Wiederherstellung nach einem Ransomware-Angriff

Rubrik Sonderausgabe

Michael G. Solomon

für dummies®

Wiederherstellung nach einem Ransomware-Angriff für Dummies®, Rubrik Sonderausgabe

Veröffentlicht von
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-84901-8 (pbk); ISBN 978-1-119-84902-5 (ebk)

Hergestellt in den Vereinigten Staaten von Amerika

10 9 8 7 6 5 4 3 2 1

Allgemeine Informationen zu unseren sonstigen Produkten und Dienstleistungen oder zur Erstellung eines individuellen *Für Dummies*-Buches für Ihr Unternehmen oder Ihre Organisation erhalten Sie von unserer Abteilung Business Development in den USA unter Tel. 877-409-4177, E-Mail: info@dummies.biz, oder besuchen Sie www.wiley.com/go/custompub. Für Informationen zur Lizenzierung der *Für Dummies*-Marke für Produkte oder Dienstleistungen kontaktieren Sie bitte: BrandedRights&Licenses@Wiley.com.

Danksagung des Verlags

Die folgenden Personen haben bei der Erstellung dieses Buches mitgewirkt:

Development Editor: Rebecca Senninger

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Business Development Representative: William Hull

Production Editor: Mohammed Zafar Ali

Inhaltsverzeichnis

EINFÜHRUNG 1
Über dieses Buch 1
Leichtfertige Annahmen 2
In diesem Buch verwendete Symbole 2
Zusätzliche Informationen 2

KAPITEL 1: **Das Ransomware-Problem** 3
Ransomware und ihre Auswirkung auf die IT 3
Das Ransomware-Problem 4
Wie sich Ransomware auf die IT auswirkt 4
Ransomware-Angriffe in der Praxis 5
Der Devisenhändler Travelex wird lahmgelegt 5
Die Stadt Durham erholt sich schnell 5
Ransomware-Trends 6

KAPITEL 2: **Maßnahmen zur Verteidigung gegen Ransomware** 9
Einen Wiederherstellungsplan entwickeln 9
Die Anforderungen ermitteln 9
Einen Plan erstellen 10
Den Plan testen 10
Die letzte Verteidigungsinstanz schützen 11
Warum die Unveränderlichkeit von Backups so wichtig ist 11
Das Konzept der Unveränderlichkeit 11
Unveränderliche Datensicherung durchsetzen 11
Daten wiederherstellen 12

KAPITEL 3: **Verhinderung von Ransomware-Angriffen** 13
Ransomware-Schwachstellen 13
Wie Ransomware Computer angreift 14
Der Benutzer wird dazu gebracht, den Computer selbst zu infizieren 14
Ein „glänzendes neues Objekt“ wird verwendet, um den Computer automatisch zu infizieren 14
Durch Schulungen verhindern, dass Anwender zu Opfern werden 15
Potenzielle Angriffe erkennen 15
Auf verdächtige Inhalte reagieren 16
Die Nachricht wiederholen 16

Bewährte Sicherheitsverfahren implementieren 16
Sicheres Benutzerverhalten fördern 17
Die IT-Umgebung stärken 17

KAPITEL 4: **Erkennen von Ransomware-Angriffen und Abschätzen des Schadensausmaßes** 19

Besser früher als später 19
Effektives Handeln durch Frühwarnungen 20
Verringerung des Wiederherstellungsaufwands (und der Wiederherstellungszeit) 20
Methoden zur Erkennung von Angriffen 20
Ransomware-Signaturen erkennen 20
Anomalien durch maschinelles Lernen erkennen 21
Auf einen Angriff reagieren 21
Das Notfallteam zusammenstellen 21
Den Schaden eingrenzen und die betroffenen Dateien identifizieren 22
Weitere Schäden verhindern 22
Den Explosionsradius abschätzen 22

KAPITEL 5: **Datenwiederherstellung mit chirurgischer Präzision** 23

Einen Plan zur schnellen Wiederherstellung erstellen 23
Datensicherung ist nur der erste Schritt 24
Die Wiederherstellungszeit ist entscheidend 24
Nur das Nötige wiederherstellen 25
Wissen, was Sie wirklich brauchen 25
Keine Zeitverschwendung 26
Die Wiederherstellung im großen Umfang automatisieren 26
APIs für die unbeaufsichtigte Wiederherstellung implementieren 26
Scripting für hohe Leistung 26

KAPITEL 6: **Zehn Tipps zum Umgang mit Ransomware-Angriffen** 27

Einführung

Dies ist *Wiederherstellung nach einem Ransomware-Angriff für Dummies* – Ihr Leitfaden zum Thema Ransomware und Wiederherstellung. Angriffe, bei denen Schadsoftware (so genannte Malware) eingesetzt wird, sind nicht mehr nur lästige Ärgernisse. Sie haben sich mittlerweile zu ernsthaften Bedrohungen entwickelt, die Geschäftsprozesse lahmlegen und Daten zerstören können. Eine Art von Malware, die immer häufiger zum Einsatz kommt, ist Ransomware. Vom Namen dieser böswilligen Software kann man auf ihr Verhalten schließen. Ransomware verschlüsselt wichtige Dateien auf dem Computer des Opfers und verlangt die Zahlung eines Lösegeldes (engl. „Ransom") für den Entschlüsselungscode. Der Angreifer zerstört die Daten zwar nicht, aber er macht sie für die Geschädigten unzugänglich, bis das Lösegeld gezahlt wird.

Meist wird empfohlen, den betroffenen Computer nach einem Ransomware-Angriff mit dem letzten Backup-Image vollständig wiederherzustellen. Dieser Ansatz mag zwar vernünftig klingen, doch er hat auch einige Nachteile. Besonders raffinierte Ransomware sucht nach Backup-Images und verschlüsselt diese ebenso wie die Hauptdaten. Selbst wenn Sie ein gutes Backup-Image haben, dauert die Wiederherstellung einer vollständigen Umgebung sehr lange. Außerdem können viele Transaktionen dabei überschrieben werden. Es muss einfach eine bessere Lösung geben!

Ein effektiver Wiederherstellungsplan für Ransomware-Angriffe sorgt dafür, dass das betroffene Unternehmen den normalen Betrieb so schnell wie möglich wieder aufnehmen kann – und das mit minimalem Datenverlust.

Über dieses Buch

Wiederherstellung nach einem Ransomware-Angriff für Dummies stellt einen vernünftigen Ansatz zur schnellen Wiederherstellung Ihrer Daten vor – für den Fall, dass Sie einen Ransomware-Angriff nicht verhindern können. Sie erfahren, welche Bedrohung Ransomware darstellt und wie Sie einen Wiederherstellungsplan erstellen können, der sinnvoll ist und Ihr Unternehmen schützt.

Nachdem Sie sich mit den Grundlagen von Ransomware vertraut gemacht haben, erfahren Sie, wie wichtig es ist, den richtigen Anbieter von Datensicherungslösungen auszuwählen, und welche Funktionen Sie benötigen, um sich gegen Ransomware zur Wehr zu setzen.

Sie erfahren außerdem, wie Sie bei der Wiederherstellung nach einem Ransomware-Angriff die einzelnen Teile des Puzzles zusammensetzen können, um einen effektiven Wiederherstellungsplan zu entwickeln. Abschließend erhalten Sie einen Überblick über die zehn besten Tipps zur Erstellung eines effektiven Wiederherstellungsplans für Ransomware-Angriffe.

Leichtfertige Annahmen

Beim Verfassen dieses Buchs habe ich einige Annahmen über Sie, den Leser, getroffen. Erstens gehe ich davon aus, dass Sie im technischen oder geschäftlichen Bereich tätig sind und schon von Ransomware gehört haben. Unabhängig von Ihrer Rolle nehme ich an, dass Sie daran interessiert sind, mehr über die Ransomware-Bedrohung zu erfahren, und wissen wollen, wie Sie eine Störung des Geschäftsbetriebs in Ihrem Unternehmen verhindern können. Ich gehe auch davon aus, dass Sie erfahren möchten, wie Sie einen effektiven Plan zur Wiederherstellung Ihrer Daten nach einem Ransomware-Angriff erstellen können.

In diesem Buch verwendete Symbole

In jedem *Für-Dummies*-Buch finden Sie an den Seitenrändern kleine Symbole – so genannte Piktogramme. In diesem Buch verwende ich die folgenden Symbole:

TIPP

Dieses Symbol macht auf Hinweise aufmerksam, die Ihnen dabei helfen sollen, bestimmte Aufgabe schneller und einfacher auszuführen.

WARNUNG

Wenn Sie dieses Symbol sehen, ist Vorsicht geboten. Hier finden Sie Ratschläge zur Umgehung der häufigsten Fallstricke.

Zusätzliche Informationen

Das Thema Ransomware ist mit diesem Buch noch lange nicht vollständig erfasst. Innovative Unternehmen haben sich eingehend mit dem Problem befasst und einige interessante und effektive Lösungen entwickelt. Rubrik ist ein führender Anbieter von Ransomware-Wiederherstellungsdiensten für Unternehmen jeder Größe. Weitere Informationen über die Angebote von Rubrik finden Sie unter `https://www.rubrik.com/en/products/polaris-overview/polaris-radar`.

