AUTOR
Julia Loisl
Rechtsanwaltsanwärterin
T +43 1 512 03 53
julia.loisl@vhm-law.at

Julia Loisl ist Rechtsanwaltsanwärterin bei VHM Rechtsanwälte.

Ihre Schwerpunkte sind Dispute Resolution und Versicherungsrecht.

„Silent Cyber“-Risiken

14.09.2020

Schlagworte: Cyberversicherung, Sachbegriff-Definition, Sachversicherung, Silent-Cyber-Risiko.

Heutzutage ist ein Zugriff auf Daten überall und jederzeit möglich. Die zunehmende Vernetzung und Digitalisierung bedeutet jedoch auch, dass wir mit einer wachsenden Zahl von Cyber-Bedrohungen konfrontiert sind: Hacker, Malware, Cyber-Kriminalität, Datenbruch, Identitätsdiebstahl, unsichere Codes, Cyber-Terrorismus, menschliches Versagen, Angriffe auf kritische Infrastrukturen ...

Durch die globalen Cyber-Attacken WannaCry, Petya und NotPetya im Jahr 2017 erlitten Unternehmen durch Schäden in sämtlichen Geschäftsbereichen erhebliche Verluste. Schätzungsweise sind durch diese Ereignisse weltweit ungefähr 3,3 Mrd. US-Dollar an wirtschafltichem Nachteil entstanden. Laut dem US-amerikanischen Analyseunternehmen für Versicherungsschäden, PCS, geht man davon aus, dass knapp 90% des gesamtem durch Petya/NotPetya verursachten industriellen Schadens als sogenannte „Silent Cyber“-Risiken zu behandeln waren.

Vavrovsky Heine Marth Rechtsanwälte GmbH

Wien – Salzburg

Fleischmarkt 1
1010 Wien, Österreich
T +43 1 512 0353
F +43 1 512 0353 – 40
office.wien@vhm-law.at

www.vhm-law.at

Was bedeutet „Silent Cyber“?

Der Begriff „Silent Cyber“ hat sich entwickelt, um potenzielle Schäden aus Cybergefahren zu beschreiben, die in konventionellen Sach- und Haftpflichtversicherungen gedeckt sind, aber nicht speziell für die Deckung dieser Risiken konzipiert wurden und daher Cyber-Risiken nicht ausdrücklich ein- oder ausschließen.

Die Deckung im Falle eines Cyber-Vorfalls könnte aufgrund der unklaren oder unvollständigen Formulierung der Polizze mehrdeutig und unklar sein. Eine nicht beabsichtigte Cyber-Exponierung im Rahmen traditioneller Polizzen kann sich daraus ergeben, dass die Polizze zur Thematik Cyber schweigt, dass die Polizze keinen Ausschluss von Cyber-Schäden enthält oder der Begriff „Cyber“ (ob beabsichtigt oder nicht) nicht umfassend definiert ist. Überdies kann es sein, dass das Bedingungswerk einen Cyber-Einschluss enthält, der jedoch mehrdeutig, unklar oder unvollständig ist.

Die oben genannten Cyber-Angriffe WannaCry und Petya/NotPetya machten daher das Problem „Silent Cyber“ deutlich, dass im Falle derartiger Ereignisse neben einer dedizierten Cyberversicherung auch anderen Versicherungssparten von Cyber-Schadensereignissen betroffen sein können.

Tatsächlich ist fast jeder konventionelle Versicherungsvertrag gegenüber Cyberrisiken exponiert, weshalb die Silent Cyber-Deckung potenziell von erheblicher Bedeutung ist.

Wie reagieren Versicherer auf Silent Cyber-Risiken?

Einige Versicherer sehen sich daher veranlasst, ihre Vertragsbedingungen für konventionelle Versicherungssparten zu überprüfen um Cyber-Risiken explizit auszuschließen. Daran anschließend werden eigenständige Cyberversicherungen angeboten um stille Cyberrisiken in eine affirmative Cyber-Deckung umzuwandeln.

Andere Versicherer hingegen haben diesen Weg (noch) nicht eingeschlagen. Als Lösung sollen hier von einigen Maklern Rückversicherungsmöglichkeiten angeboten, die Silent Cyber-Risiken, erfassen.

Gibt es einen tatsächlichen Bedarf nach eigenständigen Cyberversicherungen?[1]

Nachfolgend soll – insbesondere unter der Beleuchtung von marktüblichen Sachversicherungen in Deutschland und in Österreich – der Frage nachgegangen werden, ob tatsächlich ein Bedarf an eigenständigen Cyberversicherungen besteht. Handelt es sich bei Cyberversicherungen um einen

[1] *Kath*, ZVers 3/2019, Die Cyberversicherung Überblick über ein neues Versicherungsprodukt (2019) S 105f

überzogenen Hype oder bieten diese Verträge vielmehr eine interessens- und bedarfsgerechte Lösung einer Risikosituation, welche durch traditionelle Versicherungslösungen nicht mehr angemessen bewältigbar (gewesen) wäre.

