compact.
HERFURTH & PARTNER RECHT INTERNATIONAL.

Die Versicherung von Cyberrisiken

Konstantin Kuhle, Rechtsanwalt in Hannover

OKTOBER 2017

Viele Unternehmen geben in Umfragen an, zunehmend zum Ziel erfolgreicher oder erfolgloser Cyberangriffe zu werden. Trotzdem werden die Risiken insbesondere bei kleinen und mittleren Unternehmen nach wie vor unterschätzt. Bis ein Cyberangriff überhaupt erkannt wird, vergehen oft mehrere Monate. Um den Angriff abzustellen, wird weitere Zeit benötigt. Währenddessen können erhebliche wirtschaftliche Schäden für die betroffenen Unternehmen entstehen.

Die Versicherung von Cyberrisiken kann einen wirksamen Beitrag leisten, die negativen Folgen eines Cyberangriffs zu begrenzen. Mit dem Abschluss einer Cyberpolice sind jedoch rechtliche Probleme verbunden.

Risiken

Die Risiken, die sich aus der Nutzung digitaler Lösungen in Unternehmen ergeben, sind vielfältig. Sie reichen von Datenschutzverletzungen über Hackerangriffe, Erpressungen, Persönlichkeitsverletzungen und Rufschädigungen, Verletzung geistiger Eigentumsrechte bis hin zum Ausspähen von Geschäftsgeheimnissen.

Hinsichtlich der wirtschaftlichen Folgen aus der Verwirklichung dieser Risiken ist zwischen *Eigenschäden* und *Fremdschäden* zu differenzieren. Als Eigenschäden können etwa die Kosten einer Betriebsunterbrechung gelten. Cyberangriffe können als Eigenschäden ferner hohe Rechtsverfolgungskosten auslösen, etwa Kosten, um durch forensische Maßnahmen die Urheber eines Angriffs zu ermitteln. Unter Drittschäden sind beispielsweise die Schadensersatzansprüche von Kunden zu fassen.

Cyberpolicen

Die beschriebenen Risiken können in vielen Fällen nicht durch die bestehenden Spartenversicherungen eines Unternehmens abgedeckt werden. Für den Schadensfall einer Sachversicherung fehlt es im Falle eines Cyberangriffs in der Regel an einem Sachschaden. Die Betriebshaftpflichtversicherung des Unternehmens schließt dagegen womöglich solche Kosten aus, die das Unternehmen schon aufgrund gesetzlicher Verpflichtungen, etwa aus dem Datenschutzrecht, zu tragen hat. Selbst der vergleichsweise neue Typus einer Medienhaftpflichtversicherung knüpft möglicherweise nur in unzureichendem Maße an die eigene Infrastruktur des zu versichernden Unternehmens an, sodass Eigenschäden nicht von der Deckung umfasst sind.

Ob das bestehende Versicherungskonzept eines Unternehmens auch Schäden aus Cyberangriffen umfasst, sollte Gegenstand einer umfassenden Risikoanalyse sein. Nicht immer können die bestehenden Versicherungen um Cyber-Szenarien erweitert werden. Für diese Fälle empfiehlt sich nach einer Risikoanalyse der Abschluss einer Cyberpolice.
Die bestehenden Cyberpolicen sind meist modular aufgebaut und umfassen unterschiedliche Komponenten, die je nach dem erfassten Risiko eines Unternehmens kombiniert werden können.

Ja nach Branche und Grad der Digitalisierung im Unternehmen sind folgende Aspekte bei der Auswahl von Modulen einer Cyberpolice zu beachten:

- Die Police sollte Kosten für das Krisenmanagement im Schadensfall abdecken. Dies umfasst neben den Kosten für die Aufklärung der genauen Umstände des Angriffs auch die Kosten für die nötigen Benachrichtigungen der Kunden über Datenschutzverletzungen sowie für den Rechtsbeistand im Schadensfall. Dabei ist zu beachten, dass sich der Schadensfall über einen längeren Zeitraum hinziehen kann. Auch dem Unternehmen, welches einen verübten Cyberangriff bereits erkannt hat, können weiter Schäden entstehen.

