Neue Zürcher Zeitung

NZZ – GEGRÜNDET 1780

Mittwoch, 28. September 2022 · Nr. 226 · 243. Jg. AZ 8021 Zürich · Fr. 5.10

RECHT UND GESELLSCHAFT

Unternehmen sind immer mehr Cyberattacken ausgesetzt Eine Versicherung gegen Cyberrisiken ist Aufgabe des Verwaltungsrates RETO M. JENNY

Die Bedrohungslage durch Cyberattacken hat sich in den letzten Jahren deutlich verschärft. Dies zeigt eine kürzlich publizierte Umfrage des Industrieverbandes Swissmem. Laut ihr waren 70 Prozent der Unternehmen in den letzten zwei Jahren Ziel mindestens eines Cyberangriffs. Begünstigt wurden diese Angriffe durch den von der Corona-Pandemie getriebenen Digitalisierungsschub. Die vermehrte Arbeit im Home Office eröffnete dabei neue Schwachstellen für Cyberangreifer. Nicht nur Grosskonzerne sind deren Zielscheibe, sondern auch KMU. Gemäss einer aktuellen Studie der Mobiliar waren 31 Prozent der befragten KMU von einem Cyberangriff betroffen. Ungeachtet dessen wurden in der genannten Umfrage keine Fortschritte bezüglich technischer und organisatorischer Cybersicherheitsmassnahmen der KMU festgestellt. Die Auswirkungen einer Cyberattacke auf ein Unternehmen können massiv sein. Nicht nur finanzielle Schäden, sondern auch Reputationsschäden oder Datenschutzverletzungen gehören dazu. Der Verwaltungsrat trägt hier die Verantwortung. Er hat im Rahmen seiner Kontrollfunktion mittels Weisungen und Reglementen sicherzustellen, dass das Unternehmen Cyberangriffe abwehrt und deren Wirkungen mildert. Dazu gehört nicht nur, mögliche Risiken zu identifizieren und Mitarbeiter darauf zu sensibilisieren oder zu schulen, sondern auch Vorgaben mit Bezug auf den Versicherungsschutz gegen Cyberrisiken zu machen. Insoweit ist der Abschluss einer Cyberversicherung ein Bestandteil des Risikomanagements. Kommt der Verwaltungsrat dieser Aufgabe nicht oder unzureichend nach, kann er im Schadenfall haftpflichtig werden. Gravierende finanzielle Folgen Ein Cyberangriff ist eine beabsichtigte unerlaubte Handlung einer Person oder einer Gruppierung im Cyberraum, um die Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen und Daten oder informationsverarbeitenden Systemen zu beeinträchtigten. Ein typischer Hackerangriff ist das Einschleusen von Computerviren und -würmern oder von Ransomware. Letztgenanntes sind Schadprogramme, mit denen der Zugriff auf oder die Nutzung von Daten oder ganzen Computersystemen verhindert werden kann – oft durch Verschlüsselung von Daten. Die Angreifer fordern für die Entschlüsselung eine Lösegeldzahlung in Kryptowährung. Andere Formen sind etwa Phishing (Ausspionieren von Passwörtern oder anderen persönlichen Informationen), CEO-Betrug (fingierte dringliche Zahlungsaufforderungen durch den CEO, wobei dieser für Rückfragen nicht zur Verfügung stehe) oder Datendiebstahl. Unter Distributed Denial of Service wird ein Angriff auf Computersysteme oder Websites verstanden, um deren Verfügbarkeit durch eine grosse Zahl von Anfragen zu beeinträchtigen. Die finanziellen Folgen solcher Angriffe sind gross. Es können Eigenschäden mit Kosten für Krisenmanagement, Kosten für die Benachrichtigung der von Datenschutzverletzungen Betroffenen, Datenschutzbussen, Einbussen infolge von Betriebsunterbrüchen, Kosten für IT-Dienstleister und Erpressungszahlungen anfallen. Daneben können sich aber auch Haftpflichtrisiken manifestieren, zum Beispiel in Form von

Schadenersatzansprüchen Dritter nach Datendiebstählen oder Datenschutzverletzungen. Herkömmliche Versicherungsprodukte wie etwa Sachversicherungen, Haftpflichtversicherungen, Vertrauensschutzversicherungen und Organhaftpflichtversicherungen decken die vielfältigen Erscheinungsformen von Cyberschäden nicht oder nicht ausreichend. Zu diesem Zweck bieten Versicherungsunternehmen Cyberversicherungen für Grossunternehmen und KMU, aber auch für Privatpersonen an. Der Deckungsumfang solcher Cyberversicherungen sowie die einzelnen Versicherungsbedingungen sind recht unterschiedlich. Keine Allgefahrendeckung Typische Deckungsbausteine sind Eigenschäden, Haftpflichtansprüche Dritter sowie Assistenzdienstleistungen. Gedeckte Eigenschäden können beispielsweise Erpressungszahlungen, Betrugsschäden, Ertragsausfall durch Betriebsunterbruch, Kosten für Datenwiederherstellung, Datenschutzbussen oder Kosten für die Benachrichtigung von Behörden und Betroffenen bei Datenverlusten sein. Zu den gedeckten Haftpflichtansprüchen gehören üblicherweise Schadenersatzzahlungen für Vermögensschäden aufgrund von Datenschutzverletzungen. Cyberversicherungen sind jedoch keine Rundum-sorglos-Pakete. Zum einen bieten sie typischerweise keine Allgefahrendeckung, sondern nur Schutz gegen konkret im Vertrag definierte Einzelrisiken. Zum anderen werden die Versicherten regelmässig vertraglich verpflichtet, ihre Daten- und Zugriffssicherung sowie den technischen Stand des IT-Systems zu pflegen und Schutzsysteme einzusetzen und aktuell zu halten. Letztgenanntes umfasst Antivirussoftware, Firewalls, regelmässige Sicherheitsupdates von Betriebssystemen und Programmen sowie die Verschlüsselung von Daten. Mit diesen Obliegenheiten sind nicht unerhebliche Kosten verbunden. Werden sie nicht eingehalten, kann dies zur Kürzung und – im schlimmsten Fall – zum Verlust des Versicherungsanspruchs führen. Schliesslich sehen die Versicherungsbedingungen eine Reihe von Ausschlüssen vor, so etwa für Krieg und Terrorismus. Will ein Unternehmen angesichts dieser Komplexität auf Nummer sicher gehen, ist eine umfassende Bedarfsanalyse zum Versicherungsschutz dringend empfohlen.

Reto M. Jenny ist Partner der Zürcher Kanzlei Prager Dreifuss. Er ist unter anderem auf Organ-, Produkte- und Berufshaftpflichtversicherungen spezialisiert.