IN DIESEM KAPITEL

- Ransomware und ihre Auswirkungen auf die IT
- Ransomware-Angriffe in der Praxis
- Ransomware-Trends
- Schutzebenen zur Angriffsabwehr

Kapitel 1
Das Ransomware-Problem

Ransomware ist eine Art von Schadsoftware (Malware), die die Daten des Opfers verschlüsselt und den Entschlüsselungscode nur nach der Zahlung eines Lösegeldes freigibt. Ransomware ist eine der am schnellsten wachsenden und am meisten gefürchteten Formen von Malware. Bei einem erfolgreichen Ransomware-Angriff steht das Opfer vor einer misslichen Wahl: entweder verliert es seine wertvollen, manchmal unersetzlichen Daten oder es zahlt ein Lösegeld, um sie wiederzuerlangen. Da Daten sowohl für Privatpersonen als auch für Unternehmen einen immer größeren Wert haben, stellt Ransomware eine wachsende Bedrohung dar. In diesem Kapitel erfahren Sie, was Ransomware ist, wie sie sich auf die IT auswirkt und was Sie tun können, um sich vor Angriffen zu schützen.

Ransomware und ihre Auswirkung auf die IT

Bekanntheit erlangte Ransomware erstmals als eine Bedrohung persönlicher Daten. Die ersten Ransomware-Angriffe richteten sich hauptsächlich auf Privatpersonen und nutzten deren zunehmende Abhängigkeit von persönlichen Daten und Medien aus. Die Angst, persönliche Bilder, Videos und Dokumente zu verlieren, reichte in den meisten Fällen schon aus, um die Opfer zur Zahlung eines Lösegeldes zu

bewegen. Doch mit jeder Lösegeldzahlung wurden die Angreifer dreister und nahmen größere Ziele ins Visier.

Das Ransomware-Problem

Mittlerweile ist Ransomware nicht nur für Privatpersonen, sondern auch für Unternehmen zu einer ernsthaften Bedrohung geworden. Im Jahr 2020 nahmen Ransomware-Angreifer enger gefasste Zielgruppen ins Visier, um höhere Lösegelder zu erpressen. Einem jüngsten Bericht von Emisoft zufolge waren im Jahr 2020 „mindestens 2.354 US-Regierungsstellen, Gesundheitseinrichtungen und Schulen" von Ransomware betroffen (`https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/`). Leider gibt es keine Anzeichen dafür, dass Ransomware in nächster Zeit verschwinden wird. Die Taktiken von Ransomware-Erpressern werden immer gezielter und raffinierter.

Angreifer haben erkannt, dass Unternehmen und wichtige Service-Provider oft eher bereit sind, hohe Lösegeldsummen zu zahlen als Privatpersonen, um geschäftsschädigende Ausfallzeiten zu beenden. Die meisten Unternehmen sind heute zur Abwicklung Ihres täglichen Geschäfts auf Daten und Informationssysteme angewiesen. Wenn sie nicht mehr auf ihre geschäftskritischen Daten zugreifen können, kommt dies einer schwerwiegenden Katastrophe gleich. Zwar verfügen viele Unternehmen über Disaster-Recovery-Pläne, doch die meisten dieser Pläne beinhalten keine Maßnahmen, die einen dauerhaften Verlust kritischer Betriebsdaten verhindern können. Unternehmen müssen wissen, wie sich Ransomware von anderen Bedrohungen unterscheidet, um katastrophale Störungen ihrer kritischen Geschäftsfunktionen zu vermeiden.

Wie sich Ransomware auf die IT auswirkt

Die Aussicht, kritische Daten für immer zu verlieren, ist für Ransomware-Opfer eine reale Bedrohung. Oft herrscht die Auffassung, dass man lediglich verhindern muss, einem Angriff zum Opfer zu fallen. Dieser Ansatz klingt zwar logisch, doch er funktioniert nur, wenn er zu 100 Prozent effektiv ist. Die eigentliche Frage ist: Wie können wir uns von einem Ransomware-Angriff erholen, wenn eine unserer Abwehrfunktionen versagt hat? Dies lässt sich nur durch Pläne erreichen, die Maßnahmen zur Prävention, Bewertung und Wiederherstellung beinhalten.

Ein guter Resilienzplan sieht die Implementierung mehrerer Schutzebenen vor. Mit den richtigen Kontrollen und Plänen ist es nicht schwer, sich vor Ransomware zu schützen. Wahrscheinlich werden Sie dabei einige Änderungen an Ihrer IT-Infrastruktur in Betracht ziehen müssen. Alle Angreifer sind auf „normale" IT-Infrastrukturen angewiesen,

und für Ransomware-Kriminelle gilt das ganz besonders. Sie rechnen mit einem hohen Grad an Automatisierung und einfachen Verbindungen zu externen Speichern. Intelligentere Infrastruktur, von der Angreifer überrascht werden, ist der erste Schutz vor Ransomware-Angriffen.

Ransomware-Angriffe in der Praxis

Bevor Sie erfahren, wie Sie sich am besten auf eine Ransomware-Attacke vorbereiten können, wollen wir uns ansehen, wie zwei Angriffsopfer in der Praxis mit der Situation umgegangen sind. Der erste Geschädigte wurde von dem Angriff überrascht, während sich der andere sorgfältig auf die Möglichkeit einer Ransomware-Attacke vorbereitet hatte. Der zweite Geschädigte überlebte den Angriff nicht nur, sondern setzte den Betrieb mit minimaler Unterbrechung fort - und das, ohne sein IT-Budget zu sprengen. Das können Sie ebenfalls.

Der Devisenhändler Travelex wird lahmgelegt

In der Silvesternacht 2019 wurde das Londoner Unternehmen Travelex Opfer eines Ransomware-Angriffs durch die Sodinokibi-Bande. Die zentralen Dienstleistungen der in 26 Ländern tätigen Devisengesellschaft wurden durch den Angriff stark beeinträchtigt. Backups wurden gelöscht und 5 GB an Betriebsdaten heruntergeladen und verschlüsselt. Für die Übergabe des Entschlüsselungscodes und die Löschung der heruntergeladenen Daten verlangten die Cyberkriminellen ein Lösegeld in Höhe von 6 Millionen Dollar. Travelex verhandelte mehrere Wochen lang mit den Angreifern und stimmte schließlich der Zahlung von 2,3 Millionen US-Dollar in Kryptowährung zu, um seine Daten und die Zusicherung zu erhalten, dass diese Daten nicht offengelegt werden würden. Nach der Zahlung des Lösegeldes konnte Travelex Ende Januar 2020 seine Kernaktivitäten fortsetzen und nahm im Februar 2020 den normalen Betrieb wieder auf.

WARNUNG

Versuchen Sie, möglichst kein Lösegeld zu zahlen. Mit jedem gezahlten Lösegeld erhöht sich der Gewinn der Angreifer und sie können ihr kriminelles Geschäft fortsetzen. Durch die Zahlung eines Lösegelds präsentieren Sie sich außerdem als „leichtes Ziel“ für zukünftige Angriffe.

Die Stadt Durham erholt sich schnell

Nicht jeder Ransomware-Angriff kostet viel Geld oder führt zum Verlust großer Datenmengen. Durch gute Planung kann man verhindern, zu einer Statistik zu werden. Im März 2020 war die Stadt Durham in North Carolina Ziel einer Ransomware-Attacke. Durham hatte zuvor einen Überwachungs- und Backup-Infrastrukturplan implementiert,

dem eine Backup-Lösung von Rubrik zugrunde lag. Dieses auf dem Konzept der Unveränderlichkeit basierende System stellt sicher, dass Backups nicht kompromittiert werden können.

Als der Angriff begann, wurden mehrere kritische Dienste außer Betrieb gesetzt, einschließlich des Notrufservers. Das Personal war jedoch in der Lage, die betroffenen Dateien zu identifizieren und wiederherzustellen, damit die wichtigsten Dienste schnell aufgenommen werden konnten. Nach der Wiederaufnahme der kritischsten Dienste konnten die Mitarbeiter von Durham den Rest der vom Angriff betroffen Daten wiederherstellen. Am Montagmorgen waren alle wichtigen Geschäftssysteme wieder in Betrieb.

Ransomware-Trends

Im Bereich Ransomware haben sich inzwischen einige Trends herauskristallisiert. Keiner davon ist gut. Wenn Sie für die Daten Ihres Unternehmens verantwortlich sind, müssen Sie diese Bedrohungstrends verstehen, um sich auf mögliche Angriffe in der Zukunft vorbereiten zu können. Es gibt jedoch auch eine gute Nachricht: Obwohl Ransomware immer raffinierter wird, können Sie den Angreifern ein paar Schritte voraus sein.

Hier sind einige aktuelle Ransomware-Trends:

- **Höhere Lösegeldbeträge.** Angreifer richten ihre Angriffe auf eine geringere Anzahl von Zielen, verlangen aber deutlich höhere Lösegeldzahlungen.
- **Commodity-Malware.** Sie müssen Malware nicht selbst schreiben, um Ransomware zu nutzen. Mit Ransomware-as-a-Server (RaaS) ist es leicht, ein Cyberkrimineller zu werden.
- **Digitale Arbeits- und Studiensituationen.** Die Corona-Krise hat den Trend beschleunigt, von zu Hause aus arbeiten oder zu studieren. Angreifer nehmen daher zunehmend Collaboration- und Bildungsanbieter ins Visier.
- **Datenausschleusung.** Bei einigen Angriffen werden die Daten nicht nur verschlüsselt, sondern direkt zum Gerät des Angreifers übertragen. Diese Daten können dann gewinnbringend verkauft oder offengelegt werden. Für das Opfer hat dies gravierende Folgen wie Rufschädigungen oder Geldstrafen aufgrund von Gesetzes- oder Regelverstößen, z. B. GDPR-Bußgelder.
- **Ein zweiter Erpressungsversuch.** Ausgeschleuste Daten können verwendet werden, um zusätzliche Lösegeldzahlungen zu erpressen, damit vertrauliche Daten nicht veröffentlicht werden. Allein die

Drohung, vertrauliche Informationen zu veröffentlichen, reicht nicht selten aus, um ein Opfer zur Zahlung eines Lösegelds zu zwingen.

