COHESITY

Ransomware-Bereitschaft: Ein ausführlicher Bewertungsleitfaden

Stärken Sie Ihre Datensicherheit & Cyber-Resilienz

Inhalt

Der zunehmende Einflussbereich von Ransomware 3
Entscheidende Maßnahmen gegen Ransomware 3
Schützen Sie Ihre Backup-Daten und Ihr System 4
Ransomware verschwindet nicht 4
Verringerung des Risikos eines unbefugten Zugriffs 7
Sehen und erkennen Sie Angriffe, um Übergriffe zu stoppen 8
Stärken Sie Ihre Sicherheitslage mit Plattformerweiterbarkeit 10
Stellen Sie sicher, dass Sie Daten im großen Maßstab schnell wiederherstellen können 12
Checkliste: Bewertung der Ransomware-Bereitschaft 14
Vorbereitet auf Ransomware mit Cohesity 15

Der zunehmende Einflussbereich von Ransomware

Cyberkriminelle kommen wegen der Daten, die Ihr Unternehmen antreiben. Wie erfolgreich sie bei der Erpressung von Lösegeld sein werden, hängt davon ab, was Sie heute tun, um Ihre Umgebung zu stärken und Ihre Reaktionsfähigkeit im Falle eines Angriffs zu verbessern.

Ransomware-Bedrohungen entwickeln sich weiter. Ziele und Taktiken weiten sich aus. Falls dies noch nicht geschehen ist, werden Sie sicherlich bald gefragt, wie Sie den verschiedenen Wegen entgegenwirken, mit denen Cyberkriminelle darauf abzielen, Ihren Betrieb zu stören.

	Ransomware 1.0	Ransomware 2.0	Ransomware 3.0
Malware-Ziel	Produktionsdaten	• Backup-Daten • Backup-Systeme • Produktionsdaten	• Backup-Daten • Backup-Systeme • Produktionsdaten • Daten, die illegal entfernt werden
Angriffsmethode	Verschlüsselung	Verschlüsselung	Verschlüsselung und Exfiltration
Wie Unternehmen dem Angriff entgegentreten	Datensicherungs- und Wiederherstellungssystem	Unveränderliche Backups und Cyber-Vaulting	Früherkennung und kontinuierliche Überwachung

Entscheidende Maßnahmen gegen Ransomware

Wenn Sie sich nicht sicher sind, was Sie zuerst tun sollen, um die Cyber-Resilienz Ihres Unternehmens zu stärken, ist dieser Leitfaden genau das Richtige für Sie. Er enthält zahlreiche praktische Informationen und Bewertungskriterien darüber, worauf Sie bei einer Datenmanagement-Lösung achten sollten, um Ihre Datensicherheitsstrategie zu stärken. Sie können ihn auch verwenden, um die Tools zu ergänzen, die Ihr SecOps-Team verwendet, wenn Sie gemeinsam daran arbeiten, wie Sie am besten auf sich ständig ändernde Ransomware-Bedrohungen reagieren können. Dieser Leitfaden enthält auch eine Checkliste, mit der Sie die Effektivität Ihrer bestehenden Lösungen mit unseren modernen Data Security and Management-Lösungen vergleichen können.

Ein besserer Schutz Ihrer Daten und des Rufs Ihres Unternehmens beginnt damit, zu verstehen, wie diese fünf entscheidenden Maßnahmen Ihr Unternehmen in die Lage versetzen, Ransomware entgegenzuwirken:

- Schützen Sie Ihre Backup-Daten und Ihr System
- Verringern Sie das Risikos eines unbefugten Zugriffs
- Sehen und erkennen Sie Angriffe, um Übergriffe zu stoppen
- Stärken Sie Ihre Sicherheitslage mit Integrationen und APIs
- Stellen Sie sicher, dass Sie Daten im großen Maßstab schnell wiederherstellen können

Ransomware verschwindet nicht

1,070 %

Der Prozentsatz an Ransomware ist zwischen Juli 2020 und Juni 2021 gestiegen[1]

82 %

Die prozentualen durchschnittlichen Ransomware-Zahlungen stiegen von 2020 bis zum Ende des ersten Halbjahres 2021 auf einen Rekordwert von 570.000 USD.[2]

