makler intern QVM
03/2022

Ein Krönchen macht noch keine Prinzessin

Der OGH hat gesprochen: Ein echter Mehrfachagent missachtet das Trennungsgebot und steht nicht mehr eindeutig auf der Seite des Versicherers. Er ist demnach als Versicherungsmakler mit allen Pflichten zu qualifizieren.

Christopher DROLZ,
LL.M. WU, CIPP/E
IT Security Consultant

RISK EXPERTS
ENABLING SMART DECISIONS.

Cyber-Risiken und Cyber-Versicherungen

Warum sie auch für Makler:innen und Unternehmen immer wichtiger werden

Die aktuelle Cyber-Sicherheitssituation ist als überaus bedrohlich zu bezeichnen: moderne Cyber-Kriegsführung, konstante Zunahme der Anzahl von Cyber-Angriffen und insbesondere datenschutzrechtliche Aspekte führen dazu, dass sich sowohl Makler:innen als auch Unternehmen vermehrt mit den Themen IT-Sicherheit und Cyber-Versicherung beschäftigen müssen.

Neben den faktisch durch IT-Vorfälle möglichen Schäden, könnten darüber hinaus sogar rechtliche Konsequenzen drohen.

Wir möchten in diesem Artikel – trotz zahlreichen anderen möglichen Arten von Cyber-Attacken – auf eine ganz bestimmte Gefahr eingehen, die in letzter Zeit stark zugenommen hat – die Ransomware.

Ransomware – der aktuelle Trend

Unter einem Ransomware-Angriff versteht man einen Cyber-Angriff, der oftmals so aufgebaut ist, die Daten eines Zielsystems zu verschlüsseln. Dadurch wird erreicht, dass der Zugriff durch legitime Nutzer:innen nicht mehr möglich ist. Cyber-Kriminelle fordern in weiterer Folge ein Lösegeld. Gegen Zahlung einer meist in Kryptowährung geforderten Summe versprechen diese, einen Entschlüsselungs-Key zu übermitteln, um den Datenzugriff wieder zu ermöglichen.

Betroffene sind daraufhin verleitet, der Forderung – in der Hoffnung dadurch wieder an die Daten zu gelangen – nachzukommen. Je nach Wichtigkeit und Brisanz der verschlüsselten Daten erhöht sich der Druck. Versetzen wir uns einmal in diese Lage und stellen uns vor, dass es sich bei den verschlüsselten Daten um Gesundheitsinformationen handelt, die dringend benötigt werden (z.B.: für Operationen).

Dies könnte in diesem Fall sogar zu lebensentscheidenden Auswirkungen führen und für Betroffene eine immense psychische Belastung bedeuten.

Vorfälle zeigen praktische Relevanz

Eine kürzlich im Auftrag vom IT-Sicherheitsunternehmen „Sophos“ durchgeführte Studie ergab, dass durchschnittlich bereits 66% der Befragten (n=5600 in 31 Ländern) Opfer von Ransomware wurden und es zu durchschnittlichen Kosten in der Höhe von USD 1,4 Mio. für die Behebung der Angriffs-Folgen kam (Sophos-Whitepaper, April 2022, Ransomware-Report 2022).

Schäden und die datenschutzrechtliche Komponente eines Cyber-Angriffs

Cyber-Angriffe, wie etwa die zuvor angesprochene Ransomware, haben unter Umständen das Potenzial, Betriebsunterbrechungen zu verursachen. Zusätzlich drohen nicht unwesentliche Kosten für Schadensbehebung und Cyber-Forensik. Zu den monetären Schäden kommen meist auch noch Reputationsschäden hinzu.

Neben diesen genannten Aspekten schwebt erschwerend auch ein juristisches Damoklesschwert über den betroffenen Unternehmen. Die Rede ist von der Datenschutzgrundverordnung („DSGVO“). Vielen wird sie mittlerweile bereits ein Begriff sein. Ein Aspekt wird aber oftmals unterschätzt, nämlich die Verletzung des Schutzes personenbezogener Daten.

