DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Zahlen oder nicht zahlen?
Eine Kosten-Nutzen-Analyse für Ransomware-Lösegelder

Während Ransomware weiter rund um den Globus für Aufregung sorgt, beginnen Unternehmen langsam, ihre Sicherheitsmaßnahmen zum Schutz vor Ransomware zu verschärfen.

Es gibt nur leider ein Problem: Kein System der Welt bietet 100-prozentigen Schutz.

Wenn Sie also doch einmal Opfer von Ransomware werden, müssen Sie eine schwere Entscheidung treffen: **Sollen Sie das Lösegeld bezahlen?**

Allgemein wird empfohlen, niemals zu zahlen.

Aber das wahre Leben ist nun einmal nicht schwarz und weiß. Einige Unternehmen haben weder die Ressourcen noch das Fachwissen, um einen zuverlässigen Wiederherstellungsplan zu entwickeln, umzusetzen und kontinuierlich zu pflegen. In anderen Fällen sind auch die Sicherungen selbst befallen. Mitunter sind die Auswirkungen einer Ransomware sogar so zerstörerisch, dass das gesamte Unternehmen stillgelegt wird. In diesen Fällen kann sich das Bezahlen des Lösegeldes im Gegensatz zu den Kosten einer manuellen Systemreparatur durchaus lohnen.

In diesem Artikel werfen wir einen Blick auf die tatsächlichen Kosten einer Ransomware und ergründen die Vor- und Nachteile einer Lösegeldzahlung.

Wissen Sie, wie viel eine Ransomware Ihr Unternehmen kosten kann?

Bei der Entscheidung, ob das Lösegeld bezahlt werden soll oder nicht, gibt es einen wichtigen Aspekt zu bedenken: Wie hoch wird der finanzielle Schaden – direkt oder indirekt – durch den Angriff für Ihr Unternehmen ausfallen?

Auf den ersten Blick erscheint ein vier- oder fünfstelliges Lösegeld teuer. Doch dieser Betrag kann sich angesichts der Kosten, die Ihnen durch Ausfallszeiten, verlorengegangene Produktivität und Wiederherstellung entstehen können, als das kleinere Übel erweisen.

Bestes Beispiel hierfür ist ein 2018 erfolgter Ransomware-Angriff auf Atlanta im US-Bundesstaat Georgia, der die öffentlichen Dienste der Stadt wochenlang stilllegte. Die Cyberkriminellen hatten ein Bitcoin-Lösegeld im Wert von 51 000 USD zur Wiederherstellung der verschlüsselten Dateien gefordert … und die Stadt hatte sich geweigert. Dieser an sich noble Akt ließ den Schaden letztendlich jedoch auf insgesamt 17 Millionen USD ansteigen. Das ist das über 300-Fache des ursprünglichen Lösegeldes.

Falls Ihr Unternehmen also Opfer einer Ransomware wird, sollten Sie sorgfältig überprüfen, welche Kosten der Zwischenfall und die finanziellen Rückwirkungen im Verlauf der folgenden Wochen und Monate verursachen werden.

Während des Angriffs

Ausfallzeiten

Die von Ransomware verursachten Störungen führen häufig auch zu verpassten Geschäftsmöglichkeiten, die sich erheblich auf die Einnahmen auswirken können. Laut einer Umfrage von Datto unter mehr als 2 400 MSP entstehen einem Unternehmen durch Ransomware durchschnittlich 46 800 USD Schaden. Wie hoch wären Ihre Verluste pro Stunde, pro Tag, pro Woche … bei einem Angriff?

Personalkosten

Auch die Produktivität kann stark abnehmen, wenn Mitarbeiter aufgrund eines Angriffs nur noch eingeschränkt arbeiten können. Darüber hinaus wird höchstwahrscheinlich auch angestelltes IT- und Sicherheitspersonal seinen eigentlichen Pflichten nicht mehr nachkommen können, da es mit der Wiederherstellung befallener Systeme beschäftigt ist. Das wiederum kann andere Ergebnisse beeinträchtigen und folglich zu weiteren finanziellen Folgen im Geschäftsablauf führen.

