Innovations

LEARNING SERIES

FOUNDATION EDITION

Lessons Learned: Erholung nach einem Ransomware Angriff

Inhalt

- Ransomare-Angriffe werden immer vielfältiger
- Wissen Sie, wo Ihre Ransomware-Schwachstellen liegen?
- Wie Sie sicherstellen, dass Ihr Unternehmen einen Ransomware-Angriff überlebt

ActualTech Media | rubrik

Lesson learned: Erholung nach einem Ransomware Angriff

INHALTSVERZEICHNIS

Einführung: Die Zunahme der Ransomware-Angriffe 4

Die verschiedenen Arten von Ransomware-Angriffen 6

Bewährte Praktiken für die Wiederherstellung nach einem Ransomware-Angriff 8

Wiederherstellung schneller und einfacher ausführen 21

ActualTech Media

6650 Rivers Ave Ste 105 #22489 | North Charleston, SC 29406-4829

www.actualtechmedia.com

Danksagung des Herausgebers

EDITORIAL DIRECTOR
Keith Ward

DIRECTOR OF CONTENT DELIVERY
Wendy Hernandez

CREATIVE DIRECTOR
Olivia Thomson

SENIOR DIRECTOR OF CONTENT
Katie Mohr

PARTNER AND VP OF CONTENT
James Green

MIT SONDERBEITRÄGEN VON RUBRIK
Arushi Jain, Principal Product Marketing Manager
Damani Norman, Managing Technical Product Manager
James Knott, Senior Engagement Manager
Jonathan Hemming, Technical Director, Customer Success

Einführung: Die Zunahme der Ransomware-Angriffe

Da Unternehmen datengesteuerte Geschäftsmodelle einführen, um die Agilität zu erhöhen, sind Daten zu einem lukrativen Ziel für Cyberkriminelle geworden. Selbst in Gegenwart von robusten Verteidigungsmechanismen nehmen die Ransomware-Angriffe zu, indem sie erfolgreich die Daten zahlreicher Organisationen verschlüsseln. Gemäß dem *McAfee Labs Threat Report* von November 2020 gab es in der ersten Hälfte von 2020 etwa 2,5 Millionen neue Ransomware-Angriffe. Auch SafetyDetectives stellten fest, dass 54 % der mittelständischen und großen Unternehmen in den Vereinigten Staaten und 57 % in Großbritannien im vergangenen Jahr Opfer von Ransomware-Angriffen wurden (siehe **Abbildung 1**). Ransomware-Angriffe, die es auf Gesundheits- und medizinische Forschungsunternehmen abgesehen haben, vermehrten sich stark, denn die Cyberkriminellen wollten aus der COVID-19-Pandemie Profit schlagen. Schulen und Universitäten, die versuchten, ihren Studenten Fernlernmöglichkeiten zu bieten, wurden ebenfalls angegriffen.

DAS EINMALEINS

Eine erschütternde Statistik

Nach Angaben des OCR Cybersecurity Newsletters des US-Department of Health and Human Services im Herbst 2019 erwirtschaften Cyberkriminelle nach einer Schätzung des FBI mehr als 1 Milliarde US-Dollar an Lösegeld.

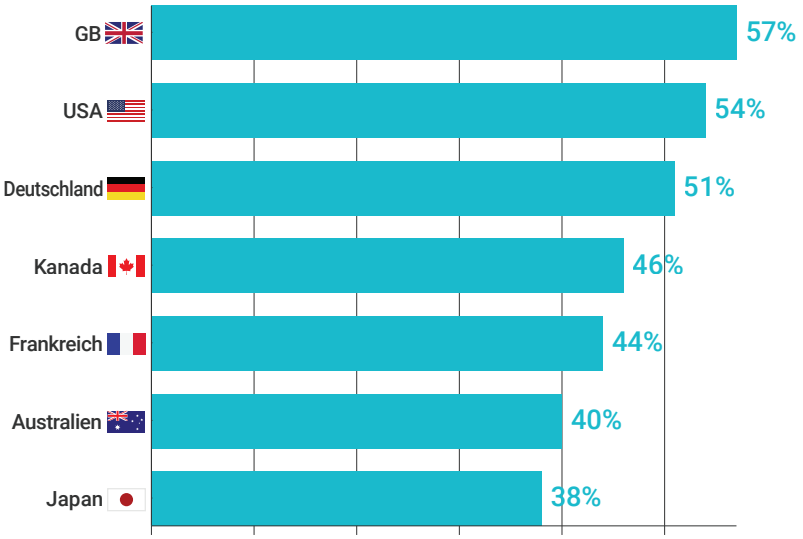

Abbildung 1: Der Anteil an Organisationen, die im letzten Jahr Ransomware-Angriffe in jedem Land gemeldet haben (Quelle: SafetyDetectives)

Die Ransomware-Seite der US-amerikanischen „Cybersecurity and Infrastructure Security Agency (CISA)“ US-CERT definiert Ransomware als:

Eine Art von bösartiger Software oder Malware, die den Zugriff auf ein Computersystem oder Daten verweigert, bis ein Lösegeld gezahlt wird. Ransomware verbreitet sich in der Regel über Phishing-E-Mails oder durch den unwissentlichen Besuch einer infizierten Website.

