Bild: Pixabay

Ransomware soll 2017 über fünf Milliarden US-Dollar an Schäden verursacht haben.

Cyber-Krisenmanagement bei Ransomware

Vorbereitet sein

Pascal Michel

Ransomware-Attacken haben ein Kennzeichen: Dateien werden verschlüsselt oder IT-Systeme sind nicht mehr zugänglich, und Erpresser fordern ein Lösegeld, um die Entschlüsselung oder den erneuten Zugriff zu ermöglichen. Für die betroffenen Unternehmen stellen sich nicht nur hinsichtlich der IT-Systeme viele Fragen, sondern auch zum übergeordneten Krisenmanagement.

Im Jahr 2017 lag die durchschnittliche Lösegeldforderung bei Ransomware-Attacken bei 1.077 US-Dollar. Der Autor erlebte 2018 auch Fälle von Ransomware-Angriffen, in denen sechsstellige Dollar-Summen in Kryptowährungen gefordert wurden. Eine der höchsten Lösegeldforderungen war aber laut Medienberichten gegen die südkoreanische Web Hosting Firma Nayama gerichtet – umgerechnet 4,4 Millionen US-Dollar. Gezahlt wurde anscheinend eine Million US-Dollar in Bitcoins.

Meistens übersteigen die Kosten für das Fallmanagement und die Wiederherstellung der IT die Lösegeldforderung um ein Vielfaches. Die Stadt Atlanta zahlte in einem Fall 2,6 Millionen US-Dollar für das Fallmanagement und die Wiederherstellung der IT – die Lösegeldforderungen entsprach 52.000 US-Dollar. Alleine 2017 soll Ransomware über fünf Milliarden US-Dollar an Schäden verursacht haben, was eine 15-fache Steigerung gegenüber zwei Jahren zuvor bedeutet. Für 2019 werden die Schäden auf bis zu elf Milliarden US-Dollar prognostiziert.

Der Krisenstab bei Cyberfällen

Es überrascht, dass einige Unternehmen für Cyberkrisenfälle einen anderen, sehr technisch ausgerichteten Krisenstab vorhalten als bei klassischen Krisen. Oder das IT-Incident-Response-Team wird mit dem Krisenmanagement beauftragt. Dies mag dem Umstand geschuldet sein, dass beim Fallmanagement der Fokus zu sehr auf IT gerichtet wird. Oftmals mit fatalen Auswirkungen. Wenn ein Cybervorfall eine wirkliche Krise für das Unternehmen darstellt, so muss dies in die Zuständigkeit des strategisch handelnden Krisenstabes fallen. Hier werden unternehmensrelevante Entscheidungen getroffen. Das IT-Incident-Response-Team handelt auf der operativ-taktischen Notfallmanagementebene. Es hat eine wichtige Funktion, ist aber nur eines von mehreren Elementen, die bei einer Cybererpressung eine besondere Rolle spielen.

Die Rolle des Krisenberaters

Der externe Krisenberater wird häufig im Zusammenhang mit der Cyberversicherung des betroffenen Unternehmens hinzugezogen. Viele Firmen verfügen neben Cyberversicherungen über Versicherungen

für Entführungs- und Erpressungsfälle, die auch Cybererpressungen mit abdecken. Mit der Police hat der Versicherungsnehmer in der Regel auch Anspruch auf IT-Forensiker, Rechtsberatung und Krisen-PR.

Der Krisenberater ist kein Spezialist für IT-Sicherheit, sondern er bringt seine Erfahrung in der Krisenreaktion und -bewältigung, auch aus früheren Cyberfällen, ein. Denn um Krisenbewältigung geht es auf der strategischen Ebene des Krisenstabes. Der Krisenberater hilft somit, das anfängliche Chaos im Krisenstab zu ordnen, zeigt Handlungsoptionen und mögliche Fallstricke auf. Für die Kommunikation mit dem Erpresser entwickelt er die Verhandlungsstrategie und -taktik. Der Krisenberater unterstützt beim Entscheidungsfindungsprozess des Krisenstabes, ohne dabei unternehmerische Kompetenzen anzutasten.

Die Krisenstabsarbeit

Ein wesentliches Element der Krisenstabsarbeit ist zu Beginn die Lagebilderstellung und Bewertung. Es geht hier um Fragestellungen wie: Was ist passiert, welche Systeme, Netzwerke und Daten wurden kompromittiert? Welche Auswirkung auf die betriebliche Kontinuität ist jetzt schon absehbar? Wie hoch sind die Lösegeldforderungen? Womit droht der Täter, wenn die Zahlungsfirst verstreicht? Sind Sicherheitskopien der Daten vorhanden und verwendbar? Welche Rechtsprobleme stellen sich?

In der Anfangsphase ist auch eine „Stakeholderanalyse“ durchzuführen, die interne und externe Akteure nach Wichtigkeit, „Freund oder Gegner“ unterteilt und priorisiert. Entscheidend ist auch, welche Informationen wann und in welcher Form an die einzelnen Akteure übermittelt werden. Dann geht es vor allem um die Fragen der betrieblichen Kontinuität und rechtlichen Vorgaben. Die Dokumentation der Krisenstabsarbeit sowie die Beobachtung von Medien und sozialen Netzwerke sollten mit Aktivierung des Krisenstabes beginnen. Je nach Fallausprägung kann später auch eine Beobachtung im Darknet erforderlich sein. Wichtige Schnittstellen zur IT-Administration, zu den IT-Forensikern sowie Behörden sind zu bilden. Bei Cyberfällen ist juristische Expertise frühzeitig hinzuzuziehen.