In **Deutschland** wird die Auffassung vertreten, dass im Rahmen klassischer Sachversicherungen die Versicherbarkeit von Eigenschäden, worunter Wiederherstellungskosten von Daten und Datenverarbeitungsanlagen bzw IT-Systemen auch die Kosten für sonstige Maßnahmen und Betriebsunterbrechungsschäden zählen, schon daran scheitere, dass bloßer Datenverlust bzw Datenblockade allein keinen ersatzfähigen Sachschaden darstellen.

Die durch Datenverlust bzw -blockade verursachte Funktionsunfähigkeit einer Maschine oder Anlage – ohne dass dabei die Sachsubstanz beeinträchtigt wird – stelle für sich keinen Sachschaden dar. Nur wenn es zu irgendeiner Beeinträchtigung der Sachsubstanz kommt, sei eine Minderung des Substanzwerts oder der Gebrauchsfähigkeit der Maschine bzw Anlage als Sachschaden anzusehen.[2]

Da der Sachbegriff des § 90 BGB Körperlichkeit voraussetzt, seien in Deutschland Daten und Programme aufgrund ihrer Unkörperlichkeit nicht als Sachen anzusehen. Datenträger seien zwar als Sachen zu qualifizieren, nicht aber Daten für sich allein.

Marktgängige Software- und Datenversicherungen bieten in der Regel auch Entschädigung für Verlust, Veränderung und Nichtverfügbarkeit von Daten und Programmen an. Hier werde aber ein dem Grunde nach versicherter Schaden am Datenträger oder der Datenverarbeitungsanlage vorausgesetzt. Liegt ein derartiger Sachschaden nicht vor, wird auch kein Ersatz für Daten und Programme geboten.

Überdies sei in diesem Zusammenhang zu berücksichtigen, dass sich der Begriff "*dem Grunde nach versicherter Schaden*" (am Datenträger, etc) nach dem jeweiligen Versicherungszweig der Sachversicherung richte. Bei einer Feuerversicherung ist dies beispielsweise ein durch Brand, Blitzschlag, Explosion, etc, ausgelöster Schaden; bei einer technischen Versicherung wären dies Schäden, die durch Ungeschicklichkeit, Bedienungsfehler, mechanische Gewalt, bestimmte Elementargefahren, Material- oder Herstellungsfehler, etc herbeigeführt wurden.

Klassische Cyberattacken wie etwa die Schädigung bzw Beeinträchtigung von Daten auf elektronischem Weg (Ransomware, Malware) wären damit aber nicht erfasst.

In **Österreich** erscheint diesbezüglich eine differenzierende Sichtweise geboten. Zwar entsprechen die Versicherungsbedingungen marktgängiger Sach- sowie Software- und Datenversicherungen im Wesentlichen der

[2] BGH 20. 4. 2010, IV ZR 250/08

geschilderten Situation in Deutschland, jedoch ist die Definition des zivilrechtlichen Sachbegriffs in Österreich weiter gefasst als jener des BGB.

§ 285 ABGB definiert als Sache im rechtlichen Sinn „*Alles, was von der Person unterschieden ist, und zum Gebrauche der Menschen dient*“ und umfasst somit auch unkörperliche Sachen.

Dass elektronische Daten und Programme für sich allein keine Sachen seien, kann in Österreich nicht mit dieser Klarheit beantwortet werden. Darüber, ob eine Software nach der Definition des ABGB als Sache zu qualifizieren ist, ist in Österreich ein geteilter Meinungsstand zu verzeichnen – dies ob des Umstands, dass im österreichischen Produkthaftungsrecht als Produkt explizit eine bewegliche „körperliche“ Sache definiert wird.

Mehr als in Deutschland erweist sich daher für Österreich die Notwenigkeit – zur Vermeidung sogenannter Silent Cyber-Deckungen aus Sachversicherungen – in den Vertragsbedingungen klarzustellen, dass Daten und Software im Rahmen der jeweiligen Sachversicherung nicht als Sachen gelten sollen oder dass Schäden an Daten bzw Programmen explizit ausgeschlossen werden.

Abgesehen von eher seltenen All-Risk-Konzepten gilt für Österreich auch, dass selbst bei prinzipieller Bejahung der Sacheigenschaft von Daten und Programmen zu berücksichtigen bleibt, dass nur Schäden durch die im Rahmen der jeweiligen Sachversicherung taxativ benannten versicherten Gefahren auch tatsächlich vom Versicherungsschutz umfasst sind, zu welchen Cybergefahren üblicherweise gerade nicht zählen.

Fazit

Zusammenfassend kann daher festgehalten werden, dass beide Standpunkte hinsichtlich der Erforderlichkeit von Cyber-Versicherungsprodukten ihre (sachliche) Berechtigung haben – mögen sie auch aus unterschiedlichen Interessesituationen resultieren.

Insgesamt musste sich daher die Produktentwicklung der Versicherungsbranche dem Bedarf der Versicherten nach Versicherungsschutz für Cyberrisiken annehmen.

Literatur- und Judikaturverzeichnis:

1. *Kath*, ZVers 3/2019, Die Cyberversicherung Überblick über ein neues Versicherungsprodukt (2019).
2. BGH 20. 4. 2010, IV ZR 250/08.