Die verschiedenen Arten von Ransomware-Angriffen

Das Konzept der Ransomware-Angriffe ist relativ einfach, denn sie zielen darauf ab, berechtigten Benutzern den Zugriff auf kritische Daten zu verweigern, in den meisten Fällen durch die Verschlüsselung der Daten, um dann ein Lösegeld zu verlangen (typischerweise in einer Kryptowährung wie z. B. Bitcoin). In der Vergangenheit waren die Lösegeldforderungen relativ niedrig, typischerweise Zehntausende von Dollar. Sie erhöhten sich jedoch rasch, wenn das Opfer die Zahlung verzögerte, um die Opfer zur Zahlung des Lösegelds zu nötigen. Der zunehmende Erfolg der Ransomware-Angriffe ließ die Lösegeldforderungen rasch auf Hunderttausende oder sogar mehrere Million Dollar ansteigen.

DEEP DIVE

Ransomware gibt es in vielen Formen

Ransomware gibt es in vielen Formen und verbreitet sich über eine Reihe von Angriffsvektoren, darunter:

- **Verschlüsselungs-Ransomware:** Verschlüsselt persönliche Dateien, Ordner und freigegebenen Netzwerkspeicher. Die anvisierten Dateien werden gelöscht, sobald sie verschlüsselt wurden, und Benutzer finden in der Regel eine Textdatei mit Anweisungen zur Lösegeldzahlung im selben Ordner wie die nun unzugänglichen Dateien.
- **Network-Attached Storage (NAS)-Ransomware:** Verschlüsselt und/oder löscht Dateien auf einem NAS-System, einschließlich

Home-Verzeichnissen, Hypervisor-Backups virtueller Maschinen (VM), Shadow-Volumes und Backup-Dateien.

- **Sperrbildschirm-Ransomware:** Sperrt den Computerbildschirm des Benutzers und verlangt eine Zahlung, aber es werden keine persönlichen Dateien verschlüsselt. Durch das Booten im abgesicherten Modus und das Entfernen des Sperrbildschirms mit Anti-Malware-Wiederherstellungstools ist die Wiederherstellung nach einem Sperrbildschirm-Ransomware-Angriff relativ einfach.
- **Hardwaresperre:** Ändert den Master-Boot-Record (MBR) des Computers, so dass der normale Bootvorgang unterbrochen wird und das Betriebssystem nicht mehr richtig starten kann. Die Wiederherstellung erfordert entweder die Reparatur des MBR oder die Wiederherstellung der Daten auf einem neuen System.
- **Anwendungs-/Webserver-Verschlüsselung:** Verschlüsselt Dateien und Webserver durch Sicherheitslücken in Anwendungen. Auf Webservern werden die Dateien index.php oder index.html durch Lösegeldanweisungen ersetzt. Die Wiederherstellung erfordert das Auffinden der infizierten Dateien und die Wiederherstellung ihres vorherigen Zustands.
- **Ransomware as a Service (RaaS):** Im Dark Web allseits erhältlich, ermöglicht RaaS praktisch jedem, ein Unternehmen mit Ransomware anzugreifen, die alle Aspekte des Angriffs verwaltet, einschließlich Zustellung, Infektion, Verschlüsselung, Zahlungseinzug und Entschlüsselung - und das alles gegen eine geringe Lizenzgebühr oder Provision.
- **Datenexfiltration:** Liest kritische Daten von den angegriffenen Systemen aus und kopiert sie auf die Angreiferseite. Diese Ransomware-Attacke wird oft mit anderen Angriffen kombiniert, die die kritischen Daten sperren.

Fortgeschrittene Ransomware hat es jetzt auf Backups abgesehen, indem sie verändert oder vollständig gelöscht werden und so die letzte Verteidigungslinie zunichte gemacht und die Chancen einer Lösegeldzahlung maximiert werden.

