



die-premiummakler.de

© Die Premiummakler Bad Endorf Nur für private Verwendung

## Cyberversicherung

Mit der zunehmenden Bedeutung der Informationstechnologie in Wirtschaftsbereichen wie Dienstleistung, Handel, Handwerk und Warenwirtschaft wachsen auch die Risiken: Was tun, wenn die wertvolle Datenbasis einem Angriff von außen ausgesetzt ist.

Was tun, wenn rufschädigende Inhalte im Internet kursieren? Was tun, wenn beispielsweise Handys abgehört werden – nicht von Geheimdiensten, wie im Falle von Kanzlerin Merkel, sondern womöglich von der Konkurrenz? So jung das Versicherungssegment *Cyberversicherung* noch ist – so rasant wächst es zurzeit auch. Der Grund liegt auf der Hand: Man muss sich vorstellen, dass es für einen Markt, der lange Jahre wegen der hohen Risiken als unversicherbar galt, nunmehr Produkte gibt – eine zumindest kleine Sensation.

## Cyberversicherung: wo sie greift

Ganz allgemein gesprochen geht es bei der Cyberversicherung um eine optionale Zusatzversicherung. Eine solche Cyberversicherung sichert Unternehmen, öffentliche Stellen, Freiberufler oder auch Privatpersonen ab gegen Erscheinungen der Cyberkriminalität. Diese können sein: Internetbetrug, Urheberrechtsverletzung im Internet, Ausspähung von Daten, Volksverhetzung. Wenn Ihnen etwa Daten beim Onlinebanking abhanden kommen – etwa durch sogenanntes Phishing – dann fällt dies in den Bereich der Cyberkriminalität – und ein eventueller Schutz in den Bereich der Cyberversicherung. Das Problem ist übrigens keineswegs rein theoretischer Natur: Mehr als 230 000 Cyber-Straftaten registriert das Bundeskriminalamt pro Jahr – Tendenz stark steigend. Rund 64 000 dieser Fälle können direkt der Computerkriminalität zugeordnet werden; Zunahme pro Jahr ca. 1 Prozent; Schadenhöhe in Deutschland zuletzt ca. 42,6 Mio. Euro. Diese Zahlen mögen gering erscheinen. Das Bundeskriminalamt konstatiert in seinem *Cybercrime Bundeslagebild 2013* allerdings eine hohe Dunkelziffer. Unter Berufung auf eine Studie des Landeskriminalamts Niedersachsen ist festzustellen, dass lediglich 9 % aller Delikte im Bereich Cybercrime überhaupt angezeigt werden. Vor allem im stark steigenden Segment Computersabotage gebe es, so die BKA-Experten, eine “große Anzahl an Straftaten, die ...über das Versuchsstadium nicht hinaus kommt.” Die oben genannten Zahlen müssten, stellt das BKA fest, mit dem Faktor 11 multipliziert werden, um ein reelles Bild der Cyberkriminalität in Deutschland zu bekommen. Damit würde sich der Schaden auf über 400 Mio. Euro jährlich belaufen. Zeit, über eine Cyberversicherung nachzudenken!

## USA Vorreiter bei der Cyberversicherung

Weltweit verursachen Cyberisiken nach einer Studie der Munich Re mehr Schäden als der Schwarzmarkt für Drogen: Auf rund 400 Milliarden Dollar beziffert der Rückversicherer die derzeitige Schadenshöhe durch Cyber-Risiken. Mehr als 400 Millionen Cyberattacken ganz unterschiedlicher Natur gibt es weltweit. Vor allem in den USA drängt die Entwicklung – und weil die Amerikaner geschäftstüchtig sind, wurden schon vor einigen Jahren die ersten Cyberversicherungen angeboten. Mittlerweile hat das Prämienvolumen bei Cyberversicherungen die Milliarden-Dollar-Grenze deutlich überschritten – während sich hierzulande gerade erst das Bewusstsein dafür entwickelt, dass eine Cyberversicherung wertvolle Dienste leistet. Mitte 2013 zogen daher die europäischen Versicherungsgesellschaften nach: Allianz Global Corporate, Zurich, HDI, Württembergische, AXA, R+V, AIG Europe Ltd., Markel Deutschland, Hiscox Deutschland – sie alle bieten nun spezielle Cyberversicherungen an.

