rubrik

E-BOOK

Wie entwickelt man einen Ransomware-Wiederherstellungsplan für Cyber-Resilienz?

INHALT

3 EINFÜHRUNG

4 AUSWAHL DER RICHTIGEN BACKUP- UND WIEDERHERSTELLUNGSLÖSUNG FÜR CYBER-RESILIENZ

- 4 Sofort-Wiederherstellung
- 5 Nativ unveränderliches Dateisystem
- 6 Granulare Wirkungsdiagnose
- 7 Mehrstufige Verteidigung mit zusätzlicher Erkennung

8 ZUSÄTZLICHE TECHNISCHE ANFORDERUNGEN AN EINE SICHERE ARCHITEKTUR

9 WICHTIGE ERKENNTNISSE AUS TATSÄCHLICHEN RANSOMWARE-ANGRIFFEN

10 CHECKLISTE ZUR WIEDERHERSTELLUNG NACH EINEM RANSOMWARE-ANGRIFF

12 HAFTUNGSAUSSCHLUSS

13 QUELLEN

Einführung

Da Unternehmen zunehmend datengesteuerte Geschäftsmodelle einführen, um ihre Agilität zu steigern, werden Cyberangriffe auf Daten immer lukrativer. Obwohl durchaus Abwehrmechanismen vorhanden sind, gibt es immer mehr Angriffe durch Ransomware, die erfolgreich die Daten von Organisationen verschlüsselt. Allein im ersten Quartal 2019 wuchs die Menge der Ransomware-Angriffe um 118 %, wobei auch neue Ransomware-Familien erkannt wurden.[1]

Backups sind eine wichtige, wenn nicht sogar die wichtigste, Verteidigungsmaßnahme gegen Ransomware. Aber wenn Ihre Backups nicht manipulationssicher sind, können sie selbst zur Schwachstelle werden. **Hochentwickelte Ransomware zielt jetzt auf Backups ab und modifiziert sie oder löscht sie vollständig. Dadurch gefährdet sie die letzte Verteidigungslinie für Daten und maximiert die Chancen auf Lösegeldzahlungen.** Obwohl vom Zahlen von Lösegeld abgeraten wird, nehmen Erpresser nach Schätzungen des FBI mehr als eine Milliarde Dollar ein.[2]

Warum zahlen Organisationen weiterhin Lösegeld, obwohl dies eine unzuverlässige Wiederherstellungsoption ist? Einfach deshalb, weil eine Wiederherstellung umständlich und zeitaufwändig sein kann – vorausgesetzt, sie verfügen überhaupt über Backups, von denen sie eine Wiederherstellung durchführen können. Außerdem können Unternehmen den Schaden oft schwer ermessen, sodass sie gezwungen sind, Massenwiederherstellungen ihrer gesamten Umgebung durchzuführen, anstatt nur die betroffenen Daten wiederherzustellen, was letztlich zu einem höheren Datenverlust führt.

Organisationen sollten nicht gezwungen sein, kostspielige Ausfallzeiten hinzunehmen, um kein Lösegeld zu zahlen. Stattdessen sollten sie sich darauf verlassen können, dass mit ihren Backups eine schnelle Wiederherstellung bei möglichst geringem Datenverlust und finanziellem Schaden möglich ist. Das Entwickeln und Testen eines überzeugenden Wiederherstellungsplans bereits vor einem möglichen Angriff sollte für IT-Organisationen oberste Priorität haben.

In diesem E-Book erfahren Sie, worauf Sie bei einer Backup- und Wiederherstellungslösung achten müssen und wie Sie einen effektiven Plan zur Wiederherstellung nach einem Ransomware-Angriff erstellen können, um sicherzustellen, dass Sie schnell auf einen Cyberangriff reagieren können, ohne Lösegeld zu zahlen.