Bewährte Praktiken für die Wiederherstellung nach einem Ransomware-Angriff

Obwohl das FBI und andere Cybersicherheitsbehörden den Opfern dringend davon abraten, ein Lösegeld zu zahlen, um ihre Daten zurückzuerlangen, bezahlt etwa ein Viertel aller Opfer das Lösegeld, so gemäß von CrowdStrike und Sophos jüngst veröffentlichter Berichte. Aber es gibt keine Garantie, sein Geld zurück zu bekommen, und gemäß Sophos verdoppeln Opfer, die ein Lösegeld zahlen, ihre Kosten im Verlauf eines Ransomware-Angriffs von etwa 730.000 $ auf 1,4 Mio. $.

Die folgenden bewährten Praktiken helfen Ihnen dabei, sich auf einen Ransomware-Angriff vorzubereiten, ihn zu erkennen und erfolgreich daraus hervorzugehen, wenn Ihr Unternehmen davon betroffen ist (siehe **Abbildung 2**).

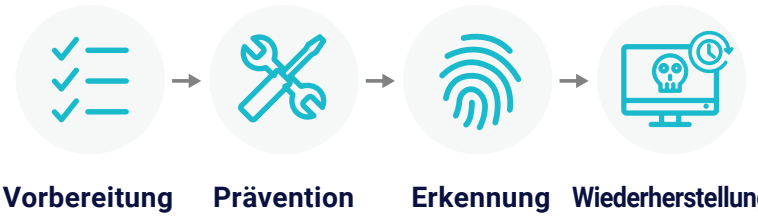

Abbildung 2: Die Ransomware-Abwehr umfasst Vorbereitung, Vorbeugung, Erkennung sowie die Anwendung bewährter Praktiken zur Antwort und Wiederherstellung

VORBEREITUNG

Sich die Zeit nehmen, um sich auf einen Ransomware-Angriff vorzubereiten, ist der Schlüssel zur erfolgreichen Wiederherstellung nach einem solchen Angriff: Einige bewährte Vorgehensweisen umfassen:

- **Erstellen Sie einen Plan:** Beginnen Sie mit der Entwicklung eines Ransomware-Reaktions- und Wiederherstellungsplans und eines unterstützenden Playbooks. Der Plan und das Playbook sollten regelmäßig überprüft und aktualisiert werden und an einem sicheren Ort aufbewahrt werden, der nicht von Ransomware angegriffen werden kann (z. B. eine gedruckte Kopie).
- **Identifizieren Sie Beteiligte und Mitglieder des Reaktionsteams:** Sie müssen die wichtigsten Stakeholder aus Management, IT, System-/Anwendungsteams und anderen Bereichen identifizieren und festlegen, wer für die Ausführung und Verwaltung des Plans für die Antwort auf den Angriff und die Wiederherstellung verantwortlich sein wird. Stellen Sie sicher, dass sich jeder seiner eigenen Verantwortung bewusst ist und weiß, wie die ihm zugewiesenen Aufgaben im Wiederherstellungsplan auszuführen sind.
- **Erstellen Sie einen Kommunikationsplan:** Die zeitnahe, genaue und gründliche interne Kommunikation innerhalb einer betroffenen Organisation ist entscheidend. Es müssen Kommunikationsmethoden identifiziert werden, die während eines Ransomware-Angriffs eingesetzt werden können. Firmen-E-Mails und Telefonanlagen können betroffen und nicht verfügbar sein. Es müssen alternative Kommunikationsmittel sowohl intern als auch mit externen Lieferanten, Vollzugsbehörden, Kunden und der breiten Öffentlichkeit bereitgestellt werden.

- **Legen Sie Prioritäten für die Systeme auf der Grundlage der Geschäftkritikalität fest:** Identifizierung der Kritikalität jedes Systems und seiner Daten für das Unternehmen. Die reibungslose und geordnete Wiederherstellung wird erleichtert, wenn man weiß, welche Systeme im Unternehmen zuerst Aufmerksamkeit benötigen und wie sie mit anderen Unternehmenssystemen interagieren. Stellen Sie auf der Grundlage des Kritikalitätsniveaus jedes Systems einen Wiederherstellungsplan auf, der identifiziert, welche Systeme in welcher Reihenfolge wiederhergestellt werden sollen.

- **Bewahren Sie Backups an einem sicheren Ort auf:** Bestimmen, wo Backup-Kopien sowohl vor Ort als auch Offsite gespeichert werden sollen. Lokale Kopien müssen auf einer unveränderlichen Speicherplattform aufbewahrt werden. Dadurch wird sichergestellt, dass Ihre Backup-Daten im Falle eines Ransomware-Angriffs nicht verschlüsselt oder verändert werden können, so dass Sie in der Lage sind, die ursprüngliche Situation schnell wiederherzustellen (siehe **Abbildung 3**). Remote-Kopien Ihrer Daten sind erforderlich, wenn Ihr Plan die Wiederherstellung an einem anderen Standort vorsieht. Besondere Aufmerksamkeit sollte der Art und Weise gewidmet werden, wie die Daten offsite gespeichert werden.

