Tintri VMstore Ransomware-Recovery: vorhanden lange bevor dies zum Trend wurde

Von DCIG Lead Analyst Storage, Ken Clipperton

Tintri

COMPANY

Tintri
9351 Deering Ave
Chatsworth, CA 91311
+1.650.810.8200

tintri.com

BRANCHE

Data Storage

LÖSUNG

Tintri VMstore

FEATURES

- Granulare Sicherung der Daten
- Intelligente integrierte Analytik
- Management auf VM-Ebene

VORTEILE

- Abwehr von Ransomware-Angriffen
- Setzt Anwendungen so schnell wie möglich wieder in Betrieb

Dieser Bericht konzentriert sich darauf, wie die Tintri VMstore Storage-Plattform Unternehmen dabei unterstützt sich von erfolgreichen Ransomware-Angriffen zu erholen.

Heute machen sich viele Menschen über Unterbrechungen der Lieferkette Sorgen. In der Tat sind zahlreiche Unternehmen davon beeinträchtigt. Wenn es jedoch um den Schutz eines Unternehmens vor Unterbrechungen geht, steht für viele Führungskräfte Ransomware an oberster Stelle. Dies ist durchaus angemessen.

Viele Jahre lang war menschliches Versagen der Hauptgrund von Datenverlust bzw. unterbrochenem Zugriff auf Daten: so zum Beispiel eine versehentlich gelöschte Datei oder ein gelöschter Ordner, ein missglücktes Upgrade oder ein Schreibfehler in einem Konfigurationsskript. Dazu zählen sogar kürzlich aufgetretene Unterbrechungen bei großen Internet-basierten Diensten.

In den letzten Jahren haben Ransomware-Angriffe jedoch so stark zugenommen, dass diese jetzt die größte Bedrohung für die Daten eines Unternehmens darstellen.

Davon ausgehen, dass ein Ransomware-Angriff erfolgreich sein wird

Jedes Unternehmen muss davon ausgehen, dass Ransomware-Angriffe die eigenen Cybersecurity-Maßnahmen erfolgreich umgehen können. Wie bei vielen Sicherheitsaspekten erfordert der Schutz eines Unternehmens die erfolgreiche Vereitelung aller Angriffe.

Schutzmaßnahmen, die 999 von 1000 Angriffen vereiteln, sind ein Misserfolg. Für Cyberkriminelle trifft das entgegengesetzte Verhältnis zu. Wenn diese nach 999 fehlgeschlagenen Versuchen auch nur ein einziges Mal die Cybersecurity-Maßnahmen eines Unternehmens umgehen können, ist dies für sie ein Erfolg.

> ***"Unternehmen müssen auf die Wahrscheinlichkeit vorbereitet sein dass ihre Cybersecurity-Verteidigung irgendwann versagen wird."***

Wie Schlagzeilen nahelegen (und Statistiken von Sicherheitsorganisationen bestätigen), haben sich Ransomware-Angriffe zu einer wesentlichen Bedrohung für nahezu jedes Unternehmen entwickelt. Deshalb müssen sich Wirtschafts- und IT-Führungskräfte auf ein Versagen des Cyberschutzes vorbereiten und einen Plan zur Wiederherstellung nach einem solchen Angriff implementieren. Die richtige Data Storage Technologie spielt hier eine wichtige Rolle beim erfolgreichen Recovery und der Wiederaufnahme des normalen Betriebes.

Ausfallzeiten des Unternehmens sind die größten Ransomware-Kosten

Die von Cyberkriminellen geforderten Lösegelder können sich auf Millionen von Dollar belaufen. Diese Lösegeldforderungen sorgen mit Sicherheit für Schlagzeilen. Die größten mit solch einem Angriff verbundenen Kosten stellen jedoch die Ausfallzeiten der Anwendungen/Applikationen dar, die zu Geschäftsunterbrechungen führen.

Zusammengenommen belaufen sich die durchschnittlichen Gesamtkosten für das Recovery/Wiederherstellung nach einem Ransomware-Angriff auf 1,85 Millionen US Dollar.[1] Und die größten Ausgaben, größer als die Zahlung selbst, sind die durchschnittlichen Kosten für die 21-tägige Betriebsunterbrechung.[2]

Außerdem kommt es häufig vor, dass ein Unternehmen aufgrund eines erfolgreichen Ransomware-Angriffs Führungskräfte verliert, Mitarbeiter entlässt oder sogar ganz schließen muss. So ist es kein Wunder, dass fast ein Viertel aller IT-Führungskräfte den Schutz ihres Unternehmens gegen solche Angriffe als ihre höchste Priorität ansehen.

