CODE42

Das Ransomware-Geschäft:

Was jeder CXO wissen sollte

Die wahren Ransomware-Kosten
Hohe Lösegeldforderungen machen Schlagzeilen, doch die wahren Kosten und Belastungen durch Ransomware kommen von der Wiederherstellung und Sanierung, und sie fallen auch dann an, wenn ein Unternehmen das Lösegeld zahlt.

64%

der Unternehmen setzen eine Woche für die Behebung der Folgen einer Ransomware-Attacke an.

3 Tage

Die Produktivitätsverluste reichen pro Anwender von neun Stunden bis zu 3 Tagen.

1/3

Jede dritte Firma verliert Umsatz.

1,5 Mio $

Reporting-Kosten und Geldstrafen variieren je nach Branche. In den USA müssen Firmen im Gesundheitswesen bis zu 1,5 Mio Dollar für die Verletzung von HIPAA-Vorschriften zahlen.

Sie haben 72 Stunden Zeit, zwei Bitcoins an die Adresse unten zu senden. Sonst werden Ihre Daten gelöscht. Keine Polizei.

Wenn Sie diese Nachricht schon einmal gesehen haben, kennen Sie die Angst. Und wenn nicht, dann wahrscheinlich bald. Im letzten Jahr hat Ransomware weltweit bei 40 Prozent aller Firmen zugeschlagen und Millionenverluste an Produktivität und Daten verursacht – zusätzlich zum Lösegeld. Außerdem wird die Taktik der Ransomware-Angriffe immer gezielter und ausgefeilter, sodass diese Zahlen in den kommenden Jahren noch steigen werden.

Und obwohl immer mehr Firmen auf die Ransomware-Epidemie aufmerksam werden, konzentriert sich ihre Reaktion weiterhin darauf, frontal gegen die Cyber-Kriminellen vorzugehen, anstatt darauf, ihre Unternehmensdaten zu schützen, um die es dabei geht. Ein Unternehmen kann und muss dafür sorgen, dass es nie den Zugang zu kritischen Daten verliert, nie einen Produktivitätsverlust erleidet oder die hohen Kosten einer langwierigen Wiederherstellungsaktion tragen muss und auch niemals Lösegeld zahlen muss. Dazu ist es erforderlich, die Sicherheit der Endgerätedaten eines Unternehmens zur Grundlage der Sicherheitsstrategie zu machen und vorrangig alle Endgerätedaten im Unternehmen zu sammeln und zu schützen.

Vom bösen Anfang zum großen Geschäft

Ransomware wurde 1989 geboren. Sie tarnte sich als AIDS-Schulungssoftware und wurde daher als „AIDS-Trojaner“ bekannt. Die Malware wurde ganz altmodisch auf Disketten per Post verteilt. Das – ebenfalls per Post versandte – Erpresserschreiben wies das Opfer an, den Drucker anzuschalten, und der spuckte dann eine Geldforderung von 189 Dollar aus. Nach der Zahlung erhielten die Opfer den Schlüssel zum Entschlüsseln der Daten – ebenfalls auf einer Diskette per Post. Nur wenige bemerkten, dass die scheinbar so harmlose AIDS-Diskette schuld war.

Seit dem einfachen „AIDS-Trojaner“ ist Ransomware zum großen Geschäft geworden: größere kriminelle Organisationen, höhere Lösegeldzahlungen und eine größere Reichweite der Malware.

Ransomware nimmt Fahrt auf

4,000
neue Angriffe jeden Tag. [1]

158%
monatlicher Zuwachs bei Angriffen. [2]

$1 Milliarde
Lösegeldeinnahmen prognostiziert. [2]

CODE42

40%

aller Unternehmen wurden im letzten Jahr von Ransomware angegriffen.[2]

68%

der Angriffe zielten auf das mittlere und obere Management.[2]

89%

aller Datenverluste im Unternehmen gehen auf interne Aktionen zurück.

93%

Verizon berichtet, dass inzwischen 93 % aller Phishing-E-Mails Ransomware enthalten. [3]

4%

Nur 4 % aller Firmen sind sich nach eigener Aussage sicher, einen Ransomware-Angriff stoppen zu können. [2]

Diese Faktoren unterstützen die Zunahme von Ransomware

Die Ransomware-Werkzeuge werden raffinierter: Von Malware, die unentdeckt unter dem Antivirus-Radar hindurchfliegt, bis zu brachialen Angriffen: Die Hacker werden immer besser. Bessere Verschlüsselung macht es den Opfern praktisch unmöglich, ihre Dateien zu entschlüsseln, ohne für den Schlüssel zu zahlen.