- **Kompromittierung von Backup-Daten.** Viele aktuelle Ransomware-Varianten beschränken sich nicht darauf, lokale Daten zu verschlüsseln. Sie machen verbundene Datenquellen ausfindig und versuchen, auch alle Backup-Kopien zu verschlüsseln.
- **Schnelle Zunahme von Angriffen.** Höhere Lösegelder, die Einfachheit der Malware-Verbreitung und eine spezifischere Zielauswahl – alle diese Faktoren haben dazu geführt, dass die Anzahl der profitgierigen Angreifer in Sachen Ransomware steigt. Erhöhte Resilienz durch zusätzliche Verteidigungsebenen

Angesichts der wachsenden Bedrohung durch Ransomware und der vielversprechenden Aussichten, die sich den Angreifern eröffnen, mag es hoffnungslos erscheinen, über eine Verteidigung nachzudenken. Durch gut durchdachte Verteidigungsmaßnahmen können jedoch viele Arten von Ransomware-Angriffen verhindert werden. Außerdem helfen sie Ihnen dabei, sich schnell zu erholen, falls es Angreifern tatsächlich gelingen sollte, Ihre Perimeter-Verteidigung zu überwinden. Der Schlüssel dazu ist der Aufbau mehrerer Verteidigungsebenen. Auf dem Gebiet der Cybersicherheit nennt man dies *Defense in Depth*, also eine in der Tiefe gestaffelte Verteidigung. Das heißt im Grunde nur, dass sich zwischen Ihren Daten und dem Angreifer möglichst viele Schutzebenen bzw. Sicherheitskontrollen befinden sollten.

Viele sind der Meinung, dass Kontrollen zur Angriffsabwehr die wichtigsten Schutzmechanismen sind. Natürlich ist es immer erstrebenswert, Angriffe erst einmal zu verhindern, doch man darf sich nicht in der Gewissheit wiegen, dass jeder Angriff tatsächlich verhindert werden kann. Wenn Sie nicht für jede Eventualität eines möglicherweise erfolgreichen Angriffs einen Plan haben, sind Sie völlig unvorbereitet, wenn der gefürchtete Ernstfall doch eintreten sollte.

Zu den Präventivmaßnahmen gehören Personalschulungen und Firewalls. Das Ziel dieser ersten Schutzebene ist die Abwehr der meisten Angreifer, bevor sie Fuß fassen können. Da die meisten Malware-Angriffe, einschließlich Ransomware, mit einem Klick auf einen bösartigen Link beginnen, müssen Mitarbeiter in der Erkennung schädlicher Nachrichten und Links geschult werden. Firewalls können Datenverkehr blockieren, der offensichtlich schädlich ist. Sie können autorisierte Benutzer jedoch nicht davon abhalten, auf bösartige Links zu klicken.

TIPP

Vorbeugung ist wichtig, doch bei der Bekämpfung von Ransomware sollte der eigentliche Schwerpunkt auf Resilienz liegen. Es reicht nicht aus, zu wissen, wie man einen Angriff vermeiden kann. Man muss

auch wissen, was zu tun ist, wenn man von einer Ransomware-Attacke betroffen ist.

Wenn ein Angriff nicht durch Ihre Präventivmaßnahmen verhindert werden kann, sollten Sie zumindest wissen, dass Sie angegriffen werden, damit Sie reagieren können. Sie benötigen eine starke Erkennungsebene, um Maßnahmen ergreifen zu können, bevor es zu spät ist. Heute gibt es Technologien zur Überwachung und Verhaltensanalyse, die nahezu sofortige Warnungen über einen laufenden Ransomware-Angriff liefern können.

TIPP

Sie benötigen ein System zur Echtzeit-Überwachung aller Primärkopien Ihrer kritischen Daten mit zusätzlichen intelligenten Funktionen zum Schutz Ihrer Backup-Daten, um eine letzte Verteidigungsinstanz zu schaffen.

Die nächste Ebene Ihrer Ransomware-Abwehr hat die Aufgabe, den Angriff zu stoppen und den entstandenen Schaden zu bewerten. Dies erreichen Sie, indem Sie die betroffenen Computer vom Netzwerk trennen und herunterfahren, wobei bestimmte Verfahrensschritte befolgt werden müssen. Wenn Sie in einer kontrollierten Umgebung einen Neustart durchführen, sind Sie in der Lage, den Schaden genau zu beurteilen. Die Containerisierung kann diesen Schritt vereinfachen. Natürlich sind die meisten Aktivitäten auf dieser Ebene von Richtlinien und Verfahren abhängig, die lange vor Beginn eines Angriffs entwickelt wurden.

Die nächste Verteidigungsebene hängt von der Backup-Lösung ab, die Sie implementiert haben. Sobald Sie wissen, welche Dateien durch den Angriff beschädigt worden sind, müssen Sie Images jeder einzelnen Datei abrufen, die ihren Zustand vor dem Angriff widerspiegelt. Ihre Backup-Lösung sollte es Ihnen leicht machen, bestimmte Datei-Images von einem bekannten Zeitpunkt schnell wiederherzustellen.

Und zu guter Letzt müssen Sie sich darüber im Klaren sein, dass Ihre Backup-Lösung ein Hauptziel für durchdachte Ransomware-Angriffe sein wird. Die einzigen Backups, denen Sie vertrauen können, sind Backups mit Integritätsgarantie. Ihre Backup-Lösung muss verhindern, dass bestimmte Prozesse, einschließlich Ransomware, ein Backup-Image verändern können, nachdem es in das Dateisystem geschrieben wurde.

Wenn Sie all diese Verteidigungsebenen implementieren, haben Sie die wesentlichen Voraussetzungen geschaffen, um sich schnell von einem erfolgreichen Angriff zu erholen.

IN DIESEM KAPITEL

- **einen Wiederherstellungsplan erstellen**
- **Schutz der letzten Verteidigungslinie**
- **das Konzept der Unveränderlichkeit**
- **Erholung nach einem Ransomware-Angriff**

Kapitel 2
Maßnahmen zur Verteidigung gegen Ransomware

Die erfolgreiche Bewältigung eines Ransomware-Angriffes darf nicht dem Zufall überlassen werden. Es gibt nur eine Möglichkeit, nicht zum „Opfer" eines Ransomware-Angriffes zu werden: Man muss auf einen Angriff vorbereitet sein und Maßnahmen zur Wiederherstellung planen, bevor ein Angriff eintritt. In diesem Kapitel erfahren Sie, wie Sie einen Plan erstellen können, der Ihnen gute Dienste leisten wird, falls Ihr Unternehmen Ziel eines Ransomware-Angriffs werden sollte.

Einen Wiederherstellungsplan entwickeln

Es ist sehr schwierig, sich von einem erfolgreichen Ransomware-Angriff zu erholen, wenn man sich nicht auf den Ernstfall vorbereitet hat. Doch selbst mit gründlicher Vorbereitung ist eine Wiederherstellung ohne einen guten Plan nicht immer möglich. Verlieren Sie jedoch nicht den Mut. Wenn Sie genau wissen, wie man einen guten Plan erstellt, ist es viel wahrscheinlicher, dass sich Ihr Unternehmen nach einem Ransomware-Angriff schnell und ohne große Schwierigkeiten erholt.

Die Anforderungen ermitteln

Bei der Planung einer Überlebensstrategie für Ransomware-Angriffe müssen Sie zunächst verstehen, was für Ihr Unternehmen wichtig ist und was für die Angreifer wichtig ist. Eine Business-Impact-Analyse (BIA) hilft dabei, die für Ihr Unternehmen wichtigen Prozesse und die Ressourcen zu bestimmen, die diese Prozesse unterstützen. Dabei geht

es im Grunde um die Frage: Was muss Ihr Unternehmen tun können, um im Geschäft zu bleiben?

Wenn Sie wissen, was Ihr Unternehmen benötigt, um kritische Geschäftsfunktionen (Critical Business Functions, CBF) auszuführen, wissen Sie auch, welche Daten für Sie wichtig sind. Ein Online-Händler wird zum Beispiel großen Wert auf seine Kunden- und Produktdatenbanken legen, während eine Sammlung von Anleitungsvideos für den täglichen Betrieb wohl kaum von kritischer Bedeutung ist.

Nachdem Sie ermittelt haben, was für Sie wichtig ist, müssen Sie überlegen, was für Angreifer wichtig sein könnte. Angreifer wollen in der Regel an die Daten gelangen, die für Sie den größten Wert haben – also die Daten, die Sie zur Ausführung Ihrer CBFs benötigen. Kriminelle wissen, dass Sie eher Lösegeld für Daten zahlen, die Sie zur Aufrechterhaltung Ihrer Geschäftstätigkeit benötigen.

