WILHELM

RECHTSANWÄLTE

Christian Drave, LL.M. Versicherungspraxis, Juli 2014

Cyberversicherung

Möglichkeiten und Grenzen der Versicherung von Cyberrisiken

1. WAS SIND CYBERRISIKEN UND MÖGLICHE SCHÄDEN?

1.1 Einführung

„Cyberrisiken“ und „Cyberkriminalität“ sind Schlagworte, die längst nicht mehr nur das Bewusstsein infolge von Medienberichten prägen. Auch die Assekuranz und die versicherungsnehmenden Unternehmen beschäftigen sich vertieft mit Cyberrisiken. Das Risikobewusstsein spiegelt auch die Frage nach bedarfsgerechtem Versicherungsschutz. Der folgende Beitrag gibt einen Überblick über die Struktur üblicher Cyberpolicen und erläutert wesentliche Leistungsbestandteile und Ausschlüsse.

1.2 Cyberrisiken im Überblick

Cyberrisiken sind komplexe Risiken. Der Begriff der Cyberrisiken ist nicht eindeutig definiert. Im Fokus stehen zielgerichtete Angriffe auf Daten oder IT-Systeme unter Ausnutzung von Informations- und Kommunikationstechnik („Hackerangriffe“). Risiken des Datenverlustes können aber beispielsweise auch in nachlässigem Verhalten der eigenen Mitarbeiter liegen. Zudem können technische Risiken und Organisationsrisiken Cyberrisiken darstellen. Als Cyberrisiken gelten insbesondere

- Datenverluste
- Datenschutzverletzungen
- Hackerangriffe
- Ausspähen von Daten / Geschäftsgeheimnissen
- Verletzung geistiger Eigentumsrechte

- Betriebsunterbrechungen infolge von IT-Ausfällen
- Erpressungen durch Hacker

1.3 Mögliche Schadenszenarien

Cyberrisiken verursachen vor allem Vermögensschäden. Jüngsten Studien zufolge beträgt der Schaden durch Cyberkriminalität weltweit etwa 330 Milliarden Euro jährlich. In keinem anderen Land soll der Schaden – gemessen an der Wirtschaftsleistung – so hoch sein, wie in Deutschland mit 1,6 Prozent des Bruttoinlandsproduktes.[1]

Schäden liegen für die betroffenen Unternehmen beispielsweise im Verlust eigener relevanter Daten – etwa durch den gezielten Diebstahl von Produkt- oder Entwicklungsinformationen.

Unternehmen verfügen regelmäßig über weitrechende Daten Dritter, insbesondere Kundendaten. Personenbezogene Daten Dritter unterliegen dem Datenschutz. Werden zu schützende Daten Dritter öffentlich, drohen gravierende Reputationsschäden.

Systemausfälle verursachen erhebliche Schäden, zumal die Systemabhängigkeit der Unternehmen steigt (ständige Verfügbarkeit von Informationen, Produkten oder Dienstleistungen). Durch Outsourcing sind Unternehmen von fremden Strukturen abhängig. Kommt es beispielsweise bei einem Logistikdienstleister zu einem Systemausfall, kann dies die Produktion oder den Vertrieb des Auftraggebers beeinträchtigen.

2. WAS LEISTEN CYBERVERSICHERUNGEN?

2.1 Überblick: Was bietet der Markt?

Mittlerweile bieten ca. 15 Versicherer Cyberversicherungen im deutschen Markt an. Eine Verbandsempfehlung zu Cyberbedingungen von Seiten der Versicherer existiert nicht. Die Policen sind häufig in Modulen/Bausteinen aufgebaut. Die angebotenen Cyberpolicen sind teilweise miteinander vergleichbar, variieren jedoch grundlegend. Aus Sicht der Versicherungsnehmer und der sie beratenden Makler besteht die Schwierigkeit, dass Bedingungswerke komplex und teilweise schwer vergleichbar erscheinen. Schadenerfahrungen mit den Deckungen fehlen weitestgehend.