> 1,85 Mio. USD

Die durchschnittlichen Kosten jetzt, um die Auswirkungen von Ransomware-Angriffen zu beheben, *ohne* das Lösegeld zu zahlen[3]

> 265 Mrd. USD

Die Höhe der globalen Ransomware-Schadenskosten – Umsatz- und Produktivitätsverlust sowie Wiederaufbau – werden Prognosen zufolge bis 2031 überschritten[4]

Schützen Sie Ihre Backup-Daten und Ihr System

Sicherheitsvorkehrungen für Ihre Daten sind von grundlegender Bedeutung, um das Vertrauen der Kunden zu wahren und Ihren Wettbewerbsvorteil zu wahren. Sie wirken den immer ausgefeilteren Ransomware-Bedrohungen entgegen, einschließlich neuer Bedrohungen wie „Lockers“, die Sie vollständig von Ihren Systemdateien und Anwendungen ausschließen, während sie Ihnen eine Countdown-Uhr mit Datum und Uhrzeit der erwarteten Lösegeldzahlung anzeigen. Ohne die Verbesserung Ihrer Sicherheitsvorkehrungen hat Ihr Unternehmen keine Möglichkeit, Ihre Daten vor einer Verschlüsselung – oder schlimmer noch, einem Diebstahl – durch Cyberkriminelle zu schützen.

Stellen Sie für eine optimale Datenresilienz in Hybrid- und Multicloud-Umgebungen sicher, dass diese sechs nicht verhandelbaren Backup-Sicherheitsfunktionen Teil jeder Datenmanagement-Lösung sind, die Sie ernsthaft in Betracht ziehen.

Unveränderliche Snapshots

Software-basierte, native unveränderliche Backup-Snapshots errichten effektiv eine Mauer gegen Ransomware-Angriffe, da sie nicht verschlüsselt, geändert oder gelöscht werden können – alles gängige Taktiken, die Cyberkriminelle anwenden, um eine Ransomware-Zahlung zu erzwingen. Das ist äußerst wichtig, um die Authentizität von Daten zu schützen, insbesondere von großen Mengen unstrukturierter Daten wie Audio- und Videodateien sowie Bildern, die in bestimmten Branchen wie der Strafverfolgung und dem Gesundheitswesen benötigt werden. Im Gegensatz zur hardwarebasierten Unveränderlichkeit werden die nativen schreibgeschützten Snapshots, die vor Ort oder in Clouds gespeichert sind, niemals einer Anwendung ausgesetzt oder extern bereitgestellt. Sie können nicht manipuliert, verändert oder entfernt werden. Das erschwert es Malware, auf Ihre Backup-Daten abzuzielen.

[1] FortiGuard Labs. „Global Threat Landscape Report“, August 2021.
[2] Palo Alto Networks. „Extortion Payments Hit New Records as Ransomware Crisis Intensifies,“ 9. August, 2021.
[3] Sophos. „The State of Ransomware 2021,“ 2021.
[4] Cybersecurity Ventures. „Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031“, 3. Juni 2021.

WORM

Mechanismen wie die WORM-Technologie (Write Once, Read Many) bieten eine weitere Schutzebene gegen Ransomware-Angriffe. Sie ermöglichen es Teams, Daten durch Richtlinien zeitgebunden zu sperren und anzuwenden und sie dann ausgewählten Jobs zuzuweisen, um die Unveränderlichkeit geschützter Daten zu verbessern. Da dies ein Schutz ist, den weder Sicherheitsbeauftragte noch Sicherheitsadministratoren ändern oder löschen können, müssen Sie sich nicht so viele Gedanken über potenzielle Insider-Bedrohungen machen.

Datenverschlüsselung

Es gibt Verschlüsselung und dann gibt es eine software-basierte FIPS-validierte AES-256-Standardverschlüsselung sowohl für Daten, die übertragen werden, als auch für solche, die sich im Ruhezustand befinden. Sie möchten, dass das kryptografische Modul vom National Institute of Standards and Technology (NIST) der Vereinigten Staaten gemäß dem Standard Federal Information Processing Standards (FIPS) 140-2 Level 1 validiert wird. FIPS 140-2 ist ein Standard der US-Regierung für kryptografische Module, der zusichert, dass das Moduldesign und die Implementierung kryptografischer Algorithmen sicher und korrekt sind. Die FIPS-validierte Verschlüsselung ist sicherer, da Produkte mit dieser Auszeichnung eine Reihe strenger Tests bestehen müssen, um weltweit anerkannt zu werden.