# Cyberversicherungen: der Markt

Die Schäden, die Hacker im Datenbestand eines Unternehmens anrichten, können enorm sein. Bei einem Angriff auf die Datenbanken eines Großunternehmens entstehen im Schnitt Schäden in Höhe von 1,8 Mio €; selbst bei kleineren Mittelständlern sind 70 000 bis 100 000 € schnell erreicht. Die Unternehmensberatung Earnest&Young hat kürzlich eine Umfrage unter deutschen Managern vorgestellt – neun von zehn Unternehmern erwarten, dass das Risiko von Cyberattacken in den nächsten Jahren deutlich steigen wird. Fazit: der Bedarf für Cyber-Versicherungen wächst rasant – und der Markt kann kaum Schritt halten. So geht es für nahezu alle Gesellschaften zurzeit darum, eventuell vorhandene Versicherungsprodukte im IT-Bereich speziell auf diese Risiken zuzuschneiden – oder eben ganz neue Angebote zu schaffen. Erst Mitte 2013 geriet der Markt durch oben angeführte und weitere Angebote so richtig ins Rollen. Die Folge ist nunmehr eine zunehmende Vertiefung der Produktpalette: der eine Anbieter integriert Risiken wie Betriebsunterbrechung aufgrund eines Datenschadens, um etwa auf Kunden im E-Commerce-Bereich (Shops) zu zielen. Ein anderer Anbieter hingegen hat soeben einen sogenannten Internet-Schutzbrief als Cyber-Versicherung für Privatleute vorgestellt: hierbei geht es um Verleumdung, Beleidigung, Veröffentlichung von reputationsschädigenden Aussagen, Fotos bzw. Videos ohne Einwilligung. Man denke hierbei nur an die berühmten, mehrfach bereits publizierten Fälle, wo sich Stellenbewerber etwa mit unerlaubt veröffentlichten, anstößigen Fotos konfrontiert sahen – oder aber an die Datenlecks in der i-Cloud von Apple, die kürzlich in den USA unter Prominenten für Furore sorgten.

## Cyberversicherung = Internetschutz

Zurzeit starten zahlreiche Versicherungsgesellschaften im Cyber-Bereich mit einer Cyberversicherung für Privatkunden so richtig durch. Ob R+V, W&W oder ARAG und viele weitere – es ist schwer, im Moment den Überblick über die Marktentwicklung im Bereich Cyberversicherung zu behalten. Auch die Begrifflichkeiten sind ganz unterschiedlich: mal ist das Produkt unter der Bezeichnung Cyber+ zu finden, mal unter Cyber-Versicherung, dann als DataProtect oder ByteProtect, Internetschutz oder InternetschutzPolice oder web@aktiv. Immer geht es dabei um Schäden, die durch Datenmissbrauch in den unterschiedlichsten Formen entstehen können: sei es beim Online-Banking, sei es durch einen Hack des Facebook-Accounts, sei es beim Online-Shopping oder durch Upload eines Virus. Die Facetten beim sogenannten Internetschutz für Privatkunden sind mindestens so zahlreich wie bei Firmenkunden – und so sollte beim Abschluss eines Internetschutzes gründlich geprüft werden, ob es das jeweilige Merkmal wirklich braucht. So sind bei manchen Schutzpolicen etwa Gegenstände integriert, die – im Internet gekauft – Schäden aufweisen. Hier gibt es aber auch z.B. auch Schutz durch große Shops wie Amazon oder Ebay – oder aber, falls die Schäden während des Versands entstehen, durch den jeweiligen Versender.

## Cyberversicherung: Was passiert im Schadensfall?

Ihre IT oder Sie selbst bemerken einen Angriff auf Ihre Datenbanken? Nun geht es darum, schnellstmöglich zu handeln, damit keine wertvollen Daten abhanden kommen. Über eine Hotline der Cyberversicherung werden IT-Forensiker verständigt, die ggf. bei Ihnen vor Ort nicht nur das Leck schließen, sondern ggf. auch orten. IT-Forensiker sind Fachleute, die digitale Spuren erfassen, analysieren und auswerten – vergleichbar den Kriminalforensikern, die man aus dem Fernsehen kennt. Natürlich rückt das Forensik-Team der Cyberversicherung nur bei Angriffen auf größere Systeme an – viele kleinere Fälle lassen sich auch *remote*, das heißt, von außerhalb lösen. Die Hotline vieler Cyberversicherungs-Gesellschaften ist übrigens rund um die Uhr besetzt. So können Sie sicher sein, dass Sie bei einem nächtlichen Daten-Hack nicht bis zum nächsten Morgen warten müssen. Ferner werden Sie im Schadensfall auch kompetent beraten, welche weiteren Spezialisten zur Wiederherstellung des Datenbestands notwendig sind.

