Stefan CHLEBNICEK,
akad. Versicherungsmakler (WU), Senior Expert, Head of Training & Academy

RISK EXPERTS
ENABLING SMART DECISIONS.

(Berater)Haftung & Cyber –

Die passende Beratungsstruktur schafft Abhilfe

Die Geschäftsführung jedes Unternehmens muss aktiv und vorausschauend agieren, um durchgehend sicherzustellen, dass ein ausreichender Schutz gegen Cyber-Risken besteht. Dafür sind neben den technischen und organisatorischen Anforderungen auch rechtliche Komponenten zu berücksichtigen.
So schnell sich technische Gegebenheiten überholen, so rasch verändern sich die rechtlichen Rahmenbedingungen für die eigene Sicherheit in der digitalen Welt.

Versäumnisse können teils schwerwiegende rechtliche und finanzielle Konsequenzen für Unternehmen und die Geschäftsführer:innen persönlich nach sich ziehen. Die Haftung der Geschäftsführung ist dann gegeben, wenn es versäumt wurde, erforderliche Cyber-Sicherheitsmaßnahmen, einschließlich des Einsatzes notwendiger IT-Lösungen, zu implementieren. Unterlässt die Unternehmensführung solche Maßnahmen zur Verbesserung der IT-Resilienz, kann mangelhaftes Risikomanagement vorgeworfen werden.

„Ich bin ja nur ein Kleiner…“ oder *„Dann geht der Computer halt nicht mehr…“* sind Sätze, die im KMU-Bereich häufig von Kund:innen gebracht werden. Aber ohne „Cyber“ geht es nicht mehr.
Im Sinne einer holistischen Kundenberatung, wenn die „angemessene Risikoanalyse“ durchgeführt werden soll, ist es unumgänglich Cyber-Risiken anzusprechen. Ihre Kund:innen werden es Ihnen danken – früher oder später.

Was bedeutet das für Sie als Berater:innen?
Eine Grundproblematik liegt für Einkäufer:innen von Versicherungsprodukten zunächst im Fehlen eines Branchenstandards hinsichtlich der Versicherungsbedingungen und der damit einhergehenden Unübersichtlichkeit der Angebote. Durch die unterschiedlichen Formulierungen in den Versicherungsbedingungen wird die Erstellung eines angemessenen Deckungskonzeptes erschwert.

Bei der Auswahl von passenden Versicherungslösungen muss ein intensiver Abgleich mit den bereits bestehenden Verträgen vorgenommen werden, um Deckungslücken zu schließen und Mehrfachversicherungen zu vermeiden.

Die Gefahr von Deckungslücken oder Mehrfachversicherungen schreckt viele Berater:innen davon ab, Cyber-Risken den gebührenden Raum in der Beratung zu geben.

„Aber in meiner Betriebsversicherung ist doch ein Cyber-Baustein inkludiert…“
Neben unnötig bezahlten Prämien kann im Worst Case auch die Deckung des Versicherers komplett entfallen, wenn bspw. eine qualifizierte Subsidiärklausel vertraglich festgehalten ist.
Dies kann auch eine gute Berater-Kunden-Beziehung auf die Probe stellen.

Aus rechtlicher Sicht birgt die Vermittlung von Versicherungslösungen für den Cyber-Bereich also ihre Tücken. Und davon einige.
Rechtliche Stolpersteine betreffen sowohl vertragsrechtliche Fragen als auch solche aus anderen Rechtsgebieten.

Die Definitionen des Versicherungsfalles können eng formuliert sein. Das kennt man nicht nur aus dem Cyber-Bereich. Gerade, wenn „Cyberrisiko-Komponenten“ in anderweitigen Versicherungsprodukten eingebettet sind, sollte man zweimal hinsehen. Häufig werden in solchen Deckungszusatzbausteinen Schäden aus „zielgerichteten“ Cyber-Attacken vom Versicherungsschutz erfasst. Mit einer solchen Formulierung würde keine Deckung bestehen, wenn man von einem nicht auf das jeweilige Unternehmen zielgerichteten Angriff betroffen ist.

Oft wird, nach dem Motto „einer wird's schon anklicken“, Malware an eine unbestimmte Zahl von Empfänger:innen versandt. Ist man, warum auch immer, der-/diejenige, die betroffen ist, kann dieser blinde Fleck im Versicherungskonzept bei der zuvor genannten Textierung, Konfliktpotenzial bedeuten.

Einschränkungen im Versicherungsschutz ergeben sich mitunter auch aus sonstigen restriktiven Beschreibungen von versicherten Gefahren. Dies kann etwa dann der Fall sein, wenn ausschließlich Schäden aus „Straftaten“ oder „strafbaren Handlungen“ von Mitarbeiter:innen gedeckt sind. Schäden, die aus bloßem Versehen entstanden sind, wären dann nicht gedeckt.