Konfigurationsaudit und Scannen

Ihr IT-Team betreibt jetzt wahrscheinlich viele verschiedene Systeme und Tools – alle mit eigenen Setups, Richtlinien und Managementschnittstellen. Die manuellen Prozesse für deren Ausführung haben oft vermeidbare menschliche Fehler zur Folge. Wäre es nicht schön, wenn es einen effizienteren Weg gäbe? Ein automatisiertes System mit geführtem Scannen, das verschiedene Datensicherheits- und Zugriffskontrolleinstellungen überprüft, hilft Ihnen, kostspieliges menschliches Versagen zu vermeiden und gleichzeitig Ihre Datenoperationen von der Einrichtung über Richtlinien bis hin zu Managementprozessen zu vereinfachen.

Fehlertoleranz

Da Datenresilienz immer ein leitendes Sicherheitsprinzip sein sollte, benötigen Sie auch ein fehlertolerantes System, das dazu beiträgt, die Datenintegrität und erfolgreiche Backups selbst unter härtesten Bedingungen sicherzustellen. Einige davon treten auf, wenn Ihre Systeme mit ihrer Rechen- oder Speicherkapazität nahezu ausgelastet sind; wenn Sie eine erhebliche Netzwerküberlastung vorliegen haben oder wenn unerwartet ein Hardwarefehler auftritt. Suchen Sie nach einer fehlertoleranten Lösung, die es ermöglicht, Backups trotz einer ausgefallenen Komponente/eines ausgefallenen Knotens fortzusetzen.

Modernes und flexibles Cyber-Vaulting

Wenn Sie Ihren Datenmanagement-Ansatz modernisieren, sollten Sie auch die Aktualisierung Ihrer Cyber-Vaulting-Strategie in Betracht ziehen. Traditionell haben sich Unternehmen auf Tape-Lösungen verlassen, um Air-Gap-Kopien zu verwalten, aber diese Methode kann nicht mehr mit den heutigen anspruchsvollen Service-Level-Agreements (SLAs) mithalten, wenn es um Wiederherstellungszeiten geht – insbesondere nicht solche, die während eines weit verbreiteten Ransomware-Angriffs benötigt werden. Lassen Sie sich nicht täuschen, auch wenn der Begriff „Air Gap" inzwischen weithin missbräuchlich genutzt wird, um Techniken zu beschreiben, die nicht wirklich für eine Isolierung sorgen. Ihre nächste Datenmanagement-Lösung sollte in jedem Fall echten Air-Gap-Schutz und moderne Optionen zur Datenisolation bieten. Diese gleichen moderne Anforderungen an das Zeitziel der Wiederherstellung und den Wiederherstellungspunkt (Recovery Time Objective, RTO / Recovery Point Objective, RPO) mit angemessenen Sicherheitskontrollen aus, indem Backup-Daten in der Cloud oder an einem anderen Ort mit einer temporären und hochsicheren Verbindung gespeichert werden. Sie erhalten dann eine manipulationssichere Umgebung, die Unterbrechungen durch Ransomware und Insider-Bedrohungen verhindert und gleichzeitig die Erfüllung Ihrer organisatorischen SLAs optimiert. Das Beste daran ist, dass Sie immer eine Kopie Ihrer Daten in einem unveränderlichen Format behalten.

DIE VIER WICHTIGSTEN FRAGEN ZU BACKUP-DATEN UND -SYSTEMEN

- Was unternimmt Ihre Datenmanagement-Lösung, um Ihre gesicherten Daten vor Ransomware-Angriffen zu schützen?
- Wie sichert Ihre Lösung Workloads auch nach dem Ausfall einer Hardware- oder Softwarekomponente kontinuierlich?
- Wie gleicht Ihre Lösung den Bedarf an höherer Sicherheit mit immer schnelleren RTOs/RPOs für digitale Unternehmen aus, die SLAs erfüllen?
- Auf welche Weise bietet Ihre Lösung Einblick in die Sicherheitslücken in der Systemkonfiguration und im Betriebsdesign?

