CYBER SCHADENFALL

Markel hat sich eine faire Schadensregulierung auf die Fahnen geschrieben. Das beweisen immer wieder Studien und Tests. Zuletzt 2022 im Rahmen der großangelegten FOCUS MONEY Studie – Fairness von Cyberversicherern, welche mehr als 1.200 Fälle untersuchte. Markel erhielt wiederholt die Note „Sehr gut". In Kombination mit direkten Ansprechpartnern kann Markel rasch auf Schadensfälle reagieren. Offene und ehrliche Kommunikation sind dabei Schlüsselelemente, die entscheidend zu einer langfristigen Kunden-/Maklerbeziehung beitragen.

Die Lösegeld Erpressung

RANSOMWARE-ATTACKE

Ausgangssituation
Der Versicherungsnehmer ist ein Servicedienstleister im Bereich der Automobilzulieferindustrie. Er besitzt ein eine eigene IT-Infrastruktur und eigenes, bei ihm angestelltes IT-Fachpersonal. Über verschiedene Schnittstellen ist sein Netzwerk an das jeweilige seiner Kunden angebunden.

Problembeschreibung
An einem Freitag um 09:36 Uhr schlug eine Überwachungssoftware internen Alarm. Während der Versicherungsnehmer noch dabei war, mögliche Ursachen zu ermitteln, trafen in mehreren E-Mail-Postfächern des Unternehmens Nachrichten ein, welche darüber informierten, dass sämtliche Daten auf den firmeneigenen Servern verschlüsselt wurden. Fast gleichzeitig begannen an den Servern angeschlossene Drucker mit dem Ausdruck der Nachricht „Your data are stolen and encrypted". Um 11:47 Uhr erhielt das Unternehmen per E-Mail eine Zahlungsaufforderung über EUR 50.000,00, um wieder Zugriff auf die verschlüsselten Daten zu erlangen. Man war Opfer eine Lösegeld-Erpressung geworden, einer Ransomware-Attacke.

Lösungsansatz
Der Versicherungsnehmer erstattete Anzeige und Markel begleitete die Aufarbeitung des Sachverhalts durch seinen Partner BeforeCrypt, einem anerkannten Spezialisten zur Datenrettung.
Der erste Schritt zur Lösung des Problems besteht in der Aktualität der Datensicherungen. Je aktueller die Sicherung, je kürzer die Sicherungsintervalle, desto weniger Schaden kann angerichtet werden. Aus Sicht einer möglichen Betriebsunterbrechung ist es von Bedeutung, ob Mitarbeiter nur Daten eines Tages, einer Woche oder eines Monats manuell erneut einpflegen müssen.
Im vorliegenden Fall zeigte sich, dass die einzig brauchbare Sicherung bereits drei Monate alt war. Das erhöhte die Erfolgswahrscheinlichkeit der Erpresser, da viele Unternehmen die Kosten einer Wiederherstellung jenen des Lösegelds gegenüberstellen. Da ist es verführerisch, das Lösegeld zu bezahlen, um keine längere Betriebsunterbrechung zu riskieren. Doch das ist ein Trugschluss. Warum sollte jemand der einen kriminellen Akt begeht, sich nach Zahlung des Lösegeldes „korrekt" verhalten und Ihnen den Verschlüsselungscode übergeben? Dafür gibt es keinerlei Garantie!
Weil es keine Garantie gibt, bringen auch Verhandlungen über die Höhe des Lösegeldes wenig. Allerdings wurden diese Verhandlungen im vorliegenden Fall bewusst eingesetzt, um Zeit zu gewinnen und die Ransomware-Attacke zu analysieren. Dadurch konnte ermittelt werden, dass es sich um einen Angriff mittels LockBit 2.0 handelte. Solche Informationen sind wichtig, da sie helfen, das Ausmaß des Schadens und damit seinen Beseitigungsaufwand abzuschätzen.
Der zweite Schritt ist die Installierung von Datensicherungen in kurzen Intervallen zur Vorbeugung.

Beurteilung durch Markel
Die Schätzung der Spezialisten von BeforeCrypt ergab, dass eine Datenwiederherstellung Mittel in Höhe von EUR 14.000,00 erfordern würde. Letztlich entschied sich der Versicherungsnehmer, die verlorenen Daten erneut manuell einzugeben.
In diesem Zusammenhang können dem Versicherungsnehmer Kosten, welche infolge von Überstunden – und in weiterer Folge zu Mehrarbeit führten – der eingesetzten Mitarbeiter zur manuellen Datenwiederherstellung entstehen, übernommen werden. Gemeinsam mit dem Versicherungsnehmer wurde zeitnah eine Einigung erzielt, welche die Erstattung eines Schätzbetrages vorsah.

Welche Kosten wurden übernommen?
Unter Bezug auf Ziffer A.1, A.2 und A.3 liegt bei Ransomware-Angriffen ein versicherter Schadenfall vor.
Markel erstattete die Kosten für die eingetretene Betriebsunterbrechung i.H.v. EUR 2.500,00, die Kosten für die Datenwiederherstellung i.H.v. EUR 14.000,00 sowie Kosten zur Systemwiederherstellung i.H.v. EUR 7.000,00.