Cyber Risiken – immer noch ein Hype oder schon angekommen in der Versicherungslandschaft?

DI René FORSTHUBER
Leiter International Development

DI (FH) Arno GINGL, MSc, MA
Geschäftsfeldverantwortlicher Sachverständigenwesen

RISK EXPERTS

Es freut uns sehr, dass die Artikelüberschrift Ihre Aufmerksamkeit erregt hat, was angesichts der unzähligen Artikel zu diesem Thema nicht mit hoher Wahrscheinlichkeit zu erwarten war. Obwohl wir Sie bei Leselaune über den gesamten Artikel halten möchten, beantworten wir die Frage dennoch bereits zu Beginn: Ja, Cyber Risiken sind definitiv in der Versicherungslandschaft angekommen.

Warum?

Beim Recherchieren der verschiedenen Internet-Auftritte der Versicherungsmakler ist das Thema zu einem sehr großen Anteil vertreten, so zeigen auch sehr kleine Büros stolz ihre Expertise in diesem neuen, vielschichtigen Versicherungsbereich. Die Prognosen von Versicherern und Rückversicherern sorgen für einen hohen Grad an Aufmerksamkeit, die diesem Thema entgegengebracht wird und selbst einschlägige Veranstaltungen widmen sich mittlerweile der Versicherung von Cyber Risiken.
Aus Sicht der Maklerhaftung ist es unumgänglich Versicherungskunden auf dieses Produkt anzusprechen, da das zu einem ganzheitlichen Umgang mit zu erwartenden Risiken dazugehört.
Dass die Versicherungsdurchdringung (noch) nicht dem Hype der Pressemeldungen der letzten Jahre entspricht und demzufolge bis jetzt zwar noch wenige, aber durchaus monetär beträchtliche bzw. den Normalbetrieb störende/beeinträchtigende Schadensfälle vorliegen, geht durchaus mit der Frühphase eines neuen Produkts einher.

Warum haben nur sehr wenige Unternehmen in Österreich eine Cyber Versicherung?

Im Rahmen einer großen Zahl von Beratungsgesprächen mit Industrieunternehmen konnten wir feststellen, dass nahezu jedes Unternehmen die Sinnhaftigkeit dieser Versicherung erkannt hat, eine positive Entscheidung dahingehend aber oft an den Kosten oder am nicht vorhandenen Gruppendruck scheiterte – nach wie vor haben nur wenige Unternehmen eine „stand-alone-cyber Versicherung". In vielen Gesprächen kommt auch das Thema Wahrscheinlichkeit ins Spiel, welches zugegebenermaßen schwierig zu bewerten ist – hier scheinen auch viele Versicherer im Moment an ihre Grenzen im Bereich der Analytik gestoßen zu sein – wobei zu bedenken ist, dass mit ziemlicher Sicherheit der Totalverlust eines Industriebetriebs (meist versichert) deutlich unwahrscheinlicher ist als ein bilanzwirksamer Cyber-Angriff (meist nicht versichert).
Zudem sind Versicherungsbedingungen meist individuell zu wählen und dementsprechend komplex. Risikoausschlüsse, die z.B. auf dem „Stand der Technik" fußen (mittlerweile diskutierbar), schaffen zusätzliche Unsicherheit.
Und wie sieht´s bei KMUs/ EPUs aus? Die Versicherungsdurchdringung ist ähnlich niedrig, vorteilhaft zeigen sich hier umfassend verfügbare Produkte und Kapazitäten mit einfacheren Versicherungsbedingungen und der Möglichkeit eines Online-Abschlusses. Negativ hingegen wirkt sich hier der meist eher niedrige Sicherheitsstandard aus, kleine Unternehmen haben nun mal nicht das Know-how, die technischen Einrichtungen und den Netzwerk-Brainpool von großen Industriebetrieben.

Ist eine Cyber Versicherung sinnvoll für Ihre Kunden?

Oder anders gefragt: benötigt nicht jedes Unternehmen eine Cyberversicherung, oder sogar jeder User? Bei der Durchführung einer Gap Analyse werden Sie als Versicherungsexperte je nach bestehendem Versicherungskonzept eine Vielzahl verschiedener Versicherungslücken feststellen, seien es Ausschlüsse reiner Vermögensschäden (z.B. übliche Haftpflichtwordings), EDV Ausschlüsse (z.B. Transportversicherung; Artikel 6 (1) e) der AÖTB) oder Ausschlüsse nicht physischer Schäden (z.B. Sach-/Betriebsunterbrechungsversicherung). Im Rahmen Ihrer Beratungstätigkeit werden Sie auf diese Lücken hinweisen, auch gegebenenfalls die Cyber Versicherung erläutern, und wofür die einzelnen Versicherungsbausteine (vereinfacht dargestellt: Eigenschäden, Schäden Dritter, Sonstige Kosten) dienlich sind.
Letztlich können Sie als versierte Versicherungsberater vor allem mit einer Entscheidungsgrundlage umfassenden Added Value bieten.

Was also spricht für eine Cyber Versicherung?
- Steigende Bedrohung durch zunehmende Cyberkriminalität (siehe hierfür unseren in Kürze erscheinenden Risk Report XI).
- Erweiterter Versicherungsschutz für Gefahren, die für fast alle Unternehmen und Gewerbetreibende zunehmen und oft in traditionellen Versicherungsprodukten nicht abgedeckt – und auch nicht abdeckbar - sind, denken wir an Automatisierung, Digitalisierung und Datenschutz.
- Viele Studien namhafter Beratungsdienstleister zeigen, dass in Europa eine Betriebsunterbrechung die relevanteste Bedrohung für Entscheidungsträger ist. Entstammt die BU einer virtuellen Ursache ist nur in einer Cyber Versicherung Schutz gegeben.
- Verfügbares Notfallbudget für einen IT-Krisenfall: vor allem kleinere Unternehmen profitieren von einer im Rahmen einer Cyber Versicherung „zugekauften Incident Response", also professioneller Unterstützung im Schadensfall durch IT-Sicherheitsexperten, Schadensabwickler, Sachverständige, Hochwertiger PR, Datenschutzjuristen, Forensiker etc.
- Jetzt ist der ideale Zeitpunkt, da mit 25.5.2018 die Datenschutzgrundverordnung in Kraft tritt. (Siehe dazu den Kommentar am Ende.)

