Versicherung

FFU Frankreich für Unternehmen

Grundlagenwissen

Cyber-Risiken und Versicherungslösungen in Frankreich

April 2022

Heutzutage gibt es zahlreiche Beispiele für Cyberattacken mit teils dramatischen Folgen. Es kam bereits zu Angriffen auf die größte Pipeline in den USA, zu verschiedenen Angriffen auf Gesundheitssysteme in Europa, Ransomware gegen Regierungsbehörden usw.

Was versteht man unter einem Cyberangriff? Wo liegen derzeit die größten Cyberrisiken? Gibt es Versicherungslösungen, um sich vor den finanziellen Folgen solcher Ereignisse zu schützen? Wir werden diese verschiedenen Punkte im Folgenden genauer unter die Lupe nehmen und versuchen, Ihnen diesbezüglich Klarheit zu verschaffen.

1. Was ist ein Cyberangriff?

Es handelt sich um einen Angriff des IT-Systems (Software, Programme, Server, Netzwerkinfrastruktur, Cloud- oder Hosting-Dienste etc.) und/oder von digitalen Daten (persönlichen, vertraulichen, medizinischen, Bankdaten etc.).

Meist führt ein Cyberangriff für Unternehmen zu Kosten und Verlusten, finanziellen Folgen, Image- oder Rufschädigung wie Datendiebstahl, Netzwerkunterbrechungen sowie Reklamationen von Dritten wie Kunden.

2. Was sind die größten Cyberbedrohungen in Europa?

In den Jahren 2019 und 2020 hat der Rat der Europäischen Union fünf große Arten von Cyberbedrohungen identifiziert, und zwar:

- Malware, d. h. Programme, die darauf ausgelegt sind, ohne das Wissen des Eigentümers auf ein Gerät zuzugreifen oder es zu beschädigen, inklusive zu Spionagezwecken,
- Webbasierte Angriffe, d. h. verschiedene Techniken, die verwendet werden, um Webbrowser auf Seiten umzuleiten, auf denen es zu Malware-Infektionen kommen kann,
- Phishing d. h. ein betrügerischer Versuch, Benutzerdaten wie Anmeldedaten oder Kreditkarteninformationen zu stehlen, indem man sich als ein vertrauenswürdiger Betreiber ausgibt,

GROUPE ROEDERER

Roederer
2, rue Bartisch
F-67100 Strasbourg

+33 (0)3 88 76 73 00
roederer@ffu.eu
www.roederer.fr

- Angriffe über Webanwendungen, d. h. das Einspeisen von bösartigem Code in anfällige Server und mobile Anwendungen, um so unbemerkt an vertrauliche Daten zu gelangen,
- Junk-Mails (SPAM), d. h. das massenhafte Versenden unerwünschter Nachrichten, die als Bedrohung der Internetsicherheit erachtet werden, da diese ein Mittel zur Verbreitung oder Befähigung anderer Bedrohungen darstellen.

Bewahrheiten sich diese Bedrohungen, so kann es für die betroffenen Unternehmen zu verschiedenen Verlusten und Schäden kommen, wie z. B. Lahmlegung der Produktionsanlagen, Lösegeldforderungen zur Herausgabe sensibler Daten, Offenlegung vertraulicher Informationen etc.

Dies führt uns zur nächsten Frage: Lassen sich diese Risiken versichern?

3. Aktuelle Cyber-Versicherungslösungen auf dem Markt

Auf dem französischen Markt bieten derzeit mehrerer Versicherer Lösungen an.

a. Die von den Cyberversicherungen getragenen Kosten

Die meisten Cyber-Versicherungsverträge auf dem französischen Markt sehen eine Deckung vor, die sich in drei wesentliche Aspekte gliedern lässt, nämlich:

➞ **Krisenmanagement und Kommunikation**

In diesem Fall decken die Verträge die Kosten für Rechtsberatung, IT-Experten, Kommunikationskosten, Meldegebühren, insbesondere an die CNIL (französischer Ausschuss für Datenschutz), Kosten zur Wiederherstellung von Daten etc.

