Spezialrisiko Cyber und damit verbundene „Haftungsfalle“ für Berater:innen

Die Dynamik des heutigen Geschäftslebens spiegelt sich in den Anforderungen an ein modernes Risikomanagement. Faktoren wie Inflation, Wirtschaftsabschwung, Fachkräftemangel, Klimawandel und geopolitische Entwicklungen bedeuten erhebliche Gefahrenpotenziale für alle Organisationen, die beachtet werden müssen.

Strukturen und Prozesse werden in so gut wie allen Unternehmen, nicht zuletzt auch aufgrund der rapide fortschreitenden Digitalisierung mit ihren innovativen Kommunikationstechnologien, immer komplexer und bedingen laufend wandelnde Geschäftsmodelle. Die rapide Veränderungsgeschwindigkeit in der globalen Wirtschaft und Politik zwingt Unternehmen kurzfristig zu handeln und ihre Risikostrategien kontinuierlich zu überdenken und regelmäßig anzupassen.

Auch wenn Unternehmen zwar Risikomanagementstrukturen implementiert haben, mangelt es häufig an ausreichenden Ressourcen, insbesondere bei Cyber-Risiken. Damit steigen gleichzeitig die Anforderungen an Versicherungslösungen, um den speziellen Bedürfnissen moderner Geschäftsbereiche und Berufe gerecht werden zu können. Die Beurteilung von Unternehmensrisiken ist dadurch herausfordernder denn je.

Für Versicherungsmakler:innen bedeutet dies, dass Beratungsansätze kontinuierlich an die sich ändernden Strukturen ihrer Kundinnen und Kunden angepasst werden müssen. Es ergeben sich immer umfangreichere Deckungskonzepte, die einerseits Einflüsse auf den Umgang mit „klassischen“ Risiken haben, aber auch neu entstehende und damit oftmals schwer vorhersehbare Risiken berücksichtigen.

Neue „Spezialrisiken“ ergeben sich in der Regel durch aktuelle Themenfelder der globalen Wirtschaft, wie derzeit Nachhaltigkeitsaspekte, technologische Entwicklungen und Cyber-Kriminalität.

Sobald ein Computer im Spiel ist, MUSS das Thema „Cyber“ angesprochen werden. In den letzten Jahren hat Künstliche Intelligenz (KI) unsere Welt tiefgreifend verändert – mit allen Vor- und Nachteilen.

Derzeit stellt sich eine entscheidende Frage in Bezug auf KI: Wer kann die neuen Technologien effektiver nutzen – Cyberkriminelle oder wir?

Eine unzureichende Cyber-Sicherheit zählt zu den größten Risikofeldern, mit denen sich Unternehmen aller Branchen und Größen heute beschäftigen, denn Cyber-Bedrohungen machen vor keiner Branche halt. Die Dunkelziffer an betroffenen Kleinen und Mittleren Unternehmen (KMU), die nicht dem öffentlichen Sektor oder der kritischen Infrastruktur angehören, ist dennoch sehr hoch – es betrifft also auch vermeintlich unattraktive Ziele. Oder gerade solche?

Jedes Unternehmen muss durchgehend sicherstellen, dass ausreichender Schutz gegen Cyber-Risiken besteht. Damit verbunden sind neben technischen und organisatorischen Anforderungen auch rechtliche Faktoren. Denn so schnell sich der Stand der Technik überholt, so rasch verändern sich die rechtlichen Rahmenbedingungen für die Sicherheit in der digitalen Welt.

Versäumnisse können schwerwiegende rechtliche und finanzielle Konsequenzen für Unternehmen und infolge für deren Geschäftsführer:innen persönlich nach sich ziehen. Wenn die Geschäftsführung eines KMU es beispielsweise versäumt erforderliche Cyber-Sicherheitsmaßnahmen zu implementieren oder den Einsatz notwendiger IT-Lösungen zur Erhöhung der betrieblichen Resilienz ablehnt, kann mangelhaftes Risikomanagement und damit ein Fehlverhalten vorgeworfen werden. Daraus ergibt sich wiederum eine Haftungsproblematik für die Leitorgane der Unternehmen, die Schadenersatzforderungen gegen diese nach sich ziehen kann.