Glücklicherweise vereinigt die Tintri VMstore Plattform zahlreiche Technologien, welche die Auswirkungen von Ransomware reduzieren.

Ransomware 2021

600% Zunahme von bösartigen E-Mails seit COVID-19[3]

$170.404 Durchschnittlicher mittlerer Auszahlungsbetrag eines Unternehmens[4]

$1,85Mio Durchschnittliche Kosten eines Unternehmens für die Wiederherstellung

21 Tage Durchschnittliche Ausfallzeit eines Unternehmens durch einen Ransomware-Angriff

Die größten Kosten **Betriebsunterbrechung**

Intelligente integrierte Analytik reduziert die Auswirkungen von Ransomware

Ein Markenzeichen der VMstore Plattform ist die detaillierte Storageanalytik. Diese Analytik ist nicht nur ein Management- und Visibility-Add-on. Sie ist vielmehr fester Bestandteil des Betriebs und der adaptiven autonomen Managementfunktionen von VMstore.

Die autonomen Managementfunktionen wurden ursprünglich dazu benutzt, konsistente Performance im Mikrosekundenbereich für jede Anwendung zu garantieren. Jetzt dienen diese dazu, Angriffe zu identifizieren, deren Ausmaß zu verstehen und ein rasches, präzises Recovery/Wiederherstellung zu ermöglichen.

Tintri VMstore umfasst zahlreiche Funktionen, die zusammenarbeiten, um ein rasches, präzises Recovery der Anwendungen zu ermöglichen.

Dazu gehören:

- Management auf VM-Ebene
- Rollenbasierte Zugriffskontrollen
- Erkennen von Angriffen mittels Analytik
- Charakteristische unsichtbare Snapshot-Pointer und Metadaten
- Leistungsfähige Snapshots
- Flexible Replikationsmöglichkeiten
- Granulare richtlinienbasierte Datensicherung und -Recovery
- Nahezu unmittelbares Recovery am Primär- oder DR-Standort

Management auf VM-Ebene ermöglicht die sofortige Wiederherstellung von Anwendungen

Ein wesentliches Unterscheidungsmerkmal zwischen Tintri VMstore und anderen Storagelösungen ist, dass VMstore speziell für das Management auf VM-Ebene konzipiert wurde. Daher auch der Name „VMstore“.

Die Wichtigkeit von VM-basiertem Management ist für erfahrene Storage Administratoren zwar leicht ersichtlich, es ist jedoch schwierig im Auge zu behalten. Das VMstore-Management ist viel granularer als LUN-Management, jedoch viel weniger zeitaufwändig. Und Tintri hat dieses Management jetzt erweitert und SQL-Datenbanken hinzugefügt, und plant, dies auch für Container zu tun.

Was die Wiederherstellung nach einem Datenverlust oder Cyberangriff betrifft, ermöglicht diese VM-basierte Managementinfrastruktur, Daten auf Anwendungsbasis zu sichern und wiederherzustellen. Das wichtigste Ergebnis dieses Unterschieds ist, dass es IT-Mitarbeiter in die Lage versetzt, Anwendungen schnellstmöglich wieder in Betrieb zu nehmen.

Rollenbasierte Zugriffskontrollen

Die rollenbasierten Zugriffskontrollen (RBAC) von VMstore reduzieren das Ausmaß eines erfolgreichen Angriffs innerhalb des Storagesystems. Anstatt nur einen Vollzugriff oder gar keinen Zugriff auf die Storageinfrastruktur zu gewähren, erteilt RBAC jeder Person bzw. jedem Geschäftsprozess nur die Berechtigungen, die zur Ausführung ihrer Aufgaben benötigt werden.