Ransomware-as-a-Service (RaaS) macht Ransomware auch für Unbedarfte einfach: RaaS nimmt auf dem schwarzen Markt zu und folgt damit dem Trend bei der legalen Software. Durch RaaS erreicht die Zugänglichkeit von Ransomware ein ganz neues Niveau. Technisch wenig versierte Menschen können Ransomware „mieten“ und dazu ihre eigenen Phishing-E-Mails entwerfen.

Bitcoin vereinfacht die Geldwäsche: Für einen Cyber-Kriminellen ist die direkte Interaktion mit dem Opfer, um dessen Zahlung zu erlangen, das Riskante an der Ransomware. Doch hat Bitcoin als legitime, gut organisierte digitale Währung seit seiner Einführung eine digitale Schicht der Anonymität zwischen Opfer und Erpresser entstehen lassen, die das Risiko weitgehend beseitigt. Zudem bietet das Dark Web in wachsender Zahl Optionen für die „Wäsche“ erpresster Bitcoins, um das Risiko für den Kriminellen weiter zu verringern.

Die Angriffe zielen auf Unternehmen: Anstatt mit einem typischen Phishing-Angriff ein weites Netz auszuwerfen, nehmen Cyber-Kriminelle zunehmend diejenigen ins Visier, die am ehesten zahlen. Firmen sind die idealen Ziele. Sie haben wertvolle Daten und können sich nicht leisten, diese zu verlieren, und sie haben viel mehr Bargeld zur Verfügung als individuelle Ziele. Datenerpresser beginnen sogar damit, ihre Lösegeldforderungen an das jeweilige Ziel anzupassen. Je mehr man zu verlieren hat, desto mehr soll man zahlen.

Der Blick auf den Verbrecher lenkt vom Verbrechen ab

Erpressung ist ein schweres, beschämendes Verbrechen. Daher überrascht es nicht, dass sowohl Führungskräfte als auch IT-Leiter ihre Zeit und Ressourcen gern für die direkte Bekämpfung von Cyber-Kriminellen opfern. Der ausschließliche Blick auf den Bedrohenden lenkt jedoch von der eigentlichen Bedrohung ab: den Zugang zu kritischen Daten zu verlieren. Das Ergebnis ist ein Teufelskreis, der die Ransomware-Epidemie nur anheizt.

Ungeschützte Daten beschleunigen den Teufelskreis Ransomware.

Eine verlorene Schlacht

1. **Unternehmen versuchen, Cyber-Kriminelle frontal anzugehen:** Angesichts der Zahl der Cyber-Kriminellen und der ausgedehnten Angriffsfläche ist Prävention unmöglich. Wichtiger noch: Präventive Antivirenprodukte können den wichtigsten und am häufigsten genutzten Eingangsweg für Ransomware nicht blockieren – die Mitarbeiter. Höhere Wälle und stärkere Schlösser können nichts ausrichten, wenn Ihre Angestellten willentlich oder unabsichtlich die Schlüssel aushändigen.

2. **Daten bleiben ohne Schutz:** Viele Unternehmen verwenden so viel Energie und Aufmerksamkeit dafür, an der Sicherheit ihrer Außenfront herumzubasteln, dass sie die Beute oft völlig ungeschützt lassen.

- Herkömmliches Server-Backup beruht auf manueller Sicherung von Endgerätedaten. Anwender halten sich unweigerlich nicht an die Regeln und lassen Endgerätedaten – das heißt mehr als die Hälfte der Unternehmensdaten – ungeschützt.
- Produkte für Enterprise File Sync and Share (EFSS) sind gut für die Zusammenarbeit, aber nicht fürs Backup.

3. **EFSS ist Anwender-orientiert und erfasst nur die Daten, welche die Anwender für die Zusammenarbeit teilen wollen.** Varianten mit automatischer Synchronisation können sogar Ransomware verbreiten, indem sie infizierte Dateien zur gemeinsamen Cloud synchronisieren und andere offenlegen.