➞ **Schaden, den die Tätigkeit Ihres Unternehmens genommen hat; Aspekt: „Schadensversicherung“**

Hierbei decken Cyberpolicen Folgendes ab:

- Betriebsverluste,
- Cyber-Erpressungen: Je nach Vertrag können Versicherer Lösegeldzahlungen, Honorare für Experten, Übersetzungskosten oder Belohnungen übernehmen,
- Ermittlungen und Sanktionen einer Behörde

GROUPE ROEDERER

Roederer
2, rue Bartisch
F-67100 Strasbourg

+33 (0)3 88 76 73 00
roederer@ffu.eu
www.roederer.fr

➡ **Schäden, die Dritten durch Ihre Tätigkeit entstehen; Aspekt: „Haftpflicht“**

Versicherungsverträge decken die Kosten für die Verteidigung und die finanziellen Folgen, die sich aus einer Beschwerde ergeben.

b. Differenzierung Ihrer Versicherungsverträge zur „allgemeinen Haftpflicht“ und zu „Sachschäden“

Mit keinem dieser zwei Verträge, welche die meisten Unternehmen abschließen, können die Kosten für das Krisenmanagement und die Kommunikation im Zusammenhang mit einem Cyberangriff gedeckt werden.

Zudem ist die Leistung Ihrer Haftpflicht- und Sachschadenversicherung möglicherweise sehr stark eingeschränkt. Sie sollten die Klauseln Ihrer Verträge stets sehr sorgfältig durchlesen, da viele von ihnen Ausschlüsse dieser Art von Risiken vorsehen und die daraus resultierenden Kostenübernahmen sehr begrenzt oder gar nicht vorhanden sein können.

Beispiel: Bei Sachschadensversicherungen werden die Kosten für die Wiederherstellung von Daten nur dann übernommen, wenn sie infolge eines Sachschadens entstehen, der durch ein versichertes Ereignis (Brand, Wasserschaden usw.) verursacht wurde.

c. Entwicklungen auf dem Versicherungsmarkt im Jahr 2021

Im Jahr 2020 wurden insgesamt 130 Mio. € an Prämien eingenommen und 217 Mio. € an Schäden reguliert, was einer Schadenquote von 167% (gegenüber 84% im Jahr 2019) entspricht. Die Cyber-Branche ist daher stark defizitär und die eingenommenen Prämien reichen den Versicherern nicht mehr aus, um die bezahlten Schäden zu begleichen. Die Häufigkeit des Auftretens von Schadensfällen war zwischen 2019 und 2020 relativ stabil, die Kosten sind jedoch stark angestiegen.

Der Markt musste sich somit zwangsläufig anpassen, und es lassen sich seit Ende 2020 folgende Phänomene feststellen:

- Verstärkte Selektivität der Risiken durch die Versicherer; insbesondere durch die Erstellung komplexer und umfangreicher Fragebögen;
- Minderung der Kapazitäten;
- Anstieg von Prämien und Selbstbehalt;
- Überarbeitung des Wortlauts der Policen. In unserem aktuellen Kontext des Krieges zwischen der Ukraine und Russland stellt sich die folgende Frage: Sind die Cyber-Angriffe von Russland versichert oder nicht? Unsere Antwort hierauf: Wir

müssen Ihren Vertrag diesbezüglich im Einzelnen prüfen, da einige diesen Ausschluss vorsehen, andere aber nicht.

Der Versicherungsmarkt arbeitet derzeit auf einen entsprechenden Reifegrad hin, um sich stabilisieren zu können. Deshalb ist es stets nötig, einen kompetenten Versicherungsmakler zur Seite zu haben, der Sie in diesem Kontext beraten kann!

4. Die Tipps von Roederer

Es ist wichtig, zu bewerten, wie stark Sie bestimmten Risiken ausgesetzt sind, und hierbei Ihre vertraglichen Verpflichtungen gegenüber Dritten sowie Erfahrungen im Hinblick auf Rechtsstreitigkeiten zu berücksichtigen.

Ferner muss auch angemerkt werden, dass Versicherungen nur einen Teil des Cyberrisikomanagements ausmachen. Alle Beteiligten müssen bemüht sein, die Herausforderungen besser zu verstehen, Prävention und Krisenmanagement zu betreiben und schließlich das Restrisiko zu übertragen.

Wenn Sie Fragen haben oder einen Kostenvoranschlag anfordern möchten, können Sie sich sehr gern an unsere Experten wenden!

Ihre deutschsprachigen Ansprechpartnerinnen:

GROUPE ROEDERER

Céline Gogniat-Schmidlin
Leiterin der internationalen Abteilung

gogniat-schmidlin@ffu.eu
+33 (0)3 88 76 73 14