

Cyber-Versicherung im Detail

Category: Firmenkunden, Schaden, Übergreifend

17. Juli 2021



Es vergeht kaum ein Tag, an dem nicht von neuen Cyber-Angriffen in der Presse zu lesen ist. Ob es sich um die fast schon [gewohnten Angriffe auf den deutschen Bundestag und bevorstehende Wahlen](#) handelt, den durch einen Hackerangriff ausgelösten [Katastrophenfall in der Kreisverwaltung Anhalt-Bitterfeld](#) oder sogar um [Attacken auf Versicherungsgesellschaften](#), an Cyberangriffe werden wir uns wohl oder übel gewöhnen müssen. Hierüber [berichteten wir bereits vor 5 Jahren](#) und halten deswegen die Cyber-Versicherung für eine der wichtigsten Versicherungen der Gegenwart und Zukunft. Manche behaupten sogar, es handele sich um die neue Feuerversicherung, d.h. wichtigste Versicherung überhaupt.

Wir möchten ausführlich erläutern, was eine Cyber-Versicherung leisten kann und worauf hierbei zu achten ist.

Lesedauer: Ca. 6 Minuten

Der Versicherungsfall in der Cyber-Versicherung

Die Cyber-Versicherer gewähren in der Regel

Versicherungsschutz für die Beschädigung, Zerstörung, Veränderung, Blockierung oder den Missbrauch Ihrer IT-Systeme, Programme und der elektronischen Daten verursacht durch

- einen unbefugten Eingriff in die IT-Systeme (Hacker-Angriff),
- einen unbefugten Angriff mit dem Ziel, die IT-Systeme zu unterbrechen (sog. DoS-Attacke),
- eine Infektion Ihres IT-Systems durch Schadsoftware, Viren, Schadcodes und Trojaner oder Bedienfehler.
- Dabei sollte darauf geachtet werden, dass nicht nur gezielte, sondern auch ungezielte Angriffe vom Versicherungsschutz umfasst sind. Ansonsten sind zufällige Schäden, z.B. durch ein weitverbreitetes Virus nicht mitversichert.

Welche Auswirkungen durch solche Angriffe abgesichert sind, bestimmen die nachfolgend aufgelisteten Bausteine, die individuell zusammengestellt werden können.

Cyber-Eigenschaden

Der Grundbaustein einer Cyber-Versicherung sind die Eigenschäden. Hierüber sind u.a. versichert:

- Wiederherstellung der eigenen IT-Systeme sowie der Website
- IT-Forensik zur Suche und Entfernung von Schadensoftware
- PR-Beratung und weitere Dienstleistungen zum Erhalt der Reputation nach einem Cyber-Vorfall

Meist inkludiert, bei einigen Versicherern aber auch separat geführt sind Cyber-Vertrauensschäden. Dies ist u.a. der Fall, wenn Mitarbeiter oder Dritte einen Betrug wie beispielsweise Unterschlagung von Geld oder Erschleichung von Zahlungen an Ihrem Betrieb durchführen. Die bekannteste Form ist der Fake President, den wir in einem [früheren Blogartikel bereits näher](#)

[beschrieben haben.](#)

Cyber-Haftpflicht

Ebenfalls meist obligatorisch ist die Cyber-Haftpflichtversicherung. Diese schützt ihr Unternehmen gegen Schadenersatz Dritter nach einem Cyber-Vorfall. Werden etwa die Daten Ihrer Kunden bei einem Hackerangriff abgefischt und für kriminelle Zwecke genutzt, können ihre Kunden den entstandenen Schaden Ihnen gegenüber geltend machen. Gleiches gilt, wenn Sie versehentlich Schadsoftware verbreiten, z.B. durch Mailanhänge oder von Ihnen genutzte Software. Die normale Betriebshaftpflichtversicherung bietet hiergegen meist nur einen sehr unzureichenden Schutz.

Betriebsunterbrechung nach Cyber-Vorfall

Selbst Unternehmen ohne Onlineshop sind heutzutage häufig extrem abhängig von ihren IT-Systemen. Die elektronische Zugangskontrolle zu den Betriebsräumen, der Mail-Account, die Kundendatenbank oder Schichtpläne – fast alles wird heute digitalisiert und ist damit angreifbar. Steht der Betrieb anschließend still, kann es schnell zu erheblichen Umsatzausfällen kommen. Dieser Schaden kann durch einen Betriebsunterbrechungsbaustein im Rahmen der Cyber-Versicherung abgedeckt werden.

