LERNEN LEICHT GEMACHT

2. Sonderausgabe von Rubrik

Wiederherstellung nach einem Ransomware-Angriff

für dummies®
A Wiley Brand

- Ransomware frühzeitig erkennen
- Methoden zur schnellstmöglichen Wiederherstellung finden
- 10 Tipps zur Bekämpfung von Ransomware

Präsentiert von

rubrik

Michael G. Solomon

Über Rubrik

Rubrik ist ein Cybersicherheitsunternehmen, das es sich zum Ziel gesetzt hat, die Daten der Welt zu sichern. Mit Zero Trust Data Security™ hat Rubrik Pionierarbeit geleistet, um Unternehmen dabei zu helfen, sich vor Cyberangriffen, böswilligen Insidern und Betriebsunterbrechungen zu schützen. Die auf maschinellem Lernen basierende Rubrik Security Cloud bietet Datenschutz und Cyber-Resilienz auf einer einzigen Plattform für Unternehmens-, Cloud- und SaaS-Anwendungen. Die Plattform automatisiert die Verwaltung und Durchsetzung von Richtlinien zur Gewährleistung der Datensicherheit über den gesamten Lebenszyklus der Daten hinweg. Rubrik unterstützt Unternehmen dabei, die Integrität ihrer Daten aufrechtzuerhalten, Datenverfügbarkeit zu gewährleisten, Datenrisiken und -bedrohungen kontinuierlich zu überwachen und Unternehmensdaten wiederherzustellen, wenn die Infrastruktur angegriffen wurde.

Wiederherstellung nach einem Ransomware-Angriff

2. Sonderausgabe von Rubrik

Michael G. Solomon

für dummies®

Wiederherstellung nach einem Ransomware-Angriff für Dummies®, 2. Sonderausgabe von Rubrik

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

ISBN 978-1-394-21559-1 (pbk); ISBN 978-1-394-21560-7 (ebk)

Allgemeine Informationen zu unseren anderen 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 auf www.wiley.com/go/custompub. Für Informationen zur Lizenzierung der *Für Dummies*-Marke für Produkte oder Services 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: Traci Martin

Editorial Manager: Rev Mengle

Business Development Representative: William Hull

Production Editor: Mohammed Zafar

Inhaltsverzeichnis

Einführung

Dies ist *Wiederherstellung nach einem Ransomware-Angriff für Dummies* – Ihr Leitfaden zum Thema Ransomware und Wiederherstellung nach einem Angriff. Angriffe, bei denen Schadsoftware (so genannte Malware) eingesetzt wird, sind heute wesentlich mehr als 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, deren Name bereits auf ihr Verhalten schließen lässt. 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 ein gutes Backup-Image vorhanden ist, dauert die Wiederherstellung einer vollständigen Umgebung nicht nur lange, sondern kann auch dazu führen, dass viele Transaktionen 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 nach einem Ransomware-Angriff vor. Sie erfahren, welche Bedrohung Ransomware darstellt und wie Sie einen Wiederherstellungsplan erstellen , der sinnvoll ist und Ihr Unternehmen schützt.

Nachdem Sie sich mit den Grundlagen von Ransomware vertraut gemacht haben, erfahren Sie, wie Sie den richtigen Anbieter für Ihre Datensicherungslösung auswählen und welche Funktionen Sie benötigen, um sich gegen Ransomware zur Wehr zu setzen. Sie lernen außerdem, wie Sie die einzelnen Teile des Puzzles zusammensetzen, um einen effektiven Wiederherstellungsplan zu entwickeln. Abschließend

erhalten Sie einen Überblick über die zehn besten Tipps für den Aufbau eines effektiven Wiederherstellungsplans für Ransomware-Angriffe.

Leichtfertige Annahmen

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

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:

MERKEN

Dieses Symbol macht Sie auf Methoden zur schnelleren und einfacheren Erledigung von Aufgaben aufmerksam.

NICHT VERGESSEN

Dieses Symbol kennzeichnet Begriffe, die Sie sich merken sollten, und weist auf andere besonders wichtige Themen hin.

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 erschöpft. Innovative Unternehmen haben sich eingehend mit dem Problem befasst und einige interessante und effektive Lösungen entwickelt. Rubrik ist ein führender Anbieter von Lösungen zur Ransomware-Erkennung und -Wiederherstellung für Unternehmen jeder Größe. Weitere Informationen über die Angebote von Rubrik finden Sie unter `https://www.rubrik.com/de/products/ransomware-investigation`.

IN DIESEM KAPITEL

- Ransomware und ihre Auswirkungen auf die IT
- Beispiele von Ransomware-Angriffen
- Ransomware-Trends
- Schutzebenen zur Abwehr von Angriffen

Kapitel 1
Das Ransomware-Problem

Ransomware ist eine Art von Schadsoftware (Malware), die die Daten des Opfers verschlüsselt und diese erst nach Zahlung eines Lösegeldes wieder entschlüsselt. Ransomware ist eine der am schnellsten wachsenden und meistgefürchteten Formen von Malware. Bei einem erfolgreichen Ransomware-Angriff steht das Opfer vor einer wenig beneidenswerten 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

Traurige Berühmtheit erlangte Ransomware zunächst als eine Bedrohung persönlicher Daten. Die ersten Ransomware-Angriffe richteten sich hauptsächlich gegen Privatpersonen und nutzten die Tatsache, dass diese immer mehr persönliche Daten auf einer Vielzahl von Medien speicherten, um sie zu erpressen. Die Angst, private 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. Etwa die Hälfte der Unternehmen hatte hat laut einem Bericht von Rubrik Zero Labs im Jahr 2022 mit Ransomware-Angriffen zu kämpfen. Im Bericht „The State of Ransomware 2022" erwähnte das Cybersicherheitsunternehmen Sophos außerdem, dass 46 Prozent der Unternehmen, die von einem Ransomware-Angriff betroffen waren, das Lösegeld zahlten, zahlten, im Durchschnitt jedoch nur 61 Prozent ihrer Daten zurück erhielten. Leider gibt es keine Anzeichen dafür, dass Ransomware in nächster Zeit verschwinden wird. Stattdessen gehen Ransomware-Erpresser immer gezielter und raffinierter vor.