Einen Plan erstellen

Sobald Sie bestimmt haben, welche Daten für Ihr Unternehmen (und die Angreifer) am wichtigsten sind, ist es an der Zeit, einen Plan zur Wiederherstellung dieser Daten zu erstellen, der zum Einsatz kommt, wenn Ihr Unternehmen von einem Ransomware-Angriff betroffen sein sollte. In Kapiteln 4 und 5 erfahren Sie, was in Ihrem Plan enthalten sein sollte. Zunächst können Sie sich jedoch überlegen, wen Sie im Planungsteam brauchen und wie Sie den Plan dokumentieren wollen. Beziehen Sie Vertreter aller Gruppen ein, die den Plan beeinflussen oder von ihm betroffen sein können.

Den Plan testen

Wenn Sie Ihren Ransomware-Wiederherstellungsplan erstellt haben, gibt es noch einige weitere Aufgaben zu erledigen. Auf einen Plan, der nicht vollständig getestet wurde, können Sie sich nicht vollständig verlassen. Schließlich wollen Sie nicht viel Zeit und Mühe in einen Plan investieren, der sich nach einem Angriff als nutzlos erweist, nur weil ein kleiner, aber wichtiger Teil fehlt. Ein Plan, der nicht funktioniert, bringt Ihnen keinen Nutzen (und versetzt Sie nicht in die Lage, sich von einem Angriff zu erholen).

Es gibt unterschiedliche Arten von Tests, die Sie durchführen sollten. Jeder der folgenden Tests kommt einem tatsächlichen Angriff immer ein Stück näher. Die meisten Unternehmen beginnen mit einem Checklistentest. Dabei gehen die Beteiligten den Plan gemeinsam durch, um sicherzustellen, dass alle Aufgaben berücksichtigt wurden. Ein umfassenderer Test ist eine Simulation. Dabei führen die Beteiligten alle Maßnahmen durch, die sie auch bei einem tatsächlichen Angriff durchführen würden. Die letzte Art von Test ist ein destruktiver Test, bei dem Dateien tatsächlich verändert werden, um zu sehen, ob das Wiederherstellungsteam sie in einem brauchbaren Zustand wiederherstellen kann. Dieser

Test ist zwar mit Risiken verbunden, doch er ist zur Prüfung eines Wiederherstellungsplans am effektivsten.

Die letzte Verteidigungsinstanz schützen

Jede Ransomware, die erfolgreich Dateien verschlüsselt, ist darauf angewiesen, dass der Geschädigte keinen Zugriff auf eine Kopie der betroffenen Datei hat. Deshalb setzen Angreifer alles daran, die Sicherungskopien der betroffenen Dateien zu finden und diese ebenfalls zu verschlüsseln. Da Automatisierung und Konnektivität heute allgegenwärtig sind, ist es oft leicht, die meisten Sicherungsspeicher zu finden und zu infizieren.

Zur Wiederherstellung von Dateien, die durch Ransomware verschlüsselt wurden, ist ein dreistufiges Verfahren erforderlich: 1) Den Angriff stoppen. 2) Die betroffenen Dateien identifizieren. 3) Eine unverschlüsselte (unverfälschte) Version der Datei aus einem Backup wiederherstellen.

Der dritte und kritischste Schritt ist nur dann möglich, wenn Sie sicher sein können, dass Ihre Backups nicht von der Ransomware verändert wurden. Deshalb ist es von entscheidender Bedeutung, den richtigen Datensicherungsdienst zur Wiederherstellung nach einem Ransomware-Angriff zu verwenden.

Warum die Unveränderlichkeit von Backups so wichtig ist

Ein erfolgreicher Wiederherstellungsplan setzt voraus, dass Sie sich auf die Unversehrtheit Ihrer Backups verlassen können. Wenn Sie sicher sein können, dass die Ransomware Ihre gesicherten Dateien nicht verändert hat, können Sie sich von einem Ransomware-Angriff erholen.

Das Konzept der Unveränderlichkeit

Die Unveränderlichkeit von Backups ist eine entscheidende Eigenschaft, die für die Widerstandsfähigkeit gegen Ransomware-Angriffe unerlässlich ist. Unveränderlichkeit bedeutet, dass einmal geschriebene Daten nicht mehr verändert werden können. Nichts und niemand – auch kein Ransomware-Prozess – ist in der Lage, die Daten nach dem Schreiben in irgendeiner Form zu ändern. Wenn Sie unveränderliche Backups haben, verfügen Sie über ein perfektes Abbild der Daten vor dem Ransomware-Angriff, das Sie zur Wiederherstellung verwenden können.

Unveränderliche Datensicherung durchsetzen

Es ist keine neue Idee, Unveränderlichkeit zur Unterstützung von Sicherheitszielen zu nutzen. Protokollierungssysteme tun dies seit vielen Jahren. Angreifer haben schon vor langer Zeit erkannt, dass sie durch das Löschen oder Ändern von Protokolldateien ihre Spuren einfach verwischen und Beweise für ihre Verbrechen vernichten können.

Sicherheitsexperten wurde schnell klar, dass sie Protokollstrategien benötigen, damit ein Service einen Protokolldateieintrag zwar schreiben, aber niemals ändern kann.

Rubrik hat für seine Backup-Lösung ein einzigartiges Dateisystem von Grund auf neu entwickelt, das Unveränderlichkeit für alle Dateien implementiert. Das Sichern einer Datei ist einfach: Sie schreiben die Datei und verwenden einen API-Aufruf von Rubrik. Sobald die Datei geschrieben ist, kann sie nicht mehr geändert werden. Das Dateisystem von Rubrik speichert alle Dateien nativ als unveränderlich, das heißt, sie sind schreibgeschützt. Es lässt keine externen Clients in das Netzwerk, die die gespeicherte Datei verschlüsseln oder löschen könnten. Sie können die Dateien über eine API lesen, doch Änderungen sind nicht erlaubt. Durch die Unveränderlichkeit des Dateisystems von Rubrik erhalten Sie die Gewissheit, über unveränderte Dateien zu verfügen, mit denen Sie sich schnell von einem Ransomware-Angriff erholen können.

Daten wiederherstellen

Vor der Wiederherstellung müssen Sie bestimmen, welche Daten von dem Ransomware-Angriff betroffen sind. Sie könnten zwar einfach alle Dateien wiederherstellen, doch das würde die Wiederherstellungszeit erheblich verlängern. Business Continuity bezieht sich auf Maßnahmen zur Minimierung von Ausfallzeiten. Dieser Ansatz schließt auch ein, dass nur jene Daten wiederhergestellt werden, die für die Fortsetzung des Geschäftsbetriebs erforderlich sind.

Sie haben sich die Zeit genommen, die Daten zu identifizieren, die für die CBFs Ihres Unternehmens entscheidend sind. Nun müssen Sie bestimmen, welche der kritischen Dateien verschlüsselt wurden. Je nach der Art der Ransomware kann es relativ einfach sein, die verschlüsselten Dateien zu identifizieren. Letztendlich ist Ransomware nur Software und benötigt ein Register, ein Verzeichnis oder eine andere Methode zur Identifizierung verschlüsselter Dateien. Schließlich müssen die Angreifer diese Dateien entschlüsseln können, nachdem Sie das Lösegeld bezahlt haben – das sollen Sie zumindest glauben!

WARNUNG

Die meisten Ransomware-Angreifer stellen nach Erhalt des Lösegeldes einen Entschlüsselungscode zur Verfügung. Allerdings ist es immer riskant, einem Cyberkriminellen zu vertrauen.

Nachdem Sie die betroffenen Dateien identifiziert haben, muss die Wiederherstellung durchgeführt werden. Dies lässt sich am besten durch die Implementierung einer Backup-Lösung erreichen, die Ihnen über Programmierschnittstellen (APIs) schnellen Zugriff auf Ihre gesicherten Dateien ermöglicht. Auf diese Weise können Sie Skripte schreiben, die verschlüsselte Dateien schnell wiederherstellen, damit Sie den Geschäftsbetrieb fortsetzen können.

IN DIESEM KAPITEL

- **Ransomware-Schwachstellen erkennen**
- **Angriffsmöglichkeiten beseitigen**
- **Anwender über Ransomware-Fallen aufklären**
- **bewährte Verfahren zur Vermeidung von Ransomware-Angriffen nutzen**

Kapitel 3
Verhinderung von Ransomware-Angriffen

In einer Zeit, in der Malware-Angriffe immer häufiger auftreten, können nur jene Unternehmen überleben, denen es gelingt, die meisten Angriffe zu verhindern und sich von den übrigen zu erholen. Das beste Szenario ist natürlich, Angriffe von vornherein zu vermeiden, doch das ist leider nicht immer möglich. Deshalb benötigen Sie einen soliden Plan zum Umgang mit Ransomware-Angriffen. Um effektiv mit jedem Ransomware-Angriff umgehen zu können, müssen Sie zunächst das Wesen dieser Angriffe verstehen. Dann können Sie Maßnahmen zu ihrer Verhinderung ergreifen und, wenn ein Angriff doch erfolgreich sein sollte, effektiv mit ihm umgehen. In diesem Kapitel erfahren Sie, welche Maßnahmen Sie zur Vermeidung von Ransomware-Angriffen ergreifen können.

