

Franke und Bornberg präsentiert erstes Cyber-Rating

Die Ratingagentur Franke und Bornberg veröffentlicht das erste Rating für gewerbliche Cyber-Policen im deutschen Markt. Untersucht wurden 35 Tarife und Bausteinlösungen von 28 Anbietern. Noch sind die Leistungsunterschiede groß und es gibt nur wenige Top-Tarife.

Die Gefährdung durch Cyber-Risiken ist vielschichtig und entwickelt sich dynamisch. Das bestätigt der Bericht zur Lage der IT-Sicherheit, den das Bundesamt für Sicherheit in der Informationstechnik (BSI) erst vor wenigen Tagen veröffentlicht hat. Cyber-Angriffe richten sich mittlerweile gezielt gegen die Grundpfeiler der Informationstechnologie. Gleichzeitig schreitet die Digitalisierung und Vernetzung von IT-Systemen, Alltagsgegenständen und Produktionsanlagen voran. Die Kombination aus neuer Angriffsqualität und beschleunigter Digitalisierung hebt die Gefährdungslage auf ein neues Niveau.

Versicherungen versprechen Schutz. Am deutschen Markt sind Cyber-Versicherungen für Unternehmen seit gut acht Jahren präsent, zunächst für Industrie-Risiken und auf Basis anglo-amerikanischer Deckungskonzepte. Spätestens mit den Cyber-Attacken auf den Deutschen Bundestag und militärische Einrichtungen im Jahr 2015 ist das Risikobewusstsein deutlich gestiegen. In diesem Jahr brachten gleich mehrere Versicherer zeitgleich neue Produkte an den Start. Die Musterbedingungen für Cyber-Versicherungen (AVB Cyber) des GDV, 2017 veröffentlicht, gaben weiteren Versicherern den Anstoß, mit Cyber-Tarifen an den Markt zu gehen. Die Bedingungen stellen ab auf kleine und mittelständische Unternehmen (KMU) mit bis zu 250 Mitarbeitern und 50 Millionen Euro Jahresumsatz.

Was eine Cyberpolice abdeckt

Im Kern tritt die Cyber-Versicherung ein für Schäden des Versicherten (Eigenschaden) oder Dritter (Drittschaden) durch ungewollte Einwirkungen, Zugriffe und Nutzung von IT-Systemen des Versicherten sowie im Zuge des Cyber-Schadens entstehende Kosten. In der Drittschadendeckung gibt es (mehr oder weniger ausgeprägte) Deckungsüberschneidungen mit klassischen Betriebshaftpflicht-, Vermögensschadenhaftpflicht-, Produkthaftpflicht- und D&O-Haftpflichtversicherungen. Im Bereich Eigenschäden entstehen teils weitreichende Überschneidungen mit Vertrauensschaden-Versicherungen, insbesondere bei zielgerichteten Hacker-Angriffen sowie Betrug und Diebstahl (Phishing, Pharming, Fake President etc.).

Keine Lust auf Finanzdienstleister

Vermittler und generell Finanzdienstleister, die sich gegen Cyber-Risiken absichern wollen, haben allerdings schlechte Karten. Sie gelten offenbar als gefahrenträchtig und nur wenige Versicherer sind bereit, ihnen Schutz zu bieten, was der Gewinnung von Vermittlern für den Vertrieb von Cyber-Produkten nicht gerade dienlich ist.

Ansonsten gibt es kaum Einschränkungen; eine Million Euro Versicherungsschutz ist, je nach Branche und Geschäftsmodell, schon für weniger als 1.000 Euro Jahresprämie erhältlich. Allerdings kennt die Assekuranz bei Cyber, wie auch in anderen Sparten, kein einheitliches Verständnis von KMU. Die Grenzlinie zwischen Gewerbe- und Industriebetrieben verläuft zwischen fünf und 50 Millionen Euro Jahresumsatz.

Orientierung dringend gesucht

Der Deckungsumfang unterscheidet sich von Versicherer zu Versicherer erheblich, konstatiert Michael Franke, geschäftsführender Gesellschafter der Franke und Bornberg Research GmbH:

„Wir beobachten deutliche Unterschiede in Aufbau und Umfang der Cyber-Bedingungen. Vom großen Komplettpaket über Baukastensysteme bis hin zu eng gefassten Kern-Deckungen ist alles vertreten. Was der eine Versicherer über eine Rechtsschutzversicherung löst, die an den Cyber-Hauptvertrag angedockt wird, webt der andere in Cyber-Drittschadendeckung und Krisen-Dienstleistungen ein. Die Konsequenzen für Versicherungsfall, Entschädigung und das Verhältnis zu anderen Versicherungsverträgen können gravierend sein. Unser Rating bietet erstmals Orientierung in diesem jungen und dynamischen Markt.“