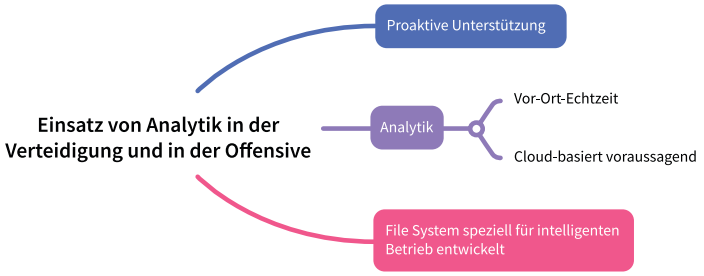
Zu den unterstützten Rollen gehören:

- Read Only
- Service Account
- Storage Administrator
- Super Administrator
- Database Administrator

Die ordnungsgemäße Zuweisung dieser Rollen ermöglicht die effektive Delegierung von täglichen Verantwortlichkeiten und befähigt die Mitarbeiter der Abteilungen ihre Aufgaben zu erfüllen. Ebenso beschränkt sie die Auswirkungen einer Verletzung jener individuellen Credentials.

Erkennen von Angriffen

VMstore bietet einen detaillierten Einblick in die Performance und Kapazität, die von einzelnen virtuellen Maschinen und SQL-Server-Datenbanken genutzt werden. Analysesichten können einfach konfiguriert werden, um Performance- und Kapazitäten-„Mover“ unter den Anwendungen eines Unternehmens aufzuzeigen. Diese Ansichten machen auch Änderungen, die außerhalb der normalen Trendlinie liegen, einfach sichtbar.



Tintri Global Center (TGC) nutzt diese Daten bereits für die Workloadverteilung in Multi-VMstore-Umgebungen. Es analysiert in regelmäßigen Abständen die Daten, die von den laufenden Workloads und den verfügbaren VM-Store-Ressourcen erzeugt werden. TGC gibt dann Empfehlungen für die Verlagerung von Workloads von einem VMstore zu einem anderen. Zusammen mit den Empfehlungen, bietet TGC eine Schaltfläche “Ausführen”, auf die ein Administrator klicken kann, um die empfohlenen Änderungen zu implementieren.

Wenn überhaupt, bieten nur wenige andere Storagesysteme diese granulare Ebene der Sichtbarkeit. Im Einklang mit dem Fokus auf eine intelligente Infrastruktur plant Tintri die Einführung von Warnmeldungen auf der Basis von Anomalie-Erkennung.

Charakteristische unveränderliche Snapshots

Manche Storageanbieter fügen ihren Lösungen jetzt Features hinzu, um diese für Ransomware-Infektionen weniger anfällig zu machen. Nicht so bei VMstore. Dieser Schutz war schon immer Teil der VMstore-Architektur.

Die Metadaten, die VMstore sammelt, um seine AIOPS-Fähigkeiten zu ermöglichen, werden separat von den Daten gespeichert. Im einzigartigen Tintri File System basieren Snapshots auf Metadaten-Pointern. Diese Metadaten werden so gespeichert, dass Ransomware sie nicht ändern kann. Deshalb sind die Metadaten und die Snapshots für Ransomware auch unsichtbar. Somit war VMstore unveränderbar, lange bevor dies zum Trend wurde.

Leistungsfähige Snapshots

Viele Enterprise Storagesysteme benutzen Snapshots als Datensicherungsmechanismus. Das gilt auch für VMstore, und VMstore Snapshots sind leistungsfähiger als die vieler anderer Storagelösungen.

Schnelle Snapshots, welche den Workload nicht beeinträchtigen. VMstore zählt zu den wenigen Enterprise Storage-Arrays, die schnelle Snapshots bereitstellen, welche den Workload nicht beeinträchtigen. Diese Snapshots ermöglichen Backups mit niedrigem RPO und Replikation. Im Fall von Tintri ermöglichen sie auch die schnelle Wiederherstellung von Anwendungen.

VMstore Snapshots bieten Granularität auf Objektebene. Die Snapshots können global, per-VM und per-SQL Server Datenbank durchgeführt werden. Durch per-VM Snapshots kann jede vDisk einzeln zum Klonen und Wiederherstellen verwendet werden.

Die Möglichkeit, Snapshots auf dieser Granularitätsebene zu verwalten, ist für viele alltägliche Vorgänge nützlich. Besonders nützlich ist dies bei der gezielten Datenwiederherstellung nach einem erfolgreichen Ransomware-Angriff.

In den meisten LUN-basierten Umgebungen teilen mehrere VMs und Anwendungen eine einzige LUN. Wenn die Daten einer Anwendung wiederhergestellt werden müssen, muss die gesamte LUN bis zu diesem Zeitpunkt wiederhergestellt werden. Dies ist im Vergleich mit der Wiederherstellung von nur den betroffenen VMs viel zeitaufwändiger und betrifft mehr als nur die notwendigen Daten.

