makler intern QM
01/2023

RECHT – ein MUSS für Versicherungsmakler?

Gesetze und Bedingungen sind im Tagesgeschäft ständiger Begleiter des Versicherungsmaklers. Ohne fundiertes, juristisches Fachwissen ist eine optimale Kundenbetreuung völlig undenkbar. Ein erfolgreicher Makler muss heutzutage jedenfalls auch ein „kleiner Jurist“ sein.

Kurt HAUSMANN,
Managing Director &
Head of Sales

RISK EXPERTS
ENABLING SMART DECISIONS.

Risk Engineering für Cyber- und Datenschutzrisiken

Was steckt dahinter? Wir haben Cyber Risiken analysiert und ein Rezept für einen passenden Cyber-Versicherungsschutz entwickelt.

Wenn wir das Wort Cyber-Risiko hören, denken wir wahrscheinlich an einen Hackerangriff, an gestohlene Passwörter oder an Kreditkartenmissbrauch bei online-Zahlungen. Um diese Gefahren zu unterbinden, gibt es bereits einige Tools, die sich im Alltag bewährt haben: Wir schützen unsere IT-Systeme, führen regelmäßig Datensicherungen durch, wir installieren Virenschutzprogramme und aktivieren unsere Firewalls.
Wir wissen jedoch nicht, wie gut diese Maßnahmen tatsächlich wirken. Und außerdem rechnen wir auch nicht damit, Opfer eines Cyber Angriffs zu werden.

Cyber-Risiko wird noch immer unterschätzt

Die meisten von uns sind reine Software-Anwender. Wir kennen verwendete Programme meist nur oberflächlich. Dies ist einer der Gründe, warum das Cyber-Thema so schwer greifbar ist. Und es erfordert, wenn es um Probleme oder komplexere Funktionen geht, Unterstützung von Spezialisten.

Die Folgen von Cyber-Schäden sind oft teuer und langwierig in Ihrer Behebung. Im KMU-Bereich nehmen diese von Jahr zu Jahr zu. Es herrscht akuter Handlungsbedarf. Aber was können wir tun?

Zum einen könnten wir uns auf einen Cyber-Angriff vorbereiten, und zum anderen gegen Cyber-Schäden auch versichern lassen.
Im Folgenden gehen wir darauf ein, wie Sie das Cyber-Risiko besser erfassen können und schildern dazu einige Szenarien.
Wenn Sie Antworten auf folgende Fragen haben, oder sogar schon Maßnahmen gesetzt haben, dann sind Sie vielen schon einen Schritt voraus:

- Was ist zu tun, wenn ein Cyber-Angriff stattgefunden hat?
- Wie reagiere ich richtig, wenn im Unternehmen die IT-Systeme ausfallen?
- Wie kann ich herausfinden, ob in meinen IT-Systemen Sicherheitslücken vorhanden sind?
- Wie gehe ich mit Lösegeldforderungen um?
- Was passiert, wenn gestohlene Kundendaten im Darknet aufscheinen und Entschädigungszahlungen von Dritten eingefordert werden?

Konkret helfen bei diesen Szenarien die Erstellung von Notfallplänen oder das Anlegen einer Adressliste mit Kontaktdaten von einschlägigen Experten. Damit verlieren Sie keine wertvolle Zeit im Schadensfall. Eine fundierte Vorbereitung berücksichtigt jedoch weitaus mehr Punkte.

Risikoanalyse als Basis für das Erkennen von Cyber-Risiken

Risk Experts ist für seine Expertise in den Bereichen Risiko- und Schadenmanagement bekannt. Seit geraumer Zeit beschäftigen sich unsere Expert:innen auch intensiv mit dem Thema Cyber. Dabei identifizieren wir Cyber- und Datenschutzrisiken von Unternehmen, analysieren diese systematisch und bewerten diese für Makler:innen, Unternehmer:innen und Versicherer.
Im Rahmen der Bewertung erheben wir einerseits bestehende Gefahren und andererseits evaluieren wir die vorhandenen Schutzmaßnahmen. Dadurch erhalten wir einen Überblick der Cyber-Sicherheitslage in einem Unternehmen.