Ransomware-Schwachstellen

Ransomware stellt zwar ein ernstes Problem dar, doch es handelt sich keineswegs eine unbesiegbare Malware. Um zu verhindern, dass Ransomware-Angriffe erfolgreich sind, muss man zunächst verstehen, wie Ransomware funktioniert. Erst dann kann man Verfahren und Kontrollen zu ihrer Abwehr entwickeln. In diesem Abschnitt beleuchten wir einige der Schwachstellen in den Plänen der Ransomware-Angreifer.

Wie Ransomware Computer angreift

Ransomware hängt von der Fähigkeit ab, ein bösartiges Programm auf dem Computer eines Opfers auszuführen. Es gibt mehrere Möglichkeiten, die ausführbare Ransomware-Datei auf das Gerät eines Opfers zu bringen. Häufig werden Benutzer dazu verleitet, einen schädlichen Link zu öffnen, auf eine bösartige Website zu navigieren oder ein infiziertes Gerät anzuschließen.

Der Benutzer wird dazu gebracht, den Computer selbst zu infizieren

Computer werden am häufigsten mit Ransomware infiziert, weil ein Benutzer eine Handlung ausgeführt hat, durch die der schädliche Code ausgeführt werden kann. Die meisten Benutzer werden dies sicher nicht absichtlich tun. Es ist jedoch erstaunlich einfach, einen Benutzer dazu zu bringen, ahnungslos für den Angreifer die Drecksarbeit zu erledigen. Der Cyberkriminelle muss lediglich einen autorisierten Benutzer davon überzeugen, eine Handlung für eine nicht autorisierte Person auszuführen. Dies wird als Social Engineering bezeichnet.

Die meisten Menschen sind anfällig für Social Engineering, weil sie hilfsbereit sein möchten, an kostenlosen Dingen interessiert sind und keinen Ärger bekommen wollen. Angreifer wissen das und meist gelingt es ihnen auch, einen oder mehrere dieser Wünsche auszunutzen. Deshalb beginnen viele Ransomware-Infektionen damit, dass ein ahnungsloser Benutzer einen Link auf einer Website oder in einer E-Mail anklickt, um jemandem zu helfen („Klicken Sie hier, um für eine wohltätige Organisation zu spenden“), seine Neugier zu befriedigen („Klicken Sie hier, um Ihr Geld abzuholen“) oder Ärger zu vermeiden („Klicken Sie hier, um Ihr Passwort zu ändern“).

Ein „glänzendes neues Objekt“ wird verwendet, um den Computer automatisch zu infizieren

Der Erfolg eines Ransomware-Angriffs hängt nicht immer davon ab, dass ein Benutzer auf einen Link klickt. Bei einem Drive-by-Download-Angriff wird bösartiger Code heruntergeladen, wenn ein Benutzer eine infizierte Website besucht. Eine andere Angriffsmethode ist das Ablegen infizierter USB-Sticks an Orten, an denen Menschen sie wahrscheinlich bemerken werden. Die meisten Menschen, die einen kostenlosen USB-Stick erhalten, werden ihn wahrscheinlich in einen Computer stecken, um zu sehen, was er enthält. Bei infizierten USB-Sticks reicht das Einstecken in den Computer schon aus, um die Ransomware zu kopieren und zu starten.

WARNUNG

Viele Angreifer nutzen den USB-Stick-Trick, um Malware einzuschleusen. Vertrauen Sie daher nicht blindlings auf USB-Sticks aus unbekannten Quellen, auch nicht auf solche, die bei Tagungen und Konferenzen kostenlos verteilt werden.

Durch Schulungen verhindern, dass Anwender zu Opfern werden

Anwendertraining ist eine der besten Investitionen, die ein Unternehmen im Kampf gegen Ransomware tätigen kann. Schließlich sind es die Anwender von Geräten, die Kriminellen fast alle Einstiegspunkte für erfolgreiche Ransomware-Angriffe bieten. Schulungen spielen eine entscheidende Rolle, um Angriffe zu verhindern. Wenn Benutzer in der Erkennung potenzieller Angriffe geschult sind und der Versuchung widerstehen, auf fragwürdige Links zu klicken, kann die Wahrscheinlichkeit eines erfolgreichen Angriffs deutlich verringert werden.

Sicherheitsschulungen sollten sich nicht ausschließlich damit befassen, was Anwender tun oder nicht sollten. Neben Anleitungen zur korrekten Nutzung sollten Ihre Schulungen auch darauf abzielen, Anwender als Sicherheitsbeauftragte zu gewinnen. Jeder einzelne Mitarbeiter trägt Verantwortung für die Sicherheit des Unternehmens, nicht nur eine kleine Gruppe von Sicherheitsspezialisten. Erinnern Sie alle Mitarbeiter daran, dass Sicherheit eine Teamleistung ist, und dass jeder wachsam sein muss. Es bedarf nur eines einzigen unbedachten Fehlers, um ein ganzes Unternehmen einem Angriff auszusetzen. Beim Kampf gegen Ransomware hat jeder eine Rolle zu spielen.

TIPP

Es hilft, Mitarbeitern mehr Verantwortung für die Sicherheit des Unternehmens zu übertragen. So können unvorsichtige zu Sicherheitsverstößen führende Handlungen weitgehend vermieden werden.

Potenzielle Angriffe erkennen

Meist sind Benutzer der einfachste Einstiegspunkt für Ransomware. Deshalb lässt sich das Angriffspotenzial erheblich verringern, wenn man Benutzern beibringt, aufmerksam zu sein und verdächtige Inhalte zu erkennen. Zeigen Sie den Benutzern Beispiele für Phishing-E-Mails und geben Sie ihnen Hinweise zur Erkennung potenzieller Angriffe.

Phishing-E-Mails werden zwar immer raffinierter, doch die meisten sind leicht zu erkennen. Geben Sie den Benutzern Tipps zur Erkennung bösartiger E-Mails. Legen Sie ihnen nahe, auf Grammatik (ergibt die Nachricht einen Sinn?), Anrede (werden Sie mit Namen angesprochen) und spezifische Inhalte (enthält die Nachricht Details oder ist sie allgemein gehalten?) zu achten, die auf bösartige Nachrichten hindeuten

könnten. Benutzer, die genau wissen, worauf sie achten müssen, können Angriffe verhindern.

Auf verdächtige Inhalte reagieren

Das Erkennen verdächtiger Inhalte ist ein wichtiger erster Schritt. Benutzer müssen aber auch wissen, was als Nächstes zu tun ist. In Ihrem Unternehmen sollte es eine Anlaufstelle zur Meldung verdächtiger E-Mail-Nachrichten, anderer Medien oder verdächtiger Verhaltensweisen geben. Richten Sie eine E-Mail-Adresse ein, an die Mitarbeiter verdächtige E-Mails weiterleiten können. Ihr Sicherheitspersonal sollte diese E-Mail-Adresse überwachen und alle gemeldeten Nachrichten prüfen. Anfangs werden Sie wahrscheinlich feststellen, dass viele Nachrichten an die überwachte E-Mail-Adresse weitergeleitet werden. Wenn Ihr Sicherheitspersonal erläutert, ob bzw. warum die jeweilige die Nachricht bösartig ist, werden Ihre Mitarbeiter verdächtige Nachrichten bald besser erkennen und die Zahl der Fehlalarme wird zurückgehen.

Die Nachricht wiederholen

Es wäre schön, wenn sich die Teilnehmer von Sicherheitsschulungen immer an das Gelernte erinnern würden. Leider ist das selten der Fall. Es kommt vor, dass Anwender vergessen, wie wichtig die Sicherheit für das Unternehmen ist, vielleicht, weil sie mit Terminen beschäftigt sind oder einfach nicht immer übervorsichtig sein wollen. Erfolgreichen Sicherheitsprogrammen ist eines gemein: sie sind fortlaufend.

Anstatt einmalige Sicherheitsschulungen anzubieten, sollten Sie regelmäßig Schulungen durchführen. Variieren Sie dabei die Art der Durchführung. Ein monatlich oder vierteljährlich abgehaltenes „Lunch and Learn“ (Vorträge in der Mittagspause) funktioniert oft besser als eine halbtägige Veranstaltung pro Jahr. Mitarbeiter sollten immer wieder daran erinnert werden, welche Rolle sie in Sachen Sicherheit spielen und wie sie diese Rolle am besten ausfüllen können.

Bewährte Sicherheitsverfahren implementieren

Beim Erstellung eines Sicherheitsplans müssen Sie das Rad nicht neu erfinden. Bewährte Verfahren sind ein guter Ausgangspunkt. Glücklicherweise haben viele Unternehmen einige bewährte Verfahren entwickelt, die bei der Verhinderung von Ransomware-Angriffen helfen können. Es gibt keine einzige allgemeingültige Sammlung bewährter Verfahren. Im folgenden Abschnitt sind jedoch einige der nützlichsten Maßnahmen aufgelistet, die ein Unternehmen ergreifen kann, um Ransomware-Angriffe zu verhindern.

