Pflicht und Kür bei Abwehr von Cybercrime

Gastbeitrag. Datenschutz und drohende materielle Schäden zwingen Unternehmen zur Vorbeugung. Cyber-Versicherungen senken das Gefahrenpotenzial.

VON ARTHUR STADLER
UND CHRISTOPHER DROLZ

Wien. Im Lichte der aktuellen Cyber-Sicherheits-Lage spielen Cyber-Versicherungen eine immer prominentere Rolle im Risikomanagement sämtlicher Unternehmen. Im Jahr 2021 stieg die Zahl angezeigter Cybercrime-Vorfälle in Österreich im Vergleich zum Vorjahr von 35.915 auf 46.179 (BMI, Cybercrime Report 2021). Die Aufklärungsrate betrug 36,9 %. Diese Zahlen sind erschreckend, wenn auch wenig repräsentativ, da von einer deutlich höheren Dunkelziffer auszugehen ist. Für das Jahr 2022, jenem Jahr, in dem Cyber-Kriegsführung aufgrund der Ukraine-Krise besondere Bedeutung erlangte, ist von einer noch größeren Zahl auszugehen.

Angriff mit Ransomware

Unter Ransomware wird eine spezielle Schadsoftware verstanden, die es Kriminellen erlaubt, legitime Datenzugriffe Betroffener mittels Verschlüsselung zu verhindern, sodass Cyber-Kriminelle von den Opfern Lösegeld für die Entschlüsselung der Daten verlangen können. Eine im Zuge des Angriffs eintretende Betriebsunterbrechung verstärkt die Wirksamkeit der Erpressung, droht doch mit jeder Minute Betriebsstillstand ein höherer Schaden für das betroffene Unternehmen einzutreten.

Neben der reinen Verschlüsselung von Daten kommen darüber hinaus auch vermehrt sogenannte Extortion-Angriffe im Zusammenhang mit Ransomware vor, in denen mit der Veröffentlichung von exfiltrierten Daten gedroht wird. Diese Entwicklung ist unseres Erachtens besonders besorgniserregend, denn bei einer reinen Verschlüsselung wären nämlich noch technische Wiederherstellungsoptionen etwa aus Backups möglich. Im Fall der drohenden Preisgabe von Daten im DarkNet helfen jedoch auch solche Maßnahmen nicht mehr. Sind die Daten erst einmal in falschen Händen sind faktische Einflussmöglichkeiten – auch durch staatliche Hilfe – äußerst begrenzt.

Eine im Auftrag des Sicherheitsunternehmens „Sophos“ durchgeführte Studie (Ransomware-Report 2022) zeigt eindrücklich die Relevanz von Ransomware: So waren 66% der 5600 Befragten in 31 Ländern bereits von dieser befallen. Alleine von den in Österreich 100 befragten Unternehmen waren laut dieser Studie 84 von einer Ransomware betroffen.

Virtuell mit realen Folgen

Vielfach wird außer Acht gelassen, dass ein rein virtueller Angriff durchaus auch dazu in der Lage ist, zu mittelbar oder unmittelbaren Folgeschäden wie etwa zu Identitätsdiebstählen, Bränden oder Explosionen zu führen. Man denke etwa an ein produzierendes Unternehmen oder an ein Kraftwerk, dessen Turbinen durch einen Cyber-Angriff zu brennen anfangen und zu einer Betriebsunterbrechung führen können.

Über den Unternehmen schwebt zudem immer das Damoklesschwert der Datenschutzgrundverordnung (DSGVO): Kommt es zu einer Verletzung des Schutzes personenbezogener Daten – dies wird in einer Vielzahl von Cyber-Angriffen zweifellos der Fall sein –, so kann eine fristunterworfene Meldung an die Datenschutzbehörde sowie die Benachrichtigung aller Betroffener erforderlich werden und gegebenenfalls zu einem darauffolgenden amtswegigen Prüfverfahren der Behörde führen, an dessen Ende möglicherweise sogar Sanktionen oder gar Klagen Betroffener stehen. Unterlässt das Unternehmen eine gebotene Meldung, so riskiert es ebenfalls empfindliche Sanktionen und Schadenersatzansprüche.