Trotzdem herrscht bei KMU die kühne Annahme, für Cyberangriffe zu unbedeutend zu sein. Dies zeigt sich in einem nachlässigen Umgang mit Datensicherungen, unregelmäßigen Updates und unzureichenden Passwort-Richtlinien.
Das ist ein gutes Argument für eine D&O-Versicherung, die im gleichen Atemzug als sinnvolle Ergänzung für die Leitorgane genannt werden kann.

Das Risikobewusstsein wächst zwar, jedoch werden die wirtschaftlichen Folgen von Cyber-Zwischenfällen häufig unterschätzt. Besonders kleinere Unternehmen leben im Glauben, dass sie für Hacker und Häcksen* kein attraktives Ziel darstellen.

Cyberkriminelle wählen ihre Opfer aber meist danach aus, dass sie mit geringem Aufwand eindringen können. Die Professionalität im Bereich Cybercrime schreitet voran und erreicht, auch durch KI, immer neue Höhepunkte. Für Organisationen aller Größen ist es daher höchste Zeit, in ihre Sicherheit zu investieren,

Stefan Chlebnicek, Akad. VersMakler[WU], Risk Experts Risiko Engineering GmbH

was wiederum im Beratungsprozess für die Versicherungslösung aufgegriffen werden müsste, denn im Sinne einer holistischen Kundenberatung mit einer „angemessenen Risikoanalyse" ist es unumgänglich, Cyber-Risiken genau zu betrachten.

Die beruflichen Anforderungen für Versicherungsmakler:innen nehmen damit massiv zu, denn eine wesentliche Grundvoraussetzung, um überhaupt Versicherungsprodukte vermitteln zu dürfen, ist neben den regelmäßigen Weiterbildungen auch über angemessene Kenntnisse zu verfügen, die mit der Tätigkeit einhergehen. (siehe Art. 10 RL (EU) 2016/97 „Berufliche und organisatorische Anforderungen" und Anhang I „Mindestanfoderungen an berufliche Kenntnisse und Fähigkeiten")

In den Zweigen der Nichtlebensversicherung muss man zumindest den Kundenbedarf für das Deckungskonzept erheben können. Das gilt damit auch für die Cyber-Versicherung. Fällt das Thema unter den Tisch oder wird gar als unwichtig abgetan, ergeben sich massive Haftungspotenziale für die Beraterin und den Berater.

Das Wissen, welches Versicherungsunternehmen welchen Deckungsumfang anbietet und welche rechtlichen Rahmenbedingungen für die jeweiligen Kund:innen relevant sind, ist essentiell für ein solides Konzept.

Um umfassend beraten zu können, und damit §28 Zi.1 MaklerG zu entsprechen, ist ein Mindestmaß an Know-how rund um die Cyber-Thematik unumgänglich, da sonst kaum im Interesse der Kund:innen gehandelt werden kann.

„Die Versicherungswirtschaft entwickelt sich laufend und insbesondere bei Themenfeldern wie der Cyber-Versicherung lohnt es sich, vorausschauend zu agieren und Kompetenz aufzubauen."

Gerade, wenn man sich frisch mit einem Thema auseinandersetzt, kann ein offener Austausch mit unabhängigen Partner:innen gute initiale Impulse setzen und durch den Zugriff auf Expert:innenwissen weitet sich die eigene Sichtweise aus.

Die Cyber-Versicherung bietet aktuell noch ein enormes Vertriebspotenzial, da sie eben noch kaum und wenn, dann sehr zurückhaltend, angesprochen wird. Es muss aber kein neuer Bildungsweg als IT-Profi eingeschlagen werden.