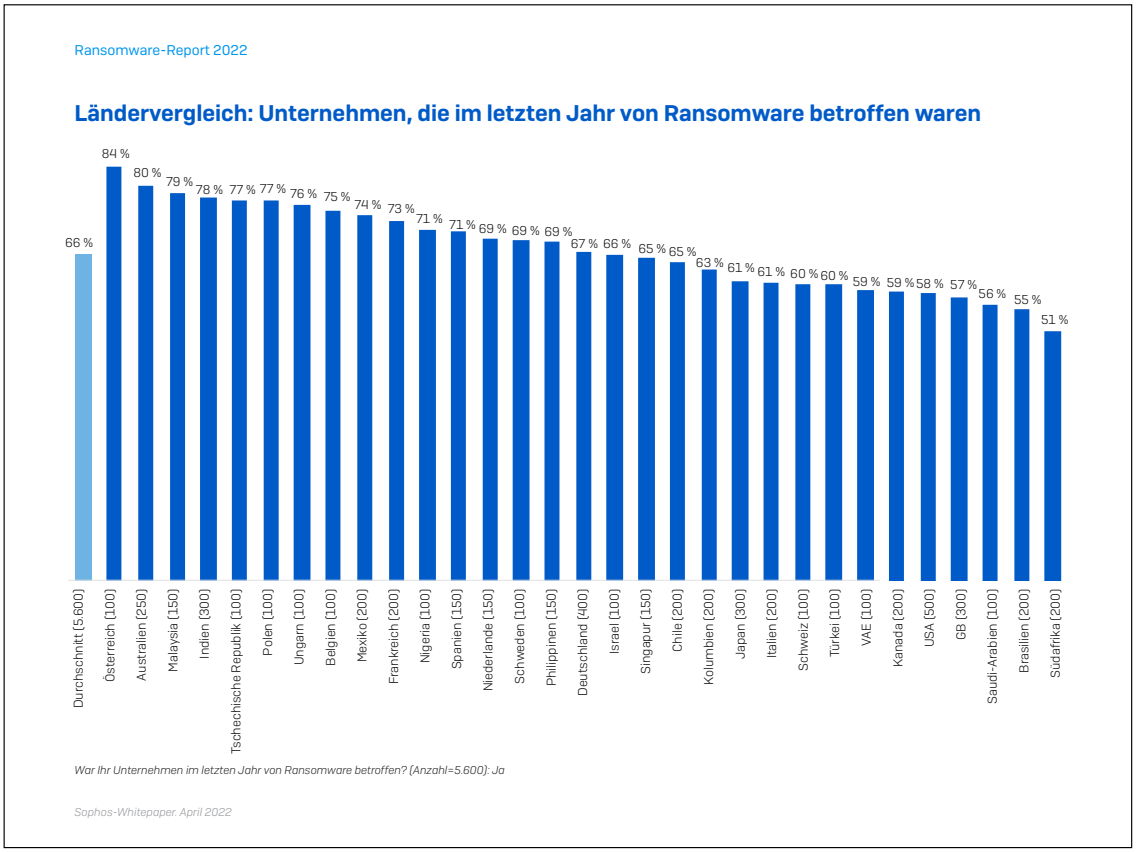
Sind personenbezogene Daten im Anwendungsbereich der DSGVO Gegenstand eines Cyber-Angriffs, so gehen damit unter Umständen umfangreiche Verpflichtungen zur Dokumentation, zur Cyber-Forensik und zu fristbewährten Meldungen an Behörden und/ oder Betroffene einher.

Haftungs- und Kostenaspekte – Datenschutzrechtliche Compliance

Werden entsprechende Verpflichtungen verletzt, drohen signifikante datenschutzrechtliche Konsequenzen für Unternehmen. Selbst im Falle einer erfolgten Meldung, birgt diese das Potenzial, sich insbesondere Schadenersatzansprüchen und behördlichen Verfahren auszusetzen.

Jedes Unternehmen sollte sich daher fragen, wie die anfallenden Kosten, insbesondere aufgrund von Schadenersatzforderungen, für die nötige Cyber-Forensik und Dokumentation sowie für eine Incident-Response getragen werden können. Darüber hinaus entstehen weitere Verluste, wenn Cyber-Angriffe Betriebsunterbrechungen verursachen.

Für all diese Fälle könnten sich sogenannte Cyber-Versicherungen – je nach Deckungsumfang – eignen und das Risikomanagement eines Unternehmens ideal ergänzen.



Cyber-Versicherung – Der Deckungsumfang und der potenzielle Kreis von Versicherungsnehmer:innen

Typischerweise umfassen Cyber-Versicherungen neben der Unterstützung bei der unmittelbaren Incident-Response auch die Kostentragung für die weitere Schadenbehebung, für etwaige Betriebsunterbrechungen, sowie für Drittschäden.

Durch die hohe praktische Relevanz der genannten Punkte und der gestiegenen Anzahl von Cyber-Angriffen ist der Kreis potenzieller Cyber-Versicherungsnehmer:innen überaus groß: von Einzelunternehmen bis hin zum multinationalen Konzern – sie alle könnten Opfer von Cyber-Vorfällen werden und darüber hinaus in den Anwendungsbereich der DSGVO fallen.

Fehlender Hinweis auf eine Cyber-Versicherung als Risiko für Makler:innen?

Sie alle kennen mit Sicherheit den Grundsatz des „Best Advice“, mit dem auch eine nicht zu unterschätzende Haftungsthematik für Makler:innen schlagend werden kann.

Im Lichte der Rechtsprechung zur Maklerhaftung birgt die Nichtberücksichtigung einer Cyber-Versicherung das nicht unwesentliche Potenzial, sich als Makler:in einer unerwünschten Haftung auszusetzen. Wir empfehlen daher, die Rahmenbedingungen einer Cyber-Versicherung zu kennen und diese im Zuge von Maklertätigkeiten ernsthaft in Erwägung zu ziehen und anzusprechen.

