaft argumentiert, Bußgelder seien aus rechtlichen Gründen nicht versicherbar. Das ist nach hier vertretener Auffassung nicht pauschal zutreffend. Die Frage der Versicherbarkeit von Bußgeldern muss als rechtlich offen angesehen werden – unter anderem auch vor dem Hintergrund aktuell anhängiger Verfahren in Zivil- und Arbeitsgerichtsbarkeit zur Erstattungsfähigkeit von Bußen. Die Frage des Versicherungsschutzes für Bußen sollte aus Sicht der Versicherungsnehmer weiter diskutiert werden, zumal in Bußen ein erhebliches Schadenpotential liegt.

4.4 Fehlende Schadenerfahrungen

Cyberversicherungen sind ein vergleichsweise neues Produkt. Auf Seiten der Versicherungsnehmer und teilweise auch auf Seiten der Versicherer fehlen Schadenerfahrungen, zumal die Schäden sehr unterschiedlich aussehen können. Umso entscheidender sind klare Regelungen im Versicherungsvertrag zu den Abläufen im Schadenfall.

5. FAZIT

Cyberrisiken stellen versicherungsnehmende Industrie und Versicherungswirtschaft vor gemeinsame Herausforderungen. Aus Sicht der Versicherungsnehmer gehört der Umgang mit Cyberrisiken zum adäquaten Risikomanagement, was eine sorgfältige Identifikation von Risiken und die Entwicklung von Schadenvermeidungsstrategien beinhaltet.

Bei der Versicherung von Cyberrisiken droht im besonderen Maße die Gefahr von Deckungslücken oder Mehrfachversicherung. Uneinheitliche Deckungskonzepte erschweren Versicherungsnehmern den Überblick über den noch jungen Markt für Cyberversicherungen. Eine regelmäßige Analyse der eigenen Risiken und ihrer Versicherbarkeit durch gegebenenfalls neue Versicherungslösungen ist daher ebenfalls wichtige Aufgabe des Cyber-Risikomanagements.

Autor: Christian Drave, LL.M.

Für Rückfragen steht Ihnen der Leiter unserer Praxisgruppe Versicherungsrecht gern zur Verfügung:

Dr. Fabian Herdter, LL.M. Eur.
Rechtsanwalt und Partner

WILHELM Partnerschaft von Rechtsanwälten mbB
Tel: +49 211 687746 50
fabian.herdter@wilhelm-rae.de