Externe Auftragnehmer

Zum Wiederherstellen Ihrer Daten müssen Sie möglicherweise entsprechende Spezialisten beauftragen. Deren Gebühren sind stark von der Größe Ihres Unternehmens sowie dem Umfang und der Komplexität des Angriffs abhängig, was sich schnell bis in den sechsstelligen Bereich hochschaukeln kann.

Nach dem Angriff

Tatsächliches Lösegeld

Dabei handelt es sich um den Geldbetrag, den Sie den Hackern – meistens in Form einer Kryptowährung – zur Entschlüsselung Ihrer Dateien zahlen. Die Höhe des Lösegeldes hängt vom Angriff ab. Zahlen von Coveware zufolge belief sich das im ersten Quartal 2019 durchschnittlich von Unternehmen bezahlte Lösegeld auf 12 762 USD.

Rechtliche Kosten und Strafen

In einigen Fällen gilt ein Ransomware-Angriff auch als Datenschutzverletzung, wobei das allerdings rechtlich noch eine Grauzone ist. Sollte Ihrem Unternehmen also hinsichtlich seiner Cybersicherheit oder der Art, wie es Daten absichert, Fahrlässigkeit vorgeworfen werden, muss es eventuell mit saftigen Anwaltsgebühren rechnen. Über 41 Prozent der Führungskräfte berichten, dass Kunden nach einer Datenschutzverletzung in ihren Unternehmen rechtliche Schritte ergriffen, wie Radware berichtet. Sie könnten im Rahmen der HIPAA- und DSGVO-Bestimmungen auch zur Entrichtung von Bußgeldern und Geldstrafen herangezogen werden.

Rufschädigung

Wenig überraschen dürfte außerdem, dass ein Ransomware-Angriff den Ruf eines Unternehmens enorm schädigen kann, wenn der Zwischenfall öffentlich bekannt wird, was

wiederum die Verkaufszahlen ruinieren kann. In einer im Auftrag von Gemalto durchgeführten Umfrage unter 10 000 Verbrauchern gaben 70 Prozent an, nicht weiter bei einem Unternehmen einzukaufen, wenn es in diesem eine Datenschutzverletzung gab.

Höhere Versicherungsprämien

Cyberversicherungen sind in den vergangen Jahren bei Unternehmen, die nach Möglichkeiten suchen, um sich vor Ransomware und anderen digitalen Bedrohungen zu schützen, immer beliebter geworden. Es ist allerdings immer noch stark umstritten, ob Versicherungsunternehmen tatsächlich für Ransomware-Angriffe schadensersatzpflichtig sind. Werden Sie Opfer eines Angriffs und machen einen Anspruch geltend, sollten Sie auch beachten, wie sehr sich Ihre Prämien erhöhen würden.

Neues IT-Budget

Für viele Unternehmen ist ein Ransomware-Angriff auch ein Weckruf, um die IT-Infrastruktur auszubauen. Wenn Ihr Unternehmen noch mit veralteter Hardware arbeitet, sollten Sie Ihr IT-Budget überprüfen und berechnen, wie viel es Ihr Unternehmen kosten würde, alle Systeme gemäß aktuell bewährter Verfahren nachzurüsten.

Zahlen oder nicht zahlen, das ist die Frage

Für die meisten Geschäftseigentümer besteht die Priorität darin, die Daten wiederherzustellen, die Kosten zu minimieren und so schnell wie möglich wieder zum üblichen Geschäftsalltag zurückzukehren. Wenn Sie überschlagen haben, wie viel der Ransomware-Angriff Sie kosten würde, könnten Sie dazu neigen, den Forderungen nachzugeben und das Lösegeld schnellstmöglich zu bezahlen.

Aber übereilen Sie nichts. Die schwierige Entscheidung, ob das Lösegeld bezahlt werden soll oder nicht, darf keinesfalls auf die leichte Schulter genommen werden.