Risikoeinschätzung und -reduktion als signifikante Komponenten

Bevor eine Cyber-Versicherung abgeschlossen werden kann, wird oftmals eine Risikoeinschätzung oder -verbesserung nötig sein. Dies geschieht nicht nur aus dem Grund, damit der Versicherer eine Basis für die festzusetzende Prämie hat, sondern auch im Eigeninteresse des Unternehmens, um die aktuelle Risikosituation zu kennen.

Folgend geben wir Ihnen einige ausgewählte Fragen zur Hand, mit denen Sie bei Ihren Kund:innen eine grobe Ersteinschätzung des Cyber-Risikos vornehmen können:

- Haben Sie ausreichende fachliche, personelle und finanzielle Ressourcen zur Bewältigung eines Cyber-Vorfalls?
- Wurden im Unternehmen personelle Zuständigkeiten und Ansprechpartner vorab definiert sowie ein IT-Notfallplan erstellt?
- Führen Sie regelmäßige und umfangreiche IT-Sicherungs- und Aktualisierungsmaßnahmen durch?
- Setzen Sie auf aktuelle und angemessene IT-Sicherheitsmaßnahmen technischer und organisatorischer Natur?
- Bestehen adäquate Maßnahmen zur Detektion und Meldung datenschutzrechtlich relevanter Vorfälle?
- Kennen Sie Ihre rechtlichen Verpflichtungen?
- Sind Mitarbeiter:innen hinsichtlich IT-Sicherheit und Datenschutz geschult?
- Ist eine adäquate Betriebsunterbrechungs- bzw. Cyber-Versicherung vorhanden?

»

Sofern ein Großteil der Fragen mit „Ja“ beantwortet werden kann, gehört ein Unternehmen bereits zu jenem kleinen Teil, der besser auf Cyber-Vorfälle vorbereitet ist.

In diesem Kontext können spezialisierte Cyber-Risiko-Produkte, wie etwa eine Cyber-Risikoanalyse oder ein Cyber-Coaching, helfen, um eine weiterführende Befundaufnahme und Risikoreduktion durchzuführen.

Unsere Unterstützung
Für weitere Informationen und Unterstützung in Sachen Cyber-Sicherheit, Cyber-Versicherung, Cyber-Risikoreduktion und -beurteilung, insbesondere hinsichtlich des Datenschutzrechts, 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/Webinare zum Thema Cyber bzw. Cyber-Sicherheit an.

Weitere Informationen finden Sie auf unserer Website **www.riskexperts.at**

Rezensionen – Bücher, die in keinem Maklerbüro fehlen sollten!

Haftung und Versicherung bei Unfällen automatisierter Fahrzeuge – Weichbold – Verlag Manz – ISBN: 978 3 214 14791 4

In diesem Buch werden haftungs- und versicherungsrechtliche Fragen im Zusammenhang mit automatisierten & fahrerlosen Fahrzeugen übersichtlich dargestellt und rechtlich fundiert beantwortet.
Der Trend zur Übertragung von Fahraufgaben weg vom Lenker hin auf das Fahrzeug selbst ist unaufhaltsam und unumkehrbar, das Bild einer weitgehend fahrerlosen Zukunft zunehmend eine bloße Frage der Zeit.
Die damit einhergehenden rechtlichen Probleme werden im vorliegenden Buch auf dem aktuellen Stand der Technik und im Hinblick auf zukünftige Entwicklungen erörtert.

Umfassend behandelt werden:
- Fragen der Haftung des Lenkers, Halters und Fahrzeugherstellers,
- Fragen der Kfz- und Betriebshaftpflichtversicherung sowie der Kfz-Kaskoversicherung und
- die rechtspolitischen Gestaltungsmöglichkeiten.

Handbuch Versicherungsmarketing – Reich/Zerres – Verlag Springer – ISBN: 978 3 662 57754 7

Lange Zeit wurde Marketing in der deutschen Versicherungswirtschaft vernachlässigt. Häufig konzentrierten sich die Unternehmen lediglich darauf, ihre Vertriebspolitik zu optimieren. Marketing im Sinne einer Unternehmensphilosophie, bei der alle betrieblichen Bereiche auf den Markt und seine Anforderungen ausgerichtet werden, erfährt nun auch in Versicherungsunternehmen eine schnell wachsende Bedeutung.
Dieses Handbuch trägt der Entwicklung Rechnung. In seinem Aufbau orientiert es sich am Dienstleistungsmarketing. Die Übertragung von Erkenntnissen aus allgemeinem und Dienstleistungsmarketing auf das Marketing von Versicherungsunternehmen ist in der Praxis allerdings mit großen Herausforderungen verbunden, da die wesentlichen Merkmale des Versicherungsgeschäftes berücksichtigt werden müssen. Das Handbuch Versicherungsmarketing unterstützt den Leser in dieser Aufgabenstellung durch wissenschaftliche und praktische Anleitung und einen hoch aktuellen, breit fundierten Erfahrungsschatz.