Cyber-Erpressung und Lösegeld

Hackerangriffe sind in vielen Fällen mit Lösegeldforderungen verbunden, [so wie man es auch im realen Leben kennt](#). Die Angreifer sperren beispielsweise die IT-Systeme des Opfers und verlangen einen Betrag zur Entsperrung. Derzeit ist dieses

Risiko noch durch einen Erpressungsbaustein im Rahmen der Cyber-Versicherung absicherbar und für viele Kunden auch sehr sinnvoll.

Jedoch gibt es seit einiger Zeit Bestrebungen, derartige Bausteine gesetzlich zu verbieten, da man davon ausgeht, dass viele Angriffe nur deswegen erfolgen, weil die Hacker auf die Leistung auf der Cyber-Versicherung hoffen. In Frankreich etwa hat der größte Versicherer bereits die Cyber-Erpressung aus dem Regal genommen.

In jedem Fall sollte über eine vorhandene Erpressungsversicherung Verschwiegenheit herrschen. Oftmals wird dies von den Versicherungsgesellschaften auch vertraglich gefordert.

Kreditkartenschäden

Verarbeiten Sie in Ihrem Unternehmen in größerem Maße Kreditkartendaten (hierzu reicht bereits das Akzeptieren von Kreditkarten als Zahlungsmittel), unterwerfen Sie sich in aller Regel dem PCI-Standard der großen Kreditkartenanbieter. In diesem ist unter anderem geregelt, dass Sie hohe Vertragsstrafen bezahlen müssen, wenn durch Ihre Systeme Kreditkartendaten gestohlen werden. Da es sich bei Vertragsstrafen juristisch gesehen nicht um Schadenersatzansprüche handelt, greift hier die Cyber-Haftpflicht meist nicht. In diesen Fällen ist dann ein Zusatzbaustein für Schäden aus dem PCI-Standard notwendig.

Schäden an Hardware

Cyber-Versicherungen sichern zunächst Vermögensschäden nach einem IT-Vorfall ab. Allerdings sind auch Schäden denkbar, bei denen die Angreifer Hardware attackieren. So können

beispielsweise Lüfter der PCs bewusst überhitzt oder auch Gebäudetechnik und Produktionsmaschinen beschädigt werden. Einige Versicherer bieten hierfür spezielle Zusatzbausteine an.

Obliegenheiten in der Cyber-Versicherung

Auch die beste und kundenfreundlichste Cyber-Versicherung ist nutzlos, wenn man als Kunde seine IT-Sicherheit vollkommen vernachlässigt. Ein gewisses Schutzniveau wird heutzutage vorausgesetzt und auch als vertragliche Obliegenheit bei Abschluss der Versicherungspolice vereinbart, z.B.:

- Regelmäßige Back-Ups (z.B. einmal wöchentlich)
- Das Nutzen eines Virenscanners
- Einspielen regelmäßiger Updates der Sicherheitssoftware

Verstößt man gegen diese Obliegenheiten, kann der Versicherer seine Leistung im Schadenfall kürzen oder ggf. ganz ablehnen.

Unabhängig von Ihren vertraglichen Pflichten ist es ratsam, Regelungen im Unternehmen festzulegen, die die IT-Sicherheit verbessern und die Auswirkungen nach einem Angriff begrenzen. Hierfür bestehen bei den meisten Cyber-Versicherern Kooperationen mit Dienstleistern, die Sie beim Thema IT-Sicherheit unterstützen.

Die richtige Versicherungssumme in der Cyber-Versicherung

Wie so oft, gibt es *DIE* richtige Versicherungssumme natürlich nicht. Dennoch gibt es natürlich Ansätze, sich der passenden Versicherungssumme zu nähern. Der Spezialanbieter Markel [hat beispielsweise ein einfaches Tool](#) entwickelt, mit der man grob die notwendige Versicherungssumme ermitteln kann. Wir nutzen

in unserer Beratung Programme, die noch detaillierter die Besonderheiten Ihres Unternehmens berücksichtigen.