Hier einige Punkte, die Sie bedenken sollten:

Vorteile der Lösegeldzahlung

Störung minimieren

Egal, in welchem Industriebereich Ihr Unternehmen tätig ist, Ransomware kann Ihren Geschäftsalltag maßgeblich beeinträchtigen und zu erheblichen finanziellen Verlusten führen. Viele Unternehmen sind daher bereit, einen relativ kleinen Betrag zu zahlen, um das Problem schnell aus der Welt zu schaffen und ihren Betrieb wieder zum Laufen zu bringen.

Könnte sich als günstiger erweisen

Die größten Kosten, die eine Ransomware verursacht, sind die damit einhergehenden Ausfallzeiten. Datto beziffert die durchschnittlichen Kosten für Ausfallzeiten auf das Zehnfache des durchschnittlich geforderten Lösegeldes. Das Lösegeld zu bezahlen und die Dateien schnell wieder zu entschlüsseln, kann sich also durchaus als günstiger erweisen, als die Systeme zeitaufwendig aus Sicherungen wiederherzustellen.

Versicherung zur Kostendeckung

Wie bereits erwähnt gibt es einige bekannte Fälle, in denen Versicherungsunternehmen sich weigerten, für Schäden durch Ransomware aufzukommen. Sollten Sie jedoch in eine gute Cyber-Haftpflichtversicherung investiert haben, stehen die Chancen gut, dass diese zumindest einen Teil der Lösegeldkosten erstattet.

Nachteile der Lösegeldzahlung

Keine Garantie für den Erhalt eines Decrypters

Sicher liegt es generell im besten Interesse der Hacker, ihren Teil der Abmachung einzuhalten. Schließlich sind Opfer eher bereit nachzugeben, wenn sie wissen, dass sie ihre Dateien nach der Zahlung wiederbekommen. Doch wir sprechen immer noch über Kriminelle, die unmoralisch und gesetzeswidrig handeln. Es gibt also keinerlei Garantie, ob Sie nach der Lösegeldzahlung das Entschlüsselungstool auch tatsächlich erhalten.

Decrypter könnte nicht funktionieren

Selbst wenn die Cyberkriminellen ihr Wort halten und Ihnen einen Decrypter zum Entschlüsseln schicken, besteht immer noch die Gefahr, dass das Tool nicht funktioniert. Nicht einmal die Hälfte der 38,7 Prozent, die sich für die Zahlung entscheiden, kann mit den von den Hackern bereitgestellten Tools seine Dateien wiederherstellen, wie eine Studie der CyberEdge Group ergab.

Erneuter Angriff

Falls Ihr Unternehmen sich also entscheiden sollte, das Lösegeld zu bezahlen, könnte es in der Zukunft wiederholt zu Angriffen kommen, da die Kriminellen nun wissen, dass Sie ein lohnendes Opfer sind.

Ethischer Konflikt

Eine Lösegeldzahlung hat auch ethische Auswirkungen. Viele Strafverfolgungsbehörden sind überzeugt, dass eine Zahlung nur weitere Angriffe provoziert, da sich die Ransomware als lukrativ erwiesen hat. Indem Sie zahlen, würden Sie also den ganzen Ransomware-Kreislauf nur noch unterstützen.

Darüber hinaus sind viele Cyberbanden auch in andere kriminelle Machenschaften verwickelt. Durch Ihre Lösegeldzahlung könnten Sie also indirekt schwere Verbrechen finanzieren, wie Drogenproduktion oder Menschenhandel.

Sollten Sie bezahlen?

Auf diese Frage gibt es keine eindeutige Antwort. Es hängt alles von der jeweiligen Situation ab.