118% **Zunahme der Ransomware-Angriffe (Q1 2019)***

Hochentwickelte Ransomware zielt jetzt auf Backup-Dateien ab

Das FBI schätzt, dass Cyberkriminelle mehr eine Milliarde Dollar an Lösegeld einnehmen**

Übertragung über eine Reihe von Mechanismen, beispielsweise Phishing-E-Mails und Exploit-Kits

* McAfee Labs Threats Report, August 2019
** OCR Cybersecurity Newsletter, Herbst 2019 – Ministerium für Gesundheitspflege und Soziale Dienste der Vereinigten Staaten

Auswahl der richtigen Backup- und Wiederherstellungslösung für Cyber-Resilienz

Die Wiederherstellung von Dateien aus einem Backup sollte Ihre sicherste und zuverlässigste Lösung für die Wiederherstellung nach einem Ransomware-Angriff sein. Wie bestimmen Sie, welcher Datenschutzanbieter Sie am besten auf einen Ransomware-Angriff vorbereitet? Es gibt zwar keinen Ansatz, der für alle ideal ist, aber es gibt wichtige Merkmale eines Plans zur Wiederherstellung nach einem Ransomware-Angriff, die alle Organisationen berücksichtigen sollten:

Sofort-Wiederherstellung

Das, was Opfern von Ransomware die größte Mühe abverlangt, ist die Wiederherstellung. Häufig verlassen sich Unternehmen auf komplexe, mehrstufige Wiederherstellungen, die fehleranfällig und ineffizient sind und letztlich zu längeren Ausfallzeiten führen. Je länger eine Wiederherstellung dauert, desto größer sind die Auswirkungen des Angriffs auf Umsatz, Mitarbeiterproduktivität und Kundentreue. Das gilt für jeden Sicherheitsvorfall, sei es Ransomware, eine Datenschutzverletzung durch Insider oder ein betrügerischer Mitarbeiter.

Eine wirksame Backup- und Wiederherstellungslösung sollte für eine schnelle und zuverlässige Notfallwiederherstellung ausgelegt sein. Selbst im Falle eines Sicherheitsverstoßes sollte es unabhängig davon, ob Sie eine vollständige oder eine partielle Systemwiederherstellung durchführen, einfach sein, die aktuellste saubere Version Ihrer Daten zu identifizieren und wiederherzustellen und Geschäftsschließungen oder den Ausfall kritischer Systeme zu vermeiden. Backup-Daten sollten sofort verfügbar sein und Ihnen eine sofortige Wiederherstellung ohne Nachbearbeitung ermöglichen. Außerdem ermöglicht eine Automatisierung über APIs eine größere Flexibilität bei der Wiederherstellung und kann die Suche und Wiederherstellung in großem Maßstab beschleunigen.

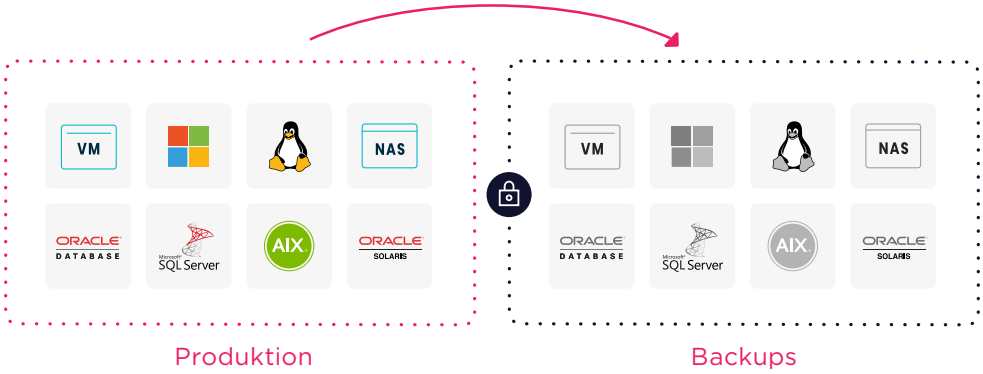
Wichtige Fragen an Anbieter

Können Sie RTOs von nahezu null für VMs, Dateifreigaben und Datenbanken bieten?