## Guter Rat zur Cyberversicherung ist nicht teuer!

Eine Cyberversicherung ist beratungsintensiv. Warum? Oft enthalten die relativ neuen Produkte Bausteine aus anderen Versicherungen – und so wird Premiümmakler Kaspar Bonleitner sorgfältig prüfen müssen, welche Bausteine aus den zahlreichen Angeboten rund um die Cyberversicherung für Sie Sinn machen. Im Privatbereich ist dies einfacher – denn welcher Privatmann hat schon zusätzliche Policen wie z.B. eine Privathaftpflichtversicherung abgeschlossen? Im gewerblichen Bereich dagegen gibt es etwa eine sogenannte Betriebsunterbrechungsversicherung,

die dann gerade steht, wenn die Produktion aus einem Schadensgrund ruht. Einen solchen Baustein noch einmal in eine Cyberversicherung zu integrieren wäre also evtl. "doppelt gemopelt". Jedoch besitzen die meisten klassischen Betriebsunterbrechungsversicherungen keinen Baustein für die Absicherung durch Cyberattacken, Systemausfällen, sowie deren finanziellen Folgen. Darum kann hier eine Ergänzung durchaus als sinnvoll und Existenz sichernd angesehen werden. Für Schäden am Eigentum Dritter – etwa der Kunden durch Datenklau – kommt unter Umständen die Betriebshaftpflicht oder aber eine spezielle Vermögensschadenshaftpflicht auf – dies vorbehaltlich einer genauen und fallbezogenen Prüfung. Auch ein solcher Baustein müsste dann nicht mehr in eine Cyberversicherung integriert sein. Schäden an Festplatten, Handys oder Computern sind unter Umständen über eine Elektronikversicherung abdeckbar.

## Cyberversicherung: "Susi Sorglos" unterwegs...

Vor allem mittelständische Unternehmen scheuen sich noch, über eine Integration einer Cyberversicherung in ihr Versicherungsportfolio nachzudenken. Warum? Man fühlt sich sicher, dank integrierter Firewall beispielsweise. Doch wie schnell ist durch einen Mitarbeiter eine E-Mail mit Malware heruntergeladen? Oder ein Mitarbeiter fängt sich ohne es zu merken auf (z.B. auf dem Buchungsportal eines Reiseportales mit speziellen Firmenkonditionen) einen Shard-Code ein, der nur darauf wartet aktiviert zu werden. Selbst der Suchmaschinen gigant Google oder Firmen wie Apple sind nicht davor gefeit, dass Lecks ganz unfreiwillig entstehen – vergessene Handies, vergessene Notebooks beispielsweise. Der Datenbestand ist schneller verseucht als man denken kann – etwa auch durch schadhafte Kreditkartendaten, die man bereits im "Papierkorb" gut entsorgt glaubt. Und wie schnell geht ein Notebook mit **Dongle** verloren? Die Funk RMCE Beratungsgesellschaft hat, teilweise onlinegestützt, im Herbst 2014 rund 400 kleine bis mittelständische Unternehmen zu möglichen Cyberrisiken befragt – mit teilweise erschreckenden Ergebnissen. Zwar rechnen die meisten Firmeninhaber damit, dass die Risiken zunehmen – sie fühlen sich jedoch durch ihre eigene IT ausreichend geschützt.

Wichtig ist die maßgeschneiderte Cyberversicherung für Sie

Die Befragung brachte zugleich weitere und interessante Ergebnisse, die in der Versicherungswirtschaft aufmerksam studiert werden dürften. Denn dass nur ca. zehn Prozent der Mittelständler eine Cyberversicherung in Erwägung zogen, lag dem Befragungsergebnis vor allem daran, dass viele die meisten neuen Produkte noch nicht kannten – oder jene, die zum Befragungszeitpunkt auf dem Markt waren, als überfrachtet bzw. für ihr jeweiliges Unternehmen als ungeeignet empfanden. Kaspar Bonleitner hierzu:

- Maßgeblich ist zum einen Produktkenntnis. Nur wer den Überblick behält kann sinnvolle Cyberversicherungs-Produkte auswählen
- Zu einem realen Vergleich gehören das Kosten-Nutzen-Verhältnis und die Risikoabwägung. Lohnt die Cyberversicherung? Welche anderen Versicherungen bestehen – vgl. obige Ausführungen
- Die Tarifrchnerprogramme von Bonleitner Versicherungsmakler liefern die leistungsstärksten Cyber-Versicherungen. Sehr wesentlich ist, dass die Programme tagesaktuell sind. Der Anbietermarkt ist, wie beschrieben, sehr dynamisch

So zieht denn auch die Studie der **Funk-Gruppe** ein klares Fazit: „Aufgrund der Heterogenität von Cyber-Risiken, die je nach Branche und Unternehmen ganz unterschiedliche Dimensionen und Ausprägungen haben, muss jede Versicherung individuell gestaltet werden. Lösungen von der Stange kommen im besten Fall für kleingewerbliche Risiken in Frage“.