Angreifer haben erkannt, dass Unternehmen und wichtige Service-Anbieter oft eher bereit sind, hohe Lösegeldsummen zu zahlen als Privatpersonen, um ihre Geschäfte möglichst rasch wieder aufnehmen zu können. Die meisten Unternehmen sind heutzutage für ihre täglichen Betriebsabläufe auf Daten und Informationssysteme angewiesen. Wenn sie nicht mehr auf geschäftskritische Daten zugreifen können, kommt dies einer echten Katastrophe gleich. Zwar verfügen viele Unternehmen über Disaster-Recovery-Pläne, doch die meisten dieser Pläne beinhalten keine geeigneten Maßnahmen, die einen dauerhaften Verlust kritischer Betriebsdaten verhindern können. Unternehmen müssen daher wissen, wie sich Ransomware von anderen Bedrohungen unterscheidet, um katastrophale Störungen ihrer kritischen Geschäftsfunktionen zu vermeiden.

Wie sich Ransomware auf die IT auswirkt

Allgemein herrscht die Auffassung, dass man lediglich verhindern muss, einem Ransomware-Angriff zum Opfer zu fallen. Das hört sich in der Theorie zwar gut an, würde aber bedeuten, dass Ihr Unternehmen eine völlig sichere Umgebung erstellen müsste und sich niemand auch nur den kleinsten Fehler erlauben dürfte. Dieser Ansatz lässt sich in der Praxis nicht wirklich umsetzen. Selbst Unternehmen, deren Cybersicherheitsmaßnahmen besonders ausgereift sind, untersuchen ihre Umgebungen regelmäßig auf neue oder unentdeckte Schwachstellen. Schließlich ist ihnen bewusst, dass eine völlig abgesicherte Umgebung ein Ding der Unmöglichkeit ist.

NICHT VERGESSEN

Auch wenn Sie über die besten Sicherheitskontrollen verfügen, kann es passieren, dass Mitarbeiter Fehler machen und etwas anklicken, das sie nicht anklicken sollten und so Bedrohungen Tür und Tor öffnen.

Die eigentliche Frage, die sich hierbei stellt, ist folgende: „Wie können wir uns von einem Ransomware-Angriff erholen, wenn eine unserer Abwehrmaßnahmen versagt hat?“ Dieses Ziel lässt sich nur durch die Implementierung von Plänen erreichen, welche die Vermeidung und Bewertung von Angriffen *und* die Wiederherstellung danach beinhalten.

Ransomware-Angriffe in der Praxis

Bevor Sie erfahren, wie Sie sich am besten gegen Ransomware wappnen können, wollen wir uns ansehen, wie zwei reale Unternehmen auf diese Angriffe reagiert haben. Das eine wurde von dem Angriff überrascht, während sich das andere sorgfältig auf die Möglichkeit eines Angriffs vorbereitet hatte.

Das Aus für Lincoln

Lincoln College, eine Universität in Illinois, die überwiegend von afroamerikanischen Studierenden besucht wurde, musste ihre Pforten nach über 150 Jahren schließen. Knapp drei Monate lang hinderte ein Ransomware-Angriff deren Personal daran, wichtige Anwerbe- und Bindungsaktivitäten bzw. Spendenaktionen durchzuführen. Nachdem Lincoln College ein Lösegeld in Höhe von 100.000 US-Dollar bezahlt und seine Daten zurückerhalten hatte, konnte das Personal die verlorene Zeit nicht mehr wettmachen und nicht genügend Studenten anwerben oder finanzielle Mittel aufbringen. Der Ransomware-Angriff verhinderte, dass sich Lincoln College von COVID-19 und anderen Herausforderungen erholen konnte, was zur endgültigen Schließung der Institution führte.

WARNUNG

Wenn Sie eine Lösegeldforderung erhalten, sollten Sie die Zahlung mit allen Mitteln verhindern. Mit jedem gezahlten Lösegeld erhöht sich der Gewinn der Angreifer und das erlaubt ihnen, ihre kriminellen Machenschaften fortzusetzen. Wenn Sie Lösegeld zahlen, weisen Sie sich außerdem als leichtes Ziel für zukünftige Angriffe aus.

Ransomware konnte die Pläne von Payette nicht zunichte machen

Am Samstagmorgen erhielt der Leiter der IT-Abteilung von Payette den Anruf, den alle IT-Manager fürchten: Die Systeme sind ausgefallen. Das Architekturbüro Payette hatte über 40 TB an Plänen, Bildern und anderen Daten in seiner IT-Umgebung gespeichert. Wie sich herausstellte,

handelte es sich um einen Ransomware-Angriff. Der Leiter der IT bei Payette wusste, dass seine Mitarbeiter dank Netzwerksegmentierung, Backup-Prozessen und sorgfältiger sorgfältiger Planung derartiger Angriffe auf diese Situation vorbereitet waren. Ohne in Panik auszubrechen, reagierten die IT-Mitarbeiter bei Payette auf die frühzeitige Warnung, stoppten die Angriffe, stellten alle betroffenen Daten wieder her und waren in weniger als 24 Stunden wieder online. Die Planung und Vorbereitung ermöglichten es dem Unternehmen, alle Systeme komplett wiederherzustellen, noch bevor die Angreifer eine Lösegeldforderung stellen konnten.

Ransomware-Trends

Im Bereich Ransomware haben sich inzwischen einige Trends herauskristallisiert, und keiner davon ist gut. Trotzdem gibt es immer noch die Möglichkeit, den Angreifern ein paar Schritte voraus zu sein.