Für den Anfang ist ein sich auseinandersetzen mit dem Thema ein guter Anfang, um es in der Beratung ansprechen zu können. Unterstützung bieten auch die jeweiligen Versicherungsanbieter und Internetrecherchen. Gerade für die Erklärung von IT-Fachbegriffen gibt es im Internet unterschiedliche Informationsquellen, wie bspw. www.cyberwiki.at mit einfachen Erklärungen für Cyber-relevante Begriffe. Es handelt sich dabei um eine Themenseite des VersicherungsWiki, die mit Unterstützung der Cogitanda laufend mit Informationen und neuen Begriffen gefüttert wird. Damit stehen einfache Erklärungen für Begriffe wie Ransomware, CEO-Fraud, Port, Databreach, Penetration-Test udgl. für alle leicht zugänglich zur Verfügung.

Neben dem „Was", also fachlichen Inhalten, ist eine durchdachte Strategie gefragt, da sich das grundlegende Tätigkeitsfeld in der Versicherungsvermittlung in den vergangenen Jahren kaum verändert hat. Der Fokus liegt nach wie vor auf dem Verkauf von Versicherungsprodukten auf Basis einer Erhebung, die aber häufig ausschließlich klassische Risiken berücksichtigt. Risikomanagement ist in der Geschäftswelt ein zentrales Element der Unternehmensführung. Dieser Zugang lässt sich für die Thematik Cyber und die damit verbundene Risikoanalyse nutzen.

Ein Punkt, der hierbei aber ein wenig Ernüchterung bringt, ist das verfügbare Angebot an Versicherungsprodukten, die Grenzen der Leistungsumfänge und die Anforderungen an die technischen und organisatorischen Sicherungsmaßnahmen, die es einzuhalten gilt.

Umso wichtiger ist es, klar darstellen zu können, wie Cyber-Risiken in herkömmlichen Versicherungspolizzen abgedeckt werden und ab wann eine spezielle Cyber-Versicherung erforderlich ist.

Abhilfe kann eine auf Cyber-Risiken angepasste Risikomanagement-Struktur schaffen, welche die Grenzen der Versicherungslösungen berücksichtigt und mit geeigneten Maßnahmen Deckungslücken abschwächt. Ergänzend zu den Fragebögen der Versicherungsgesellschaften, die im Zuge der Antragserrichtung zur Anwendung kommen, kann so eine genauere und umfassendere Darstellung der Abweichungen zwischen SOLL- und IST-Situation nach den individuellen Unternehmens-Charakteristika erfolgen. Diese Vorgehensweise schafft zudem Sensibilisierung für das Thema bei Kund:innen. ▸

Je nach Größe und Komplexität des zu analysierenden Betriebs lohnt es sich erfahrene Expert:innen hinzuzuziehen. Beispielsweise berücksichtigt das bei Risk Experts entwickelte Cyber-Risk Engineering eigene Bewertungskriterien mit rund 150 Risiko-Aspekten für die umfassende Bewertung der individuellen Situation des analysierten Unternehmens.

Die Herangehensweise ähnelt dabei jener, die auch im „traditionellen" Risk Engineering angewandt wird. Durch Begehungen vor Ort, Datenerhebungen und Analyse-Gespräche mit Geschäftsführung und IT-Verantwortlichen, wird die aktuelle Situation sichtbar gemacht, bewertet und anschließend mit geeigneten Maßnahmen hinterlegt, welche eventuelle Schwächen verbessern sollen.

Das macht für Unternehmen aller Größen Sinn, wird aber von kleineren Unternehmen aufgrund des Umfangs nicht immer von Beginn an in Betracht gezogen. Alternativ kann für kleine Unternehmen ein eigener Fragenkatalog für die Analyse erarbeitet werden, der zur Anwendung kommt und die allgemein gehaltenen Fragebögen der Versicherer ergänzt.

