Absicherung für Privatkunden:

Auch für Privatkunden bieten Versicherer zunehmend Cyber-Tarife an. Cyber-Policen für Privatkunden sichern beispielsweise finanzielle Verluste beim Onlineshopping ab oder bieten psychologische Hilfe gegen Cyber-Mobbing an. Dazu werden häufig Hard- und Softwareschutz sowie diverse Cloud-Dienste angeboten. Die Prämien beginnen in der Regel bereits bei 60 Euro im Jahr.

Ob derartige Versicherungen notwendig sind oder nur ein Nice-to-have für Privatkunden, hängt sicherlich vom persönlichen Nutzungsverhalten und den eigenen Präferenzen ab. Einige sehr gute Haftpflichttarife bieten überdies bereits einen Baustein Internetschutz in ihren Bedingungen an.

Absicherung gegen die Folgen von Hackerangriffen

VERSICHERUNG Das Thema EU-Datenschutzgrundverordnung (DSGVO) ist aktuell bei Unternehmern in aller Munde. Doch Datenschutz, Datendiebstahl und Cyber-Attacken sind Inhalte, mit denen sich Unternehmen ganz grundsätzlich auseinandersetzen müssen. Die deutsche Versicherungswirtschaft hat sich dieser Themen angenommen und bietet entsprechende Absicherungslösungen.

Nahezu jeder Betrieb agiert heutzutage in der ein oder anderen Weise digital. Ob es um die Speicherung von Kundendaten geht, die Kundenkommunikation, Produktionssteuerung, Marketing oder Vertrieb, nichts geht mehr ohne IT.
In den vergangenen Jahren wurden vor allem die Chancen, die sich durch die Digitalisierung ergeben, gesehen und IT, Online-Präsenzen sowie entsprechende Aktivitäten massiv ausgebaut. Durch die Datenschutzinitiative der EU, die bis Ende Mai in Deutschland umgesetzt werden musste und den Namen DSGVO trägt, wird nun der Blick auf die Risiken der Digitalisierung gelenkt.

Die aktuelle Situation

Spötter lächeln über das Zitat des früheren FBI-Direktors James Comey, der vor drei Jahren sagte: „Es gibt nur zwei Arten von Unternehmen – solche, die bereits gehackt wurden, und solche, die noch nicht gehackt wurden."
Tatsächlich ist das Risiko, Opfer eines Cyber-Angriffs zu werden, jedoch hoch. Beim Bundeskriminalamt wurden 2016 mehr als 82.000 derartiger Fälle registriert; Tendenz steigend. Die Dunkelziffer der Opfer von Cyberkriminellen dürfte vermutlich wesentlich höherer liegen. Laut einer Umfrage sind in Deutschland bereits zwei Drittel aller kleinen und mittelständischen Betriebe (KMU) Opfer von Cyberkriminalität geworden. Der geschätzte wirtschaftliche Schaden beläuft sich auf ca. 55 Mrd. Euro pro Jahr!

Ist ein Betrieb erst einmal von einem Cyber-Angriff betroffen, können die Auswirkungen massiv sein. IT-Systeme müssen wiederhergestellt werden, Betriebsunterbrechungen folgen, die Produktion steht in der Zwischenzeit still, Schadensersatzforderungen drohen. Schnell summieren sich die Kosten auf zigtausende Euro und können sogar existenzbedrohend werden.
Doch eine Firmen-IT zu 100 % zu sichern, ist laut führenden IT-Sicherheitsexperten selbst bei größtem Aufwand nicht möglich. Ein Restrisiko eines erfolgreichen Hackerangriffs oder einer Infektion ist nie ganz auszuschließen. Hier kommt dann eine Versicherungslösung als ergänzende Absicherung ins Spiel.

An dieser Stelle soll auch mit einem weit verbreiteten Irrtum aufgeräumt werden. Viele Unternehmer glauben, dass ihre Firma uninteressant für Hacker sei und dass man deshalb selbst von der Problematik nicht betroffen sei. Tatsächlich sind aber drei Viertel aller Cyber-Attacken sog. nichtzielgerichteten Attacken zuzuordnen, das Unternehmen wird also „zufällig" Opfer.
Von Cyberschäden können alle Firmen betroffen sein, die mit Kundendaten und IT-Systemen arbeiten. Besonders gefährdet sind Unternehmen, die mit sensiblen Kundendaten wie Gesundheits- oder Finanzdaten agieren. Beispielhaft seien hier Ärzte, Rechtsanwälte und Steuerberater genannt. Ebenso haben natürlich alle Arten von Produktionsbetrieben genauso wie Onlineshop-Betreiber ein erhöhtes Risiko.

Verzerrte Wahrnehmung

Laut einer Forsa-Umfrage unter kleineren und mittleren Unternehmen im Frühjahr 2018 schätzen die Entrepreneure das Risiko von Cyberkriminalität in Deutschland mehrheitlich als sehr hoch ein. Das eigene Unternehmen als Angriffsziel sehen aber viele nicht.