- Zudem sollte die Police eine Komponente enthalten, mit der Ansprüche Dritter wegen Datenschutzverletzungen abgesichert werden. Falls diese bereits im bestehenden Versicherungskonzept enthalten ist, ist zu prüfen, ob der Versicherungsschutz nach dem Inkrafttreten der neuen EU-Datenschutzgrundverordnung angepasst werden muss. Diese ist ab Mai 2018 anzuwenden und enthält weitreichende Bußgeldvorschriften, um personenbezogene Daten zu schützen.

- Die Beschreibung des Schadensfalls im Versicherungsvertrag muss hinreichend offen sein, um unterschiedliche Konstellationen aus dem zu versichernden Unternehmen zu erfassen. Die Beschreibung muss darüber hinaus auch solche Schäden erfassen, die zur Beseitigung eines Cyberangriffs erforderlich sind. So kann etwa die durch einen Cyberangriff ausgelöste Betriebsunterbrechung oft nur beendet werden, indem hohe Wiederherstellungskosten für beeinträchtigte Daten aufgewandt werden.

- Der Versicherungsschutz darf nicht geographisch beschränkt sein. Schließt eine Cyberpolice etwa Schäden aus, die in den USA entstehen, so kann im Schadensfall ein großer Teil der Einbußen nicht geltend gemacht werden.

- Die Risikoanalyse, die dem Abschluss einer Cyberpolice vorausgeht, sollte auch Aspekte der so genannten Auftragsdatenverarbeitung umfassen, wenn das zu versichernde Unternehmen ein anderes Unternehmen mit der Datenverarbeitung beauftragt hat.

- Viele Versicherungsprodukte für Cyberschäden sind vergleichsweise neu auf dem Markt. Die Deckungssummen bestehender Policen erreichen daher zum gegenwärtigen Zeitpunkt noch nicht die Höhe, bis zu der das zu versichernde Unternehmen in anderen Versicherungsbereichen, z. B. bei der Feuer- oder Gebäudeversicherung, versichert ist. Angesichts des sich verändernden Marktes für Cyberpolicen und der dynamischen technologischen Entwicklung sollte die Höhe der Deckungssumme regelmäßig überprüft und angepasst werden.

Versicherungsrechtliche Obliegenheiten

Mit dem Abschluss einer Cyberpolice ist der Versicherungsnehmer keinesfalls von einer besonderen Überwachung seiner digitalen Infrastruktur befreit. Die Versicherungen knüpfen ihre Leistung im Schadensfall in der Regel an umfangreiche Obliegenheiten. Kommt der Versicherungsnehmer diesen nicht nach, so erfolgt keine Leistung durch die Versicherung.

Dabei handelt es sich oftmals um folgende Anforderungen:

- Der Versicherungsnehmer hat die Pflicht, den digitalen Zugang zu sensiblen Informationen nach einzelnen Nutzern und Befugnisebenen zu differenzieren. Dazu bedarf es individueller Zugänge für die Mitarbeiter, die mit hinreichend komplexen Passwörtern gesichert sind. Administrative Zugänge sollten nur an ausgewählte Gruppen von Mitarbeitern vergeben werden.

- Je höher das Risiko eines Cyberangriffs, umso höher muss der Schutz gegen unberechtigte Zugriffe ausgestaltet sein. Ein hohes Risiko besteht dort, wo Geräte über das Internet erreichbar sind. Besondere Schutzmaßnahmen können sein: Firewall, 2-Faktor-Authentifizierung bei Servern, Verschlüsselung von Datenträgern mobiler Geräte oder Diebstahlsicherung.

- Es sollte ein wirksamer Schutz gegen mögliche Schadsoftware bestehen, der automatisch auf dem neuesten Stand gehalten wird, etwa Virenscanner, Code Signing oder Application Firewall.