Bestimmte Fokusbereiche sollten, wenn es um Cyber-Risiken geht, immer bei der Analyse behandelt werden:

- Allgemeine Unternehmenssituation
  u.a. Prozesse, Strukturen, Grad der IT-Abhängigkeit, Marktposition
- Technische IT-Sicherheit
  u.a. Security-Software, Serverlandschaft
- Organisatorische IT-Sicherheit
  u.a. Awareness bei der Belegschaft, Schulungen
- Datenschutz
  u.a. welche Daten werden verarbeitet, Datensicherheit
- Betriebsunterbrechungsrisiken inkl. PML-Berechnung
  u.a. Resilienzanalysen, Notfallpläne

Anders als bei einer Checkliste, empfiehlt sich die Dokumentation als Freitext zu schreiben. So werden die Eindrücke genauer festgehalten und die Antwortmöglichkeiten auf die gestellten Fragen werden, anders als bei Ja/Nein-Fragen, offen und tendenziell ehrlicher beantwortet.

Mit einer solchen Wissensbasis lassen sich die weitere Vorgehensweise und Notfallpläne gestalten.

Kundenbindungsinstrument: Cyber-Notfallplan

Ein wesentliches Standbein für die „gesunde" IT-Landschaft eines Unternehmens ist der verschriftlichte Notfallplan. Dieser hält fest, wie auf Sicherheitsvorfälle und Cyberangriffe reagiert werden soll. Schadenfolgen können dadurch minimiert bzw. im besten Fall sogar verhindert werden. Zudem wird die Wiederherstellung beschleunigt und die Erfüllung von rechtlichen sowie regulatorischen Anforderungen gewährleistet.

Der Aufbau sollte möglichst einfach gehalten sein und folgende Elemente beinhalten:

- Ziel des Notfallplans
  bspw. „Reaktion auf Cyber-Angriff", „Erfüllung der rechtlichen Vorgaben", …
- Relevante Ressourcen
  Auflistung vorhandener Systeme, Priorisierung von Daten, …
- Erkennen & Analysieren
  Prozessbeschreibung zur Erkennung und Bewertung eines Vorfalls
- Verantwortlichkeiten & Rollen
  Definition jener Personen, die im Bedarfsfall reagieren müssen
- Maßnahmen
  (Sofort)maßnahmen zur Eindämmung eines Vorfalls, um zu verhindern, dass sich die Bedrohung weiter ausbreitet
- Wiederherstellung
  Verfahren bis zur vollständigen Beseitigung der Bedrohung aus den betroffenen Systemen und zur Wiederherstellung der betroffenen Dienste oder Daten
- Kommunikationsplan
  Vorgehensweisen für die interne und externe Kommunikation (ggf. inkl. Datenschutzbehörde) während und nach einem Vorfall inkl. Definition wer an wen was berichtet
- Nachbereitung & Bewertung
  Analyse des Vorfalls um Verbesserungsmöglichkeiten zu finden und den Plan anzupassen.

Hexenwerk ist ein Cyber-Notfallplan keines. Der Nutzen als modernes Beratungsinstrument steht im Vordergrund. Es handelt sich um ein lebendiges Dokument, das regelmäßig überprüft und angepasst werden soll, um mit den sich entwickelnden Cyber-Bedrohungen und Geschäftsanforderungen Schritt zu halten. Somit für Beratende ein Garant für regelmäßige Touchpoints mit Geschäftskund:innen.

Die Cyber-Versicherung ist bereits bei manchen Vermittler:innen fixer Bestandteil im Beratungsgespräch; und das nicht nur im Großkundensegment. Dieses Thema bietet erfahrungsgemäß viele Möglichkeiten Brücken zu anderen Themenfeldern zu schlagen, um Kund:innen noch umfänglicher betreuen zu können. •

* Als Häckse bezeichnet man die weibliche Form eines Hackers, also einer Person, die in Computer-Systeme, Netzwerke oder Software eindringt.

Von Stefan Chlebnicek

Akad. VersMakler[WU]; Risk Experts Risiko Engineering GmbH