Können Sie eine sofortige Dateiwiederherstellung ohne Nachbesserungen bieten?

Nativ unveränderliches Dateisystem

Einer der Gründe, weshalb sich Unternehmen nicht von einem Ransomware-Angriff erholen können, ist, dass Backups beschädigt werden und IT-Teams gezwungen sind, entweder das Lösegeld zu zahlen oder eine Wiederherstellung von Offsite-Backups durchzuführen. Seien Sie vorsichtig bei Datenschutzanbietern, die Offsite-Backups als primäre Wiederherstellungsoption empfehlen. Diese Art der Wiederherstellung kann Wochen bis Monate dauern und ist oft mit Einschränkungen bei der Datenintegrität verbunden, was zu längeren RTOs führt. Zusätzlich raten einige Backup-Anbieter dazu, eine isolierte Wiederherstellung zu implementieren, um Ransomware-Angriffen zu begegnen. Dies ist zwar eine praktikable Option, aber die Implementierung ist mit einem hohen Kostenaufwand und einer komplexen Verwaltung verbunden, vergleichbar mit dem betrieblichen und finanziellen Aufwand einer DR-Infrastruktur.



Unveränderliche Dateisysteme verhindern, dass bei einem Angriff auf Daten zugegriffen oder diese verschlüsselt werden können.

Wie können Sie sicherstellen, dass Ihre Online-Backups nicht durch Ransomware gefährdet werden? Der beste und einfachste Weg ist die Auswahl eines Backup- und Wiederherstellungsanbieters, der alle Anwendungen und Daten in einem unveränderlichen Format speichert, was bedeutet, dass kein externer Client Daten lesen, ändern oder löschen kann, nachdem sie einmal erfasst wurden. Backup-Daten sollten zu keinem Zeitpunkt im Lese-/Schreibmodus für einen externen Client zugänglich sein, da sie dann von einem Angreifer manipuliert oder gelöscht werden können.

Wichtige Fragen an Anbieter

Wie können Sie garantieren, dass Ihre Backups nicht für Ransomware anfällig sind?

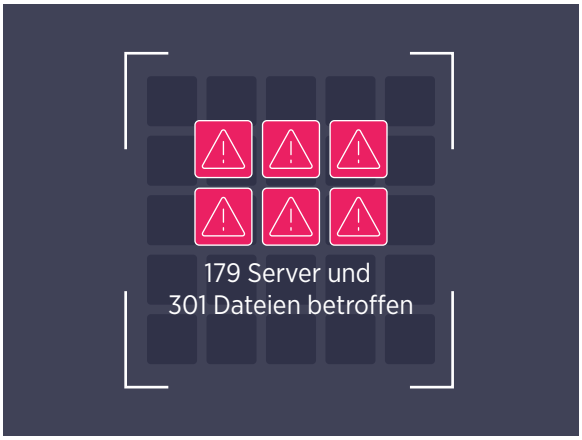
Speichern Sie Ihre Backups in nativen Formaten, die angreifbar sind?

Benötigen Sie einen offenen Lese-/Schreib-SMB- oder NFS-Share für Backup-Archive?

Verschlüsseln Sie jedes Backup und nehmen davon einen digitalen Fingerabdruck, um seine Integrität zu gewährleisten?

Granulare Wirkungsdiagnose

Die Datenwiederherstellung ist nur ein Teil der Systemwiederherstellung. Es ist in der Regel schwieriger, herauszufinden, *welche Anwendungen und Dateien wiederhergestellt werden müssen und wo sie sich befinden*. Um den Datenverlust durch einen Ransomware-Angriff zu minimieren, müssen IT-Teams in der Lage sein, die Auswirkungen eines solchen Angriffs schnell zu erkennen. Zum manuellen Verfahren zur Beurteilung des Schadensumfangs gehört in der Regel das Sichten von Millionen von Dateien, um das Ausmaß des Angriffs festzustellen. Dies kann Tage bis Wochen dauern, und die meisten Unternehmen greifen auf Massenwiederherstellungen der gesamten Umgebung zurück, einschließlich unbeschädigter Daten, um weitere Verzögerungen zu vermeiden.