Hier sind einige aktuelle Ransomware-Trends:

- **Höhere Lösegeldbeträge:** Angreifer richten ihre Angriffe gegen eine geringere Anzahl von Zielen, verlangen aber deutlich höhere Lösegeldzahlungen.
- **Neue Commodity-Malware:** Cyberkriminelle müssen Malware nicht selbst schreiben, um Ransomware zu nutzen. Ransomware-as-a-Service (RaaS) erleichtert es ihnen, Ransomware-Angriffe zu starten.
- **Angriffe gegen Remote-Arbeitskräfte/Studierende:** Durch die steigende Anzahl an Remote-Mitarbeitenden und -Studierenden infolge der Corona-Pandemie konzentrieren sich Angreifer verstärkt auf Anbieter von Zusammenarbeits- und Schulungslösungen. Obwohl fast alle Einschränkungen in Verbindung mit COVID-19 gelockert oder aufgehoben wurden, wird immer noch gern auf Remote-Basis gearbeitet oder studiert.
- **Datenausschleusung:** Bei diesen Angriffen werden Daten nicht nur verschlüsselt, sondern manchmal auch Kopien von ihnen gestohlen. Diese Daten können dann gewinnbringend verkauft oder veröffentlicht werden, um den Ruf eines Unternehmens zu schädigen oder es einer Klage- oder Bußgeldwelle auszusetzen.
- **Ein zweiter Erpressungsversuch:** Cyberkriminelle nutzen ausgeschleuste Daten häufig auch dazu, um mehr Geld von ihren Opfern zu erpressen. In diesen Fällen versprechen sie oft, die Daten nur dann nicht zu veröffentlichen, wenn das Opfer ihnen eine bestimmte Geldsumme bezahlt.

- **Suche nach und Kompromittierung von Backups:** 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:** Größere Lösegeldforderungen, der einfache Zugriff auf Malware und bessere, zielgerichtetere Strategien haben dazu beigetragen, dass sich mehr Angreifer auf Cyberkriminalität spezialisieren.

Erhöhte Resilienz durch zusätzliche Verteidigungsebenen

Angesichts des Ausmaßes und der Raffiniertheit dieser Angriffe erscheint die Abwehr von Ransomware als gewaltige Aufgabe. 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 Verteidigungslinien zu durchbrechen. Eine typische Strategie ist der Aufbau mehrerer Verteidigungslinien, was im Bereich der Cybersicherheit auch als *Defense in Depth* bezeichnet wird. Das heißt im Grunde nur, dass sich zwischen Ihren Daten und dem Angreifer möglichst viele Kontrollebenen befinden sollten.

Viele sind der Meinung, dass Kontrollen zur Angriffsabwehr die besten Kontrollen sind. Natürlich ist die Abwehr von Angriffen der Idealfall. Verlassen Sie sich jedoch nicht darauf, dass jeder Angriff tatsächlich verhindert werden kann. Wenn Sie nicht mit einem erfolgreichen Angriff rechnen, werden Sie für den Ernstfall auch nicht ausreichend vorbereitet sein.

Präventive Kontrollen bilden die erste Verteidigungslinie, zu der Personalschulungen und Firewalls gehören. Mithilfe dieser Maßnahmen sollen die meisten Angriffe abgewehrt werden, bevor sie in der Umgebung überhaupt Fuß fassen können. Die meisten Malware-Angriffe, zu denen auch Ransomware-Angriffe zählen, beginnen mit einem Klick auf einen bösartigen Link. Firewalls können dabei helfen, offensichtlich verdächtigen verdächtigen Datenverkehr zu blockieren. Sie können aber autorisierte Benutzer nicht davon abhalten, auf diese Links zu klicken. Schulen Sie daher Ihr Personal darin, bösartige Nachrichten und Links zu erkennen.

Vorbeugung ist eine wichtige Strategie - aber letztlich ist niemand unfehlbar. Deshalb sollten Sie auch wissen, was zu tun ist, wenn Ransomware Ihre ersten Verteidigungslinien durchbricht. Wenn dies

geschieht, müssen Sie umgehend darüber darüber informiert werden, dass Ihre Systeme angegriffen werden. Eine starke Erkennungsebene wird Sie auf die Bedrohung aufmerksam machen und Ihnen helfen, Maßnahmen zu ergreifen, bevor es zu spät ist. Heutzutage kann Überwachungs- und Verhaltensanalysetechnologie Sie fast augenblicklich über einen laufenden Angriff informieren.

TIPP

Sie sollten über eine Echtzeit-Überwachungslösung für alle primären Kopien Ihrer kritischen Daten sowie über zusätzliche Informationen zu Ihren Backup-Daten verfügen, um eine letzte Verteidigungslinie zu schaffen.

Nachdem Sie die Bedrohung identifiziert haben, müssen Sie den Angriff stoppen und den entstandenen Schaden bewerten. Dies erreichen Sie, indem Sie unter Einhaltung bestimmter Verfahrensschritte die betroffenen Computer vom Netzwerk trennen und herunterfahren. Wenn Sie in einer kontrollierten Umgebung einen Neustart durchführen, sind Sie in der Lage, den Schaden zu beurteilen.

Die nächste Verteidigungsebene hängt von der Cybersicherheitslösung ab, die Sie implementiert haben. Sobald Sie die beschädigten Dateien identifiziert haben, können Sie Images davon aus Ihrem Backup abrufen, die eine Kopie der Version vor dem Angriff enthalten. Ihre Wiederherstellungslösung sollte es Ihnen leicht machen, bestimmte Datei-Images von einem bekannten Zeitpunkt vor dem Cyberangriff schnell wiederherzustellen.