Noch kann von Standards keine Rede sein, wie Franke am Beispiel der „versicherten Gefahren“ zeigt. Es herrsche eine fast babylonische Sprachverwirrung. Versicherer verwenden unterschiedlichste Begriffe, die sie mehr oder weniger klar definieren. Als versicherte Gefahren werden genannt:

- „Netzwerksicherheitsverletzung“
- „IT-Sicherheitsverletzung“
- „Hacker-Angriff“
- „Cyber-Angriff“
- „Cyber-Einbruch“
- „Cyber-Attacke“
- „Cyber-Rechtsverletzung“
- „Cyber-Sicherheitsvorfall“

In der Summe beschreiben die meisten Begriffe zwar einen ähnlichen Zustand, aber im Detail unterscheiden sie sich sehr – mit unabsehbaren Konsequenzen für Vermittler und Kunden. Ein anderes Thema, dasselbe Problem: die Cloud in Worte zu fassen und das mit der Nutzung von ausgelagerten IT-Prozessen einhergehende Risiko zu beschreiben. Kaum eine Definition gleicht der anderen, sofern es sie überhaupt gibt.

Neue Risiken, keine Erfahrung

Noch herrscht hohe Unsicherheit bei der Entwicklung einer für Kunden wirkungsvollen und für den Versicherer tragbaren Risikodeckung. Mangels Erfahrung entstehen die Bedingungen entweder auf der grünen Wiese (mit deutlichen Einflüssen der jeweils führenden Haftpflicht- oder TV-Sparte) oder durch Kopieren von US-Wordings. Der Blick zurück bietet keine Hilfe. Auch wenn es eine Schadenhistorie gäbe, hätte sie, anders als beispielsweise in der Feuerversicherung, keine Aussagekraft für die Zukunft. Weil Versicherer die sich dynamisch entwickelnden Cyber-Risiken nicht einschätzen können, versuchen sie, das Risiko an vermeintlich besonders kritischen Stellen in den Bedingungen zu begrenzen. Das Ergebnis ist nicht selten eine Mogelpackung, ergab die Analyse von Franke und Bornberg. So werben einige Angebote damit, den Cloud-Ausfall zu versichern. Beim Blick ins Kleingedruckte zeigt sich jedoch, dass beispielsweise SaaS-Dienste (Software as a Service) ausgeschlossen oder nur DoS-Angriffe (Denial of Service = Nichtverfügbarkeit) auf den Cloud-Anbieter versichert sind. Zudem sublimitieren die meisten Anbieter Angriffe auf den Betreiber einer Cloud – und in deren Folge Betriebsunterbrechungsschäden beim Versicherungsnehmer – stark oder schließen diese Gefahr vom Versicherungsschutz gleich vollständig aus.

Wie findet man die richtige Deckung?

Vermittler stellt die Cyber-Versicherung vor eine anspruchsvollen Herausforderung: Sie müssen das Geschäftsmodell des Kunden (und nicht die Betriebsart wie in Sach/Haftpflicht) verstehen

und in Verbindung mit dem technischen und organisatorischen Setup das tatsächliche Risiko ermitteln. So ist das Cyber-Risiko einer lokalen Boutique völlig anders als das eines (auch kleinen) Onlinehändlers, auch wenn beide Kundendaten sammeln, Kreditkartendaten verarbeiten, ihre Daten und Systeme selbst betreiben oder vollständige durch Dritte betreiben lassen. Mit der Betriebsart „Handel – Einzelhandel – Textilien“ käme man nicht sehr weit. Dann heißt es, die passende Deckung finden, Schwachstellen identifizieren und darüber ggf. verhandeln sowie diesen Prozess zur eigenen Entlastung hinreichend dokumentieren. Das Cyber-Rating von Franke und Bornberg bietet Orientierung; dessen Analysetools unterstützen den Beratungsprozess und geben Vermittlern Sicherheit.

Cyber-Rating gibt Orientierung

Für das aufwändige Ratingverfahren nutzt Franke und Bornberg ausschließlich selbst recherchierte Daten. Die Bewertungen stützen sich nur auf das, was in den rechtlich bindenden Unterlagen geregelt ist. Denn nur darauf können sich Versicherte im Ernstfall auch verlassen.

Eine Besonderheit im Gewerbegebiet ist, dass auf Nachfrage so gut wie alle Positionen verhandelbar sind. Das Cyber-Rating von Franke und Bornberg bewertet, was Versicherer standardmäßig bieten. Die Basis bilden die Haus-Wordings der Versicherer, inklusive standardisierter Klauselbögen und Sideletter. Untersucht wurden Kompaktprodukte, einzeln wählbare Leistungsbausteine sowie Zwischenformen inklusive aller angebotenen Bausteine / Optionen.