Technologien, die dabei helfen, die Bewertung der Auswirkungen eines Angriffs zu automatisieren und sich einen klaren Überblick darüber zu verschaffen, welche Anwendungen und Dateien verschlüsselt wurden und wo sich diese befinden, ermöglichen IT-Teams eine schnelle Wiederherstellung auf einer genauer eingegrenzten Ebene. Dadurch wird das mit Massenwiederherstellungen verbundene Risiko von Datenverlusten minimiert.

Wichtige Fragen an Anbieter

Wird bei ungewöhnlichen Dateizugriffen und verschlüsselten Dateien automatisch ein Alarm ausgelöst?

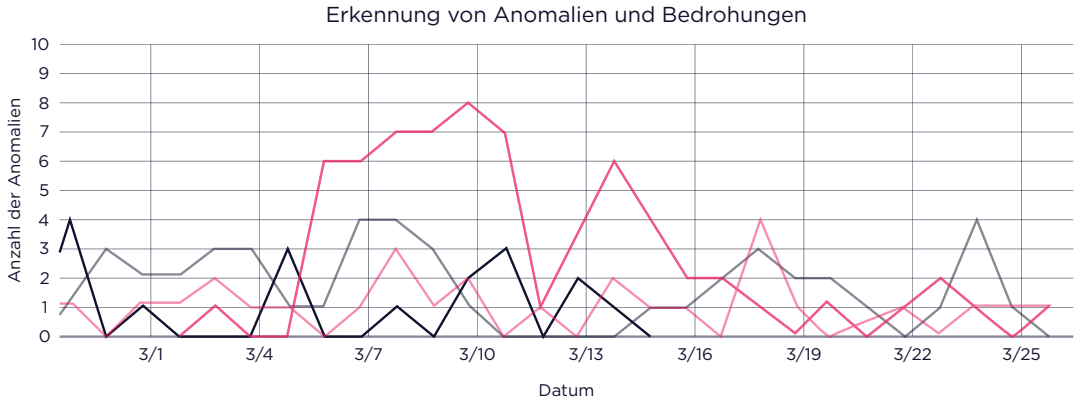
Sind Sie in der Lage aufzuzeigen, welche Dateien von einem Ransomware-Angriff betroffen sind?

Ermöglichen Sie die präzise Wiederherstellung auf Dateiebene ausschließlich von betroffenen Dateien und Daten?

Mehrstufige Verteidigung mit zusätzlicher Erkennung

Ransomware wird immer raffinierter, was bedeutet, dass Sie trotz der besten Präventionsmaßnahmen immer noch verwundbar sein können. Laut dem Verizon Data Breach Investigations Report 2019 (DBIR) dauerte es bei 56 % der analysierten Datenschutzverletzungen Monate oder noch länger, bis sie erkannt wurden.[3] Eine verzögerte Erkennung kann sich direkt auf die Integrität von Backup- und Wiederherstellungsdaten auswirken.

Moderne Technologien, die sich Modelle des maschinellen Lernens zunutze machen, können dazu beitragen, Sicherheitsbedrohungen anhand einer gründlichen Analyse von Dateisystemen und Inhaltsverhalten zu erkennen. Backups enthalten umfangreiche Metadaten, die sicher analysiert werden können, um mit ML-basierten Technologien als letzte Verteidigungslinie zur Ergänzung Ihrer Echtzeit-Erkennungs- und Präventionswerkzeuge anomale Aktivitäten zu erkennen und Warnmeldungen zu generieren. Wenn ungewöhnliches Verhalten, beispielsweise Ransomware, entdeckt wird, sollten IT-Teams sofort alarmiert werden, um Wiederherstellungsoptionen zu untersuchen und bei Bedarf eine schnelle Wiederherstellung durchzuführen.