Verringerung des Risikos eines unbefugten Zugriffs

Schädliche Akteure arbeiten für sich selbst, Syndikate und Nationalstaaten. Aus diesem Grund ist es für Ihr Unternehmen ein zunehmend strategischer Schritt, eine Datenmanagement-Lösung mit strengen Zugriffskontrollen zu haben. Diese Funktionen können den unbefugten Zugriff von externen Hackern oder betrügerischen internen Fachleuten, die sich kompromittierte Zugangsdaten zunutze machen, effektiver stoppen.

Um Ihr Risiko von Datendiebstahl und -verlust zu verringern, suchen Sie nach einer Lösung, die auf den Prinzipien der geringsten Rechte und Aufgabentrennung mit granularer Sicherheit aufbaut – einschließlich der folgenden vier unverzichtbaren Funktionen. Sie sorgen für die Sicherheit Ihrer Daten und das Vertrauen Ihrer Kunden.

Multifaktor-Authentifizierung

Selbst die kreativsten Passwörter, die regelmäßig kompromittiert werden, können nur einen minimalen Sicherheitsschutz für digitale Unternehmen bieten. Die Multifaktor-Authentifizierung (MFA) ist ein Schritt nach vorn bei der Abwehr von Phishing-Schemata und anderen Passwort-Hacks. Jeder, der auf Ihre Backup- oder Datenmanagement-Lösung zugreift, muss sich einem mehrstufigen Verifizierungsprozess unterziehen. Sie müssen sich authentifizieren – sowohl mit etwas, das sie „kennen“ (z. B. ein Passwort), als auch mit etwas, das sie „haben“ (z. B. einen Fingerabdruck, der von einem Single-Sign-On [SSO]-Anbieter validiert wird), um zu beweisen, dass sie derjenige sind, für den sie sich ausgeben. Bestehen Sie darauf, dass jede Ihrer in die engere Wahl gezogenen Lösungen eine MFA erfordert.

Überwachte Veränderung

Da ein Beobachter ausreichen kann, um einen Angriff zu vereiteln, benötigen Sie eine Funktion, die verhindert, dass ein kompromittierter Berechtigungsnachweis oder eine Person kritische Elemente Ihrer Datenmanagement-Lösung ändern kann. Bestehen Sie auf einer Plattform, die zur Durchsetzung von Sicherheitsvorkehrungen beiträgt, z. B. wenn eine Root-Level- oder andere kritische Systemänderung von mehr als einer Person autorisiert werden muss, damit Sie sich vor böswilligen Absichten und gestohlenen Anmeldeinformationen schützen können.

Granulare, rollenbasierte Zugriffskontrolle

Wenn es um Daten geht, sind ein effektives Identitäts- und Zugriffsmanagement zunehmend die Eckpfeiler einer guten Cyber-Hygiene. Die Reduzierung von Ransomware und Insider-Bedrohungen hängt jetzt davon ab, dass IT-Mitarbeiter jeder Person ein Mindestmaß an Zugriff auf alle Daten des Unternehmens gewähren, die für eine bestimmte Aufgabe erforderlich sind, und gleichzeitig kritische Datenprozesse und -funktionen auf IT-Rollen verteilen, damit ein einzelner Administrator nicht Ihr gesamtes Geschäft gefährden kann. Organisationen mit Datenmanagement-Lösungen, die Ansätze für eine granulare, rollenbasierte Zugriffskontrolle (RBAC) vereinfachen, können besser unbefugten Zugriff sowie die Gefährdung von Daten verhindern, während sie ihren Benutzern effizient die entsprechenden Berechtigungen für ihre Arbeit gewähren.

DIE 3 WICHTIGSTEN FRAGEN ZUR REDUZIERUNG DES RISIKOS UNAUTORISIERTEN ZUGRIFFS

- Was unternimmt Ihre Datensicherungs- oder Datenmanagement-Lösung, um unbefugten Zugriff auf Geschäftsdaten zu verhindern?
- Wie schützt Ihre Lösung sowohl vor Ransomware als auch vor Insider-Bedrohungen?
- Wie richte ich die Multibenutzergenehmigung für kritische Vorgänge ein?