- Um Lücken in der eingesetzten Software oder in den bereits angewandten Schutzmechanismen zu finden, ist ein so genanntes Patch-Management-

Verfahren einzusetzen, mit dem eine unverzügliche Installation von relevanten Sicherheitspatches sichergestellt wird. Systeme und Anwendungen mit bekannten Sicherheitslücken dürfen nicht ohne zusätzliche Maßnahmen zur Absicherung eingesetzt werden.

- Daten müssen mindestens wöchentlich gesichert werden. Dabei ist darauf zu achten, dass die Sicherungsdatenträger physisch getrennt von den Originalen aufbewahrt werden. Im Schadensfall darf auf Originale und Duplikate nicht gleichzeitig zugegriffen werden können. Auch eine gleichzeitige Manipulation oder Zerstörung ist auszuschließen. Das zu versichernde Unternehmen muss im Schadensfall gegenüber dem Versicherer möglicherweise darlegen, dass die Sicherungs- und Wiederherstellungsprozesse ordnungsgemäß stattgefunden haben. Dazu empfehlen sich ein regelmäßiger Sicherungsturnus sowie eine Protokollierung der Sicherungsvorgänge.

- Das zu versichernde Unternehmen ist der Versicherung gegenüber verpflichtet, alle gesetzlichen, behördlichen sowie vertraglich im Verhältnis zu Dritten vereinbarten Sicherheitsvorschriften einzuhalten. Dies betrifft nicht nur die Betreiber so genannter kritischer Infrastrukturen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, die nach § 8a des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) verpflichtet sind, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. Betroffen sind auch Unternehmen außerhalb kritischer Infrastrukturen, die nach der neuen EU-Datenschutzgrundverordnung oder nach anderen Regelungen zu bestimmten Vorkehrungen verpflichtet sind. Meldepflichten hinsichtlich eines Cyberangriffs mit Datenverlust können sich zudem aus vertraglichen Vereinbarungen ergeben und dürften sogar als ungeschriebene vertragliche Nebenpflicht zu werten sein.

- Der Versicherer kann das zu versichernde Unternehmen auffordern, bestimmte gefahrdrohende Umstände innerhalb einer angemessenen Frist zu beseitigen. Dies bezieht sich insbesondere auf Umstände, die bereits in der Vergangenheit einen Schadensfall ausgelöst haben.

Eine erhöhte Sensibilität für die Einhaltung der beschriebenen Obliegenheiten erfüllt zwei Funktionen: Einerseits kann sicher gestellt werden, dass im Schadensfall bestimmte Schäden durch die Versicherung abgedeckt werden. Andererseits führt eine Einhaltung der Obliegenheiten auch zu einem erhöhten Sicherheitsniveau im Unternehmen, sodass ein Schadensfall im Vorfeld unwahrscheinlicher wird.

Vorkehrungen im Vorfeld des Schadensfalls

Neben der Schulung der Mitarbeiter hinsichtlich der Erfüllung versicherungsrechtlicher Obliegenheiten können weitere Nachteile des Schadensfalls durch bestimmte Vorkehrungen minimiert werden.

So ist in Abhängigkeit vom Geschäftsmodell des zu versichernden Unternehmens zu prüfen, welche Risiken das Unternehmen selbst zu tragen hat und welche Risiken bei etwaigen Vertragspartnern liegen sollen. Durch eine entsprechende Gestaltung von Allgemeinen Geschäftsbedingungen (AGB) sowie Disclaimern kann eine Risikoteilung erreicht werden, beispielsweise indem bestimmte Verschlüsselungsmodi zur Voraussetzung für eine Kommunikation mit dem zu versichernden Unternehmen gemacht werden.
Auch Compliance-Regelungen und Cybersecurity-Checklisten führen dazu, dass eine höhere Sensibilität im Schadensfall einen geringeren Schaden auslöst.