Manche Anbieter verwenden eine signaturbasierte Erkennung, die Muster und Sequenzen mit einem System bekannter Malware-Varianten abgleicht. Dieser Ansatz ist jedoch nicht immer effektiv, da Ransomware leicht mutieren kann. Außerdem ist die signaturbasierte Erkennung nur anwendbar, wenn Sie nicht das erste Opfer sind. Die meisten Ransomware-Angriffe verwenden Morphing und Code-Verschleierung mit einer Zero-Day-Signatur, sodass die signaturbasierte Erkennung erst nach dem ersten erfolgreichen Angriff eingesetzt werden kann. Ein besserer Ansatz besteht darin, einen Anbieter auszuwählen, der eine verhaltensbasierte Erkennung anwendet, die selbst Zero-Day-Ransomware-Angriffe erkennt

Wichtige Fragen an Anbieter

Welche Methode wenden Sie zur Erkennung von Ransomware-Angriffen an?

Nutzt Ihre Plattform ML-basierte Technologien?

Zusätzliche technische Anforderungen an eine sichere Architektur

Um einen angemessenen Schutz vor Ransomware sicherzustellen, sind strenge Sicherheitskontrollen bei den besten Anbietern von Backup- und Wiederherstellungslösungen ein fester Bestandteil des Designs. Folgendes sind einige technische Anforderungen bei der Bewertung der zugrunde liegenden Architektur:

- Es kann ausschließlich der Anbieter zur Durchführung von Lese-/Schreiboperationen auf das Dateisystem zugreifen, niemals ein externer Client.
- Der Anbieter stellt keine Standard-Speicherprotokolle wie NFS oder SMB für die Interaktion mit dem Dateisystem bereit.
- Der Anbieter gewährt externen Clients keinen Lesezugriff auf Daten in nativem Format.
- Der Anbieter führt Backup-Validierungsprüfungen durch, um sicherzustellen, dass die Backup-Daten niemals geändert werden. Dadurch wird sichergestellt, dass Sie nur genau das wiederherstellen, was in der Originalkopie enthalten war.
- Das Dateisystem ist nativ unveränderlich und erfordert keine Benutzerkonfiguration oder Verwaltung.

Wichtige Erkenntnisse aus tatsächlichen Ransomware-Angriffen

Die folgenden Berichte sind reale Beispiele dafür, wie unterschiedliche Organisationen auf Ransomware-Angriffe reagiert haben. Daraus lassen sich Erkenntnisse darüber ableiten, was eine wirksame Strategie ausmacht.

Kern Medical Center stellt schnell 100 % seiner geschützten Systeme wieder her

Das Kern Medical Center, eine führende Gesundheitsorganisation im Central Valley, wurde im Juni 2019 von Ransomware angegriffen, die in ihre Umgebung eindrang und begann, Produktionsdaten zu verschlüsseln und damit unbrauchbar zu machen. Der Angriff wurde nach einer Stunde entdeckt, als Benutzer meldeten, dass sie nicht auf ihre Systeme zugreifen konnten. Dank Rubrik war das Kern Medical Center in der Lage, 100 % der betroffenen Systeme innerhalb von Minuten wiederherzustellen, einschließlich ihres geschäftskritischen elektronischen Patientendatensystems. Nach dem Angriff verlagerte das Kern Medical Center mehr von seinen Altsystemen zu Rubrik, um sich vor möglichen zukünftigen Angriffen zu schützen, und nannte unveränderliche Backups als Hauptgrund für diese Entscheidung.

ASL Airlines France entwickelt eine mehrstufige Strategie zur Verteidigung gegen Ransomware

ASL Airlines France, eine Fracht- und Passagierfluggesellschaft mit Sitz in Tremblay-en-France im Bâtiment Le Séquoia, ist in einer Branche tätig, die in hohem Maße von Ransomware-Angriffen betroffen ist. Aufgrund dieses hohen Risikos ist es für ASL und andere Fluggesellschaften unglaublich schwierig, eine Cyber-Versicherung abzuschließen. Das Unternehmen nutzte die mehrstufige Verteidigung von Rubrik, um die Erkennung von Cyberangriffen zu beschleunigen, eine detaillierte Folgenabschätzung zu erhalten und die Wiederherstellung nach einem Ransomware-Angriff zu vereinfachen. Mit dieser Lösung kann ASL Airlines eine Cyber-Versicherung abschließen, um das Unternehmen proaktiv vor Cyberattacken zu schützen.