Auch Ausschluss-Klauseln ist gebührende Aufmerksamkeit zu schenken. Ein „Klassiker“ ist der Ausschluss, wenn keine regelmäßigen Aktualisierungen der IT-technischen Sicherheitsmaßnahmen durchgeführt werden. Firewalls, Viren-Schutz und Co. müssen stehts aktuell sein und auch die IT-Infrastruktur „dem Stand der Technik“ entsprechen.
Einfach gesagt bedeutet dies, dass veraltete Hard- und Software die Antagonisten für die Versicherungsleistung sind.
Standardmäßige Ausschlüsse wie Schäden aus kriegerischen Ereignissen, bieten im Anlassfall ebenfalls Futter für Diskussionen. „Wurde der Angriff durch einen ausländischen Hacker im Rahmen einer kriegerischen Aktion ausgeführt?“ ist in der aktuellen Zeit eine berechtigte Frage des Versicherers.

Alles in Allem wird das Berater:innen-Leben nicht einfacher.
Für Sie als Versicherungsberater:innen nehmen die beruflichen Anforderungen laufend 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 und Anhang I)
In den Zweigen der Nichtlebensversicherung, wozu die Cyber-Versicherung zählt, muss man zumindest so viel wissen, um den Kundenbedarf erheben zu können, um dies im Deckungskonzept zu berücksichtigen.
Das bedeutet, dass man wissen muss, welcher Versicherer welche Deckungen anbietet und welche rechtlichen Rahmen für die jeweiligen Kund:innen relevant sind. Damit geht naturgemäß Haftungspotenzial für die Berater:innen einher, denn *„wehe dem, der …“*

Um umfassend beraten zu können, und damit §28 Zi.1 MaklerG zu entsprechen, ist es also erforderlich, sich ein Mindestmaß an Knowhow rund um die Cyber-Thematik anzueignen, da sonst kaum im Interesse der Kund:innen gehandelt werden kann. Man muss aber keinen neuen Bildungsweg als „Cyber-Guru“ starten. Sich der möglichen Risiken bewusst zu sein und dies auch weiter zu kommunizieren, ist ein guter Anfang.

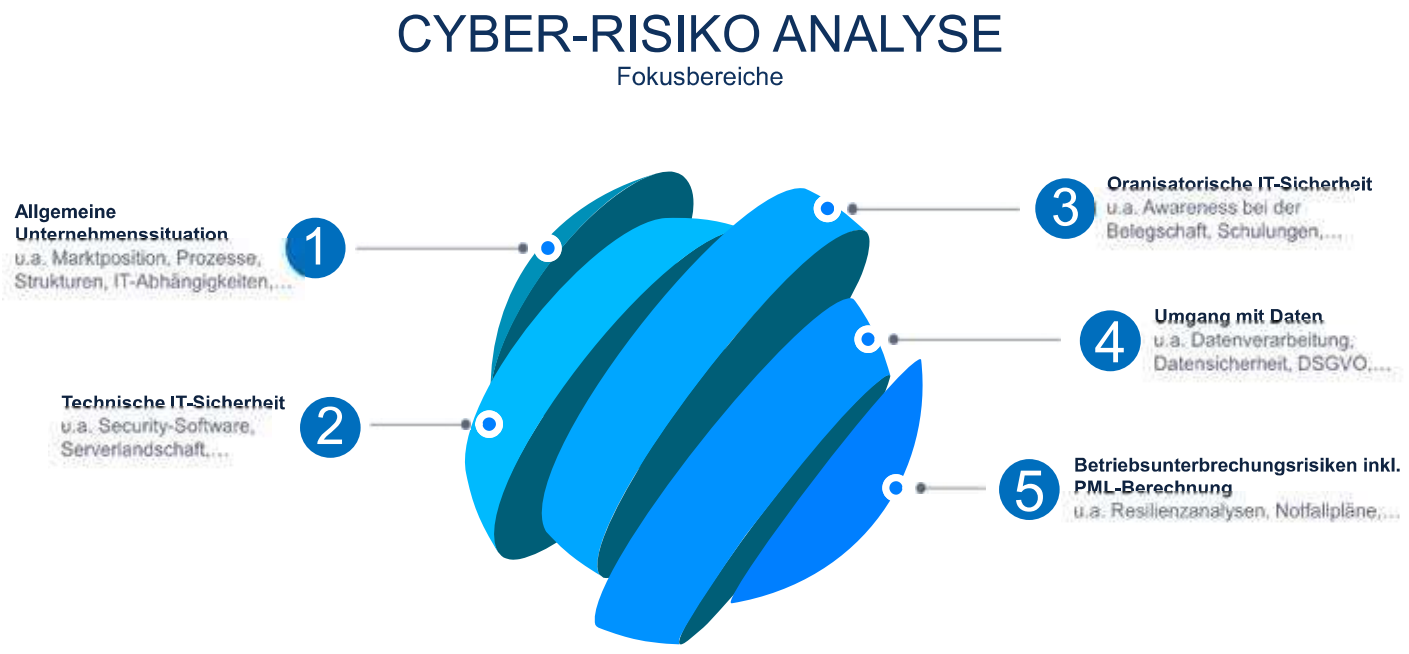
Auch vor einer „neuen Sprache“ mit unzähligen technischen Vokabeln muss man sich nicht scheuen. Abhilfe dafür schafft eine Internetrecherche, bspw. über www.VersicherungsWiki.at, um einzelne Begriffe seinen Kund:innen schnell und einfach erklären zu können.