Für unsere Methodik haben wir führende IT-Expert:innen befragt und fast alle international verwendeten Versicherungs-Cyber-Fragebögen unter die Lupe genommen. Daraus entstand die Basis für eine strukturierte und allgemein anwendbare Risikoanalyse.
Unsere Vorgehensweise ermöglicht, Cybersicherheit verständlich zu erfassen und sinnvoll zu bewerten – und unter dem Titel „Cyber Risk Engineering“ anzubieten.

Der Fokus des Cyber Risk Engineerings liegt auf folgenden Schwerpunkten

1 Allgemeine Unternehmenssituation
2 Organisatorische IT-Sicherheit
3 Technische IT-Sicherheit

4 Datenschutz
5 Betriebsunterbrechung
6 Höchstschadensszenarien
7 Risikoverbesserungsempfehlungen

Zusammengeführt werden diese Erkenntnisse in einem Executive Summary (Gesamtbewertung), um mit einem Blick den tatsächlichen IST-Stand des vorhandenen Risikos darzustellen. In jeder Kategorie wird ebenfalls eine kurze Übersicht geboten, um die darin enthaltenen Hauptrisiken, Stärken und Schwächen des analysierten Unternehmens aufzuzeigen.

Zentrale Vorteile dabei sind, dass komplexe Cyberrisiken in die versicherungstechnische Sprache übersetzt werden, sowie eine objektive und fundierte Risikoeinschätzung durchgeführt wird. Zusätzlich entsteht ein Mehrwert, dass Cyber-Risiken besser eingeschätzt werden können, sowohl für Unternehmen als auch für Versicherer. Mittels konkreten Verbesserungsmaßnahmen und Empfehlungen zur Risikoverminderung kann die Cyber-Sicherheit im Unternehmen erhöht werden.

Was wird nun bei der Beurteilung des Cyber-Risikos betrachtet?
Um dies besser zu erklären, gehen wir im Folgenden kurz auf die oben erwähnten Fokusbereiche ein:

1 Bei der **allgemeinen Betrachtung der Unternehmenssituation** werden jene Themen beleuchtet, die darüber Aufschluss geben, welche Schutzmaßnahmen in einem Unternehmen bereits vorhanden sind.
Dies betrifft unter anderem die Anzahl an IT-Equipment, die Organisationsstruktur (Töchterunternehmen, Umsätze, etc.), externe (IT-)Dienstleister und vorhandene Softwaretools.

2 **Organisatorische IT-Sicherheit** beinhaltet jene Schutzmaßnahmen, wie Aktionen, Strategien und Prozesse, die dazu beitragen, die Betriebs-Ziele einer Organisation zu erreichen. Sie umfassen die Entwicklung und Umsetzung von Aufgaben, Strukturen, Verfahren und Systemen, um die Ressourcen und Aktivitäten einer Organisation effizient, effektiv und wirtschaftlich zu koordinieren und zu verwalten. Sie können auch die Einrichtung eines Berichtswesens, die Entwicklung von Richtlinien und Verfahren, die Durchführung von Schulungen, die Planung und Implementierung von Programmen und die Kontrolle des Betriebs umfassen.