Die Stadt Durham kann dank nativ unveränderlicher Backups eine schnelle Wiederherstellung durchführen

Die Stadt Durham stellte am Freitag, dem 6. März, einen Ransomware-Angriff fest und die Stadtverwaltung verdankte ihre schnelle Reaktion der Backup-Lösung von Rubrik. Dank der integrierten Unveränderlichkeit von Rubrik konnten die Behörden wichtige städtische Dienstleistungen, einschließlich des Notrufzugriffs, schnell wiederherstellen. Darüber hinaus betonte Kerry Goode, CIO von Durham, dass die wichtigsten Geschäftssysteme, einschließlich der Systeme zur Verwaltung der Gehaltsabrechnungen, zu Beginn der Geschäftswoche wieder online waren.

> **„Die Stadt kann sich darauf verlassen, dass unsere Backups sehr gut sind, weil sie unveränderlich sind. Daher konnten sie nicht durch Ransomware beschädigt werden.“**
>
> **Kerry Goode**
> CIO der Stadt Durham

Checkliste zur Wiederherstellung nach einem Ransomware-Angriff

Die Fähigkeit, die Auswirkungen eines Cyberangriffs schnell zu erkennen und sich davon zu erholen, ist das Ziel jedes Ransomware-Wiederherstellungsplans. Um eine schnelle Wiederherstellung zu ermöglichen und sicherzustellen, dass Geschäftsziele auch nach einem Angriff noch erreicht werden, müssen IT-Teams ihre Reaktionsstrategie planen und rigoros testen.

Im Folgenden werden Schritte genannt, die für den Fall empfohlen werden, dass Sie von Ransomware angegriffen wurden:

- ☐ **Isolieren Sie das infizierte Gerät vom Netzwerk.**
  Der Erfolg eines Ransomware-Angriffs hängt davon ab, wie schnell sich die Ransomware in Ihrem Netzwerk verbreiten kann. Eine schnelle Reaktion kann die Auswirkungen auf Ihre Organisation stark eindämmen und eine Ausbreitung der Infektion verhindern. Um die Infektion zu isolieren, fahren Sie sofort alle betroffenen Geräte herunter und trennen Sie sie vom Netzwerk und allen gemeinsam genutzten Speichern. Schalten Sie alle Geräte ab, die noch nicht infiziert wurden, um den Schaden einzudämmen.

- ☐ **Stellen Sie sicher, dass die Backups nicht beschädigt wurden.**
  Ransomware wird immer raffinierter, wodurch die Integrität von Backups zunehmend gefährdet wird. Damit Ihre Backups geschützt sind, müssen Backup-Daten unveränderlich sein. Das bedeutet, dass einmal geschriebene Daten niemals im Lese-/Schreibmodus für externe Clients verfügbar sind und von einem Angreifer in Ihrem Netzwerk weder gelesen noch geändert oder gelöscht werden können. Dies ist die einzige Möglichkeit, eine Wiederherstellung bei Beschädigung von Produktionssystemen sicherzustellen.

  Außerdem sollten Sie etwaige Backup-Prozesse anhalten, bis Sie wissen, wo die Infektion begann, alle sicherheitsforensischen Untersuchungen abgeschlossen haben und die aktuellsten sauberen Snapshots endgültig identifiziert haben.