---

[1] Vgl. die Studie des Centers for Strategic and International Studies (CSIS), abgerufen am 16. Juni 2014 unter http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

2.2 Typische Leistungsbestandteile von Cyberpolicen

Cyberpolicen weisen typische Leistungsbestandteile auf. Die Leistungsbestandteile kennzeichnen die Policen. Die Klauseln regeln die Leistungsbestandteile unterschiedlich, beispielsweise in der Definition des Versicherungsfalls. Ein effektiver Versicherungsschutz erfordert somit eine individuelle Risikoprüfung.

Übliche Cyberbedingungen weisen im Wesentlichen die folgenden Leistungsbestandteile auf:

- Eigenschadendeckung
- Haftpflichtdeckung („Drittschadenversicherung“)
- Weitere Leistungsbestandteile (z.B. Krisenmanagement)

2.2.1 Eigenschadendeckung

Schäden durch Cyberrisiken können am Vermögen des versicherten Unternehmens selbst eintreten („Eigenschäden“). Als ein wesentlicher Leistungsbestandteil greift hier die Eigenschadendeckung von Cyberpolicen.

Beispiel 1: Ein Hacker stielt Entwicklungsinformationen der nächsten, innovativen Produktgeneration eines Unternehmens. Das Unternehmen muss feststellen, dass unmittelbar vor der beabsichtigten Markteinführung ein Wettbewerber ein gleichartiges Produkt auf den Markt bringt.

Beispiel 2: Ein Hacker nimmt Zugriff auf interne Daten, die Reisekosten des Vorstands oder etwa die Geschäftsstrategie betreffen, und erpresst das Unternehmen. Das Unternehmen zahlt ein Lösegeld, um eine Veröffentlichung der Informationen zu verhindern.

Der Versicherer ersetzt Eigenschäden des Versicherungsnehmers beispielsweise in Form von

- Schadenbeseitigungskosten, Kosten der Wiederherstellung der Daten oder der technischen Verfügbarkeit des IT-Systems
- Betriebsunterbrechungsschäden
- Kosten der Information gegenüber Dateninhabern bei Verlust personenbezogener Daten
- Lösegeldzahlungen an Hacker bei Erpressungen nach Datenverlust

Eine Schadenposition mit erheblicher praktischer Relevanz sind *Betriebsunterbrechungsschäden*. Diese Schadenposition ist in der Praxis häufig der größte Schadenteil. Betriebsunterbrechungen können schnell existenzgefährdende Ausmaße für Unternehmen erreichen – wie etwa im Fall eines Einzelhändlers/Onlinehändlers, der seinen Vertrieb nach einer Hackerattacke für Tage nicht betreiben kann. Aber auch produzierende Unternehmen oder Dienstleistungsunternehmen können beispielsweise bei Ausfällen von IT-Systemen durch einen Cybervorfall unter existenziellen wirtschaftlichen Druck geraten. Ein Problem von erheblicher Relevanz im Zusammenhang mit Betriebsunterbrechungsschäden ist in der Regulierungspraxis – nicht nur im Bereich der Cyberversicherung – der Nachweis des Schadens durch den Versicherungsnehmer gegenüber dem Versicherer. Teilweise regeln Cyberbedingungen die Berechnungsmethoden des Betriebsunterbrechungsschadens und sehen im Einzelfall Beweiserleichterungen für den Versicherungsnehmer vor.

Eine weitere Position der Eigenschadendeckung sind *Informationskosten*. Unternehmen sind nach § 42 a Bundesdatenschutzgesetz verpflichtet, im Fall eines Verlustes von personenbezogenen Daten nicht nur die zuständige Behörde, sondern auch sämtliche Betroffenen zu informieren. Aus Medienberichten sind aktuelle Fälle bekannt, in denen Hacker auf Datensätze Millionen Betroffener Zugriff nahmen. Entsprechend hoch können Informationskosten sein, die das Unternehmen treffen. Informationspflichten und gegenüber dem nationalen Recht verschärfte Sanktionen für den Fall der unterlassenen oder unzureichenden Information sieht auch der Entwurf der geplanten Datenschutz-Grundverordnung der EU vor.

2.2.2 Haftpflichtdeckung

Schäden durch Cyberrisiken können auch am Vermögen Dritter eintreten (“Drittschäden”). Der zweite wesentliche Leistungsbestandteil von Cyberpolichen ist die Haftplichtdeckung. Die Haftpflichtdeckung zielt auf den Fall, dass das versicherte Unternehmen bei einem Dritten durch einen Cybervorfall einen Vermögensschaden verursacht und der Dritte infolge dessen Schadenersatz verlangt.