Allerdings werden auch Ihre Backups ein Hauptziel für ausgeklügelte Ransomware-Angriffe sein. Die einzigen Backups, denen Sie vertrauen können, sind Backups mit Integritätsgarantie. Ihre Wiederherstellungslösung muss letztendlich auch 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 gegen Cyberangriffe zu verteidigen und sich im Ernstfall schnell zu erholen.

IN DIESEM KAPITEL

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

Kapitel 2
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 rasch wieder zu erholen. Wie im vorherigen Kapitel erläutert, benötigen Sie einen soliden Plan für den Umgang mit Ransomware-Angriffen. Das beste Szenario wäre natürlich, Angriffe von vornherein zu vermeiden, doch das ist leider nicht immer möglich. Zunächst müssen Sie die Art dieser Angriffe genau verstehen. Dann können Sie Maßnahmen zu ihrer Verhinderung ergreifen und, wenn ein Angriff doch erfolgreich sein sollte, diesen effektiv entschärfen. In diesem Kapitel erfahren Sie, welche Maßnahmen Sie zur Vermeidung von Ransomware-Angriffen ergreifen können.

Ransomware-Schwachstellen

Ransomware ist zwar ein ernstes Problem, aber keineswegs unbesiegbar. Wenn Sie die Funktionsweise von Ransomware verstehen, können Sie Verfahren und Kontrollmechanismen anwenden, die die meisten solcher Angriffe vereiteln. In diesem Abschnitt beleuchten wir einige vorhandene Schwachstellen und sehen uns an, wie Ransomware-Angreifer ihre Pläne in die Tat umsetzen.

Wie Ransomware Computer angreift

Ransomware hängt von der Fähigkeit ab, ein bösartiges Programm auf dem Computer eines Opfers auszuführen. Es gibt mehrere Möglichkeiten, um eine ausführbare Ransomware-Datei auf das Gerät eines Opfers zu bringen. Besonders häufig werden Benutzer dazu verleitet, einen schädlichen Link zu öffnen, eine bösartige Website aufzurufen oder ein infiziertes Gerät anzuschließen. Jede dieser Aktionen führt zum Herunterladen und Ausführen eines Schadprogramms, das den Ransomware-Angriff startet.

Wie Benutzer dazu gebracht werden, ihren Computer selbst zu infizieren

Computer werden am häufigsten mit Ransomware infiziert, weil ein Benutzer eine Aktion ausgelöst hat, durch die der bösartige Code ausgeführt werden kann. Die meisten Benutzer werden dies sicher nicht absichtlich tun. Es ist jedoch erstaunlich einfach, einen Benutzer dazu zu bringen, ahnungslos die schmutzige Arbeit für den Angreifer zu erledigen. Der Cyberkriminelle muss lediglich einen autorisierten Benutzer davon überzeugen, eine Handlung für eine nicht autorisierte Person auszuführen. Das nennt man Social Engineering.

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, dass sie eine oder mehrere dieser Motivationen ausnutzen können. Aus diesem Grund beginnen viele Ransomware-Infektionen damit, dass ein ahnungsloser Benutzer auf einen Link auf einer Website oder in einer E-Mail klickt, 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“).

Andere Tricks, um 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 besteht darin, infizierte USB-Sticks an Orten zu hinterlassen, an denen sie wahrscheinlich von Personen bemerkt werden. Steckt jemand den USB-Stick in einen Computer, wird die Ransomware kopiert und gestartet.

WARNUNG

Viele Arten von Angreifern nutzen den USB-Stick-Trick oder attraktive herunterladbare Dateien, um Malware einzuschleusen. Vertrauen Sie nicht blindlings einem Gerät oder einer Datei aus unbekannter Quelle, insbesondere wenn diese kostenlos angeboten werden.

Sensibilisierung der Benutzer, damit diese nicht 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 bei der Angriffsprävention. Wenn Benutzer darin geschult werden, potenzielle Angriffe zu erkennen und der Versuchung zu widerstehen, auf fragwürdige Links zu klicken, kann die Wahrscheinlichkeit eines erfolgreichen Angriffs erheblich verringert werden.

Sicherheitsschulungen sollten sich nicht ausschließlich damit befassen, was Anwender tun oder nicht tun 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.

NICHT VERGESSEN

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 müssen alle mithelfen.

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 relativ leicht zu erkennen. Bringen Sie Benutzern bei, auf die Grammatik zu achten (ist die Nachricht verständlich?), auf die Anrede (werden Sie mit ihrem Namen angesprochen?) und auf bestimmte Inhalte, die auf bösartige Nachrichten hindeuten können (enthält die Nachricht Details oder ist sie allgemein gehalten?). Benutzer, die genau wissen, worauf sie achten müssen, sind weniger empfänglich für Angriffe.

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 geben, bei der verdächtige E-Mail-Nachrichten, andere Medien oder verdächtige Verhaltensweisen gemeldet werden können. Richten Sie auch eine E-Mail-Adresse ein, an die Mitarbeiter verdächtige E-Mails weiterleiten können. Ihr Sicherheitspersonal sollte diese E-Mail-Adresse überwachen, alle gemeldeten Nachrichten prüfen und die Benutzer darüber informieren, ob die Nachricht bösartig war und woran sie das erkennen können.

Die Nachricht wiederholen

Es wäre schön, wenn sich die Teilnehmer von Sicherheitsschulungen immer an das Gelernte erinnern würden. Leider ist das oft nicht der Fall. Anwender vergessen oft, wie wichtig die Sicherheit für das Unternehmen ist, vielleicht, weil sie mit anderen Themen beschäftigt sind oder weil sie einfach nicht immer übervorsichtig sein wollen. Erfolgreiche Sicherheitsprogramme haben eine wichtige Gemeinsamkeit: 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 erfüllen können.