Die Analysten haben insgesamt 34 Cyber-Tarife für KMU von 28 Gesellschaften durchleuchtet. Konzepte von Deckungskonzeptanbietern und Maklerpools sind derzeit noch nicht öffentlich zugänglich. Herangezogen wurden exakt 115 Ratingkriterien in 21 Bereichen. Franke und Bornberg analysiert für das Rating vor allem Merkmale, die für die Mehrheit der KMU relevant sind und typischerweise in bisherigen Haftpflicht- und Sachversicherungen nicht gedeckt sind. Nicht berücksichtigt wurden hingegen Deckungsbestandteile, die in aller Regel in anderen etablierten Sparten gedeckt sind, beispielsweise Personenschäden und Schäden aus Produkthaftung.

Besonders hoch bewertet Franke und Bornberg folgende Kriterien

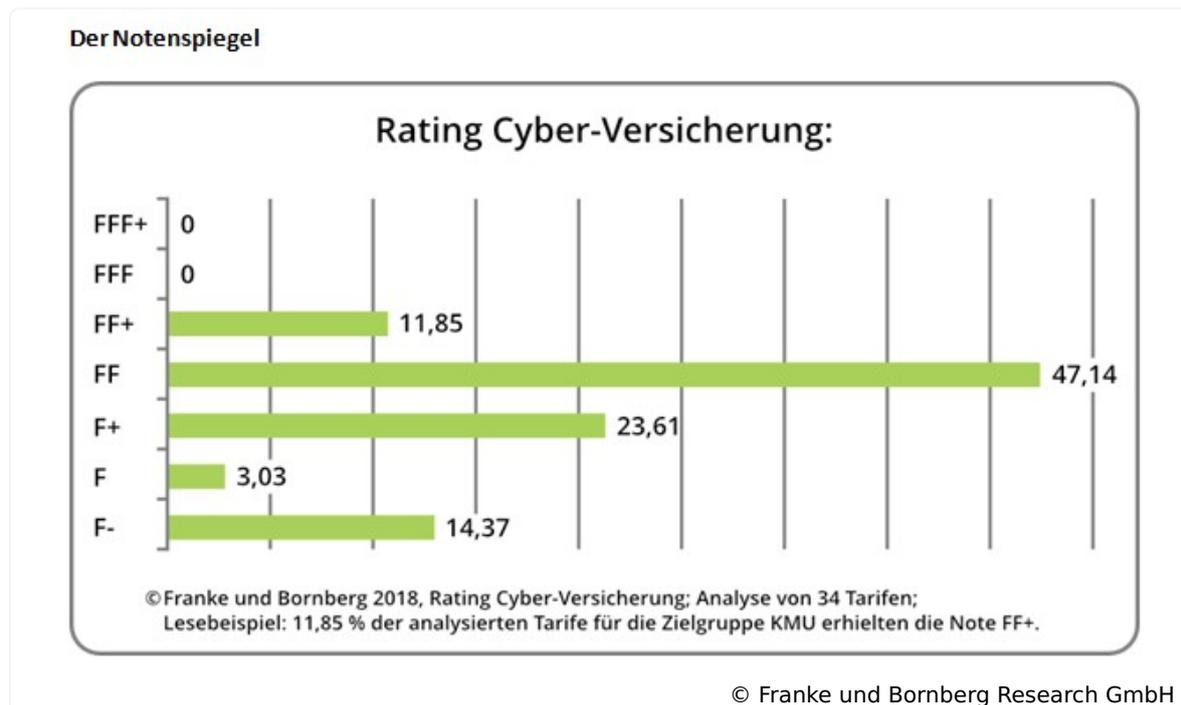
- Ertragsausfall & Mehrkosten
- Betriebsunterbrechung durch Cloud-Ausfall
- Durch Freistellungserklärung übernommene gesetzliche Haftpflicht Dritter
- Vertragliche Haftung
- Verletzung von Persönlichkeitsrechten
- Geografischer Wirkungsbereich
- Umgang mit Gefahrerhöhung
- Benachrichtigungspflichten bei Datenschutzverstößen
- Krisenmanagement
- Klarheit der Formulierung der Obliegenheiten
- Definition der versicherten Gefahren
- Definition der versicherten IT-Systeme sowie
- Einschränkungen bei der Wiederherstellung der IT-Systeme

Noch Luft nach oben

Während viele Tarife im durchaus positiv zu bewertenden Mittelfeld landen, ist die Leistungsspitze noch dünn – kein Produkt hat das Höchststrating FFF+ erreicht. „Hier gibt es noch Luft nach oben“, weiß Michael Franke. „Erfahrungsgemäß haben unsere Ratings spürbaren Einfluss auf die Produktqualität. Produktentwickler orientieren sich an den Bewertungskriterien. Ich bin deshalb optimistisch, dass sich das Leistungsniveau und die Präzision der Formulierungen in dieser noch jungen Sparte in den nächsten Jahren spürbar verbessern werden. Aus anderen Produktbereichen wissen wir, dass gerade bei jungen Produktkonzepten die Bildung von Standards in Kernbereichen Voraussetzung für Umsatzwachstum ist. Hierzu tragen wir mit unserem Cyber-Rating bei.“