Was spricht dagegen:
- Kosten durch die Versicherungsprämie.
- Das ist alles.

Wie sieht eine optimale Beratung für Cyber Versicherungen aus?

Medienberichte schildern 12 Monate als den üblichen Zeitraum zwischen der Interessensbekundung eines Versicherungsnehmers bis hin zum Versicherungsabschluss. Obwohl dieser Zeitraum z.B. für Banken eher kurz gewählt ist, kann man Kunden meist in einem deutlich kürzeren Zeitraum in der nötigen fachlichen Tiefe beraten.
Versicherungsmakler sollten dafür selbst oder mit einschlägig tätigen Risikomanagement Partnern die folgenden Punkte abdecken:

1) Sie verstehen das Geschäftsmodell Ihrer Kunden und antizipieren gemeinsam wohin es kurz- bis mittelfristig führt.
2) Somit werden insbesondere digitalisierte Prozesse erkennbar. Mit einer Gap Analyse loten Sie darauf basierend Versicherungslücken aus und können diese entweder durch Wordingverbesserungen, einer Cyber-Versicherung oder anderen Produkten wie Vertrauensschadenversicherung oder Tech E&O (Errors & Omissions) abdecken.
3) Abhängigkeiten innerhalb des Unternehmens aber auch von externen Partnern – insbesondere im IT Bereich – sind bekannt und Ausfälle können monetär eingeschätzt werden.
4) Sie können die Attraktivität eines Kunden für Cyber Kriminalität einschätzen und kennen auch die besonderen Bedrohungen für bestimmte Branchen. Hier sind vor allem die Verwundbarkeit der Geschäfte durch IT-Ausfälle, Online Finanztransaktionen, Potential für Industriespionage, Menge der sensiblen Daten und Abhängigkeit von externen IT Partnern wesentlich.
5) Idealerweise können Sie Ihren Kunden auch hinsichtlich einer Risikooptimierung beraten und bieten eine (Basis-)Expertise in der IT-Security. Diesen Punkt werden Sie aber vermutlich eher mit Netzwerkpartnern bestreiten.
6) Sie führen eine Exposure- inkl. Business Impact - Analyse durch und können dementsprechend die passende Versicherungssumme wählen. Oftmals ist Versicherungsnehmern schon dahingehend geholfen, mit niedrigen Deckungssummen eine hochwertige incident response zu ermöglichen.
7) Wichtig ist zu wissen, welche nötigen Schritte nach einer DDos Attacke oder einem Data Breach zu wählen sind, um zum Einen einem drohenden Gewinnentgang möglichst wirksam entgegen treten zu können, aber auch um allen gesetzlichen Erfordernissen zu entsprechen.
8) Sie sind mit dem Versicherungsmarkt im Bereich Cyber exzellent vernetzt, kennen die Stärken und Schwächen der Anbieter und auch die Spezialisierungen auf bestimmte Branchen und unterstützen den Versicherungsnehmern beim Komplettieren der Fragebögen.
9) Für den etwaigen Schadensfall sind Sie gewappnet, Sie setzen gemeinsam mit dem Versicherer ein incident response team ein und aktivieren zuvor festgelegte Prozesse ein, um einen etwaigen BU-Schaden adäquat für die Schadensabwicklung zu dokumentieren.
10) Sie halten Ihre Kunden stets über neue Entwicklungen am Versicherungsmarkt am Laufenden, denn die Cyber Versicherung ist ein sehr lebendiges, sich ständig veränderndes Produkt.

Als Versicherungsmakler können Sie insbesondere mit Ihrer Expertise in puncto Cyber Risiken Ihren Added Value als Experte auch für zukünftige Risiken sicherlich sehr eindrucksvoll hervorheben.

Viel Erfolg bei Ihren Beratungen!

Kommentar: DSGVO

Im Zusammenhang mit der Implementierung der EU-DSGVO (EU-Datenschutz-Grundverordnung) in die nationale österreichische Rechtsprechung durch das Datenschutz-Anpassungsgesetz 2018 ergeben sich im Vergleich mit der bisherigen rechtlichen Situation einerseits erhöhte Anforderungen an den Schutz personenbezogener Daten und anderseits aber auch ein signifikant höherer Strafrahmen im Fall von negativen Abweichungen. Da die Übergangsfrist zur Anwendung der Richtlinie bzw. des Datenschutz-Anpassungsgesetzes 2018 bereits mit dem 25.05.2018 endet, sollte der bis dahin verbleibende Zeitraum genützt werden, um die in Kraft befindlichen Maßnahmen und Vorkehrungen zum Schutz personenbezogener Daten (Privacy by Design & Privacy by default) hinsichtlich der zukünftigen Erfordernisse zu analysieren und gegebenenfalls zu erweitern oder zu ändern. Im Ergebnis einer solchen Analyse sollen Unternehmen in die Lage versetzt werden, die Risiken einer allenfalls lückenhaften Vorbereitung zu erkennen und im Sinne eines ganzheitlichen Risikomanagement- Ansatzes auf entsprechende, auch auf die Zukunft ausgerichtete Handlungsalternativen, zu verweisen.