Beispiel: Ein Onlinehändler wird Opfer eines Hackerangriffs. Die Hacker nehmen Zugriff auf Millionen von Kreditkartendaten der Kunden des Unternehmens. Mittels der gestohlenen Kreditkarteninformationen tätigen die Hacker bzw. weitere Personen, die die Daten ihrerseits von den Hackern kauften, Umsätze bei Einzelhändlern oder heben Barbeträge ab. Bestand bei dem Onlinehändler ein Datenleck, so können den geschädigten

Kreditkarteninhabern, Kreditkarteninstituten und Einzelhändlern Schadenersatzansprüche gegen den Onlinehändler zustehen.

2.2.3 Weitere Leistungsbestandteile

Insbesondere der Verlust von persönlichen Daten von Kunden oder Geschäftspartnern birgt für Unternehmen das Risiko schwerwiegender Reputationsschäden. Das zur Schadenbegrenzung erforderliche Krisenmanagement wie z.B. Pressekommunikation können betroffene Unternehmen regelmäßig nicht im notwendigen Umfang und abrufbereit betreiben. Cyberpolicen können deshalb als zusätzliche Bestandteile Unterstützungsleistungen vorsehen, etwa durch Experten wie PR-Fachleute, Rechtsanwälte, IT-Forensiker zur Datenwiederherstellung oder durch die Bereitstellung zusätzlicher Serverkapazitäten.

2.3 Grenzen des Deckungsschutzes und Ausschlüsse

Cyberversicherungen bieten keine Allgefahrendeckung, sondern Versicherungsschutz gegen benannte Einzelrisiken.

2.3.1 Versicherungsfälle und versicherte Risiken – primäre Risikobegrenzungen

Risikobegrenzungen auf Ebene der sogenannten primären Risikobegrenzung enthalten vor allem die *Versicherungsfalldefinitionen* in den Cyberversicherungsbedingungen.

Deckt der Versicherer beispielsweise nur Schäden durch „zielgerichtete Angriffe Dritter“, so erscheint beispielsweise problematisch, ob der Versicherungsschutz auch Schäden erfasst,

- die durch Schadsoftware („malware“) wie etwa Viren entstehen, die nicht nur zielgerichtet gegen das versicherte Unternehmen eingesetzt wird, sondern gerade eine unbestimmte Vielzahl von Systemen verseuchen soll oder
- die auf (fahrlässigem) Fehlverhalten von eigenen Mitarbeitern beruhen – wobei auch fraglich sein kann, ob ein Mitarbeiter „Dritter“ im Sinn der Versicherungsbedingungen ist.

Cyberbedingungen enthalten regelmäßig mehrere Versicherungsfalldefinitionen (für Eigenschadenteil, Haftpflichtteil oder z.B. Betriebsunterbrechungsdeckung). Hinzu kommen unterschiedliche Definitionen der versicherten Risiken oder Schäden. Dies macht die Bedingungen komplex und kann einen Bedingungsvergleich erschweren.

2.3.2 Ausschlüsse – sekundäre Risikobegrenzungen

Durch *Ausschlüsse* schränken Cyberbedingungen die Reichweite der Deckung auf Ebene der sogenannten sekundären Risikobegrenzung weiter ein.

Cyberpolicen können beispielsweise Ausschlüsse für Programmierfehler enthalten, so dass kein Versicherungsschutz besteht, wenn etwa Entwicklungsfehler eines Programms bei der Anwendung zu Tage treten und einen Systemausfall verursachen. Ebenfalls ausgeschlossen sind regelmäßig Schäden, die darauf beruhen, dass Programme nicht auf dem aktuellen Stand sind. In der Praxis erfordert dieser Ausschluss daher, dass der Versicherungsnehmer aktuelle Sicherheitssoftware verwendet (Firewall, Antivierensoftware) und erkannte Sicherheitslücken in verwendeten Programmen über „patches“ schließt.