Vorgaben für Sicherheit

Rechtliche Vorgaben an die Cyber-Sicherheit und -Resilienz finden sich insbesondere in Art 32 DSGVO sowie in § 17 des derzeit noch geltenden Netz- und Informationssystemsicherheitsgesetzes. In mittelbarer Zukunft spielen darüber hinaus europarechtliche Einflüsse, insbesondere aufgrund der noch geplanten Umsetzung der NIS2-Richtlinie sowie der Verordnung (EU) 2022/2554, besser bekannt als „Digital Operation Resilience Act“ (Dora), eine noch größere Rolle.

Neben den datenschutzrechtlichen Handlungspflichten samt Haftungs- und Sanktionspotenzial drohen im Ergebnis auch kostspielige Betriebsunterbrechungs- und Eigenschäden, denn ein Cyber-Vorfall muss oftmals kostenintensiv durch Fachkräfte behoben werden. Der Versicherungsmarkt hat das Potenzial erkannt und aus den verschiedenen Komponenten ein Produkt entwickelt: die Cyber-Versicherung. Diese besteht üblicherweise aus einer Eigenschadens-, Betriebsunterbrechungs- sowie Haftpflichtkomponente und ermöglicht so eine relativ umfangreiche Deckung der mit einem Cyber-Schaden typischerweise verbundenen Auswirkungen. Überdies bieten manche Versicherer weitere sinnvolle Komponenten wie etwa begleitende PR-Maßnahmen oder der überaus wichtigen Incident Response, bei der erste IT-Sofortmaßnahmen inkludiert sind, an.

Bevor eine Cyber-Versicherung vonseiten der Versicherer jedoch gezeichnet wird, muss sich das betroffene Unternehmen bewusst sein, wie es technisch und datenschutzrechtlich aufgestellt ist, denn üblicherweise verlangen die Versicherer das wahrheitsgemäße Ausfüllen eines umfangreichen Fragebogens zur Einschätzung des Cyber-Risikos. In Zeiten steigender Cyber-Schäden tendieren diese vermehrt dazu, beim Abschluss zurückhaltender zu sein, sodass im Einzelfall sogar ein zusätzliches Sachverständigengutachten zur Frage technischer, organisatorischer und datenschutzrechtlicher Risikoeinstufung verlangt werden kann. Werden gravierende Mängel identifiziert, kann dies einer Versicherbarkeit oder attraktiven Versicherungsbedingungen entgegenstehen. Umso wichtiger ist es daher für Unternehmen, sich technisch sowie rechtlich bereits vor Versicherungsabschluss entsprechend aufzustellen – dies sollte freilich auch im Eigeninteresse des Unternehmens liegen.

Wie bei jeder Versicherung sollten auch bei der Cyber-Versicherung die konkreten Konditionen und das Bedingungswerk verglichen und mit dem Bedarf des Unternehmens abgeglichen werden. Oftmals bestehen Sub-Limits oder vom Versicherungsnehmer zu berücksichtigende Obliegenheit vor und im Schadenfall, deren Verletzung Leistungsfreiheit zur Folge haben kann. Adäquate Vorbereitung auf Cyber-Risiken sowie eine fundierte Analyse des Bedingungswerks tragen dazu bei, Überraschungen im Versicherungsfall zu verhindern. Um dies sicherzustellen ist es für das Unternehmen essentiell, gegebenenfalls externe technische Unterstützung sowie auch Rechtsberatung heranzuziehen.

Risikomanagement essenziell

Die Cyber-Sicherheitslage ist so angespannt wie schon lange nicht mehr. Umso wichtiger ist es für Unternehmen sich möglichst gut auf Cyber-Vorfälle vorzubereiten. Dazu gehören insbesondere technische, organisatorische und datenschutzrechtliche Anpassungen und Vorbereitungen. Cyber-Versicherungen stellen hierbei eine durchaus sinnvolle Ergänzung eines gesamtheitlichen Risikomanagements dar, setzen aber oftmals ein akzeptables Cyber-Risiko des Unternehmens bzw. eine gute Vorbereitung auf einen Cyber-Vorfall voraus. Ein hohes Maß an Cyber-Sicherheit im Unternehmen ist genauso wie eine exakte Analyse der konkreten Bedingungen und Leistungen unerlässlich.

Dr. Arthur Stadler ist Partner;
Christopher Drolz, LL.M. (WU), CIPP/E,
ist RAA bei Stadler Völkel Rechtsanwälte.