Wiederherstellung zu einem beliebigen Zeitpunkt und sogar zu mehreren Zeitpunkten. VMstore unterstützt mehr als 100 Snapshots pro geschütztem Objekt, und SyncVM ermöglicht das Recovery aus mehreren Snapshots. Mit SyncVM können IT-Mitarbeiter mehrere Wiederherstellungspunkte testen, um den besten Snapshot zu ermitteln, der für die Wiederherstellung der Anwendung zu verwenden ist.

Die platzsparenden und zeitgestempelten Snapshots von VMstore sind Pointer- und Metadaten-basiert. Unternehmen, die einen erfolgreichen Ransomware -Angriff erlitten haben, können diese Snapshots nutzen, um die forensische Analyse nach Wiederaufnahme des Normalbetriebes zu ermöglichen.

Richtlinienbasierte skalierbare Datensicherung. Zahlreiche Tintri-Umgebungen unterstützen mehr als 100.000 VMs, Datenbanken oder Container. Die Tintri Global Center Management-Anwendung bietet eine richtlinienbasierte Planung von Snapshot- und Replikationsaufgaben. Dadurch kann ein Unternehmen konsistenten Schutz auf Anwendungsebene einsetzen, indem es VMs der entsprechenden Richtlinie zuordnet. Unternehmen können die Datensicherung mittels PowerShell und REST APIs auch dynamisch und skalierbar verwalten.

Effiziente Verwaltung von Datenkopien verbessert die Agilität. Unternehmen können die VM-zentrierte, schnelle Snapshot-Technologie von VMstore nutzen, um die Anwendungsentwicklung zu beschleunigen. SyncVM kann die Produktionsdaten für mehrere Entwicklungsserver mit minimaler Datenbewegung aktualisieren.

Mit SyncVM entfällt die mühsame, zeitaufwändige und schwierige Aufgabe, Anwendungsentwicklern einen vollständigen und einigermaßen aktuellen aktuellen Datensatz für die Entwicklung bereitzustellen. Weiterhin gewährt VMstore mit seinem Auto-QoS Entwicklern Zugriff zu schnellem Storage, ohne die Leistung von Produktionsanwendungen zu gefährden. So können Unternehmen VMstore nutzen, um Overhead-Kosten im Anwendungsentwicklungsprozess zu eliminieren, und gleichzeitig die Entwicklungszyklen und Qualität zu verbessern.

Für Ransomware unsichtbar. TxOS, das VMstore Betriebssystem, reserviert intern Speicherplatz für Metadaten. Dieses Metadaten-Repository ist für Anwendungen, Hosts oder Clients unsichtbar. Demzufolge ist die Pointer- und Metadaten-basierte Snapshot-Architektur von TxOS für Ransomware unsichtbar. Dies ist wichtig, da viele Ransomware-Angriffe Datensicherungsmechanismen zu umgehen versuchen und Backups bereits zu Beginn eines Angriffs verschlüsseln.

Flexible Replikation

Tintri VMstore unterstützt asynchrone Replikation mit RPO/RTO via ProtectVM mit einer Häufigkeit von bis zu 1-minütigen periodischen Intervallen. VMstore unterstützt hochfrequente Snapshots für bis zu 200 Schlüssel-VMs mit einem RPO von einer Minute; Standardintervalle liegen typischerweise bei 15 Minuten. Zu den zusätzlichen Replikationsfunktionen gehören synchrone Replikation, One-to-One, One-to-Many und Many-to-One. Bei diesen Replikationsoptionen geht es in erster Linie darum Disaster Recovery und Business Continuity zu ermöglichen.

Eine weitere Replikationsoption, die sich am meisten auf den Schutz vor Ransomware bezieht, ist die Fähigkeit von VMstore auf S3-Storage in mehreren Public Clouds zu replizieren. Tintri verfügt über Unterstützung bei AWS, IBM und Wasabi. Die Wasabi-Option ist interessant, da Wasabi den Schwerpunkt auf Performance legt und da keine Gebühren für die Nutzung oder den Export der Objektdaten anfallen. Durch die Replikation auf S3 werden die Snapshots aus dem primären Storagesystem entfernt, was eine weitere Sicherungsebene darstellt. Snapshots, die auf S3-Storage repliziert wurden, können dann auf jeder VMstore-Appliance wiederhergestellt werden.