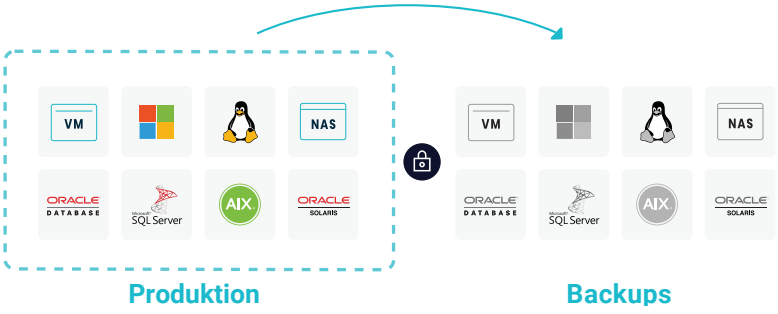

Abbildung 3: Unveränderliche Plattformen verhindern, dass Ransomware-Angriffe auf Online-Backup-Systeme und Daten zugreifen oder diese verschlüsseln können

In Offsite-Archiven gespeicherte Daten sind nicht vor Ransomware-Angriffen geschützt, da die Speicherplattform, auf der die Backups gespeichert sind, unveränderlich sein könnte. Darüber hinaus kann die Wiederherstellung von Offsite-Backups komplex und zeitaufwändig sein. Auf Cloud-Archive kann ebenfalls von außen zugegriffen werden, wenn sie nicht auf angemessene Weise gesichert sind. Verlässt man sich auf Archivstandorte, um die Wiederherstellung nach einem Ransomware-Angriff durchzuführen, müssen angemessene Maßnahmen getroffen werden, um diese Standorte zu sichern.

- **Testen Sie Ihre Wiederherstellungspläne regelmäßig:** Testen Sie die Datenwiederherstellung, um auf einen tatsächlichen Vorfall vorbereitet zu sein. Ohne Tests kann man sich nicht sicher sein, dass der Wiederherstellungsplan im Falle eines Angriffs funktioniert. Diese Tests verleihen dem für die Antwort und Wiederherstellung verantwortlichen Team die erforderliche Erfahrung und das Vertrauen, dass ein Angriff schnell und erfolgreich behoben werden kann. Die Tests müssen so realistisch wie möglich sein, ohne den Geschäftsablauf zu unterbrechen, und regelmässigen sowie unregelmässigen Abständen durchgeführt werden. Die Tests dienen auch dazu, auf das Unerwartete vorbereitet zu sein.

Obwohl das FBI und andere Cybersicherheitsbehörden den Opfern dringend davon abraten, ein Lösegeld zu zahlen, um ihre Daten zurückzuerlangen, bezahlt etwa ein Viertel aller Opfer das Lösegeld, so gemäß von CrowdStrike und Sophos jüngst veröffentlichter Berichte.

PRÄVENTION

Zu den bewährten Methoden zur Ransomware-Prävention gehören Schulungen zur Sensibilisierung der Endbenutzer, damit diese, die bösartigen Links, Email Anhänge und bösartigen Websites, die Ransomware verbreiten, erkennen können. Spam- und Phishing-E-Mails, schwache Passwörter und bösartige Websites sind die am verbreitesten Methoden für eine Ransomware-Infektion (siehe **Abbildung 4**). Die Schulung sollte interaktiv und ansprechend sein, ähnlich wie die Anti-Phishing-Schulungen, die viele Unternehmen heute anbieten. Zusätzliche Präventionsmaßnahmen umfassen das Aktualisieren und Patchen Ihrer Betriebssysteme und Anwendungen, das Aktivieren von Link- und Anhangsfiltern in E-Mails (wie Safe Links und Safe Attachments in Office 365). Darüber hinaus muss man sich vergewissern, dass Anti-Malware-Software auf allen Ihren Endgeräten installiert und auf dem neuesten Stand ist.

ERKENNUNG

Leider ist Prävention nicht immer möglich. Die Sicherheitsbranche erkennt zunehmend, dass eine effektive Cybersicherheit sowohl Präventions- als auch Erkennungs-/Reaktionsfunktionen erfordert. Für den Fall, dass Ransomware Ihre Präventionsbemühungen vereitelt, müssen Sie über die richtigen Prozesse und Tools verfügen, um Ransomware zu erkennen, bevor sie vollständig aktiviert wurde. Echtzeiterkennung und Warn-Tools stellen die erste Verteidigungslinie dar.

