# Cyber-Versicherungen

## Whitepaper




2020

## Sind Cyber-Versicherungen sinnvoll?

Seit einigen Jahren bieten auch in Deutschland diverse Versicherungsunternehmen Cyberversicherungen an. Vor dem Hintergrund spektakulärer, von den Mainstream-Medien aufgegriffener Fälle von Angriffen (Locky, Goldeneye, etc.) rücken diese Produkte derzeit stärker ins Rampenlicht. Die Produktkategorie ist zwar noch recht neu, weist aber hohe Wachstumsraten auf, zumindest in den USA, wo Zahlen vorliegen. In den USA beträgt das Marktvolumen – je nach Quelle - zwischen 1,3 und 2 Milliarden Dollar[1].

Da Cyber-Risiken in der Tat zunehmen, stellt sich die Frage, ob es sich für Unternehmen lohnt, eine Cyber-Versicherung abzuschließen. Wir meinen, für die meisten Unternehmen lautet die Antwort eher nein. Natürlich enthält die Antwort auch eine kommt-darauf-an-Komponente.

### Grundlegendes

Um die oben gestellte Frage zu beantworten, sollte man sich ins Gedächtnis rufen, wann Versicherungen generell Sinn machen und wann nicht.

- Eine Versicherung macht immer dann Sinn, wenn der potenzielle Schaden groß bis existentiell ist und die Eintrittswahrscheinlichkeit gering bis sehr gering ist (bzw. das Schadensereignis selten ist) und der Schaden daher für eine einzelne Person oder Unternehmen nicht kalkulierbar ist.
- Sich gegen selten auftretende und überschaubare Schäden abzusichern, macht aus offensichtlichen Gründen keinen Sinn.
- Kommt das Schadensereignis öfters vor, die Schadenshöhe ist aber gering, ist meist die Eigenversicherung sinnvoller (privat: sparen, Unternehmen: Kosten in das Produkt einkalkulieren).
- Ist der potenzielle Schaden groß und das Schadensereignis kommt öfter vor (hohe Eintrittswahrscheinlichkeit), sollte man eher etwas Grundlegendes ändern als eine Versicherung abzuschließen. Zumal man für solch eine Konstellation i.d.R. keinen Versicherungs-Anbieter findet.

Die beschriebenen Szenarien müssen natürlich an der zu zahlenden Versicherungsprämie gespiegelt werden.

Damit ist die Fragestellung eingegrenzt:

1. Hat ein Unternehmen einen in IT-Anwendungen und Infrastruktur begründeten hohen bis sehr hohen Schaden zu befürchten?
2. Wie hoch ist die zu leistende Prämie im Verhältnis zum potenziellen Schaden?

[1] https://www.reuters.com/article/fitch-us-cyber-insurance-industry-grows/fitch-u-s-cyber-insurance-industry-grows-35-loss-rates-improve-idUSFit8PFGH3 und https://www.aba.com/Tools/Function/Documents/2016Cyber-Insurance-Buying-Guide_FINAL.pdf

**Was decken Cyber-Versicherungen überhaupt ab?**

Cyber-Versicherungen decken eine ganze Reihe von Schadensfällen ab, wobei es letztlich auf den Anbieter und den Vertragsinhalt ankommt. Wie bei vielen anderen Versicherungen auch, gibt es Wahl- und Ausgestaltungsmöglichkeiten, z.B. bezüglich der Leistungen und der maximalen Versicherungssumme.

Die Versicherungen unterteilen sich grundsätzlich in zwei (Teil-)Versicherungen:

- Versicherung gegen Drittschäden („Cyber-Haftpflichtversicherung“)
- Versicherung gegen Eigenschäden

Im ersten Fall werden Schadenersatzansprüche von Dritten versichert (sofern nichts anderes vereinbart ist: aufgrund von Vermögensschäden), die z.B. aus einem Datenverlust oder einer Datenrechtsverletzung resultieren. Mit letzterem ist u.a. eine Verletzung der am 25.05.2018 in Kraft tretenden DSGVO gemeint.

Im zweiten Fall sind die Kosten gemeint, die dem Unternehmen selbst entstehen, z.B. durch Betriebsunterbrechungen (entgangener Gewinn) oder Kosten der Daten-Wiederherstellung.

**Wie finde ich heraus, ob eine Cyber-Versicherung sich für mich lohnt?**

Um die Sinnhaftigkeit einer Cyber-Versicherung zu beurteilen, muss man betrachten:

- welches Risiko besteht überhaupt?
- wie hoch ist der potenzielle Schaden?
- kann ich mich möglichst „maßgeschneidert“ versichern?
- und wie hoch ist die Versicherungsprämie?

Gehen wir ein paar Beispiele durch:

**Cyber-Haftpflicht**

**In Ihrer Webshop-Datenbank sind Kundendaten gespeichert. Durch einen Hacker-Angriff werden diese gestohlen.**

Üble Sache. Aber Ihre Cyber-Haftpflicht-Versicherung übernimmt ja den entstandenen Vermögensschaden. Aber worin besteht dieser nun? Wir als Systemhaus sind keine Anwaltskanzlei und können daher keine rechtsverbindliche Auskunft geben. In diesem Szenario ist jedoch folgendes wahrscheinlich: Damit ein Schaden beglichen werden kann, muss er beziffert werden.

Sind z.B. nur Namen, Mailadressen und Passwörter gehackt worden, ist unwahrscheinlich, dass die betroffenen Kunden einen Schaden tatsächlich nachweisen können.