- ☐ **Identifizieren Sie die Infektion.**
  Es ist absolut notwendig, zu wissen, wie weit die Infektion verbreitet ist, um sie einzudämmen. Ein Ansatzpunkt besteht darin, zu ermitteln, worauf der erste infizierte Computer zugegriffen hat. Eine weitere Möglichkeit ist die Überprüfung der Ransomware-Registry, in der alle verschlüsselten Dateien aufgelistet sind, sodass die Software weiß, welche Dateien nach Zahlung des Lösegelds entschlüsselt werden müssen. Nehmen Sie bei der Durchführung der forensischen Untersuchungen die Unterstützung Ihres Sicherheitsteams oder von Spezialisten in Anspruch.

- ☐ **Aufbewahrungszeiten überprüfen.**
  Es kann von Vorteil sein, die Aufbewahrungszeiten Ihrer Backups während der Auswirkungsanalyse und Wiederherstellung zu verlängern. Kurze Aufbewahrungszeiten erhöhen das Risiko, dass Backups vor dem Abschluss von Wiederherstellungsmaßnahmen ablaufen. Eine Verlängerung der Aufbewahrungszeiten trägt dazu bei, sicherzustellen, dass die Wiederherstellung auf den letzten sauberen Zustand vor der Infektion erfolgt.

☐ **Aktivieren Sie Ihren Reaktionsplan.**

Abschließend ist es an der Zeit, Ihr Vorfallsreaktionsteam zu verständigen, die wichtigsten Beteiligten zu benachrichtigen und Ihre Optionen auszuwerten, damit Sie Ihre Daten abrufen und wieder online gehen können. Das sind die verfügbaren Handlungsoptionen:

Option 1: Stellen Sie Ihre Dateien aus einem Backup wieder her. Der zuverlässigste Weg, sich von einem Ransomware-Angriff zu erholen, ohne das Lösegeld zu zahlen, ist die Wiederherstellung der betroffenen Geräte auf den letzten sauberen Stand. Deshalb ist das Vorhandensein eines umfassenden Backup-Plans, der regelmäßig getestet wird, für jeden effektiven Ransomware-Reaktionsplan von entscheidender Bedeutung.

Beachten Sie, dass nicht alle Datenschutzlösungen Ihre Backups im Falle eines Angriffs schützen und dass Backups beschädigt werden können. Aus diesem Grund wird dringend empfohlen, eine Lösung zu wählen, die verhindert, dass Ransomware jemals Ihre Backup-Daten verändert, und die gleichzeitig schnelle Wiederherstellungen und größere Transparenz bietet.

Option 2: Suchen Sie nach einem passenden Entschlüsselungsprogramm. Sobald Sie den genauen Ransomware-Typ bestimmt haben, ist es vielleicht möglich, ein Entschlüsselungsprogramm über Websites Dritter zu finden. Neuere Ransomware-Versionen sind jedoch ausgefeilter und mutieren schnell, sodass es weniger wahrscheinlich ist, dass ein Entschlüsselungsprogramm verfügbar ist.[4] Wenn Sie sich auf ein Entschlüsselungsprogramm eines Drittanbieters verlassen, riskieren Sie außerdem, zusätzliche Malware herunterzuladen. Daher ist diese Option weder zuverlässig noch ratsam.

Option 3: Tun Sie nichts und nehmen Sie den Datenverlust hin. Organisationen, die vor einem Angriff keine geeignete Backup-Strategie entwickelt haben oder die kein Entschlüsselungsprogramm finden können, können sich auch dafür entscheiden, ihre Dateien nicht wiederherzustellen. Natürlich sollte danach ein zuverlässiger Ransomware-Wiederherstellungsplan entwickelt, getestet und implementiert werden, um im Falle eines künftigen Angriffs eine rasche Wiederherstellung sicherzustellen.