Unter anderem muss ein Top-Tarif können:

- Betriebsunterbrechung: Deckung von Ertragsausfällen
- Drittschäden: Deckung für auch für immaterielle Schäden
- Mehrere Versicherungsverträge: keine Subsidiarität der Cyber-Deckung
- Rückwärtsdeckung: Deckungsausschluss nur für vor Abschluss bekannte Ursachen / Schäden (nicht für solche, die hätten bekannt sein müssen)
- Wiederherstellung von IT-Systemen: Zeitliche Befristung der Wiederherstellung auf nicht weniger als 12 Monate nach Schadenfeststellung



Ergebnisse im Detail

Das Cyber-Rating von Franke und Bornberg bietet Entscheidungshilfe für Vermittler und deren gewerbliche Kunden (KMU).

Die Höchstnote FFF+ erreichte, trotz Berücksichtigung des jeweiligen Maximalangebots, auf Anheb keins der angebotenen Cyber-Produkte. Die zweitbeste Note FFF wurde von den stärksten Produkten denkbar knapp verpasst.

Die mit FF+ stärksten Policen liefern

- AIG CyberEdge 3.0, Stand 06.2018
- HDI Cyberversicherung für Firmen und Freie Berufe, Stand 10.2018
- Hiscox CyberClear, Stand 01.2018
- Markel Pro Cyber, Stand 01.2018

Die nächst folgenden Unternehmen und Tarife (FF) sind (Auswahl, in alphabetischer Reihenfolge):

- Allianz CyberSchutz, Stand 04.2017
- Axa ByteProtect, Stand 07.2017
- Basler Cyber-Police, Stand 06.2017
- ERGO Cyber-Versicherung, Stand 01.2018
- Gothaer Cyber-Versicherung für Gewerbekunden, Stand 10.2018
- HDI Global SE Cyber+ Smart, Stand 01.2017
- Provinzial NordWest Cyber-Versicherung, Stand 01.2017
- R+V CyberRisk-Versicherung, Stand 09.2017
- Signal Iduna Cyberrisiko-Versicherung, Stand 01.2017
- VHV CyberProtect, Stand 02.2018
- Württembergische Cyber-Police, Stand 01.2018

Das Rating gibt einen Hinweis auf die grundsätzliche Qualität eines Versicherungsproduktes und bereitet damit optimal für eine individuelle Beratung vor. Die numerischen Schulnoten erlauben zudem eine weitere Differenzierung innerhalb einer Leistungsstufe. Franke und Bornberg setzt auf Transparenz. Alle Ratingergebnisse sowie die Bewertungsrichtlinien stehen auf der Internetseite <http://www.franke-bornberg.de/ratings/> kostenlos bereit. Die Ergebnisse sind Bestandteil der Analyse- und Beratungstools fb>xpert, fb>data sowie fb>vertragscheck.

Ausblick

Der Markt für Cyber-Policen ist momentan noch durch große Unsicherheit geprägt. Versicherungsbedingungen und Leistungsumfang ändern sich manchmal im Monatsrhythmus; handwerkliche Fehler werden schnell behoben. Besserstellungsklauseln werden bei eigenen Bestandsumstellungen angeboten, beziehen sich aber meistens nur auf die eigene Deckung des Versicherers. Michael Franke zeigt sich optimistisch: „Ich bin zuversichtlich, dass sich in der Branche, auch mit unserer Hilfe, einheitliche Begrifflichkeiten für versicherte Gefahren und Leistungen etablieren können. Das Bedingungswerk des GDV schafft eine gute Grundlage, lässt aber an einigen Stellen noch die gebotene Präzision und Trennschärfe vermissen. Spannend wird sein, ob sich die Cyber-Versicherung als Ergänzung der klassischen Produktpalette im Markt etabliert oder ob sie den angestammten Sparten nach und nach das Wasser abgräbt. Dann könnte zum Beispiel eine Betriebshaftpflichtversicherung zum Annex einer Cyber-Versicherung werden. In jedem Fall sind Transparenz und Fairness gefragt. Unser Rating sorgt dafür, dass Mogelpackungen auf Sicht keine Chance haben werden.“

Kontakt

Janine Sachs:

Telefon +49 (0) 511 357717 54

Email: janine.sachs@fb-research.de

Auf der Fachmesse DKM vom 23. – 25. Oktober gibt Franke und Bornberg erste Einblicke in das neue Cyber-Rating.