Weg des geringsten Widerstands gesucht und gefunden

Ein Funk Kunde machte 2018 eine unangenehme Erfahrung mit Cyber-Kriminellen. Die Anatomie eines zielgerichteten Cyber-Angriffs.

Der Sommer 2018 ging als Anomalie in die europäische Wetteraufzeichnung ein. Einem etablierten, mittelständischen Unternehmen in der deutschsprachigen Schweiz wird diese Phase des Jahres nicht nur aufgrund der andauernden überdurchschnittlichen Temperaturen in Erinnerung bleiben, denn die zweite Anomalie trat in den IT-Systemen des besagten Unternehmens auf. Ein zielgerichteter Cyber-Angriff führte zu einem Umdenken der Führungskräfte und zur nachhaltigen Umstellung der IT-Sicherheitsorganisation.

An einem Mittwoch im Juli 2018 fiel dem IT-Support eine Unregelmässigkeit in der Auslastung der Server auf. «Wir stellten eine deutliche Zunahme von Aktivitäten auf unseren Servern fest, was jedoch keine Auswirkungen auf Verfügbarkeit der IT-Systeme hatte» so der CFO des betroffenen Unternehmens. Stunden später fiel der Mail-Server kurzfristig aus. Auch dann erwartete niemand das Schlimmste. Am Donnerstagmorgen kam jedoch das böse Erwachen. «Der IT-Support musste feststellen, dass die Dateien auf 17 der insgesamt 22 Server vollständig verschlüsselt waren» erinnert sich der CFO. Der Angriff war besonders heimtückisch, denn neben den Core-Applikationen wurden teilweise auch die Dateien der Backup-Applikationen verschlüsselt. Dies verunmöglichte eine sofortige Wiederherstellung der Daten. In den verschlüsselten Dateien war die Forderung der Cyber-Kriminellen enthalten. Das Unternehmen sollte 24 Bitcoins für die Entschlüsselung der Daten und damit für die sofortige Fortführung der Geschäftstätigkeiten bezahlen.

Angriff war kein Zufall

Drei Indizien deuteten auf einen zielgerichteten und von langer Hand geplanten Cyber-Angriff hin. Erstens begann dieser just dann, als sich der IT-Leiter in den Sommerferien befand. Zweitens sollte das Datensicherungskonzept nach der Ferienabwesenheit des IT-Leiters vollständig überarbeitet werden. Drittens wurden die Konfigurationen der Backups so verändert, dass die Spezialisten im Nachgang nur eine unvollständige Datensicherung vorfanden.

Das Führungsteam war am Anfang davon überzeugt, kein Lösegeld zu bezahlen und meldete den Vorfall den zuständigen Behörden. Währenddessen wurde die Krisenorganisation hochgefahren. Ein IT-Service- sowie ein IT-Security-Provider spannten mit dem Unternehmen zusammen und bildeten einen Krisenstab. Der IT-Security-Provider startete seine Arbeiten am Freitag und isolierte zuerst das Unternehmensnetzwerk von der Aussenwelt, um allfällige Datenabflüsse zu unterbinden.

Kommunikation im Fokus

Inzwischen begannen die Aufräumarbeiten. Am Wochenende wurden alle Laptops und Clients mit einem DeepScan überprüft und von jeglichen Schadprogrammen bereinigt. Um die vitalen Kommunikationsfunktionen wiederherzustellen, wurde bis Montag ein Notserver beschafft und konfiguriert. Nun konnte das Unternehmen zumindest wieder in gewohnter Art mit seinen Kunden kommunizieren. Der Datenserver konnte ebenfalls wieder zur Verfügung gestellt werden. Demgegenüber lief die Produktion langsam leer, da die Arbeitsvorbereitung nur mittels spezifischer Applikationen erfolgen konnte. Der CFO erinnert sich an die neuen Herausforderungen: «Die Anspannung war auch bei unseren Mitarbeitenden zu spüren, die während dieser Phase ihre Gleitzeiten abbauten. Während der Sommerzeit waren zudem viele Mitarbeiter in den Ferien. Da auch die Lohnzahlung in der besagten Woche anstand, vereinbarten wir mit unserer Geschäftsbank, die gleichen Zahlungen zu veranlassen wie im vergangenen Monat. Die interne und externe Kommunikation war zudem besonders wichtig, um Mitarbeitenden und Kunden Sicherheit zu vermitteln.»

«Als die ernüchternde Erkenntnis vorlag, dass unsere Backups teilweise nicht verwendbar waren und der IT-Security Provider auch keine passende Decryptor-Software finden konnte, mussten wir umdenken» beschreibt die Führungskraft die unbequeme Ausgangslage. Die Rekonstruktion hätte zu viel Zeit in Anspruch genommen und die Reputation hätte Schaden genommen. Der Krisenstab kam zu der Entscheidung, einen spezialisierten amerikanischen Unterhändler für die Verhandlungen mit den Cyber-Erpressern zu mandatieren.

Nachdem die Formalitäten mit dem Unterhändler geregelt waren und eine Anzahlung für das Lösegeld und die Verhandlungskosten geleistet wurde, nahm dieser am Freitag die Verhandlungen mit den Cyber-Kriminellen im DarkNet auf. Tatsächlich gelang es dem Unterhändler, das Lösegeld von 24 auf 12 Bitcoins zu reduzieren und am Montag in den Besitz des Schlüssels zu gelangen. Für die rasche Entschlüsselung wurde Tag und Nacht gearbeitet, trotzdem nahm dies zusätzliche 48 Stunden in Anspruch, sodass die Geschäftstätigkeit erst am Donnerstag wieder vollständig hergestellt wurde.

Es kann jeden treffen

«Rückblickend betrachtet haben wir bei den IT-Sicherheitsmassnahmen zu stark auf die klassischen Methoden vertraut. Das Ausmass einer professionellen Attacke konnten wir nicht abschätzen. «Die 'busines first'-Einstellung» führte zu einer offenen IT-Architektur und machte es den Angreifern zu einfach, unsere IT-Systeme zu kompromittieren. Wir sind stets davon ausgegangen, dass unser Unternehmen zu uninteressant für Cyber-Kriminelle ist. Doch die Angreifer achten nicht auf die Attraktivität des Ziels. Im Gegenteil, sie suchen sich den Weg des geringsten Widerstandes. Ich bin überzeugt, dass 99 von 100 Unternehmen die Möglichkeiten von Hackern unterschätzen. Der Vorfall hat uns die Augen geöffnet, seitdem ist IT-Security mindestens genauso wichtig wie das Tagesgeschäft.»

Der zweiwöchige Ausfall der IT-Systeme kostete das Unternehmen umgerechnet rund 400'000 Schweizer Franken. Neben den rund 10'000 verlorenen produktiven Stunden, dem Lösegeld, den Beratungskosten und den Kosten für den Notserver, investierte das Unternehmen im Nachgang rund 200'000 Schweizer Franken in ein Security Operation Center (SOC) und weitere IT-Security-Massnahmen. Glück im Unglück hatte das Unternehmen im Nachhinein dann trotzdem noch, denn das Lösegeld und die Beratungskosten der involvierten Parteien waren im Rahmen einer Kidnap & Ransom-Versicherung abgedeckt.

Kontakt: Max Keller
E-Mail: max.keller@funk-gruppe.ch
Telefon: +41 58 311 05 51