Option 4: Verhandeln Sie und zahlen Sie das Lösegeld. Für diejenigen, die es mit allen anderen Mitteln versucht haben und ihre Dateien nicht wiederherstellen können, kann das Zahlen des Lösegeldes als die letzte mögliche Lösung erscheinen. Das FBI und die meisten Sicherheitsexperten warnen jedoch eindringlich davor, Lösegeld zu zahlen, da dies keine Garantie dafür ist, dass Sie alle oder einen Teil Ihrer Daten zurückerhalten. Ein Bericht der CyberEdge Group von 2019 zeigt auf, dass 17 % der Organisationen, die sich für das Zahlen des Lösegeldes entschieden haben, trotzdem keinen Zugang zu ihren verschlüsselten Daten oder infizierten Systemen erhalten haben.[5] Das Zahlen des Lösegeldes ist auch ein Anreiz für weitere Angriffe – möglicherweise um ein höheres Lösegeld –, wodurch Ihr Unternehmen noch anfälliger wird und wodurch der Zyklus aus Angriffen am Rollen gehalten wird, indem die Angreifer belohnt werden.

- ☐ **Ermitteln Sie das Ausmaß der Infektion.**
  Um den Datenverlust durch einen Ransomware-Angriff minimieren zu können, müssen IT-Teams in der Lage sein, die betroffenen Anwendungen und Dateien schnell zu erkennen – ein Prozess, der mit herkömmlicher Technologie einige Tage oder gar Wochen dauern kann. Es ist jedoch entscheidend, zunächst festzustellen, welche Anwendungen und Dateien betroffen sind und wo ein Rollback auf granularer Ebene durchgeführt werden muss. Dadurch wird das Risiko von Datenverlusten bei Massenwiederherstellungen unter Einbeziehung unbeschädigter Daten minimiert.

- ☐ **Alarmieren Sie die Behörden.**
  Informieren Sie nach einem Angriff Strafverfolgungsbehörden, Kunden und alle anderen maßgeblichen Behörden. Bestimmte Organisationen können gesetzlich verpflichtet sein, Behörden und Benutzer zu benachrichtigen; dies hängt stark von Ihrem Unternehmen, Ihrer Branche und Ihrem Standort ab.

Haftungsausschluss

Dieses Dokument soll die bestehenden Ransomware-Reaktions-, Wiederherstellungs- und Notfallwiederherstellungspläne ergänzen, nicht ersetzen.

Diese Vorlage wird auf „as-is"-Basis und ohne Gewähr zur Verfügung gestellt und impliziert keinerlei Haftung für Schäden, die aus der Verwendung der in dieser Vorlage enthaltenen Informationen entstehen. Sie wurde von keiner offiziellen Stelle oder Organisation gebilligt.

Damit diese Vorlage zum gewünschten Erfolg beiträgt, müssen Sie die Vorlage an Ihre Bedürfnisse anpassen und den Plan testen.

Quellen

1 *McAfee Labs Threats Report, August 2019.* McAfee, www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf.

2 *OCR Cybersecurity Newsletter, Herbst 2019: What Happened to My Data?: Update on Preventing, Mitigating and Responding to Ransomware.* Das Ministerium für Gesundheitspflege und Soziale Dienste der Vereinigten Staaten, https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2019/index.html

3 *2019 Data Breach Investigations Report.* Verizon, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

4 Alessandrini, Adam. *RANSOMWARE: Hostage Rescue Manual.* KnowBe4, 2016, www.wired.com/wp-content/uploads/2016/03/RansomwareManual-1.pdf.

5 *2019 Cyberthreat Defense Report,* CyberEdge Group, LLC. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

rubrik

Hauptsitz
1001 Page Mill Rd., Building 2
Palo Alto, CA 94304
USA

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik, das Multi-Cloud Data Control™-Unternehmen, ermöglicht es Unternehmen, seine zunehmend über Rechenzentren und Clouds verstreuten Daten besser zu nutzen. Rubrik bietet eine einzige, richtliniengesteuerte Plattform für Datenwiederherstellung, Governance, Compliance und Cloud-Mobilität. Weitere Informationen finden Sie unter www.rubrik.com. Folgen Sie uns auch auf Twitter unter @rubrikInc. © 2019 Rubrik. ubrik ist eine eingetragene Marke von Rubrik, Inc. Andere Marken können Marken ihrer jeweiligen Eigentümer sein.

20200716_v1