Granulare, richtlinienbasierte Datensicherung ermöglicht nahezu unmittelbares Recovery

Da VMstore von Grund auf für das Management von VMs—und jetzt auch von SQL -Datenbanken und Containern - konzipiert wurde, kann es richtlinienbasierte Datensicherung und Wiederherstellung/Recovery auf der gleichen Granularitätsebene bieten. Dies befähigt Tintri VMstore-Infrastrukturen dazu, den Normalbetrieb innerhalb von Minuten- oder Stunden wiederaufzunehmen, und nicht die 21-tägige Ausfallzeit in Kauf nehmen zu müssen, welche die meisten Unternehmen nach einem erfolgreichen Ransomware-Angriff erleiden.

Aufgrund der Häufigkeit dieser Angriffe hat Tintri Tools zur Recovery-Automatisierung via Scripts hinzugefügt. Dies beschleunigt zusätzlich die Anwendungswiederherstellung bei gleichzeitiger Reduzierung der Wahrscheinlichkeit von menschlichem Versagen während des gesamten Prozesses.

Über die derzeitigen Möglichkeiten der Ransomware-Abwehr hinaus

Multi-Faktor-Authentifizierung. Zusätzlich zu den oben beschriebenen rollenbasierten Zugriffskontrollen plant Tintri, die Sicherheit mittels Multi-Faktor-Authentifizierung weiter zu verbessern. Multi-Faktor-Authentifizierung (MFA) verhindert das Einloggen von Angreifern in die VMstore-Infrastruktur, selbst wenn diese den Benutzernamen und das Passwort eines Administrators erlangt haben. Sie erfordert einen zusätzlichen Mechanismus zur Authentifizierung eines Anmeldeversuches, häufig durch Anforderung eines physischen Sicherheitsschlüssels oder eines Telefons mit einer Authentifizierungsanwendung. MFA ist ein bewährtes Sicherheitserfahren.

Warnungen auf Basis von Anomalie-Erkennung. Tintri plant die Erweiterung seiner intelligenten Infrastruktur-Fähigkeiten durch eine Warnfunktion, die auf Anomalie-Erkennung basiert. VMstore bietet einen robusten Kernsatz an AIOPS-Fähigkeiten, welche die Servicequalität für jede Anwendung überwachen und automatisch optimieren. Die Erkennung von Anomalien im Zusammenhang mit Cyberangriffen und Ransomware-Infektion stellt eine natürliche Erweiterung dieser AIOPS-Fähigkeiten dar, und adressiert ein Problem, das bis in die Vorstandsetage hineinreicht.

Tintri VMstore bietet herausragende Ransomware-Abwehr und -Recovery

Ransomware-Angriffe werden von Jahr zu Jahr deutlich ausgefeilter und erfolgreicher. Demzufolge muss jedes Unternehmen davon ausgehen, dass es das nächste Ziel sein wird, und muss dementsprechend planen. Diese Pläne müssen sich auf die Eindämmung einer Ransomware-Infektion konzentrieren, die Identifizierung der betroffenen Anwendungen und dann die schnellstmögliche Wiederherstellung jener Anwendungen zum normalen Betriebszustand.

Tintri kombiniert eine umfassende Palette von Datensicherungsfunktionen der Unternehmensklasse, die auf dem charakteristischen Management-per-VM aufbauen, um herausragende Ransomware-Abwehr und schnelle Wiederherstellung/Recovery von Anwendungen zu liefern.

Manche werden sagen, dass Tintri-Kunden angesichts dieser Ransomware-Bedrohung einen unfairen Vorteil bei der Aufrechterhaltung ihres Betriebes haben. Ich bezeichne diesen Vorteil nicht als unfair. Ich behaupte vielmehr, dass Tintri seinen Kunden einen intelligenten Vorteil bietet.

Für weitere Informationen darüber, wie Ihr Unternehmen von Tintri profitieren kann, besuchen Sie bitte die Tintri-Webseite unter www.tintri.com/de oder kontaktieren Sie Ihren bevorzugten Tintri-Vertriebspartner. ■

Quellen:

1. https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469 Referenced 8/12/2021
2. https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020 Referenced 8/12/2021
3. https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542 Referenced 8/12/2021
4. https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469 Referenced 8/12/2021