Bewährte Sicherheitsverfahren implementieren

Beim Erstellung eines Sicherheitsplans müssen Sie das Rad nicht neu erfinden. Etablierte Verfahren sind ein guter Ausgangspunkt. Glücklicherweise haben viele Unternehmen bereits 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 verstehen,wie Ransomware funktioniert, sind eher bereit, Richtlinien für das Online-Verhalten zu akzeptieren. 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 sie dem Absender nicht vertrauen
- generell keine unerwarteten Anhänge öffnen
- keinen in E-Mail-Nachrichten enthaltenen Links folgen
- nicht auf verdächtig aussehende Nachrichten reagieren
- verdächtige Nachrichten an das Sicherheitsteam weiterleiten
- nur Websites besuchen, denen sie vertrauen
- keine persönlichen Daten zur Verfügung stellen, es sei denn, sie vertrauen der Website und dem Grund, warum die Daten benötigt werden. Die Bereitstellung persönlicher Daten darf nur für Interaktionen erfolgen, die vom Benutzer selbst initiiert wurden.
- kein externes Gerät (z. B. einen USB-Stick) anschließen, wenn die Quelle nicht vertrauenswürdig ist
- immer ein virtuelles privates Netzwerk (VPN) verwenden, wenn sie sich von einem Remote-Standort aus verbinden
- dafür sorgen, dass ihre Software und das Betriebssystem gepatcht und auf dem neuesten Stand sind.

Wenn diese bewährten Verfahren befolgt werden, fällt es Angreifern schwer, erfolgreiche Ransomware-Angriffe zu starten.

Die IT-Umgebung stärken

Auch für IT- und Sicherheitspersonal gibt es etablierte 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 (VPN) 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, Angriffe soweit als möglich zu verhindern und sich auf die Wiederherstellung vorzubereiten, falls Sie doch einmal von einem Angriff betroffen sein sollten.

IN DIESEM KAPITEL

- Einen Wiederherstellungsplan erstellen
- Schutz der letzten Verteidigungslinie
- Das Konzept der Unveränderlichkeit
- Erholung nach einem Ransomware-Angriff

Kapitel 3
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 tatsächlich einmal Ziel eines Ransomware-Angriffs werden sollte.

Einen Wiederherstellungsplan entwickeln

Ohne Vorbereitung ist es sehr schwierig, wenn nicht gar unmöglich, sich von einem erfolgreichen Ransomware-Angriff zu erholen. Verlieren Sie jedoch nicht den Mut. Unternehmen, die genau wissen, wie man einen guten Plan erstellt, haben eine bessere Chance, sich nach einem Ransomware-Angriff schnell und ohne große Schwierigkeiten zu erholen, als jene, die einfach nur improvisieren.

Die Anforderungen ermitteln

Bei der Planung einer Überlebensstrategie für Ransomware-Angriffe müssen Sie sich zunächst einen Überblick darüber verschaffen, welche Daten und Prozesse für Ihr Unternehmen am wichtigsten sind. Ein

Business Impact Assessment (BIA) ist eine wichtige Maßnahme, bei der Sie Ihre kritischsten Prozesse und die ihnen zugrundeliegenden Ressourcen identifizieren. 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, haben Sie auch eine gute Vorstellung davon, 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 das Tagesgeschäft eines Einzelhändlers wohl kaum von kritischer Bedeutung ist.

Angreifer wollen in der Regel an die Daten gelangen, die für Sie den größten Wert haben – also die Daten, die Sie zur Ausführung Ihrer kritischen Geschäftsfunktionen benötigen. Die Wahrscheinlichkeit ist größer, dass Sie ein Lösegeld für Daten zahlen, die Sie zur Aufrechterhaltung Ihrer Geschäftstätigkeit benötigen.

Einen Wiederherstellungsplan erstellen

Sobald Sie wissen, 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. Ihr Plan stärkt die *Datenresilienz* (d.h. die Fähigkeit, nach einem Verlust wichtiger Primärdaten den Betrieb wieder aufzunehmen). In den 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 Wiederherstellungsplan beeinflussen oder von ihm betroffen sein können.

Den Plan testen

Sobald Sie Ihren Ransomware-Wiederherstellungsplan ausgearbeitet haben, müssen Sie ihn testen, um sicherzustellen, dass er auch wirklich funktioniert. Schließlich wollen Sie nicht Zeit und Mühe in die Entwicklung eines Plans zur Stärkung der Datenresilienz 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 verleiht Ihnen nicht die Fähigkeit, sich von einem Angriff zu erholen).

Es gibt unterschiedliche Arten von Tests, die Sie durchführen können. Jeder von ihnen kommt einem tatsächlichen Angriff jeweils ein Stück näher, damit Sie sich darauf verlassen können, dass Ihr Plan im Ernstfall funktioniert. Die meisten Unternehmen beginnen mit einem

Checklistentest. Dabei gehen die Beteiligten den Plan gemeinsam durch, um sicherzustellen, dass alle Maßnahmen 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 Angriff, bei dem Dateien tatsächlich verändert werden, um zu sehen, ob das Wiederherstellungsteam sie in einem brauchbaren Zustand wiederherstellen kann. Dieser Test ist natürlich mit Risiken verbunden, doch er ist zur Prüfung eines Wiederherstellungsplans am effektivsten.

Die letzte Verteidigungslinie 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 die meisten Backup-Strategien einem ähnlichen Ansatz folgen, ist es für Angreifer oft relativ einfach, Backup-Repositories zu finden und zu infizieren.

Zur Wiederherstellung von Dateien, die durch Ransomware verschlüsselt wurden, ist ein dreistufiges Verfahren erforderlich: 1) Den Angriff erkennen und stoppen. 2) Das Ausmaß des Schadens bestimmen. 3) Unverschlüsselte (unverfälschte) Versionen der beschädigten Dateien 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

Damit Ihre Daten widerstandsfähig sind, müssen Ihre Backups unveränderlich sein, d. h. sie können nach dem Schreiben nicht mehr verändert werden - auch nicht durch Ransomware. Wenn Sie unveränderliche Backups haben, verfügen Sie über ein perfektes Repository von Daten

aus der Zeit 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. Und auch Sicherheitsexperten wurde schnell klar, dass sie Protokollstrategien benötigen, damit ein Service einen Protokolldateieintrag zwar schreiben kann, aber niemals seine Änderung zulässt.