Die meisten Strafverfolgungsbehörden raten daher dringend davon ab, mit den Cyberkriminellen zusammenzuarbeiten, und empfehlen eine Lösegeldzahlung nur, wenn Sie

wirklich alle anderen Optionen ausgeschöpft haben. Das FBI dazu (übersetzt aus dem Englischen):

„Vor der Zahlung eines Lösegeldes gilt es, schwerwiegende Risiken zu bedenken. [Die Regierung der USA] unterstützt keine Lösegeldzahlungen an kriminelle Akteure. Nachdem jedoch Systeme kompromittiert wurden, ist eine Lösegeldzahlung eine ernsthafte Entscheidung, bei der alle Optionen zum Schutz der Anteilseigner, Arbeitskräfte und Kunden gegeneinander abgewogen werden müssen."

Das bedeutet nicht zwangsläufig, dass Sie niemals das Lösegeld zahlen sollten. Es zeigt jedoch, wie wichtig eine Kosten-Nutzen-Analyse ist, bevor Sie eine Entscheidung treffen.

Eine Lösegeldzahlung könnte sinnvoll sein, wenn:

- Sie Ihre Systeme nicht aus Sicherungen wiederherstellen können.
- Sie Ihre Dateien nicht mit einem kostenlosen Ransomware-Decrypter entschlüsseln können.
- die verschlüsselten Daten absolut unerlässlich sind.
- die Ausfallzeiten Ihr Geschäft, Ihre Kunden und Ihre Anteilseigner stark beeinträchtigen.

Als allgemeine Faustregel gilt, dass Sie ein Lösegeld nur bezahlen sollten, wenn es absolut keine andere Möglichkeit gibt und Sie die Daten auf keinen Fall verlieren dürfen.

Firmen zur Ransomware-Entschlüsselung

Ob Sie sich nun für oder gegen eine Zahlung entscheiden, vielleicht haben Sie auch schon darüber nachgedacht, einen Dienstleister zur Ransomware-Entschlüsselung zu beauftragen. Es gibt eine Reihe von Unternehmen, die versprechen, die Ransomware zu beseitigen und beim Wiederherstellen der verschlüsselten Dateien zu helfen.

Hierbei muss angemerkt werden, dass diese Unternehmen auch keine magischen Entschlüsselungsverfahren zu bieten haben. Meistens bezahlen sie lediglich das Lösegeld an die Angreifer, um das Wiederherstellungstool zu erhalten. Daran ist an sich nichts Verwerfliches. Wiederherstellungsdienste haben das Fachwissen, um eine reibungslose Überweisung sicherzustellen und möglicherweise sogar für Sie ein niedrigeres Lösegeld auszuhandeln. Leider sind jedoch nicht alle Firmen zur Ransomware-Entschlüsselung transparent bezüglich ihrer Verfahren, was verständlicherweise Misstrauen und Argwohn fördert.

Haben Sie vor, einen derartigen Anbieter zu nutzen, empfehlen wir ein vertrauenswürdiges Unternehmen wie Coveware. Coveware ist transparent bezüglich seiner Dienstleistungen und verfügt über eine hervorragende Erfolgsbilanz bei der Unterstützung von Ransomware-Opfern. Die Experten im Emsisoft-Labor arbeiten eng mit Coveware zusammen, um maßgeschneiderte Lösungen für bestimmte Ransomware-Versionen zu entwickeln.

Jeder Fall ist anders

Kein Ransomware-Zwischenfall ist wie der andere. Daher ist es auch unmöglich zu sagen, ob Ihr Unternehmen das Lösegeld zahlen sollte oder nicht. Es ist sicher verlockend, das Problem durch die Zahlung schnell zu beheben. Allerdings muss immer bedacht werden, dass es keinerlei Garantie gibt, ob die Kriminellen auch ihren Teil der Abmachung einhalten oder der Decrypter funktioniert.

Indem Sie die wahren Kosten der Ransomware berechnen und eine gründliche Kosten-Nutzen-Analyse durchführen, können Sie eine informierte Entscheidung treffen, ob Sie das Lösegeld zahlen oder nicht.

Quelle: https://blog.emsisoft.com/de/33791/zahlen-oder-nicht-zahlen-eine-kosten-nutzen-analyse-fuer-ransomware-loesegelder/?ref=ticker190820