Sehen und erkennen Sie Angriffe, um Übergriffe zu stoppen

Das digitale Geschäft schreitet schnell voran. Geschäftsinhaber müssen zunehmend wissen, welche sensiblen Daten sie haben, wo sie sich befinden und wer Zugriff darauf hat. Das ist der Schlüssel zur Einhaltung von branchenspezifischen oder gesetzlichen Vorschriften, zur Aufrechterhaltung des Vertrauens und zur schnellen Reaktion auf Angriffe mit zweierlei Druckmitteln (auch bekannt als Datenexfiltration).

Um den potenziellen Einflussbereich von Ransomware zu minimieren, suchen Sie nach einer Datenmanagement-Lösung mit integrierter Datenauswertung, damit Sie vertrauliche Daten automatisch erkennen und klassifizieren können, während Sie Bedrohungserkennung nahezu in Echtzeit genießen. Suchen Sie eine Lösung, die Ihrem Team hilft, intelligenter anstatt härter zu arbeiten, und die vier entscheidende Funktionen für proaktive Reaktionen enthält – egal, welche Bedrohungen auf Sie zukommen.

Unterstützt durch künstliche Intelligenz/maschinelles Lernen

Ihre Organisation braucht Daten, um erfolgreich zu sein. Aber diese Daten nehmen exponentiell zu, was es einigen Datenmanagement-Lösungen unmöglich macht, einen effektiven Musterabgleich und eine Datenklassifizierung durchzuführen, damit Sie wissen, was am wichtigsten ist. Im Gegensatz dazu hilft eine moderne Data Security and Data Management-Lösung, die auf künstlicher Intelligenz und maschinellem Lernen (KI/ML) basiert, Ihrem Unternehmen, Abweichungen genauer zu erkennen und Fehlalarme zu reduzieren, ohne das Personal aufstocken zu müssen. Sie können KI/ML-Techniken nutzen, um sie mit „funktionstüchtigen“ Datensätzen abzugleichen, und dies effektiver und effizienter tun, da Ihre „bekannten sensiblen Daten“ abgeglichen und an den KI/ML-Algorithmus zurückgemeldet werden. Stellen Sie sich das so vor, als ob Sie die Nadel im Heuhaufen finden möchten ohne viele schwere Heuballen zu heben.

Anomalieerkennung nahezu in Echtzeit

Je schneller Sie einen Eindringling finden, desto weniger Schaden kann er Ihrem Unternehmen zufügen – und desto weniger Nächte und Wochenenden belasten Sie Ihre IT-Profis. Die leistungsstarke automatisierte Anomalieerkennung nahezu in Echtzeit als Teil einer Datenmanagement-Lösung verfolgt kontinuierlich den normalen Systembetrieb, um schnell Unregelmäßigkeiten und abnormales Benutzerverhalten zu erkennen, die auf einen Ransomware-Angriff hindeuten können. Zusammen mit den Warnmeldungen signalisieren diese Funktionen nicht nur potenzielle Gefahren, sondern können auch Abhilfemaßnahmen einleiten. Mit der Anomalieerkennung nahezu in Echtzeit können Sie sowohl Verschlüsselungs- als auch Datenexfiltrationsangriffe schnell erkennen und die Auswirkungen von Ransomware minimieren.

Einschätzen von Angriffsfolgen

Nutzen Sie beim Erkennen von Anomalien ML/NLP, um zu bestimmen, ob sensible Daten betroffen sind, und legen Sie die erforderlichen Wiederherstellungs- und Compliance-Verfahren fest. Stellen Sie sicher, dass Sie globale Bereitstellungen mit vorkonfigurierten und anpassbaren Strukturen unterstützen können.

Erkennen von potenziellen Bedrohungen in Wiederherstellungsdaten

Verringern Sie Ihr Recovery-Risiko, indem Sie eine auf Threat Intelligence und Deep Learning basierende Bedrohungserkennung nutzen, die sicherstellt, dass Ihre Backup-Daten frei von Malware sind. Nutzen Sie Threat-Intelligence-Feeds, um Indicators of Compromise (IOCs) zu identifizieren, die auf einen bevorstehenden Angriff hindeuten.