Sicheres Benutzerverhalten fördern

Mitarbeiter, die die Funktionsweise von Ransomware verstehen, sind eher bereit, sich an Richtlinien für das Online-Verhalten zu halten. Benutzer können viele Dinge tun (oder vermeiden), die die IT-Umgebung sicherer und weniger anfällig für Ransomware-Angriffe machen. Hier sind einige Maßnahmen, mit denen sich Benutzer schützen können:

- vor dem Öffnen einer E-Mail den Absender überprüfen
- keine Anhänge öffnen, wenn der Absender nicht bekannt ist
- keine unerwarteten Anhänge öffnen
- keinen in E-Mail-Nachrichten enthaltenen Links folgen
- nicht auf verdächtig aussehende Nachrichten reagieren
- verdächtige Nachrichten an die Sicherheitsgruppe weiterleiten
- nur vertrauenswürdige Websites besuchen
- keine persönlichen Daten zur Verfügung stellen, es sei denn, sie vertrauen der Website und dem Grund, warum die Daten benötigt werden, und die Interaktion wurde von ihnen initiiert
- kein externes Gerät (z. B. einen USB-Stick) anschließen, sofern die Quelle nicht vertrauenswürdig ist
- immer ein virtuelles privates Netzwerk verwenden, wenn sie sich von einem Remote-Standort aus verbinden
- Software und das Betriebssystem gepatcht und auf dem neuesten Stand halten.

Die Befolgung dieser bewährten Verfahren macht es Angreifern schwer, erfolgreiche Ransomware-Angriffe zu starten.

Die IT-Umgebung stärken

Auch für IT- und Sicherheitspersonal gibt es bewährte Verfahren. Durch die Umsetzung der folgenden bewährten Verfahren können Sie eine sichere Umgebung für Ihre Benutzer schaffen und bewahren.

- alle kritischen Daten identifizieren
- regelmäßige Sicherungskopien aller kritischen Daten erstellen
- einen umfassenden Wiederherstellungsplan entwickeln und testen
- alle Computer und Geräte mit den neuesten Sicherheits-Patches aktualisieren
- ein virtuelles privates Netzwerk für alle Fernzugriffe vorschreiben

- Antivirus-/Antimalware-Software auf allen Computern und Geräten vorschreiben
- Malware-Scans und -Filtern auf Mail-Servern implementieren.
- Firewalls mit restriktiven Regeln an jeder Vertrauensgrenze implementieren
- fortlaufende Sicherheitsschulungen des gesamten Personals durchführen.
- eine Support-Funktion einrichten, die gemeldete verdächtige Nachrichten oder Websites prüft, und alle Mitarbeiter darüber informieren.

Keine Präventionsmaßnahme ist zu 100 Prozent wirksam, doch jede kann einen wichtigen Beitrag leisten. Jeder Ransomware-Angriff, den Sie verhindern, ist ein Angriff, von dem Sie sich nicht erholen müssen. Die beste Strategie besteht darin, jeden möglichen Angriff zu verhindern und sich auf die Wiederherstellung vorzubereiten, falls Sie doch von einem Angriff betroffen sein sollten.

IN DIESEM KAPITEL

- **Angriffe erkennen, während sie stattfinden**
- **die richtigen Personen alarmieren**
- **das Ausmaß des Schadens abschätzen**

Kapitel 4
Erkennen von Ransomware-Angriffen und Abschätzen des Schadensausmaßes

Trotz aller Bemühungen kann es passieren, dass Kriminellen ein erfolgreicher Ransomware-Angriff gelingt. In diesem Kapitel erfahren Sie, wie Sie einen Ransomware-Angriff erkennen, sobald er beginnt, und wie Sie das Ausmaß des Schadens einschätzen können.

Besser früher als später

Bei einem erfolgreichen Ransomware-Angriff werden ein oder mehrere Systeme infiziert, indem wichtige Dateien ausfindig gemacht und dann verschlüsselt werden. Da die Verschlüsselung von Dateien einige Zeit in Anspruch nimmt, ist es wichtig, einen Angriff so zeitig wie möglich zu erkennen und zu stoppen, damit möglichst wenige Dateien wiederhergestellt werden müssen.

Effektives Handeln durch Frühwarnungen

Wie bei jeder Art von Angriff (nicht nur bei Cyberattacken) ist eine frühzeitige Erkennung entscheidend, um den Schaden einzugrenzen und die Daten so schnell wie möglich wiederherzustellen. Angreifer möchten so viel Schaden wie möglich anrichten. Wenn sie ihnen rechtzeitig Einhalt gebieten, gibt es weniger zu bereinigen.

Die frühzeitige Einleitung von Wiederherstellungsmaßnahmen hängt ganz von Ihrem Frühwarnsystem ab. Einer aktuellen Studie zufolge wird über die Hälfte der gemeldeten und analysierten Ransomware erst nach über einem Monat entdeckt. In den meisten Fällen haben Angreifer also wochenlang Zeit, um ihr Unwesen zu treiben. Sie können verhindern, ein Teil dieser Statistik zu werden.

Verringerung des Wiederherstellungsaufwands (und der Wiederherstellungszeit)

Selbst wenn Sie einen Angriff in weniger als einem Monat entdecken, wird wahrscheinlich viel Arbeit auf Sie zukommen. Je mehr Zeit bei einem Angriff vergeht, desto mehr Dateien werden verschlüsselt. Durch Frühwarnungen und schnelles Reagieren kann das Ausmaß der erforderlichen Wiederherstellungsarbeit erheblich reduziert werden. Wenn Sie nicht zu lange warten, bevor Sie etwas unternehmen, müssen Sie weniger Dateien wiederherstellen und können den Betrieb schneller wieder aufnehmen.

Methoden zur Erkennung von Angriffen

Ransomware-Software verhält sich anders als ein normales Programm. Dateien können zwar auch von anderen Anwendungen verschlüsselt werden, doch der Unterschied besteht darin, dass Ransomware viele Dateien innerhalb kurzer Zeit verschlüsselt. Ransomware-Angriffe fallen meist durch ungewöhnliche Verhaltensweisen oder bestimmte Veränderungen auf. In diesem Abschnitt werden zwei unterschiedliche Ansätze zur Erkennung von Ransomware-Angriffen vorgestellt.

Ransomware-Signaturen erkennen

Ein Ansatz zur Erkennung von Ransomware ist eine Erweiterung der allgemeinen Malware-Erkennung. Es ist nicht schwer, bekannte Malware zu erkennen, wenn man einen Teil des Codes eines ausführbaren Programms mit einer Datenbank von Codesignaturen vergleicht. Wenn Sie eine Übereinstimmung finden, haben Sie wahrscheinlich ein Malware-Programm gefunden. Der Vergleich von Ransomware-Signaturen funktioniert genauso. Dieser Ansatz hat jedoch den Nachteil, dass Sie Ihre Signaturdatenbanken stets auf dem neuesten Stand halten müssen,

da neue oder geringfügig modifizierte Ransomware sonst nicht erkannt wird. In diesem Fall wird man erst dann auf einen neuen Angriff aufmerksam, wenn jemand ihn meldet und seine Signatur der nächsten Version der Signaturdatenbank hinzugefügt wird.

WARNUNG

Der Signaturabgleich hat noch einen weiteren Nachteil. Da Ransomware immer intelligenter wird und sich schnell weiterentwickelt, gibt es immer wieder neue Signaturen.

Anomalien durch maschinelles Lernen erkennen

Ein weiterer Ansatz zur Erkennung von schädlichem Verhalten ist die Verwendung von Algorithmen des maschinellen Lernens (ML). Dabei werden das normale Verhalten und der Zustand des Dateisystems mit dem aktuellen Verhalten verglichen. ML-Algorithmen lernen, wie „normales" Verhalten aussieht, und machen auf Verhalten aufmerksam, das ungewöhnlich erscheint. ML-Algorithmen können laufende Prozesse und die von ihnen verwendeten Ressourcen untersuchen und ungewöhnliche Veränderungen am Dateisystem erkennen.

Rubrik Radar zum Beispiel ist eine Anwendung, die ML zur Analyse von Dateisystemänderungen verwendet. Radar untersucht die Art und Häufigkeit der Änderungen und erkennt Anzeichen von Verschlüsselung und Entropieänderungen. Darüber hinaus kann Radar als zusätzliche Intelligenzschicht Warnungen über ungewöhnliches Verhalten liefern.

TIPP

Ihre erste Verteidigungslinie sollte aus einer Reihe von Echtzeit-Erkennungs- und Überwachungsprogrammen bestehen, um verdächtige Änderungen frühzeitig zu erkennen.

Auf einen Angriff reagieren

Wenn ein Sicherheitsvorfall wie ein Ransomware-Angriff erkannt werden sollte, können Sie ganz einfach Ihrem Vorfallreaktionsplan folgen. Das setzt natürlich voraus, dass Sie einen Plan und ein geschultes Team haben, das diesen Plan umsetzen kann.

Das Notfallteam zusammenstellen

Sie müssen so zeitig wie möglich ein Notfallteam zusammenstellen und schulen, das bei einem Ransomware-Angriff für die Wiederherstellung verantwortlich ist. Dabei kann es sich um dasselbe Team handeln, das auch auf andere Sicherheitsvorfälle reagiert. Es muss jedoch spezielle Ransomware-Schulungen erhalten. Es ist entscheidend, dass Sie ein Team zusammenstellen, dieses Team schulen und dann den

Vorfallreaktionsplan testen lassen, damit Sie sicher sein können, dass es auf Ransomware-Angriffe vorbereitet ist.