Herausforderungen im Schadensfall

Im Falle eines Cyberangriffs sind zunächst die gesetzlichen Mitteilungspflichten einzuhalten. Sollte es etwa zu einer Verletzung des Schutzes personenbezogener Daten kommen, sind Betreiber öffentlich zugänglicher Telekommunikationsdienste nach § 109a TKG verpflichtet, unverzüglich der Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit von der Verletzung zu benachrichtigen. Weitere Mitteilungspflichten finden sich in § 15a TMG sowie in § 42a BDSG. Auch nach der neuen Datenschutzgrundverordnung sowie nach dem BSI-Gesetz bestehen weitreichende Mitteilungspflichten. Diese können sich zudem aus Verträgen bzw. als Nebenpflicht ergeben.

Bei der Aufarbeitung eines Cyberangriffs ist es denkbar, dass das Unternehmen Ansprüche gegen seine eigene Geschäftsleitung hat. Vor dem Hintergrund von § 93 Abs. 2 Satz 1 AktG und § 43 Abs. 2 GmbHG kommt es in Betracht, dass ein unzureichender Schutz der IT-Infrastruktur als Pflichtverletzung zu werten ist. Auch der betriebliche Datenschutzbeauftragte kann in Haftung genommen werden.

Nach einem Cyberangriff müssen Schadensersatzansprüche gegen den Verursacher der Schädigung durchgesetzt werden. Hat sich das zu versichernde Unternehmen externer Dienstleister bedient, etwa um die Sicherheit vor Cyberangriffen zu gewährleisten, ist nach dem Schadensfall zu prüfen, inwiefern diese Dienstleister haften. Aus diesen Verhältnissen können Ansprüche auf den Anbieter der Cyberpolice übergehen.

+++

IMPRESSUM

HERAUSGEBER

HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, D-30159 Hannover
Fon 0511-30756-0 Fax 0511-30756-10
Mail info@herfurth.de, Web www.herfurth.de
Hannover · Göttingen · Brüssel
Member of the ALLIURIS GROUP, Brussels

REDAKTION

Leitung: Ulrich Herfurth, Rechtsanwalt, zugelassen in Hannover und Brüssel (verantw.)

Mitarbeit: Angelika Herfurth, Rechtsanwältin, FA für Familienrecht; Sibyll Hollunder-Reese, M.B.L. (HSG), Rechtsanwältin; Thomas Gabriel, Rechtsanwalt; JUDr. Yvona Rampáková, Juristin (CR); Dr. Jona Aravind Dohrmann, Rechtsanwalt; Marc-André Delp, M.L.E., Rechtsanwalt; Prof. Dr. jur. Christiane Trüe LL.M. (East Anglia; Uzunma Bergmann, Attorney at Law (New York/USA), Solicitor (England & Wales), Advocate and Solicitor (Nigeria); Günter Stuff, Steuerberater; Cord Meyer, Jurist und Bankkaufmann; Martin Heitmüller, Rechtsanwalt, Maître en Droit (FR); Dr. jur. Reinhard Pohl, Rechtsanwalt (D); Xiaomei Zhang, Juristin (CN); Mag. Iur.; Dennis Jlussi, Rechtsanwalt; Sabine Reimann, Rechtsanwältin (D), Elena Duwensee, Juristin (Ru), Master of Law (Ru), Araceli Rojo Corral, Abogada (ES) .

KORRESPONDENTEN

u.a. Amsterdam, Athen, Bratislava, Brüssel, Budapest, Bukarest, Helsinki, Istanbul, Kiew, Kopenhagen, Lissabon, London, Luxemburg, Mailand, Madrid, Moskau, Oslo, Paris, Prag, Sofia, Stockholm, Warschau, Wien, Salzburg, Zug, New York, Toronto, Mexico City, Sao Paulo, Buenos Aires, Dubai, Kairo, New Delhi, Bangkok, Singapur, Peking, Tokio, Sydney.

VERLAG

CASTON GmbH, Law & Business Information
Luisenstr. 5, D-30159 Hannover,
Fon 0511 - 30756-50 Fax 0511 - 30756-60
Mail info@caston.info; Web www.caston.info