Entdeckung von Cyber-Schwachstellen

Es ist bekannt, dass Cyberkriminelle Software und Cyber-Schwachstellen ausnutzen, die häufig aufgrund ungepatchter Software offen bleiben, um Zugriff auf Ihre Produktionsumgebung zu erhalten. Die effektivsten Datensicherungs- und Datenmanagement-Lösungen sollten Ihrem Team helfen, diese Schwachstellen zu erkennen. Es sollte Ihnen auch dabei helfen, diese proaktiv anzugehen und zu vermeiden, dass bereits behobene Cyber-Schwachstellen erneut in Ihre Produktionsumgebung eingefügt werden, während Sie sich von einem Angriff erholen.

DIE VIER WICHTIGSTEN FRAGEN, DIE SIE STELLEN SOLLTEN, UM EINDRINGLINGE ZU STOPPEN

- Wie hilft Ihre Lösung dabei, Daten zu klassifizieren und sensible Informationen zu identifizieren, die gefährdet sein könnten?
- Was unternimmt Ihre Datensicherungs- oder Datenmanagement-Lösung, um detaillierte Einblicke zu bieten, Software- und Cyber-Schwachstellen zu identifizieren und Anomalien nahezu in Echtzeit zu erkennen?
- Wie integriert Ihre Lösung KI/ML, um Anomalien zu erkennen, die auf eine Bedrohung oder einen Ransomware-Angriff hindeuten können?
- Wie erkennt Ihre Lösung Anomalien auf Systemebene und im Benutzerverhalten, die auf unterschiedliche Angriffsvektoren hinweisen?

Stärken Sie Ihre Sicherheitslage mit Plattformerweiterbarkeit

Ransomware ist keine einzelne Bedrohung. Sie entwickelt sich weiter und wird mit jeder Iteration ausgefeilter. Das bedeutet, dass Ihre Datenmanagement-Lösung weder unflexibel sein noch isoliert arbeiten kann. Sie muss zukunftssicher und erweiterbar sein. Integrierte und interoperable Lösungen ermöglichen es Ihrem Unternehmen, Bedrohungen schneller zu erkennen, zu untersuchen und zuverlässig darauf zu reagieren. Sie besiegen auch am ehesten schädliche Akteure.

Suchen Sie nach einer modernen Datenmanagement-Lösung, die die Zusammenarbeit mit Drittanbietern unterstützt, um Ihre Datensicherheit zu verbessern; eine Lösung, die Flexibilität gewährleistet und dennoch sichere Möglichkeiten bietet, den Betrieb zu vereinfachen und Ihre Daten produktiv zu machen. Um eine starke Sicherheitslage aufzubauen, sollte jede Lösung, die Sie in Betracht ziehen, diese drei unverzichtbaren Funktionen enthalten und gut mit anderen zusammenarbeiten.

Vorkonfigurierte Integrationen

Bedenken hinsichtlich der Datensicherheit rauben Geschäftsführern den Schlaf. Sie könnten besser schlafen, wenn sie darauf vertrauen könnten, dass ihre bewährten Sicherheitsprodukte nahtlos zusammenarbeiten, um Cyberkriminalität zu bekämpfen. Finden Sie eine Datenmanagement-Lösung, die bereits eng in führende Security Orchestration, Automation and Response (SOAR)- sowie Security Information Event Management (SIEM)-Lösungen integriert ist. Sie beschleunigt die Erkennung, Untersuchung und Behebung von Ransomware-Angriffen. Stellen Sie sicher, dass sie auch über vorkonfigurierte, integrierte Workflows verfügt, die erweiterbar sind, sodass SecOps sie für die automatisierte Reaktion auf Vorfälle und einheitliche Abläufe für Sicherheits-, IT- und Netzwerkteams erweitern kann.

Individuell anpassbare Integrationen

Alles unterliegt beständigen Veränderungen. Aber nicht alle Datenmanagement-Plattformen helfen Ihnen, damit Schritt zu halten. Ihr Unternehmen benötigt eine cyberresistente Lösung, die Ransomware entgegenwirkt und gleichzeitig einzigartige Geschäftsanforderungen erfüllt. Stellen Sie neben vorkonfigurierten Integrationen sicher, dass die von Ihnen gewählte Lösung über ein sicheres Software Development Kit (SDK) und anpassbare Management-APIs verfügt, die Ihnen die Flexibilität geben, Ihre Umgebung so zu betreiben, wie Sie es möchten.