Rubrik ist ein Unternehmen, das unveränderliche Backups anbietet. Rubrik hat ein einzigartiges Dateisystem von Grund auf entwickelt, das alle von ihm erstellten Sicherungsdateien unveränderlich macht. Backups können direkt über die API (Application Programming Interface) von Rubik erstellt werden. Es ist nicht möglich, die Daten nach dem Schreiben zu ändern. Durch die Unveränderlichkeit des Dateisystems erhalten Sie die Gewissheit, über unveränderte Dateien zu verfügen, mit denen Sie sich schnell von einem Ransomware-Angriff erholen können.

Daten wiederherstellen

Bei einem Ransomware-Angriff müssen Sie zunächst herausfinden, welche Dateien betroffen sind, bevor Sie sie wiederherstellen können. Sie könnten zwar einfach alle Dateien wiederherstellen, doch das würde die Wiederherstellungszeit erheblich verlängern. Sie müssen die Ausfallzeiten minimieren, um die Geschäftskontinuität aufrechtzuerhalten. Dabei sollten Sie darauf achten, dass nur das wiederhergestellt wird, was für die Fortsetzung des Geschäftsbetriebs erforderlich ist.

Bei der Erstellung Ihres Wiederherstellungsplans haben Sie die mit den kritischen Geschäftsfunktionen Ihres Unternehmens verbundenen Daten identifiziert. Nun müssen Sie bestimmen, welche der kritischen Dateien verschlüsselt wurden.

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, müssen sie wiederhergestellt werden. In den nächsten beiden Kapiteln werden wir uns ansehen, wie man Bedrohungen erkennt, ihr Schadensausmaß bestimmt und eine Wiederherstellung durchführt.

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 Explosionsradius

Trotz aller Bemühungen kann es passieren, dass Kriminellen ein erfolgreicher Ransomware-Angriff gelingt. In diesem Kapitel erfahren Sie, wie Sie einen Ransomware-Angriff erkennen und 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. Um einen Angriff frühzeitig zu stoppen, müssen Sie in der Lage sein, Ihre Daten effektiv zu überwachen. Datenüberwachbarkeit bezieht sich auf die Fähigkeit, Daten auf Risiken zu überwachen und Kompromittierungsindikatoren zu erkennen, damit Sie schnell reagieren können.

Effektives Handeln durch Frühwarnungen

Wie bei jeder Art von Angriff haben Sie bei einer frühzeitigen Erkennung eine bessere Chance, den Schaden einzugrenzen und die Daten so schnell wie möglich wiederherzustellen. Wenn Sie frühzeitig eingreifen, kann der Angreifer nicht so viel Schaden anrichten und die „Aufräumarbeiten" sind weniger aufwändig.

Ob Sie bereits frühzeitig mit der Wiederherstellung beginnen können, hängt ganz von Ihrer Fähigkeit ab, verdächtige Veränderungen Ihrer Daten zu erkennen. Bei den jüngsten Ransomware-Angriffen betrug der Zeitraum zwischen dem Beginn des Angriffs und der Lösegeldforderung nicht mehr über einen Monat, sondern nur noch etwa drei Tage (siehe `https://venturebeat.com/security/ransomware-3-days/`). Dies deutet darauf hin, dass die Angreifer immer effizienter vorgehen.

Reduzierung des Wiederherstellungsaufwands

Selbst wenn Sie einen Angriff schon nach ein paar Tagen entdecken, wird wahrscheinlich viel Arbeit auf Sie zukommen. Jede Sekunde, die vergeht, gibt den Cyberkriminellen mehr Zeit zum Verschlüsseln von Dateien. Eine rechtzeitige Warnung und eine schnelle Reaktion können die Anzahl der wiederherzustellenden Dateien, den Umfang der Wiederherstellungsarbeiten und die Zeit bis zur Wiederaufnahme des Normalbetriebs drastisch reduzieren.

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. Ob ein Ransomware-Angriff erkannt wird, hängt nicht nur davon ab, wie gut Ihr Unternehmen seine Daten überwacht. Es muss auch in der Lage sein, ungewöhnliches Verhalten oder Änderungen an den Daten zu erkennen. Ihre Fähigkeit, Daten zu überwachen und mit Anomalien umzugehen, ist entscheidend für eine effektive Reaktion auf einen Ransomware-Angriff. 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 feststellen, 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 oder völlig erneuern 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 ständig 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 können sehr gut erlernen, wie „normale“ Verhaltensmuster aussehen und machen auf Verhaltensweisen bzw. Konfigurationen aufmerksam, die ungewöhnlich erscheinen. ML-Algorithmen können laufende Prozesse und die von ihnen verwendeten Ressourcen untersuchen und ungewöhnliche Veränderungen am Dateisystem erkennen.

Um an unser vorheriges Beispiel anzuknüpfen: Rubrik verwendet ML, um Dateisystemänderungen zu analysieren. Der Ransomware Monitoring & Investigation Service untersucht, wie sich die Daten verändern und wie schnell diese Veränderungen stattfinden. Außerdem wird nach Anzeichen für Verschlüsselungen und Änderungen der Datei-Entropie gesucht.

TIPP

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

Auf einen Angriff reagieren

Wird ein Sicherheitsvorfall, zum Beispiel ein Ransomware-Angriff, erkannt, können Sie ganz einfach Ihrem Reaktionsplan folgen.