Spam- und Phishing-E-Mails, schwache Passwörter und bösartige Websites sind die am verbreitesten Methoden für eine Ransomware-Infektion.

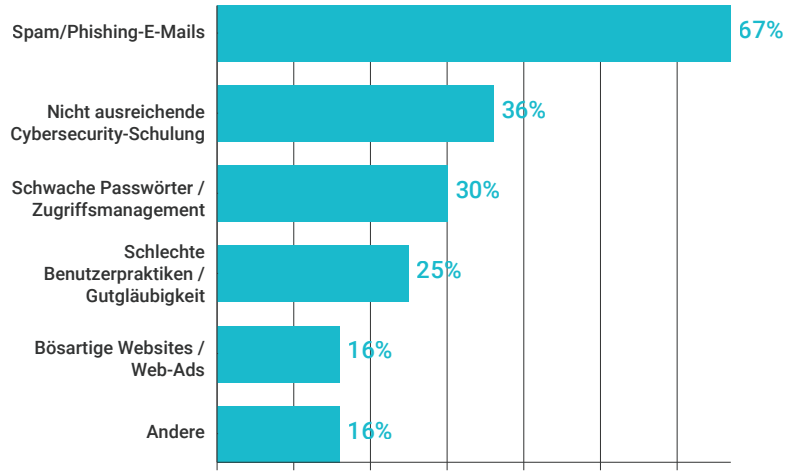

Abbildung 4: Häufige Methoden von Ransomware-Infektionen in Nordamerika (basierend auf MSPs, die Angriffe auf Unternehmen melden) (Quelle: SafetyDetectives)

Diese Tools müssen ebenfalls die Überwachung und die Analyse umfassen, um die Integrität und Verfügbarkeit ihrer letzten Verteidigungslinie – ihrer Backup Daten – zu gewährleisten. Einige bewährte Praktiken umfassen:

- **Angepassten Schutz der geschäftlichen Verpflichtungen:** Sicherstellen, dass alle Systeme und Daten auf eine Weise geschützt werden, die gewährleisten, dass so genannte Recovery Point Objektives (RPOs) und Recovery Time Objectives (RTOs) erreicht werden. Sorgen Sie außerdem für eine ausreichende

Für den Fall, dass Ransomware Ihre Präventionsbemühungen vereitelt, müssen Sie über die richtigen Prozesse und Tools verfügen, um Ransomware zu erkennen, bevor sie vollständig aktiviert wurde.

Datenhaltung für den Fall, dass eine Ransomware-Infektion erst nach Wochen oder Monaten entdeckt wird.

- **Identifizierung betroffener Daten auf granularer Ebene:** Implementierung von Tools, um auf Datei- oder Objektebene zu ermitteln, welche Daten mit Ransomware infiziert wurden (siehe **Abbildung 5**). Diese Daten während eines Angriffs zur Verfügung zu haben, ist von unschätzbarem Wert, um die Wiederherstellung zu beschleunigen und nicht infizierte Daten zu bewahren. Innovationen wie Machine Learning (ML) können trainiert werden, um Trends über alle Muster von Backup-Daten zu erkennen und neue Daten nach ihren Ähnlichkeiten ohne menschlichen Eingriff zu klassifizieren. Diese Analyse basiert zum großen Teil auf der Verhaltens- und Content-Analyse des Dateisystems anhand von Metadaten des Dateisystems. Es werden Eigenschaften wie unter anderem,

Abbildung 5: Tools, die die Auswirkungen eines Angriffs automatisch einschätzen und eindeutig identifizieren, welche Anwendungen und Dateien verschlüsselt wurden und wo sie sich befinden, ermöglichen eine schnellere Wiederherstellung auf granularer Ebene, die den Datenverlust minimiert.

die Anzahl hinzugefügter Dateien, die Anzahl gelöschter Dateien analysiert, um Ausreisserverhalten zu entdecken und diese, der IT- und den Sicherheitsteams zu melden. Sie kann ebenfalls als zusätzliche intelligente Schicht dienen um Anomalien in Backup-Daten, als letzte Verteidigungslinie, zu entdecken.