Interoperabilität von Anwendungen mit Mehrwert

Zusätzlich zu vorkonfigurierten und anpassbaren Integrationen innerhalb einer API-reichen Architektur, die zur Optimierung des Betriebs beiträgt, benötigen Sie eine Plattform, die Möglichkeiten bietet, zukunftssicher zu sein und gleichzeitig die Datensicherheit zu verbessern. Anstatt Kopien von Daten zu erstellen und sie zu verschieben, suchen Sie eine Lösung, die es Ihnen ermöglicht, die Daten vor Ort wiederzuverwenden, indem Sie Anwendungen für routinemäßige und anspruchsvollere Aufgaben auf Daten zuweisen – von Virenscans und Datenmaskierung bis hin zur Analyse von Datei-Audit-Protokollen und dem Klassifizieren von Daten. Eine erweiterbare Plattform trägt dazu bei, Ihren Speicherplatzbedarf und Ihre Angriffsfläche zu reduzieren, und versetzt Sie in die Lage, mit Ihren Investitionen einen höheren Mehrwert zu generieren.

DIE VIER WICHTIGSTEN FRAGEN, DIE SIE STELLEN SOLLTEN, UM DIE ERWEITERBARKEIT UND INTEROPERABILITÄT ZU GEWÄHRLEISTEN

- Welche Sicherheitsintegrationen unterstützt Ihre Datensicherungs- oder Datenmanagement-Lösung?
- Wie funktioniert Ihre Lösung bei anderen führenden Sicherheitsprodukten und -plattformen?
- Wie extrahiert Ihre Lösung Erkenntnisse und schützt gleichzeitig die Daten?
- Wie verbessert Ihre Datensicherungs- oder Datenmanagement-Lösung die Teamzusammenarbeit, indem Plattform-, Personen- und Prozesssilos beseitigt werden?

Stellen Sie sicher, dass Sie Daten im großen Maßstab schnell wiederherstellen können

Sollte das Worst-Case-Szenario eintreten und Ransomware einen Weg in Ihre Produktionsumgebung finden, benötigen Sie eine Lösung, die Ihnen erlaubt, die Zahlung von Lösegeld zu verweigern. Suchen Sie nach einer Lösung mit diesen drei nicht verhandelbaren Datenwiederherstellungsfunktionen, um Ihnen dieses Vertrauen zu geben.

Sofortige, skalierbare Wiederherstellung

Wenn Ransomware-Angreifer zuschlagen, haben sie es nicht mehr auf eine oder zwei virtuelle Maschinen (VMs) oder Datenbanken abgesehen. Vielmehr wollen sie in den Systemen so viele Ihrer Daten wie möglich unzugänglich machen. Daher benötigen Unternehmen heute eine Datenmanagement-Lösung, die Hunderte von Systemen schnell wiederherstellen kann. Dank der Fähigkeit zur sofortigen Wiederherstellung im großen Maßstab können Sie Hunderte von VMs, große Datenbanken oder große Mengen unstrukturierter Daten sofort und in großem Umfang zu jedem Zeitpunkt und an jedem Ort wiederherstellen.

Saubere Wiederherstellung
*In-Place-Wiederherstellung

Die Bereitstellung einer sauberen Umgebung nach einem Angriff kann einige Zeit in Anspruch nehmen, und die Wiederherstellung der ursprünglichen Umgebung könnte die forensischen Bemühungen beeinträchtigen. Das kann Ihre Wiederherstellungsbemühungen verlangsamen (was Sie definitiv nicht wollen, wenn Sie hart daran arbeiten, alles wieder zum Laufen zu bringen). Suchen Sie eine Datenmanagement-Lösung, mit der Sie Daten direkt an Ort und Stelle auf derselben Plattform wiederherstellen können – ohne einen neuen Server oder eine neue Datenbank einzurichten. Sie wird Ihnen Zeit und Geld sparen.