Die Fehler, die man als Krisenberater in Cyberfällen beobachtet, sind oftmals die gleichen wie in klassischen Krisen: Im Rahmen der operativen Hektik werden Entscheidungen getroffen, bevor die Lage wirklich umfassend bewertet wurde. Dadurch wird beispielsweise zu früh oder zu spät nach außen kommuniziert oder ohne festgelegte Strategie vorschnell dem Erpresser geantwortet. Rechtliche Vorgaben werden übersehen, es wird zu wenig zur Lage und den Maßnahmen visualisiert und es bleibt lange unklar, wer für welche Maßnahmen verantwortlich ist und was prioritär ist.

Die Krisenkommunikation

Während ein Datendiebstahl für die Belegschaft in der Regel nicht offensichtlich ist, ist eine Ransomware-Attacke intern schnell erkennbar. Hier muss die Kommunikation mit der Belegschaft zeitnah einsetzen. Externe Akteure wie Medien, Kunden, Lieferanten und Aufsichtsbehörden sind auch zu berücksichtigen. Bei einer Ransomware-Attacke auf ein modernes Krankenhaus wunderten sich die Patienten, dass nun wieder mit Papier und Stift gearbeitet wurde und die Belegschaft sehr gestresst wirkte. Eine frühzeitige Kommunikation hätte hier einige Folgeprobleme abgefedert.

Erschwert wird die Krisenkommunikation häufig durch den Ausfall der IT, so dass eine rasche, zeitgleiche Kommunikation mit vielen Akteuren schwierig wird. In einem Fall, als Medien auf einen Ransomware-Angriff aufmerksam wurden, riefen innerhalb weniger Stunden über 30 Journalisten beim Unternehmen an. Das Ausmaß der Krisenkommunikation sollte mithin nicht unterschätzt werden.

Zahlen oder nicht?

Erpresser sind treue Kunden. Dies gilt auch in der Cyberwelt. Wie bei einer Entführung, in der es keine Garantie gibt, dass die Täter nach Erhalt des Lösegeldes das Opfer freilassen, besteht auch bei Cybererpressungen nicht die Sicherheit, dass Täter die Entschlüsselung ermöglichen. Laut Kaspersky, einem Unternehmen für Sicherheitssoftware, haben 20 Prozent der Firmen, die Lösegeld zahlten, ihre Daten nicht entschlüsseln können. „Cyber Threat Intelligence“ kann helfen, Informationen zu den Tätern und deren „Vertrauenswürdigkeit“ zu sammeln.

Behörden empfehlen häufig, nicht zu zahlen. Was aber, wenn kein verwendbares Backup vorhanden ist, es noch keinen frei verfügbaren Entschlüsselungscode gibt und jeder Tag, an dem die IT nicht genutzt werden kann, hohe Kosten verursacht? Im Falle eines Krankenhauses in Los Angeles verursachte alleine der Ausfall der Computertomographie pro Tag einen Verlust von über 100.000 US-Dollar. Eine Entscheidung für oder gegen eine Lösegeldzahlung hängt von vielen Faktoren ab und kann nicht pauschal beantwortet werden.

Die Verhandlung mit dem Täter

Die Verhandlung mit dem Erpresser verfolgt mehrere Ziele. Zum einen soll oft Zeit gewonnen werden, da die forensischen Untersuchungen nicht sofort Ergebnisse liefern, diese aber für Entscheidungen im Krisenstab wichtig sind. Auch die Wiederherstellung der IT dauert. Entschließt man sich zu zahlen, dann geht es auch darum, in der Zukunft kein attraktives Ziel für Erpresser zu sein.

Wer zahlen muss, sollte verhandeln. In einem Fall, in dem der Autor tätig war, hatte das betroffene Unternehmen vor Konsultation des Krisenberaters dem Erpresser geantwortet, dass man zahle, da man kein verwendbares Backup habe. Dennoch konnte anschließend, durch eine entsprechende Verhandlungsstrategie, die Summe um ein Drittel heruntergehandelt werden. Aber nicht in allen Ransomware-Fällen gibt es die Möglichkeit der Kommunikation mit dem Erpresser.

Die Unsicherheit bleibt

Auch wenn die Täter die Entschlüsselung ermöglichen, sollte das Entschlüsselungstool vor der Anwendung von IT-Forensikern überprüft werden. Selbst bei einem verwendbaren Backup nimmt der Wiederherstellungsprozess einige Zeit in Anspruch.

Gerade bei kleineren Unternehmen erlebt man es immer wieder, dass auf eine saubere Datenanalyse und Untersuchung verzichtet wird, nachdem die Daten wieder entschlüsselt wurden. Dies kann ein fataler Fehler sein. Man sollte wissen, wie es überhaupt zu dem Vorfall kam und ob die IT nun frei von Schadsoftware ist.

Pascal Michel, Geschäftsführer der SmartRiskSolutions GmbH, www.smartrisksolutions.de