Aussage	Zustimmung
„Das Risiko von Cyberkriminalität für mittelständische Unternehmen in Deutschland ist eher bzw. sehr hoch.“	75 %
„Das Risiko von Cyberkriminalität für das eigene Unternehmen ist eher bzw. sehr hoch.“	36 %

Quellen: Forsa-Umfrage im Auftrag des GDV, www.gdv.de

Was leistet eine Cyber-Versicherung?

Entsprechend sollte zu einer umfassenden Absicherung eines Unternehmens auch eine entsprechende Cyber-Versicherung zählen. Eine gute Cyberdeckung beinhaltet folgende Bausteine:

Eigenschäden:
Zu den sog. Eigenschäden zählen zunächst einmal wirtschaftliche Schäden durch Betriebsunterbrechung. Beispiel: Ein Virus verschlüsselt alle Rechner eines Unternehmens. Die IT benötigt mehrere Tage, um die Rechner wieder funktionsfähig zu machen, die Produktion steht mehrere Tage still. Aber auch die Kosten für IT-Forensik, Wiederherstellung der Daten und Systeme zählen zu den Eigenschäden.

Drittschäden:
Als Drittschäden werden in der Regel Schadensersatzforderungen von Dritten wegen Datenmissbrauch, Lieferverzug, o. Ä. angesehen. Darüber hinaus zählt auch die Abwehr ungerechtfertigter Ansprüche zum Leistungskatalog.

Serviceleistungen:
Gerade für kleine und mittlere Unternehmen dürften jedoch auch die Serviceleistungen von besonderer Wertigkeit sein. Soforthilfe an 365 Tagen im Jahr, 24 Stunden am Tag ist von den üblichen IT-Dienstleistern der Unternehmen wohl nur in den seltensten Fällen darstellbar. Der Umfang der Serviceleistungen umfasst neben der Soforthilfe in der Regel auch IT-Analyse, Beweissicherung, Schadensbegrenzung sowie Leistungen für Krisenkommunikation und PR-Management zur Eindämmung eines Imageschadens.

Auf was ist zu achten

Neben den bereits angesprochenen möglichst umfassenden Leistungen für Eigen- und Drittschäden sowie Serviceleistungen sollte auf eine ausreichende Höhe der Versicherungssumme geachtet werden. Ein Cyberschaden kann schnell sechsstellige Summen erreichen. An der Versicherungssumme sollte keinesfalls gespart werden.
Neben erheblichen Unterschieden im Deckungsumfang und der Prämie zeigen sich bis dato auch deutliche Unterschiede in der „Risikoprüfung“. Gerade kleinere Betriebe können die Vorgaben von manchem Versicherer kaum erfüllen, während sie bei anderen Gesellschaften problemlos versicherbar sind. Der Weg zum Versicherungsmakler empfiehlt sich also auch beim Abschluss einer Cyber-Versicherung.

Welche Voraussetzungen müssen gegeben sein?

Für den erfolgreichen Abschluss einer Cyber-Versicherung müssen gewisse Grundvoraussetzungen unternehmensseitig erfüllt sein. Diese sind zwar in aller Regel auch Voraussetzung für DSGVO-konformes Arbeiten. Trotzdem soll explizit darauf hingewiesen werden, dass eine ausreichende Sicherung der IT-Systeme Grundvoraussetzung für den erfolgreichen Abschluss einer Cyber-Versicherung ist. Die nachfolgende Aufzählung ist nicht abschließend, von Gesellschaft zu Gesellschaft unterschiedlich und soll nur die wichtigsten Kernpunkte darstellen:

- Aktuelle Virenschutzprogramme und Firewall,
- regelmäßige Datensicherung/Backup,
- vorschriftsgemäße Verschlüsselung,
- zentrale Admin-Struktur,
- sicherer Datenaustausch mit Dritten.

Fazit

Eine Cyber-Deckung gehört für mittelständische Unternehmen heute unbedingt ins Absicherungsportfolio. Aber auch viele kleinere Betriebe sollten über den Abschluss einer solchen Versicherung nachdenken. Die Jahresprämie liegt für Unternehmen bis 5 Mio. Euro Umsatz in der Regel nicht über dem Tagessatz eines IT-Dienstleisters. Wenn man dem die versicherten Leistungen gegenüberstellt, kann man nur zu einem Schluss kommen: Abschließen!

Erik Altmann
Versicherungsexperte der SdK e.V.

SdK

Sie haben Fragen zu Versicherungsprodukten und sind Mitglied der SdK Schutzgemeinschaft der Kapitalanleger e.V.?

Dann wenden Sie sich unter Angabe Ihrer Mitgliedsnummer an unseren Versicherungsexperten, entweder per E-Mail unter **versicherungen@sdk.org** oder telefonisch unter 089 324965-10.