DIE VIER WICHTIGSTEN FRAGEN, DIE SIE STELLEN SOLLTEN, UM ZU BESTÄTIGEN, DASS SIE DATEN SCHNELL UND SKALIERBAR WIEDERHERSTELLEN KÖNNEN

- Was leistet Ihre Datensicherungs- oder Datenmanagement-Lösung, damit Sie Daten schnell, sauber und vorhersehbar in großem Umfang wiederherstellen können?
- Verfügt Ihr Sicherungssystem über ausreichende Ressourcen, um eine schnelle Wiederherstellung zu jedem Zeitpunkt und an jedem Ort zu unterstützen?
- Welche Funktionen unterstützt Ihre Lösung, um den Zustand eines Snapshots zu bewerten und unstrukturierte Daten ohne zusätzliche Investitionen wiederherzustellen?
- Wie führt Ihre Datenmanagement-Lösung eine Wiederherstellung unstrukturierter Daten vor Ort durch, um Ausfallzeiten zu reduzieren?

Checkliste: Bewertung der Ransomware-Bereitschaft

Cyberkriminelle sind stets fleißig. Sie benötigen eine Datensicherungs- oder Datenmanagement-Strategie, die Ihnen hilft, mit den immer ausgefeilteren Bedrohungen Schritt zu halten und die Auswirkungen von Ransomware zu minimieren. Das Überdenken Ihrer Datenmanagement-Lösung ist ein guter Ausgangspunkt. Bei der Bewertung Ihrer Optionen kann Ihnen diese Checkliste der wichtigsten Funktionen dabei helfen, die Lösung zu finden, die für Ihr Unternehmen am besten geeignet ist.

Maßnahme	Schlüsselfunktion	Anbieter 1	Anbieter 2	Anbieter 3	Anbieter 4
Schützen Sie Ihre Backup-Daten und Ihr System	Unveränderliche Snapshots				
	WORM				
	Datenverschlüsselung				
	Konfigurationsaudit und Scannen				
	Fehlertoleranz				
	Modernes und flexibles Cyber-Vaulting				
Verringern Sie das Risikos eines unbefugten Zugriffs	Multifaktor-Authentifizierung (MFA)				
	Überwachte Veränderung				
	Granulare, rollenbasierte Zugriffskontrolle (RBAC)				
Sehen und erkennen Sie Angriffe, um Übergriffe zu stoppen	KI/ML-gestützt				
	Anomalieerkennung nahezu in Echtzeit				
	Automatisierte Warnmeldungen				
	Entdeckung von Cyber-Schwachstellen				
Stärken Sie Ihre Sicherheitslage mit Plattformerweiterbarkeit	Vorgefertigte Integrationen				
	Anpassbare Integrationen				
	Interoperabilität von Anwendungen mit Mehrwert				
Stellen Sie sicher, dass Sie Daten im großen Maßstab schnell wiederherstellen können	Sofortige, skalierbare Wiederherstellung				
	Saubere Wiederherstellung				
	Wiederherstellung vor Ort				

Vorbereitet auf Ransomware mit Cohesity

Mit Cohesity kann Ihr Unternehmen auf einfache Weise Ihre Daten sichern, managen, sichern und einen Mehrwert daraus generieren – im Rechenzentrum, im Edge-Bereich und in der Cloud. Verwenden Sie die Cohesity-Software, um die Dateninfrastruktur direkt zu managen, oder lassen Sie sie über einen Cohesity-SaaS-Service verwalten, oder beides. Cohesity löst die Fragmentierung großer Datenmengen, macht die Einhaltung von Daten zum Kinderspiel und hilft Unternehmen, Ransomware-Angriffe zu verhindern.

Cohesity wurde zum Leader im Gartner Magic Quadrant für Datensicherungs- und -Wiederherstellungslösungen für Rechenzentren und zum Leader bei „The Forrester Wave™: Data Resiliency Solutions“ ernannt Das Unternehmen ist 2022 in der Forbes Cloud 100 vertreten (zum vierten Mal), von CRN unter den Coolest Cloud Companies 2022 gelistet (zum dritten Mal) und der führende von 16 Anbietern des GigaOm Radar for Unstructured Data Management.

Modernisieren Sie noch heute Ihre Plattform für Datensicherheit und Datenmanagement
www.cohesity.com/de

Erfahren Sie mehr auf cohesity.com/de

COHESITY