Das Notfallteam zusammenstellen

Sie müssen die Mitglieder Ihres Reaktionsteams für Ransomware-Angriffe auswählen und schulen, bevor sie in der Lage sind, Ihr Unternehmen nach einem Angriff zu unterstützen. Dabei kann es sich um dasselbe Team handeln, das auch auf andere Sicherheitsvorfälle reagiert. Es muss jedoch spezielle Ransomware-Schulungen erhalten.

Den Schaden eingrenzen und die betroffenen Dateien identifizieren

In der ersten Phase des Wiederherstellungsprozesses geht es darum, den Angriff einzudämmen und sein Schadensausmaß zu bewerten.

Weitere Schäden verhindern

Das Reaktionsteam sollte bereits eine gute Vorstellung davon haben, welche Computer an dem Angriff beteiligt sind, wenn es die Protokolle der an die betroffenen Knoten gerichteten Netzwerkaktivitäten analysiert. Die erste Maßnahme sollte darin bestehen, die Ransomware-Prozesse zu stoppen und alle betroffenen Computer herunterzufahren.

Nachdem Sie die betroffenen Computer und Geräte von allen Netzwerken getrennt haben, können Sie mit der Beseitigung der Ransomware beginnen, ohne den Schaden auf andere Knoten zu übertragen.

Den Explosionsradius abschätzen

Das Ausmaß des bereits entstandenen Schadens wird oft als Explosionsradius bezeichnet. Der Begriff Explosionsradius bezieht sich auf die Gesamtheit der Dateien, die bei einem 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 eine Datei mit Metadaten, die die verschlüsselten Dateien beschreiben. 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 einen soliden, sorgfältig getesteten Ransomware-Plan haben, sollte die Wiederherstellung einfach sein.

IN DIESEM KAPITEL

- **einen Plan zum Erreichen der Wiederherstellungsziele aufstellen**
- **nur wiederherstellen, was Sie brauchen**
- **Geschwindigkeit und Zuverlässigkeit durch automatisierte Wiederherstellung**

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 Ihr Unternehmen nach einem Ransomware-Angriff wieder auf Kurs bringt.

Einen Plan zur schnellen Wiederherstellung erstellen

Ein effektiver Ransomware-Wiederherstellungsplan sollte Ihnen die Flexibilität bieten, Dateien auf granulare Weise wiederherzustellen, d. h. Sie sollten in der Lage sein, problemlos saubere Kopien der von dem Angriff betroffenen Dateien abzurufen, ohne alle gesicherten Dateien

wiederherstellen zu müssen. Sobald Sie wissen, welche Dateien Sie wiederherstellen müssen, können Sie die erforderlichen Schritte zur Wiederherstellung dieser Dateien ausführen.

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, da die Backups außerdem unveränderbar und leicht zugänglich sein müssen. Ihr Wiederherstellungsplan sollte auch detaillierte und einfache Verfahren zur Wiederherstellung von Daten und zum Testen des Plans selbst 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. Sie müssen also sorgfältig abwägen, wie Sie Ihren Wiederherstellungsplan testen, um kein übermäßiges Risiko einzugehen.

Die Wiederherstellungszeit ist entscheidend

Eine wichtige geschäftliche Anforderung jedes Wiederherstellungsplans ist die Erfüllung von Zielen in Bezug auf den Wiederherstellungspunkt (Recovery Point Objective, RPO) und die Wiederherstellungszeit (Recovery Point Objective, RTO) des Unternehmens. Das RPO ist die maximale Datenmenge, die Ihr Unternehmen verlieren kann, ohne dass kritische Geschäftsfunktionen ernsthaft beeinträchtigt werden. Das RPO wird in Zeiteinheiten gemessen. Wenn das RPO also 24 Stunden beträgt, entspricht die maximale Datenmenge, die verlorengehen kann, der Menge, die 24 Stunden vor einem Angriff oder Ausfall erstellt wurde. Das RTO ist die maximale Zeitspanne, die benötigt wird, um den normalen Betrieb nach einem Angriff oder Ausfall wiederherzustellen.

In Ihrem Wiederherstellungsplan muss detailliert beschrieben sein, wie das Unternehmen sein RPO innerhalb des RTO wiederherstellen kann. Wenn der Wiederherstellungsprozess länger dauert als die RTO, werden Ihre Geschäftsprozesse beeinträchtigt.

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. Ein

guter Plan zur Beseitigung von Bedrohungen ist selektiver. 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 dabei hilft, Mehrarbeit zu vermeiden und Zeit zu sparen.

Wissen, was Sie wirklich brauchen

Durch ein ungeschicktes Vorgehen bei der Wiederherstellung nach einem Ransomware-Angriff kann das Ausmaß des Schadens noch vergrößert werden. Im Rahmen der normalen täglichen Geschäftsabläufe werden routinemäßig Aktualisierungen und Änderungen an Daten vorgenommen. Viele dieser Änderungen werden über mehrere Dateien, Datenbanken oder sogar Computer hinweg koordiniert. Wenn Sie Opfer eines Ransomware-Angriffs geworden sind und eine umfassende Wiederherstellung durchführen, gehen alle Aktualisierungen verloren, die seit der Erstellung des Backups an den Daten vorgenommen wurden - selbst dann, wenn diese Daten nicht von dem Ransomware-Angriff betroffen waren. Dies kann dazu führen, dass Sie nicht mehr mit anderen Systemen synchronisiert sind oder wichtige Informationen verlieren, z. B. Transaktionsdaten.

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 diesem Plan entsprechend 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 Rubrik Data Remediation in Ihren Wiederherstellungsplan einzubinden, mit dem es einfacher ist, nur das Benötigte wiederherzustellen.

Sie vermeiden nicht nur einen Prozess bei dem zu viele Daten überschrieben werden, sondern können zudem die Daten, die Sie tatsächlich benötigen, schneller wiederherstellen - besonders dann, wenn der Anbieter Ihrer Backup-Lösung APIs zur Verfügung stellt, die Sie nutzen können.