Zur Wahrheit gehört aber auch, dass sich nicht seriös sagen lässt, wozu Hacker in Zukunft in der Lage sein werden. Daher kann jedes Berechnungstool nur einen Ansatz zur Bestimmung einer geeigneten Versicherungssumme geben. Generell gilt daher: je höher die Versicherungssumme, desto besser.

Anbieter für Cyber-Versicherungen

Zunächst wurde der Markt der Cyber-Versicherung vor allem von amerikanischen und britischen Versicherern dominiert. Heute bietet nahezu jeder Versicherer eine Cyber-Versicherung an, wobei die Qualität höchst unterschiedlich ausfällt.

Bisher haben sich vor allem Spezialanbieter wie Hiscox, Markel, AIG, Chubb und Cogitanda in diesem Marktsegment profiliert, aber auch große Versicherer wie Allianz, HDI oder AXA haben nennenswerte Marktanteile und in einigen Fällen sehr vernünftige Produkte. Der Markt ist jedoch noch sehr jung und dynamisch, weshalb sich die Produktauswahl schnell ändern kann.

Was kostet eine Cyber-Versicherung?

Der Preis für Cyber-Versicherungen hängt sehr stark von den Versicherungssummen, der Unternehmensgröße und der Branche ab. Kleine Unternehmen erhalten einen vollwertigen Cyber-Schutz bereits in einer Größenordnung von 300€ pro Jahr. Bei größeren Unternehmen mit Umsätzen im Millionenbereich muss eher mit 1.000€ aufwärts gerechnet werden.

Da der Versicherungsschutz, die Versicherungssummen und Selbstbehalte in den einzelnen Bausteinen sehr individuell gestaltet werden können, ist eine pauschale Aussage zum Preis

aber nicht im Voraus möglich.

Cyber-Schutz in anderen Policen

Unternehmen besitzen in ihren vorhandenen Versicherungsverträgen vereinzelt bereits Schutz bei Cyber-Vorfällen. So enthalten einige Betriebs- und Vermögensschäden bereits eine Cyber-Haftpflicht, auch kann über die Elektronikversicherung ein gewisser Schutz für verlorene Daten bestehen. Wirklich umfassend und lückenlos sind diese Einschlüsse in aller Regel nicht. Auch der für wenig Geld zubuchbare Cyberschutz in vielen Unternehmenspolicen ist meist mit einer echten Cyber-Versicherung vergleichbar. In Einzelfällen kann er für kleine Unternehmen aber dennoch sinnvoll sein, wenn die finanziellen Ressourcen für eine komplette Cyber-Versicherung nicht ausreichen und das Unternehmen nur leicht gefährdet ist, Opfer eines Hacker-Angriffs zu werden.

Cyber-Versicherung für Privatkunden

Obwohl Sie bereits vor Jahren von verschiedenen Versicherern angekündigt wurde, warten wir bis heute auf die erste vollumfängliche Cyber-Versicherung für Privatkunden. Vielmehr bietet der Markt bislang nur Teillösungen, z.B. Cyber-Rechtsschutzversicherungen, Schutz gegen Phishing oder Persönlichkeitsverletzungen. Auch enthalten einige gängige Produkte wie Privathaftpflicht- und Hausratversicherungen einzelne Komponenten zum Cyber-Schutz.

Eine umfängliche Lösung scheitert bisher vermutlich noch am Preis und der Tatsache, dass bei Privatkunden harte Obliegenheiten wohl kaum durchsetzbar wären.

Angebot zur Cyber-Versicherung

Um ein Angebot zur Cyber-Versicherung zu erhalten, genügt in vielen Fällen ein Gespräch mit uns, in dem wir Ihren Bedarf und die passenden Versicherungssummen ermitteln. Dies ist in der Regel kurzfristig [im Rahmen einer Onlineberatung](#) möglich.

Nur selten wird darüber hinaus ein AUDIT nötig, bei dem ein IT-Fachmann Ihre Systeme im Detail untersucht und Schwachstellen aufzeigt. Meist ist dies nur bei sehr hohen Umsätzen oder besonders sensiblen Branchen obligatorisch.

Sie haben weitere Fragen zum Thema Cyber-Versicherung? [Dann kommen Sie gerne auf uns zu.](#)

©Bild: Jefferson Santos / Unsplash