REAKTION UND WIEDERHERSTELLUNG

Sobald ein Ransomware-Angriff entdeckt wird, trägt die sofortige Benachrichtigung der Stakeholder und der Mitglieder des Reaktionsteams (einschließlich der Support-Anbieter) dazu bei, sicherzustellen, dass die richtigen Personen so schnell wie möglich eingeschaltet und mobilisiert werden. Die Beurteilung des Ausmaßes des Angriffs und die Isolierung aller Systeme, bei denen der Verdacht besteht, dass sie infiziert sind, ist der erste Schritt einer effektiven Reaktion. Stellen Sie einen Plan bereit, um infizierte Systeme zu isolieren und zu verhindern, dass die Ransomware sich weiter in Ihrem Netzwerk verbreiten kann. Stellen Sie außerdem einen Plan bereit, um infizierte Systeme und Daten, die von Ihrem Netzwerk getrennt wurden, wiederherzustellen. Kann die Ransomware nicht sicher neutralisiert werden, kann eine Wiederherstellung auf neuen Systemen in einem separaten Netzwerk erforderlich sein. Weitere bewährte Praktiken umfassen:

- **Die Bestimmung, welche Wiederherstellungsmethoden für die einzelnen Arten von Wiederherstellung verwendet werden sollen.** Optionen wie Live Mount für VMs von VMware bieten die Möglichkeit, die Systeme innerhalb weniger Minuten wiederherzustellen. Sie basieren jedoch auf dem Zurückrollen ganzer Systeme bis zu einem sicheren Zeitpunkt, wobei nicht

infizierte Daten verloren gehen können. Wiederherstellungen auf Datei- und Database-Ebene für infizierte Daten könnten eine bessere Option sein. Eine geeignete Methode muss im Vorfeld ermittelt werden, damit sie während eines Angriffs schnell bereitsteht.

- **Die Automatisierung nutzen, um Reaktionen zu beschleunigen und menschliche Fehler zu minimieren.** Ein Schlüsselfaktor während der Wiederherstellung ist die Automatisierung, da dadurch das Risiko menschlicher Fehler minimiert wird. Sie beschleunigt ebenfalls die Wiederherstellung und hilft bei der Nachverfolgung ihres Fortschritts. Der Anbieter Ihrer Backup- und Recovery-Software sollte über einen vollständigen Satz an APIs und SDKs verfügen, um die Automatisierung der Wiederherstellung zu unterstützen. Sie können mit Automatisierungs-Tools wie Ansible, Terraforma, Pupet, Chef, PowerShell und Python integriert werden. Sobald ein Recovery-Plan und die Priorisierung festgelegt sind, ist die Automatisierung der nächste Schritt, um eine solide Recovery-Kapazität aufzubauen.

Sobald Ransomware erkannt wurde, sollte der Ablauf von Snapshots sorgfältig überprüft werden, um sicherzustellen, dass keine gültigen Snapshots enden, was die Datenwiederherstellung beeinträchtigen würden. Service-Level-Agreements (SLAs) mit kurzfristigen Datenhaltungsrichtlinien sollten um mindestens ein Jahr für die Dauer des Ransomware-Vorfalls verlängert werden. Es sollte darauf geachtet werden, die ursprünglichen Aufbewahrungsfristen zu notieren, damit sie nach dem Ransomware-Vorfall zurückgesetzt werden können.

Bevor der Recovery-Prozess beginnt, muss man wissen, welche Art von Wiederherstellung erforderlich ist. Hat die Ransomware nur Dateien auf Servern oder Benutzerfreigaben auf einem NAS infiziert, kann eine dateibasierte Wiederherstellungsmethode verwendet werden. Hat die Ransomware jedoch die virtuellen Festplatten-Images für einen Hypervisor oder die MBR-Datensätze eines physischen Systems angegriffen, kann eine vollständige Systemwiederherstellung erforderlich sein. Bewährte Praktiken für die Wiederherstellung umfassen:

- **Bewährte Praktiken für eine allgemeine Wiederherstellung** (betrifft alle Wiederherstellungsszenarien):

Fragen Sie Ihren Anbieter, ob er Nahe-Null-RTOs für VMs, Dateifreigaben und Datenbanken liefern und eine sofortige Dateiwiederherstellung ohne Datenhydration durchführen kann.

  - *Sicher wiederherstellen:* Mit der Wiederherstellung nur dann beginnen, wenn die Ransomware neutralisiert ist. Das kann bedeuten, dass die Daten abgeschottet oder in neuen Systemen wiederhergestellt werden müssen. Die Wiederherstellung von Systemen oder Daten, bevor die Ransomware neutralisiert wurde, kann dazu führen, dass das System oder die Daten erneut infiziert werden. Kann die Ransomware nicht rechtzeitig isoliert und neutralisiert werden, besteht die Alternative darin, die Systeme abgeschottet dort wiederherzustellen, wo sie nicht erneut infiziert werden können.