Cyberbedingungen können Ausschlüsse vorsätzlichen oder grob fahrlässigen Verhaltens enthalten. In diesem Zusammenhang ist maßgeblich, wessen Verhalten dem Versicherungsschutz nach den Bedingungen konkret schadet. Aus Sicht des versicherten Unternehmens ist entscheidend, dass der Kreis der Personen, deren vorsätzliches Verhalten („Datendiebstahl“) mitversichert sein soll, klar definiert und nicht durch einen zu weit reichenden Vorsatzausschluss eingeschränkt wird.

3. CYBERPOLICEN UND „KLASSISCHE“ DECKUNGEN

3.1 Partieller Versicherungsschutz über andere Versicherungsverträge

Bestehende Versicherungsverträge und Deckungskonzepte können bestimmte Schäden durch Cyberrisiken abdecken und insoweit partiellen Versicherungsschutz gegen Cyberrisiken bieten.

Beispiel 1: Ein Cybervorfall führt zu einem Sachschaden an einer Sache, die dem Betrieb des versicherten Unternehmens dient. Daraufhin kommt es zu einer Betriebsunterbrechung. Hier besteht Versicherungsschutz unter der klassischen Betriebsunterbrechungsversicherung des Unternehmens, da ein versicherter Sachschaden eintrat und den Betriebsunterbrechungsschaden als Vermögensfolgeschaden verursachte.

Beispiel 2: Ein unzufriedener Mitarbeiter greift gezielt auf das Firmennetzwerk zu und veröffentlicht sensible Unternehmensdaten. Der dem Unternehmen dadurch entstehende Vermögensschaden kann von der Vertrauensschadenversicherung des Unter-

nehmens gedeckt sein. Die Vertrauensschadenversicherung ersetzt Vermögensschäden bei vorsätzlichen unerlaubten Handlungen durch Mitarbeiter ("Vertrauenspersonen").

3.2 Gefahr von Deckungslücken

Einen umfassenden Versicherungsschutz gegen relevante Cyberrisiken bieten klassische Deckungskonzepte nicht. Relevante Schäden durch Cyberrisiken fallen unter Ausschüsse traditioneller Deckungen, wie beispielsweise den Ausschluss mittelbarer Schäden.

Einen „allumfassenden" Deckungsschutz bieten Cyberpolicen nicht. Die Reichweite des Versicherungsschutzes ist zu analysieren, um Deckungslücken zu vermeiden. Im Einzelfall kann es unter dem Gesichtspunkt des Risikomanagements wirtschaftlich sinnvoll sein, bestehenden Versicherungsschutz um Cyberrisiken zu erweitern. Stimmige Deckungslösungen von Cyberrisiken erfordern eine Abstimmung von Cyberpolicen und bestehenden Versicherungsverträgen. Dabei erfordern Subsidiaritätsklauseln besonderes Augenmerk um klarzustellen, welcher Versicherungsschutz greift bzw. vorgeht und um eine Mehrfachversicherung zu vermeiden.

4. FAZIT

Cyberrisiken und mögliche Schadenszenarien sind komplex. Mit der Abhängigkeit der Unternehmen von funktionierenden Informationssystemen und der zunehmenden Datenfülle steigt auch das Risiko von Eigen- oder Drittschäden.

Unternehmen sehen sich steigenden Anforderungen an Datenschutz, Datensicherheit und Compliance ausgesetzt. Unternehmen sollten die individuelle Risikolandschaft im Hinblick auf Cyberrisiken analysieren. Bedarfsgerechter Versicherungsschutz erfordert eine detaillierte Prüfung der Risiken und der Leistungsangebote der Versicherer. Insbesondere die Reichweite des bestehenden bzw. beabsichtigten Versicherungsschutzes und Ausschlüsse sind zu prüfen.

Christian Drave, LL.M.
Rechtsanwalt
Master of Insurance Law
Fachanwalt für Transport- und Speditionsrecht

Wilhelm Rechtsanwälte
Partnerschaft von Rechtsanwälten mbB

Reichsstraße 43
40217 Düsseldorf

Telefon: + 49 (0)211 687746 - 43
Telefax: + 49 (0)211 687746 - 20

www.wilhelm-rae.de
christian.drave@wilhelm-rae.de