4. **Unternehmen ohne umfassende Endgerätesicherheit entscheiden sich oft dafür, das Lösegeld zu zahlen:** Sobald einem Unternehmen klar wird, dass seine Daten nicht geschützt sind, steht es vor einer schweren Entscheidung: Das Lösegeld zahlen oder die Daten endgültig verlieren. Angesichts der kritischen, sensiblen Natur der typischerweise gestohlenen Daten sehen viele Unternehmen die Zahlung des Lösegelds als besten Weg an, den Schaden zu minimieren und den Geschäftsbetrieb wieder aufzunehmen.

5. **Wer Lösegeld zahlt, heizt den wachsenden Ransomware-Markt weiter an:** So lange Opfer weiterhin das Lösegeld zahlen, strömt Geld in den wachsenden schwarzen Ransomware-Markt und treibt die Verfeinerung der Angriffstaktiken voran. Es gibt bereits eine breite Palette von Hilfsdiensten, mit denen Datenerpresser ihre Angriffe starten und Zahlungen erlangen können. Über Ran$umBin, einer Art eBay für gestohlene Daten, können Hacker gestohlene Informationen an den Meistbietenden verkaufen. Mehr Geld, mehr Hacker, mehr Angriffe und höhere Lösegelder: Das sind die wahren Kosten, die durch das Zahlen von Lösegeldern erst entstehen.

Den Teufelskreis durchbrechen: Es geht um die Daten

Die Zahlen zu Ransomware – und der oben beschriebene Teufelskreis – malen ein trostloses Bild. Das Mittel gegen Ransomware ist aber eigentlich ganz einfach: Den Fokus wechseln: von denen, die Daten stehlen wollen, auf die Daten, die gestohlen werden sollen. Schließlich liegen die größten Risiken für ein Unternehmen in den Produktivitätsverlusten und hohen IT-Kosten langwieriger Wiederherstellungen und letztlich in dem Problem, wertvolle Daten endgültig zu verlieren. Ein Unternehmen sollte sich darauf konzentrieren sicherzustellen, dass alle Daten gesammelt und geschützt werden, und so eine schnelle, saubere Wiederherstellung nach einer Ransomware-Attacke ermöglichen. Damit wird die Malware erfolgreich bekämpft.

Ransomware entwaffnen

1. **Daten sammeln und schützen:** Zuverlässiger und umfassender Schutz von Unternehmensdaten bedeutet: eine Lösung, die Daten dort schützt, wo sie sich befinden – auf dem Endgerät. Die Lösung darf sich nicht auf das Benutzerverhalten verlassen und sie darf die Anwenderproduktivität nicht behindern, weil die Mitarbeiter sie dann umgehen. Modernes Sammeln von Endgerätedaten muss automatisch, kontinuierlich und reibungslos laufen. Das gibt der IT die Sicherheit, dass jeder Benutzer, jedes Gerät, jede Datei und jede Version abgedeckt ist.

2. **Keine Angst, wenn Ransomware zuschlägt:** Wenn Laptop- und Desktop-Daten kontinuierlich gesichert werden, verliert Ransomware ihren Schrecken. Unternehmen haben dann die Werkzeuge für eine effiziente, erfolgreiche Wiederherstellung an der Hand.

3. **Saubere, schnelle Wiederherstellung:** Der umfassende Schutz von Endgerätedaten macht die bisher teure, oft wochenlang dauernde Wiederherstellung zu einem schnellen Vorgang auf Knopfdruck. Anstatt verlorene Daten manuell zuzuordnen, nach verlorenen Dateien zu suchen und bei jedem Gerät eine Wiederherstellung jeder Datei einzeln durchzuführen, geht die IT zum letzten bekannten einwandfreien Zustand zurück, um Dateien pauschal wiederherzustellen. Sie kann auch die Wiederherstellung in Eigenregie erlauben und damit die Datenmigration an einem Tag oder weniger ermöglichen.

4. **Niemals an den Erpresser zahlen:** Wenn ein Unternehmen weiß, dass eine komplette, effiziente Wiederherstellung der Daten nur einen Tag dauert, kann es Lösegeldforderungen getrost ignorieren.

5. **Den Ransomware-Markt auslöschen:** Wenn die Werkzeuge zur Hand sind, um der Ransomware die Zähne zu ziehen, kann die Gemeinschaft der Unternehmen den Geldstrom abschneiden und damit beginnen, den Ransomware-Markt auszutrocknen.