Ob der Ablauf der eigenen Beratung angepasst werden muss, hängt davon ab, wie sehr man in die Tiefe geht. In vielen Fällen genügt es im seichten Gewässer zu plantschen. Wichtig ist das Ansprechen. Dafür muss man kein Cyber-Experte bzw. keine Cyber-Expertin sein. Wichtig ist es zu verstehen wie das jeweilige Unternehmen aufgestellt ist und „der Hase läuft“.

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

1. **Allgemeine Unternehmenssituation**
   u.a. Marktposition, Prozesse, Strukturen, Grad der IT-Abhängigkeit, etc.
2. **Technische IT-Sicherheit**
   u.a. Security-Software, Serverlandschaft, etc.

»



3. **Organisatorische IT-Sicherheit**
   u.a. Awareness bei der Belegschaft, Schulungen, etc.
4. **Datenschutz**
   u.a. welche Daten werden verarbeitet, Datensicherheit, DSGVO,
5. **Betriebsunterbrechungsrisiken inkl. PML-Berechnung**
   u.a. Resilienzanalysen, Notfallpläne, etc.

Kundenbindungsinstrument: Cyber-Notfallplan

Ein wesentliches Standbein für die „gesunde" IT-Landschaft eines Unternehmens ist ein Notfallplan, der verschriftlicht festhält, wie auf Sicherheitsvorfälle reagiert werden soll.

Damit werden die Reaktionen auf Cyberangriffe koordiniert, Schäden minimiert bzw. im besten Fall sogar verhindert, die Wiederherstellung beschleunigt und die Erfüllung von rechtlichen sowie regulatorischen Anforderungen gewährleistet.

Ein solcher Cyber-Notfallplan ist kein Hexenwerk und kann für Berater:innen ein modernes Instrument zur Kund:innenbindung darstellen.

Es handelt sich um ein lebendiges Dokument, das regelmäßig überprüft und angepasst wird, um mit den sich entwickelnden Cyber-Bedrohungen und Geschäftsanforderungen Schritt zu halten. Somit ein Garant für regelmäßige Touchpoints mit Geschäftskund:innen.

Ein umfassender Cyber-Notfallplan sollte die folgenden Elemente beinhalten:

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

Unsere Unterstützung für Sie und Ihre Kund:innen

Risk Experts ist ein unabhängiges Beratungsunternehmen, das auf die Bereiche Risikomanagement und Sachverständigendienstleistungen spezialisiert ist.
Für die Etablierung eines ausreichenden und vor allem passenden Versicherungsschutzes ist eine fundierte Risikoanalyse unerlässlich – ob für Unternehmen, Makler:innen oder Versicherer. Das Risk Experts Cyber Risk Engineering basiert grundsätzlich auf Strukturen und Vorgehensweisen des klassischen Risk Engineering und umfasst alle Elemente, die für die Wahl des richtigen Versicherungsschutzes erforderlich sind. Beginnend bei dem Schutz von Sachwerten, über die Einhaltung der rechtlichen Rahmenbedingungen bis hin zu den Folgen einer cyberbedingten Betriebsunterbrechung. Zudem werden individuelle Handlungsmaßnahmen aufgezeigt, welche die jeweilige Risikosituation verbessern.

Auch nach Eintritt eines Schadens lassen wir Sie nicht allein und stehen als Schadenmanager an Ihrer Seite.
Für weitere Informationen und Unterstützung in Sachen Cyber-Sicherheit, Cyber-Versicherung und Cyber-Risikoreduktion stehen Ihnen die Expert:innen von Risk Experts gerne zur Verfügung.

Wenn Sie mehr über dieses Thema wissen möchten, besuchen Sie unsere Homepage (www.riskexperts.at) oder treten direkt mit uns in Kontakt unter office@riskexperts.at