Den Schaden eingrenzen und die betroffenen Dateien identifizieren

Sobald Sie Ihren Ransomware-Wiederherstellungsprozess eingeleitet haben, ist es an der Zeit, mit der Arbeit zu beginnen. Das Hauptziel besteht darin, den Angriff und weitere Schäden zu stoppen und anschließend alle betroffenen Computer und Dateien wieder in einen betriebsbereiten Zustand zu versetzen. In der ersten Phase des Wiederherstellungsprozesses geht es darum, den Schaden des Angriffs einzudämmen und sein Ausmaß zu bewerten.

Weitere Schäden verhindern

Das Notfallreaktionsteam sollte bereits eine gute Vorstellung davon haben, welche Computer an dem Angriff beteiligt sind. Die erste Maßnahme sollte darin bestehen, die Ransomware-Prozesse zu stoppen und alle betroffenen Computer herunterzufahren. Als Nächstes müssen Sie überprüfen, ob andere Computer aktiv an dem Angriff beteiligt sind, und diese ebenfalls herunterfahren.

Sie können die betroffenen Computer wieder in Betrieb nehmen, nachdem Sie sie von allen Netzwerken getrennt haben. So können Sie auf die Computer und Speichergeräte zugreifen, um die Ransomware zu entfernen.

Den Explosionsradius abschätzen

Sobald Sie den Angriff gestoppt haben, können Sie den Schaden abschätzen. Das Ausmaß des bereits entstandenen Schadens wird oft als Explosionsradius bezeichnet. Bei einem Ransomware-Angriff bezieht sich der Begriff Explosionsradius auf die Gesamtheit der Dateien, die bei dem Angriff verändert wurden. Die meisten Ransomware-Programme fügen jeder verschlüsselten Datei entweder eine Dateinamenerweiterung hinzu oder ändern diese, was die Identifizierung beschädigter Dateien letztendlich erleichtert. Einige Ransomware-Programme erstellen ein Verzeichnis, während sie Dateien verschlüsseln. In jedem Fall sollten Sie in der Lage sein, die Größe Ihres Explosionsradius zu bestimmen. Der Explosionsradius hängt mit der Angriffszeit zusammen – je länger Sie warten, desto größer der Schaden, den Sie bereinigen müssen.

Die Ermittlung des Explosionsradius bereitet Sie auf den nächsten Schritt vor – die Wiederherstellung. Wenn Sie sich gut auf einen Ransomware-Angriff vorbereitet und Ihre gesicherten Dateien geschützt haben, sollte die Wiederherstellung kein Problem sein.

IN DIESEM KAPITEL

- **einen Plan zum Erreichen der Wiederherstellungsziele aufstellen**
- **nur wiederherstellen, was Sie brauchen**
- **Geschwindigkeit und Zuverlässigkeit durch automatisierte Wiederherstellung**
- **mehrere Verteidigungsebenen für eine nahtlose Reaktion auf Ransomware-Angriffe**

Kapitel 5
Datenwiederherstellung mit chirurgischer Präzision

Sobald Sie einen Angriff erkannt, den Schaden eingegrenzt und die betroffenen Dateien identifiziert haben, ist es an der Zeit, Ihren Wiederherstellungsplan in Gang zu setzen. Ein guter Wiederherstellungsplan sorgt dafür, dass die Rückkehr zum normalen Betrieb so schnell und schmerzlos wie möglich erfolgt. Präzision und Geschwindigkeit sind für eine schnelle und zuverlässige Wiederherstellung von entscheidender Bedeutung. In diesem Kapitel erfahren Sie, wie Sie einen Wiederherstellungsplan für Ransomware erstellen, testen und umsetzen können, der Sie vor jeder Ransomware-Bedrohung schützt.

Einen Plan zur schnellen Wiederherstellung erstellen

Nach einem Ransomware-Angriff müssen Sie flexibel genug sein, um Dateien auf granulare Weise wiederherstellen zu können. Granulare Wiederherstellung bedeutet, dass Sie Kopien der von dem Ransomware-Angriff betroffenen und verschlüsselten Dateien zurückbekommen, ohne alle gesicherten Dateien wiederherstellen zu müssen. Sobald Sie wissen, welche Dateien Sie wiederherstellen müssen, sieht der Plan vor, die erforderlichen Schritte zur Wiederherstellung dieser Dateien auszuführen.

Datensicherung ist nur der erste Schritt

Eine gute Backup-Strategie ist die Grundlage für die Wiederherstellung nach einem Ransomware-Angriff. Der Plan sieht jedoch noch weitere Schritte vor. Backups, denen Sie vertrauen und die Sie zur Wiederherstellung nach einem Ransomware-Angriff verwenden können, müssen Unveränderlichkeit garantieren und für autorisierte Personen leicht zugänglich sein. Ihr Plan muss detaillierte und einfache Verfahren zur Wiederherstellung einer Liste von Dateien enthalten. Er sollte auch Leitlinien zur Entwicklung der Wiederherstellungsmaßnahmen und zur Einschätzung der für die Wiederherstellung erforderlichen Zeit bieten.

Einer der wichtigsten Bestandteile eines Wiederherstellungsplans sind seine Bewertungsanforderungen. Jeder Wiederherstellungsplan sollte Richtlinien zu den verwendeten Testmethoden und Häufigkeit der Tests enthalten.

TIPP

Verlassen Sie sich niemals auf einen ungetesteten Plan. Tests sollten in regelmäßigen Abständen und mit unterschiedlicher Intensität durchgeführt werden – vom einfachen Durchlesen des Plans bis hin zur vollständigen Wiederherstellung. Das Risiko nimmt zu, je näher Sie dem Testen eines vollständigen Ausfalls kommen. Planen Sie Ihre Tests daher sorgfältig, damit Sie kein allzu großes Risiko eingehen. Es ist nicht schwer, Dateien zunächst in einer Nicht-Produktionsumgebung wiederherzustellen, um die Tauglichkeit der Wiederherstellungsverfahren zu testen. Anschließend können Sie nicht-kritische Dateien in einer Produktionsumgebung wiederherstellen und einen vollständigen Wiederherstellungstest durchführen.

Die Wiederherstellungszeit ist entscheidend

Eine wichtige geschäftliche Anforderung, die jeder Wiederherstellungsplan erfüllen muss, ist die Einhaltung von Zielen in Bezug auf die Wiederherstellungszeit (Recovery Point Objective, RTO) des Unternehmens. Ihr Wiederherstellungsplan muss das Unternehmen innerhalb der angestrebten Wiederherstellungszeit (RTO) so wiederherstellen, dass ein bestimmter Wiederherstellungspunkt (Recovery Point Objective, RPO) erreicht wird. Der RPO definiert die Bedingungen, die erfüllt werden müssen, um CBFs wiederherzustellen und den normalen Betrieb fortzusetzen.

Ihr Wiederherstellungsplan muss also dafür sorgen, dass der Betrieb gemäß dem RPO wiederhergestellt wird, und zwar vor Ablauf der durch die RTO vorgegebenen Frist. Wenn der Wiederherstellungsprozess länger dauert als die RTO, werden Ihre Geschäftsprozesse beeinträchtigt. Betrachten Sie RPO und RTO als Grenzen, die festlegen, wie viel Sie tun sollten und wie lange die Wiederherstellung dauern darf. Wenn Sie mehr tun, als den RPO einzuhalten, laufen Sie fast immer Gefahr, die RTO zu überschreiten.

Nur das Nötige wiederherstellen

Viele Wiederherstellungspläne für Ransomware basieren auf der Wiederherstellung ganzer Computer. Ob Sie nun Virtualisierung und Kontrollpunkte oder ein vollständiges Backup-Image zur Wiederherstellung eines Computers verwenden – Sie greifen damit immer sehr weit. Bei einem Ransomware-Angriff werden nicht alle Dateien verschlüsselt. Deshalb sollten Sie zur Datenrettung auch nicht alle Dateien wiederherstellen. In diesem Abschnitt wird eine bessere Methode beschrieben, die Ihnen bei der Wiederherstellung Arbeit und Zeit spart.

Wissen, was Sie wirklich brauchen

Durch ein ungeschicktes Vorgehen bei der Wiederherstellung nach einem Ransomware-Angriff kann das Ausmaß des Schadens noch vergrößert werden. Sie müssen nur die von der Ransomware verschlüsselten Dateien wiederherstellen – warum sollten Sie sich also mit dem Rest befassen?

Bei normalen täglichen Geschäftsabläufen werden Daten routinemäßig geändert. Viele dieser Änderungen werden über mehrere Dateien, Datenbanken oder sogar Computer hinweg koordiniert. Jeder Prozess, der Datenänderungen überschreibt, indem eine frühere Version der Daten wiederhergestellt wird, macht die Änderungen effektiv „rückgängig". Wenn Sie Dateien wiederherstellen, die nicht von einem Ransomware-Angriff betroffen waren, können Sie Transaktionen verlieren oder es kann passieren, dass die Synchronität mit anderen Systemen nicht mehr gegeben ist.

Nehmen wir zum Beispiel an, Ihr Unternehmen verkauft Haustierartikel online. Bei einem Ransomware-Angriff werden zunächst Microsoft Word- und Adobe Acrobat-Dokumente auf Ihrem zur Auftragsabwicklung verwendeten Server verschlüsselt. Sie entdecken den Angriff erst nach einigen Stunden und befolgen ein veraltetes Wiederherstellungsverfahren. Das Notfallreaktionsteam fährt entsprechend diesem Plan die Computer herunter und setzt alles auf einen Zeitpunkt vor dem Angriff zurück. Anstatt nur die betroffenen Dateien wiederherzustellen, werden alle seit Beginn des Angriffs eingegangenen Bestellungen eliminiert und Bestellungen, die bereits an Ihre Versandabteilung geschickt wurden, sind nun verwaist. Ihre Rechnungsabteilung ärgert sich über das durch Ihre „Wiederherstellung" verursachte Chaos.