1/2

so lange

Stellen Sie sicher, dass Ihre Anwender morgen (oder früher) wieder arbeiten können: Schnelle, garantierte Wiederherstellung bedeutet, dass Anwender Ihre Rechner und Daten nach einem Tag oder früher wiederbekommen, anstatt Tage oder sogar Wochen mit Leihgeräten und ohne ihre business-kritischen Daten zubringen zu müssen.

CODE42

Anwenderbericht: Sportartikelhändler verweigert Lösegeldzahlung und sorgt mit Endgeräte-Datenschutz für schnelle Wiederherstellung

Als Ransomware einen globalen Sportartikelhändler traf, verbreitete sie sich zu über 20 Anwendern und störte bereits einen Netzwerkserver, ehe der erste Anruf beim IT-Helpdesk landete. Zum Glück war bei der Firma eine robuste Lösung für Endgerätesicherheit vorhanden, die für die kontinuierliche, automatische Sicherung aller Endgerätedaten sorgte. „Ohne diese Lösung hätten wir im besten Fall ein Szenario vor uns, mindestens eine Woche lang jedes Gerät sorgfältig durchsuchen zu müssen und jede Datei einzeln wiederherzustellen“, erläuterte ein IT-Administrator. „Die IT-Kosten wären riesig gewesen, und für die Produktivität der Angestellten wäre es ein schwerer Schlag gewesen. Ehrlich gesagt, hätten wir uns ernsthaft überlegt, das Lösegeld zu zahlen.“ Durch das umfassende Sammeln und Schützen der Endgerätedaten hatte die IT die Gewissheit, dass alle betroffenen Daten gesichert waren. „Wir konnten bei Null anfangen und eine saubere Wiederherstellung vom Zustand unmittelbar vor dem Ransomware-Angriff durchführen.“ Die pauschale Wiederherstellung halbierte die Dauer der Datenmigration, und die Anwender konnten schon nach einem Tag statt erst nach einer Woche oder später weiterarbeiten. Diese nicht so erschreckende Erfahrung stärkte das Vertrauen des Händlers in seine Lösung zum Endgeräteschutz. „Ich tue alles, was ich kann, damit Ransomware uns nicht noch einmal trifft“, erklärte der IT-Administrator, „aber wenn sie es doch tut, sind wir nicht von unseren Daten abgeschnitten. Ich weiß, dass die Anwender dann nicht ohne ihre Geräte und Daten dastehen. Und ich weiß auch, dass wir das Lösegeld nicht zahlen werden.“

Sammeln und schützen bringt Sicherheit

Sie werden mit Statistiken, Schlagzeilen und persönlichen Erfahrungsberichten über die wachsende Bedrohung durch Ransomware bombardiert. Und doch: Kein Geschäftsführer, kein Leiter der Informationssicherheit und kein IT-Team will akzeptieren, dass Verletzungen der Datensicherheit unabwendbar sind. Stattdessen wenden viele Firmen Geld und Energie dafür auf, die wendigen Angreifer selbst zu bekämpfen, und lenken damit von der eigentlichen Bedrohung für das Unternehmen ab: dem Verlust kritischer Daten.

Die erfolgreichsten Firmen machen das Sammeln und Schützen der Daten zur Grundlage ihrer Sicherheitsstrategie, anstatt sich ausschließlich auf die Verteidigung ihrer Außenfront zu konzentrieren. Ein Unternehmen kann den ständigen Zugang zu seinen Daten garantieren, indem es eine moderne Lösung für Endgerätesicherheit einrichtet, die für den automatischen, kontinuierlichen und umfassenden Schutz aller Unternehmensdaten auf jedem Laptop und Desktop-Rechner sorgt. Ohne die Sorge, kritische Daten zu verlieren, ohne längere Ausfallzeiten befürchten zu müssen, ohne Produktivitätsverlust und hohe IT-Kosten und ohne die Hilflosigkeit beim Zahlen des Lösegelds können Unternehmen Ransomware wirksam entwaffnen und aus der bedrohlichen Gefahr eine harmlose Belästigung machen.

1 www.justice.gov/criminal-ccips/file/872771/download

2 www.trustwave.com/Resources/Trustwave-Blog/New-Report-on Phishing-and-Ransomware-Helps-Prepare-You-for-the-Fight

3 www.verizonenterprise.com/verizon-insights-lab/dbir/2016

FIRMENANSCHRIFT ROSA-BAVARESE-STR. 3 | 80639 MÜNCHEN | DEUTSCHLAND | +49 89 416 1169 40 | CODE42.COM