- *Lokale isolierte Wiederherstellung:* Häufig sind Ransomware-Angriffe so tiefgreifend, dass eine Wiederherstellung an den ursprünglichen Speicherorten zu Sekundärinfektionen führt. Die Wiederherstellung in einer lokalen Umgebung, die von der infizierten Umgebung abgeschottet ist, ist der beste Weg, um eine Sekundärinfektion zu vermeiden. Die Planung während der Vorbereitungsphase (siehe oben) sollte die Identifizierung und das Testen der lokalen Wiederherstellung in einer abgeschotteten Umgebung umfassen.

- *Priorisierte Wiederherstellung:* Wie in der Präventionsphase geplant, erfolgt die Wiederherstellung auf der Grundlage der Priorisierung von Anwendungen und Geschäftsbereichen. Sicherstellen, dass grundlegende Dienste, die für die Basisfunktionalität erforderlich sind, wie DNS, DHCP und Authentifizierung, zuerst ausgeführt oder wiederhergestellt werden. Ohne diese grundlegenden Dienste könnten die wiederhergestellten Systeme möglicherweise nicht richtig funktionieren.

- **Best Practices für die reine Dateiwiederherstellung** (diese gelten für Szenarien, in denen nur Dateien und Verzeichnisse wiederhergestellt werden müssen):

  - *Überprüfung des Betriebssystems:* Überprüfen, ob das zugrunde liegende Betriebssystem vertrauenswürdig ist und nicht durch den Ransomware-Angriff kompromittiert wurde.

  - *Wiederherstellung auf einem „sauberen" System:* Wenn das ursprüngliche System nicht vertrauenswürdig

ist, die Dateien auf einem nachweislich guten System wiederherstellen. Dabei kann es sich um ein neu aufgebautes System handeln, das von der Produktionsumgebung abgeschottet ist.

- *Dateien für die Wiederherstellung identifizieren:* Anhand von automatisierten Tools die Dateien identifizieren, die von der Ransomware infiziert wurden, und diese wiederherstellen.

- **Best Practices für die Wiederherstellung von VMs und Datenbanken** (diese kommen zur Anwendung, wenn die VM selbst nicht verwendet werden kann, was passieren kann, wenn der NAS-Speicher, auf dem die VM läuft, kompromittiert wurde oder wenn die Ransomware die VM nicht mehr bootfähig macht). Sofortige Wiederherstellungsfunktionen sind nicht bei allen Anbietern üblich. Ein moderner Anbieter von Datensicherungslösungen wie Rubrik bietet diese Funktionen und ermöglicht schnelle und genaue Wiederherstellungen:

  - *Wiederherstellung kleinerer Datensätze:* Die Instant-Recovery-Fähigkeiten ermöglichen es, VMs und Datenbanken direkt aus dem Speicherort zu mounten, wodurch die Zeit eingespart wird, die für das Zurückkopieren von Backups in den Primärspeicher erforderlich wäre, bevor die Ressourcen verfügbar sind. Einmal gemountet, können VMs im Hintergrund zurück auf den Primärspeicher verschoben werden, während sie ihre regulären Dienste bereitstellen. Datenbanken können ausgeführt werden, bis eine Unterbrechung geplant werden kann, um die Datenbanken zurück in den Primärspeicher zu verschieben.

- *Direkt in den Primärspeicher exportieren:* Moderne Datensicherungslösungen verfügen über eine Exportfunktion, mit der eine VM oder Datenbank direkt im Primärspeicher wiederhergestellt oder kopiert werden kann. Nach dem Kopieren kann die VM oder Datenbank wieder online gestellt werden. Diese Methode bietet die schnellste Datenübertragungsleistung zurück zum Primärspeicher und ist am besten für die Wiederherstellung vieler VMs geeignet.

- *Mix von sofortiger Wiederherstellung und Export:* Sofortige Wiederherstellung und Export-Wiederherstellungs-Workloads können gemischt ausgeführt werden, dies sollte jedoch mit äußerster Vorsicht geschehen. Bei Exporten werden die gesamten Ressourcen des Speicher-Clusters genutzt, um Daten zurück in den Primärspeicher zu verschieben. Die sofortige Wiederherstellung kann mit dem Datenverkehr, der wiederhergestellt wird, in Konflikt kommen. Dies kann zu Leistungseinbußen der VMs und Datenbanken führen, die mit sofortiger Wiederherstellung wiederhergestellt wurden. Die gemischte Wiederherstellung von Workloads sollte von Fall zu Fall eingeschätzt werden.