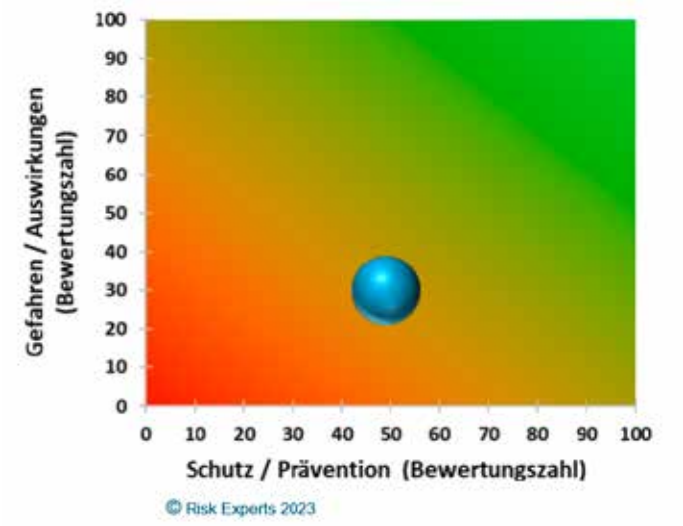
3 **Technische IT-Sicherheit** bezieht sich auf Strategien, die verwendet werden, um die IT-Infrastruktur eines Unternehmens zu schützen. Dazu gehören die Einrichtung/ Konfiguration von Firewalls, die Verwendung von Antivirensoftware, die Verwendung verschiedener Sicherheitsprotokolle und die Durchführung regelmäßiger Sicherheitsüberprüfungen. Diese Maßnahmen helfen, die Systeme eines Unternehmens vor Cyber-Angriffen und Datendiebstahl zu schützen. Dabei werden die technischen Schutzmaßnahmen im Unternehmen evaluiert und bewertet.

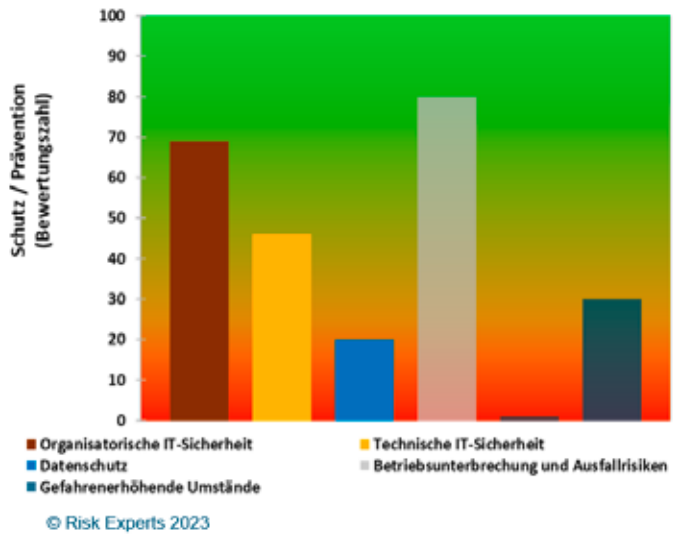
4 **Datenschutz**-Themen: Dabei geht es in erster Linie um jene Maßnahmen, die die Datensicherheit im Unternehmen erhöhen. Dabei werden nicht nur das DSG, die DSGVO, sondern auch weitere Richtlinien und Obliegenheiten von Versicherern berücksichtigt.

5 und **6** Im **Höchstschadenszenario** werden die **Betriebsunterbrechungsrisiken** und die dazu notwendigen Schutzmaßnahmen wie Notfallpläne, Risikomanagement, Business Impact Analyse und weitere Alarmpläne behandelt. Auch eine EML/PML-Berechnung erfolgt im Hinblick auf das Cyberrisiko.

Das Ergebnis unseres Berichtes wird graphisch aufbereitet und für die einzelnen Unternehmensbereiche angeführt:

»





Fazit

Für das Erlangen eines ausreichenden Versicherungsschutzes ist eine vorausgehende und fundierte Risikoanalyse unerlässlich – ob für Unternehmen, Makler:innen oder Versicherer. Das von Risk Experts entwickelte Cyber Risk Engineering basiert grundsätzlich auf derselben Struktur und Vorgehensweise wie ein klassisches Risk Engineering. Unsere aus Sach- und BU-Analysen gewonnenen Erfahrungswerte werden dabei mit neuen Erkenntnissen und Anforderungen aus dem Cyberbereich kombiniert und angewandt.

Unsere Unterstützung

Risk Experts ist ein unabhängiges Beratungsunternehmen, das auf die Bereiche Risikomanagement und Sachverständigendienstleistungen spezialisiert ist.
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, bietet die Risk Experts Academy Seminare und Webinare zum Thema Cyber bzw. Cyber-Sicherheit an. Details dazu finden Sie auf unserer Homepage: **www.riskexperts.at**