Die Wiederherstellung im großen Umfang automatisieren

Der letzte 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, sorgt die Automatisierung für einen schnelleren und zuverlässigeren Wiederherstellungsprozess für alle Dateien. In diesem Abschnitt lernen Sie einige praktische Strategien zur schnellen und effektiven Wiederherstellung von Dateien durch Automatisierung kennen.

APIs für die unbeaufsichtigte Wiederherstellung implementieren

Die Verwendung von APIs ist eine effektive Methode, um schnell auf Dateien aus einem unveränderlichen Sicherungsdateisystem zuzugreifen und diese abzurufen. APIs können bei Bedarf über eine Vielzahl von Hostsprachen sicheren Zugriff auf Dateien bieten. Mit flexiblen APIs können Sie Software für den Zugriff auf Ihre Dateien in Ihrer bevorzugten Sprache schreiben. Der Vorteil effektiver APIs besteht darin, dass Sie eine unflexible Benutzeroberfläche umgehen und direkt auf die Daten zugreifen können. Es sind schließlich Ihre Daten und Sie sollten in der Lage sein, in jeder gewünschten Form auf sie zuzugreifen.

Skripting für hohe Leistung

Obwohl APIs häufig für den direkten Zugriff auf einzelne Dateien verwendet werden, kann durch das Einbetten dieser APIs in Skripte ein hoch performanter Zugriff auf mehrere Dateien erreicht werden. APIs für den Zugriff auf Daten, die von Skripten aus aufgerufen werden, sind das Sahnehäubchen bei der Wiederherstellung nach einem Ransomware-Angriff. 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 APIs Ihrer Wiederherstellungslösung unterstützt werden, versetzen Ihr Unternehmen schnell und effizient wieder in einen betriebsbereiten Zustand.

Eine gute Wiederherstellungslösung, wie die von Rubrik, die wir in diesem Buch als Beispiel verwendet haben, bietet effektive APIs, die den einfachen Zugriff auf bestimmte Dateien und deren Wiederherstellung schnell und in großem Umfang ermöglichen.

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 jedoch 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 sogar gestärkt 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 Benutzer in seiner Anwendung.
- **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.
- **Identifizieren Sie kritische Daten.** 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 Geschäftstätigkeit Ihres Unternehmens wichtig sind. Diese Liste von Daten sollte den Schwerpunkt Ihrer Schutz- und Wiederherstellungsstrategie bilden.
- **Wählen Sie den richtigen Datensicherungsanbieter aus.** Wählen Sie einen Anbieter von Datensicherungsdiensten, der unveränderliche

Backups und einen einfachen Zugriff auf unverschlüsselte Dateien über flexible und sichere APIs garantieren kann. Diese beiden Merkmale sind ein wesentlicher Bestandteil der Rubrik Security Cloud.

- **Sichern Sie Dateien an einem unveränderlichen Speicherort.** Sichern Sie regelmäßig alle Dateien in Ihrem Verzeichnis bei einem Sicherungsdienstleister, der Unveränderlichkeit garantiert, damit Ihre Sicherungskopien nicht durch Ransomware verschlüsselt werden können.
- **Erstellen Sie einen effektiven Wiederherstellungsplan.** Die Sicherung kritischer Daten ist zwar ein wichtiger erster Schritt, doch Sie müssen auch einen offiziellen Plan für die Wiederherstellung dieser Daten haben. Dokumentieren Sie die Bedingungen, unter denen die Dateien wiederhergestellt werden sollten, wer die Wiederherstellung durchführen wird, wie die wiederherzustellenden Dateien identifiziert werden und auf welche Weise die Wiederherstellung dieser Dateien erfolgen soll.
- **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 regelmäßigen Tests teilnimmt, damit alle darauf vorbereitet sind, im Ernstfall angemessen zu reagieren.
- **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. Ihr Plan sollte auch Skriptvorlagen enthalten 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 regelmäßig 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. Auch Ihre Backup-Standorte sollten überwacht werden. Achten Sie auf nicht autorisierte Änderungen an Backups oder ungewöhnliche Änderungen an zuvor gesicherten Dateien und stellen Sie sicher, dass Ihr Sicherungsdienstleister in solchen Fällen Warnmeldungen ausgibt.

Schnellere Erholung von Ransomware-Angriffen

Unternehmen sind auf Daten angewiesen. Cyberkriminelle sind sich dessen bewusst und werden immer besser darin, herkömmliche Infrastrukturen und Sicherheitssysteme zu durchdringen, wichtige Daten zu verschlüsseln und Lösegeld zu erpressen. Ransomware ist zu einer ernsthaften Bedrohung geworden. Mithilfe der in diesem Buch enthaltenen Anleitungen können Sie jedoch lernen, Ransomware erfolgreich zu bekämpfen. *Wiederherstellung nach einem Ransomware-Angriff für Dummies* zeigt Ihnen, wie Ransomware funktioniert, wie Sie sich darauf vorbereiten und nach einem Angriff schnell wieder erholen.

Der Inhalt ...

- Ransomware-Angriffe in der Praxis
- Bewährte Verfahren zur Verhinderung von Ransomware-Angriffen
- Erstellung eines zuverlässigen Wiederherstellungsplans
- Schnellstmögliche Wiederaufnahme des Geschäftsbetriebs

rubrik

Michael G. Solomon, PhD, ist ein Cybersicherheitsberater, der Kunden auf Führungsebene dabei hilft, Compliance-Anforderungen mit strategischen Zielen in Einklang zu bringen. Dr. Solomon ist Professor an der University of the Cumberlands und hält einen Doktortitel in Computerwissenschaften und Informatik von der Emory University.

ISBN: 978-1-394-21559-1
Nicht für den Wiederverkauf

für dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.