- **Best Practices für die Wiederherstellung von Hypervisor-Managern** (die Wiederherstellung von vCentern oder anderen Hypervisoren mit dem entsprechenden Support-Team koordinieren, um eine reibungslose Wiederherstellung zu gewährleisten):

    - *vCenter-Wiederherstellung:* Vorsicht ist geboten, wenn ein vCenter wiederhergestellt werden muss oder wenn VMs in ein neues vCenter wiederhergestellt werden sollen.

Die Duplizierung oder Wiederverwendung der VMware Managed Object ID (MOID) kann zu Problemen bei der Wiederherstellung von VMs führen. Wenn das vCenter kompromittiert wurde, sollte es vorzugsweise aus dem Backup wiederhergestellt werden, anstatt ein neues leeres vCenter zu erstellen und die VMs in diesem wiederherzustellen.

- *Wiederherstellung und/oder Neuinstallation von Nicht-VSphere-Hypervisor-Managern:* Wenn Hypervisor-Manager wie der System Center Virtual Machine Manager (SCVMM) von Microsoft oder Nutanix Prism durch Snapshots geschützt werden, wenden Sie sich an Ihren Anbieter für Sicherungs- und Wiederherstellungsoptionen. Wenn der Hypervisor-Manager mit integrierten Backup-Methoden geschützt wird, sollten Sie sowohl den Hypervisor-Anbieter als auch Ihren Backup- und Recovery-Anbieter einschalten.

Wiederherstellung schneller und einfacher ausführen

Ransomware breitet sich immer weiter aus und kostet Unternehmen Millionen von Dollar. Darüber hinaus hat sie sich weiterentwickelt und ist raffinierter geworden. Ransomware blockiert nicht nur den Zugriff auf Systeme, sondern verschlüsselt oder löscht auch aktive Daten, einschließlich Backups auf anfälligen Systemen.

Wenn die Vorbeugung eines Ransomware-Angriffs fehlschlägt, ist ein unveränderliches Backup, das nicht gelöscht oder verschlüsselt werden kann, für die Wiederherstellung entscheidend. Wenn man die Möglichkeit hat, verschlüsselte Daten intelligent zu identifizieren und zu bereinigen, wird die Wiederherstellung einfacher und schneller und reduziert gleichzeitig Datenverluste und Ausfallzeiten.

Rubrik hilft Unternehmen, sich schneller von Ransomware-Angriffen zu erholen, mit innovativen Funktionen wie Rubrik Instant Recovery, Rubrik Radar für detaillierte Auswirkungsanalysen und Anomalieerkennung, und Rubrik Sonar für die Erkennung sensibler Daten. Erfahren Sie mehr unter https://rubrik.com/ransomware-recovery.

Über Rubrik

Rubrik hilft Unternehmen, die Datenkontrolle zu erlangen, um die Resilienz des Unternehmens, die Cloud-Mobilität und die Einhaltung gesetzlicher Vorschriften zu unterstützen. Rubrik überbrückt die Lücke zwischen eigener, lokaler Infrastruktur und der Cloud, indem es die Daten durch eine softwaredefinierte Struktur vom Rechenzentrum entkoppelt und eine einzige Verwaltungsebene für alle Daten bietet, ungeachtet dessen, ob sie sich vor Ort oder in der Cloud befinden. Umfassendes Datenmanagement wird durch sofortigen Zugriff, automatisierte Orchestrierung sowie Datenschutz und Resilienz der Enterprise-Klasse gewährleistet.

Über ActualTech Media

ActualTech Media ist ein B2B-Technologiemarketing-unternehmen, dass Lieferanten von Enterprise-IT-Lösungen durch innovative Lead-Generierungsprogramme und maßgeschneiderte Inhaltserstellungsservices mit Käufern verbindet.

Bei ActualTech Media verstehen wir, was IT-Unternehmens-kunden brauchen, da unsere Mitarbeiter selbst einmal Kunden für Enterprise-IT-Lösungen waren.

Unser Führungsteam besteht aus ehemaligen CIOs, IT-Managern, Architekten, Fachexperten und Marketingspezialisten, denen unsere Kunden nicht lange zu erklären brauchen, wozu ihre Technologie dient. Stattdessen können sie ihre Zeit für die Entwicklung von Strategien aufwenden, mit denen echte Ergebnisse erzielt werden.

Wenn Sie ein IT-Anbieter sind und Ihre eigene Gorilla Guide®-Ausgabe für Ihr Unternehmen erhalten möchten, besuchen Sie https://www.gorilla.guide/custom-solutions/