Handelt es sich um Kreditkarten, sieht die Sache schon etwas anders aus. Die Kreditkartengesellschaften können die Schäden sicherlich genauer beziffern. Haben Sie den Angriff schnell bemerkt – was nicht immer der Fall ist – und die Kreditkartengesellschaft hat die Karten schnell gesperrt, hält sich der finanzielle Schaden vermutlich noch in Grenzen.

Bleibt der Schaden durch abwandernde Kunden und der Reputationsschaden. Da es sich hierbei um Ihren eigenen Schaden handelt, fällt dies in den Bereich der Eigenschadenversicherung. Viele Eigenschadenversicherung decken diesen Fall jedoch nicht ab und da dies sowieso kein Vermögensschaden ist, gehen Sie an der Stelle leer aus.

An diesem Beispiel sieht man schon, dass die Sinnhaftigkeit nicht einfach zu beantworten ist. Wobei z.B. beim Betreiben eines Webshops die Frage der Sinnhaftigkeit sicherlich ernsthaft beleuchtet werden sollte. Je nach Branche, Geschäftsmodell und – trotz Sicherungsmechanismen - von außen zugänglicher Daten, kann der potenzielle Schaden im Einzelfall enorm sein.

Ein anderes Beispiel ist: Wenn ein Mittelständler für einen Automobilhersteller arbeitet und ein Angreifer über dessen IT Zugriff auf Entwicklungsgeheimnisse erhält, kann der Schaden existenzgefährdend sein.

Eine Leitfrage, die daher als Ausgangspunkt einer Risikobetrachtung für alle Unternehmen gestellt werden kann, lautet:

Wie ist Ihr Unternehmen über IT-Schnittstellen nach außen exponiert? Wenn der einzige Weg nach draußen Ihr Email-System ist, ist ihre Risiko-Exposition und die Sinnhaftigkeit der Cyber-Haftpflichtversicherung deutlich geringer, als wenn Sie einen Webshop betreiben.

## Eigenschadensversicherung

Schauen wir uns einige Kostenpositionen an, die Eigenschadensversicherung abdecken:

Kosten für:

- Wiederherstellung von Daten
- Betriebsunterbrechung[2]
- Lösegeld / Cyber-Erpressung (Verschlüsselungstrojaner)
- Denial-of-Service-Angriff (mögliche Ursache für Betriebsunterbrechung)
- Benachrichtigungskosten (Informationspflicht nach § 42a BDSG)
- Krisenmanagement- und Public-Relations-Maßnahmen
- Kreditüberwachungsdienstleistungen
- Schadenermittlung / Kosten für Computer-Forensik
- Rechtsverfolgungskosten

Auch hier ist eine absolute Generalisierung – „*sehr sinnvoll*!“ vs. „*braucht-man-nicht*“ - sicher nicht richtig. Wenn man jedoch die einzelnen Positionen durchgeht und eine – zugegebenermaßen geschätzte - potenzielle Schadenssumme daneben schreibt, wird man feststellen: Es kann ins Geld gehen – existenzgefährdend sind die Summen nicht. Und: den entgangenen Betriebsgewinn muss man auch erst mal nachweisen.

[2] Auszug aus den Versicherungsbedingungen der RvU: „Der Betriebsunterbrechungsschaden besteht aus den fortlaufenden Kosten und dem Betriebsgewinn in dem versicherten Betrieb, die der Versicherungsnehmer (…) nicht erwirtschaften kann, weil der frühere Zustand versicherter Daten wiederhergestellt werden muss.“

**Fazit: Ist eine Cyberversicherung sinnvoll oder nicht?**

Zunächst sollte man sich vor Augen führen: Eine Cyberversicherung ersetzt keine notwendigen und angemessenen technischen Maßnahmen. Und wenn man sich derart bedroht fühlt oder einen großen Schaden befürchtet, dass man über eine Cyberversicherung nachdenkt, sollte man zunächst prüfen, ob die technischen und organisatorischen Maßnahmen überhaupt dem empfohlenen Mindestmaß entsprechen.

So sollte zum Beispiel jedes Unternehmen einen Wiederherstellungsplan haben, der die Maßnahmen und Informationswege beschreibt, die notwendig sind, wenn unternehmenskritische Systeme nicht mehr funktionieren. In der Praxis verfügen die wenigsten Unternehmen über solch einen Plan, geschweige denn, dass zumindest Einzelschritte daraus – z.B. das Rücksichern von Backups – regelmäßig getestet werden.

Wenn ein angemessenes Schutzniveau erreicht ist, und man darüber hinaus einen zusätzlichen Schutz durch eine Versicherung haben möchte, weil man einem erhöhten Risiko ausgesetzt ist, kann eine Cyberversicherung durchaus Sinn machen. Dann ist es letztlich eine Frage der Höhe der Versicherungsprämie und der eigenen – durchaus subjektiven - Risiko-Bewertung, ob diese den zusätzlichen Schutz wert ist.

**Update Januar 2022**

Die Prämien für Cyberversicherungen sind im Jahr 2021 stark angestiegen. Was kein Wunder ist, da die Vorfälle deutlich zugenommen haben. Diese Entwicklung kann man in zwei Richtungen interpretieren: Einerseits kann man das als Begründung ansehen, warum Cyberversicherungen notwendig sind. Andererseits deutet es darauf hin, dass zunächst das Schutzniveau der IT-Sicherheit überprüft und ggf. angepasst werden sollte. Ersteres ist sowieso in regelmäßigen Abständen angeraten.

Die Aussage des Whitepapers bleibt unterm Strich jedoch dieselbe: Die Grundlage ist eine gute IT-Sicherheit. Auf dieser Basis muss jedes Unternehmen für sich abwägen, ob die Prämien für eine Cyberversicherung den potenziellen (d.h. im Schadensfall eintretenden) finanziellen Schutz wert sind.