TIPP

Ein weitaus besserer Ansatz wäre es gewesen, einen mehrschichtigen Service wie die Wiederherstellungsdienste von Rubrik in einen Wiederherstellungsplan einzubinden, mit dem es einfach ist, nur das Benötigte wiederherzustellen.

Keine Zeitverschwendung

Wenn Sie nur das wiederherstellen, was Sie benötigen, vermeiden Sie nicht nur einen Wiederherstellungsprozess, bei dem zu viele Daten überschrieben werden. Der gesamte Vorgang ist auch schneller. Wenn Ihr Backup-Lösungsanbieter APIs offenlegt, um Ihnen die Wiederherstellung bestimmter Dateien zu erleichtern, lassen sich die benötigten Daten schnell und einfach wiederherstellen. Rubrik bietet Ihnen die Möglichkeit, die betroffenen Dateien zu identifizieren und nur diese Dateien aus einem vertrauenswürdigen, unveränderlichen Backup-Repository in einem Zustand vor dem Ransomware-Angriff wiederherzustellen.

Die Wiederherstellung im großen Umfang automatisieren

Der letzte entscheidende Schritt für einen reibungslosen Ransomware-Wiederherstellungsprozess ist die Fähigkeit, sich wiederholende und redundante Abläufe zu automatisieren. Wenn Sie 10.000 Dateien haben, die durch einen Angriff verschlüsselt worden sind, macht die Automatisierung des Wiederherstellungsprozesses für alle Dateien den Prozess zuverlässiger und schneller. In diesem Abschnitt erfahren Sie, wie Rubrik die schnelle und effektive Wiederherstellung von Dateien durch Automatisierung unterstützt.

APIs für die unbeaufsichtigte Wiederherstellung implementieren

Rubrik bietet APIs für den Zugriff und das Abrufen von Dateien aus seinem unveränderlichen Backup-Dateisystem. Die Rubrik-APIs bieten einen sicheren Zugriff auf Ihre Dateien, wann immer Sie ihn benötigen und durch jede Host-Sprache. Sie können Software für den Zugriff auf Ihre Dateien auch in Ihrer bevorzugten Sprache schreiben. Rubrik zwingt Ihnen keine unflexible Benutzeroberfläche als einzige Möglichkeit für den Zugriff auf Ihre Daten auf. Schließlich sind es Ihre Daten. Sie können auf sie zugreifen und dabei die flexiblen und sicheren APIs nutzen.

Scripting für hohe Leistung

Bei der Wiederherstellung nach einem Ransomware-Angriff sind die Rubrik-APIs für den Datenzugriff das Tüpfelchen auf dem „i". Sobald Sie eine Liste der Dateien identifiziert haben, die bei dem Ransomware-Angriff verschlüsselt wurden, können Sie zur Wiederherstellung ein Skript in Ihrer bevorzugten Skriptsprache schreiben. Für jede Datei in Ihrer Liste müssen Sie Ihre Backup-Daten lediglich mit der API von Rubrik abfragen, um die letzte Backup-Version vor dem Angriff zu finden, und dann zur Wiederherstellung eine andere API aufrufen. Ihre Skripte, die von den Systemen von Rubrik unterstützt werden, versetzen Ihr Unternehmen schnell und effizient wieder in einen betriebsbereiten Zustand.

Kapitel 6
Zehn Tipps zum Umgang mit Ransomware-Angriffen

Wer sich eingehend über Ransomware informiert hat, gewinnt oft den Eindruck, dass es extrem schwierig ist, einen Angriff zu überleben. Wenn Sie verstehen, wie Ransomware-Angriffe funktionieren, wie man sie vermeiden kann und wie man sich davon erholt, ist die Planung für den Notfall meist relativ einfach. Die folgende Liste enthält zehn hilfreiche Tipps zur Erstellung eines Plans, mit dem Sie Ransomware-Angriffe nicht nur überleben, sondern auch erfolgreich aus ihnen hervorgehen können.

- **Führen Sie Anwenderschulungen durch, um Ransomware-Angriffe zu verhindern.** Alle Anwender sollten in der Erkennung und Verhinderung gängiger Ransomware-Angriffe geschult werden. Richten Sie ein Verfahren zur Meldung verdächtiger Nachrichten oder Websites ein und schulen Sie die Anwender in der Erkennung und Meldung verdächtiger Vorfälle.
- **Verwenden Sie E-Mail-Filterung.** Mailserver bieten die Möglichkeit bzw. unterstützen Add-ons zur Filterung von E-Mail-Nachrichten und Anhängen, um verdächtige Inhalte zu blockieren. Bringen Sie in Erfahrung, wie Sie diese Funktion für Ihren Mailserver aktivieren und nutzen können.
- **Bestimmen Sie, welche Dateien geschäftskritisch sind.** Machen Sie eine Bestandsaufnahme der kritischen Geschäftsfunktionen Ihres Unternehmens und der Daten, die für jede dieser Funktionen benötigt werden. Erstellen Sie ein Verzeichnis der Dateien, die für die Aufrechterhaltung der Geschäftstätigkeit Ihres Unternehmens wichtig sind. Diese Liste von Dateien sollte den Schwerpunkt Ihrer Schutz- und Wiederherstellungsstrategie bilden.

- **Wählen Sie den richtigen Datensicherungsanbieter aus.** Wählen Sie einen Anbieter von Datensicherungsdiensten aus, der unveränderliche Backups und einen einfachen Zugriff auf unverschlüsselte Dateien über flexible und sichere APIs garantieren kann. Diese beiden Merkmale sind ein wesentlicher Bestandteil des Dienstleistungsangebots von Rubrik.
- **Sichern Sie kritische Dateien an einem unveränderlichen Speicherort.** Sichern Sie regelmäßig alle Dateien Ihres Verzeichnisses kritischer Dateien bei einem Sicherungsdienstleister, der Unveränderlichkeit garantiert, damit Ihre Sicherungskopien nicht durch Ransomware verschlüsselt werden können. Rubrik ist ein solcher Anbieter.
- **Entwickeln Sie einen Plan zur Wiederherstellung von Dateien.** Die Sicherung kritischer Dateien ist ein wichtiger erster Schritt. Sie müssen aber auch einen formellen Plan für die Wiederherstellung von Dateien entwickeln, falls eine Wiederherstellung erforderlich sein sollte. Dokumentieren Sie die Bedingungen, unter denen die Dateien wiederhergestellt werden sollten, wer die Wiederherstellung durchführen wird, wie die wiederherzustellenden Dateien identifiziert werden und wie die identifizierten Dateien wiederhergestellt werden.
- **Erstellen Sie Automatisierungsvorlagen für eine schnelle Wiederherstellung.** Sollte es erforderlich sein, Ihren Plan zu aktivieren, müssen Sie nichts weiter tun, als eine Liste der wiederherzustellenden Dateien bereitzustellen. Skriptvorlagen sollten in Ihren Plan einbezogen werden, damit Sie den Wiederherstellungsprozess für eine beliebige Liste von Dateien ausführen können. Mit Skriptvorlagen haben Sie auch die Möglichkeit, den Wiederherstellungsprozess mehrmals zu testen und eine Feinabstimmung des Prozesses vorzunehmen.
- **Testen Sie Ihren Plan häufig.** Neben einzelnen Skripten müssen Sie auch den gesamten Wiederherstellungsplan häufig testen. Ihr Plan ist nur dann tauglich, wenn er Ihre RPO- und RTO-Anforderungen erfüllen kann. Stellen Sie sicher, dass alle beteiligten Mitarbeiter mit ihren jeweiligen Rollen und dem Ablauf des Plans vertraut sind. Durch häufige Tests wird die Wirksamkeit des Plans in sich ändernden Umgebungen bestätigt und das Personal ist jederzeit auf dem neuesten Stand und einsatzbereit.
- **Überwachen Sie kritische Dateien auf verdächtige Änderungen.** Implementieren Sie Funktionen zur Überwachung der Dateiintegrität bei Produktionsdateisystemen, um verdächtige Änderungen zu erkennen, die auf Ransomware hindeuten können. Als zusätzliche Schutzmaßnahme sollten Sie eine ähnliche Überwachung für Backup-Speicherorte implementieren. Achten Sie auf nicht autorisierte Änderungen an Backups oder ungewöhnliche Änderungen an zuvor gesicherten Dateien und stellen Sie sicher, dass Ihr Sicherungsdienstleister Warnmeldungen für verdächtige Sicherungsänderungen ausgibt.
- **Schulen Sie ein Notfallteam und setzen Sie es im Ernstfall ein.** Stellen Sie ein Team von Mitarbeitern zusammen, das speziell darauf vorbereitet ist, auf vermutete Ransomware-Angriffe zu reagieren. Das Team sollte mit dem Wiederherstellungsplan und seinen klar definierten Rollen vertraut sein. Stellen Sie sicher, dass jedes Teammitglied an häufigen Tests teilnimmt, damit alle darauf vorbereitet sind, im Ernstfall angemessen zu reagieren.