Aufbau eines Cyber Resilience Vault mit Zerto

Wie man nach Ransomware-Angriffen eine schnelle Air-Gapped-Wiederherstellung erreicht

Die Bedrohungslage durch schwerwiegende und raffinierte Ransomware und Cyberangriffe verschärft sich. Eine aktuelle Studie von IDC ergab, dass die meisten Disaster Recovery (DR)-Vorfälle in den letzten 12 Monaten auf Ransomware und Malware zurückzuführen waren. Angriffe lassen sich dank der zunehmenden Verbreitung von Ransomware-as-a-Service immer kostengünstiger ausführen, und erfolgreiche Lösegelderpressungen ermuntern Cyberkriminelle zur Entwicklung von Malware der nächsten Generation.

Unternehmen brauchen eine starke, proaktive Defense-in-Depth-Strategie, um Angriffe zu verhindern und zu unterbinden – sogenannte „Left of Boom"-Technologien. Genauso wichtig sind aber auch die „Right of Boom"-Technologien, die sich auf die Wiederherstellung nach einem Angriff konzentrieren. Unternehmen müssen auf maßgeschneiderten Datenschutz setzen, um eine schnelle, skalierbare Lösung zur schnellen Erkennung, Behebung und Wiederherstellung aufzubauen.

Warum gerade jetzt?

Obwohl präventive Left-of-Boom-Lösungen heute effektiver sind als je zuvor, werden an die Unternehmens-IT immer strengere Anforderungen gestellt. Anbieter von Cyberversicherungen fordern von Unternehmen schärfere Sicherheitsvorkehrungen, wie etwa die Einführung von Data Vaults. Speziell in den USA plant die US-Börsenaufsichtsbehörde SEC noch strengere Anforderungen für Aktiengesellschaften, einschließlich der Benennung von Verantwortlichen für die Cyberresilienz Strategie. Noch nie war der Bedarf an einem umfassenden und entschiedenen Ansatz so groß wie heute.

Traditionelle Vaults sind nicht sicher genug

Die gängigen Methoden zur Verbesserung der Cyberresilienz stützen sich auf riskante Vault-Technologien und -Architekturen. Einer der größten Nachteile ist die Geschwindigkeit der Wiederherstellung, d. h. Recovery Time Objective (RTO). Daten von Bandspeichern oder aus einer niedrigen Speicherebene abzurufen kann die Wiederherstellung um Tage oder Wochen verlängern. Das Suchen nach sauberen Kopien verlängert den Prozess noch weiter, ebenso wie die Wiederherstellung auf etwas anderes als produktionstaugliche Arrays. Wenn Strafverfolgungsbehörden oder Sicherheitsteams forensische Analysen in der Produktionsinfrastruktur durchführen, müssen sie die Workloads nach der Wiederherstellung möglicherweise für einige Zeit an einem anderen Ort ausführen – etwas, das keine speziell entwickelte Backup-Appliance (Purpose-Built Backup Appliance, kurz: PBBA) und kein Cold Cloud Storage unterstützen kann. Der Geschäftsbetrieb muss schnell wieder aufgenommen werden, doch herkömmliche Sicherungs- und Archivierungslösungen sind darauf nicht ausgelegt.

Schnelle Wiederherstellung mit Zerto

Zerto, ein Unternehmen von Hewlett Packard Enterprise, ermöglicht es Unternehmen, einen unangreifbaren Wiederherstellungs-Vault zu erstellen und anzupassen, der selbst die verheerendsten Ransomware-Szenarien entschärfen kann.

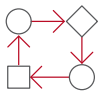
Der Zerto Cyber Resilience Vault stützt sich auf drei Säulen, die eine dezentralisierte Zero-Trust-Architektur nutzen, um eine schnelle Air-Gapped-Wiederherstellung zu erreichen.

Replizieren und erkennen

Durch die nahezu synchrone Streaming-Datenreplikation wird jeder Schreibvorgang in der Produktion geschützt und verdächtige Anomalien werden sofort erkannt und gemeldet.

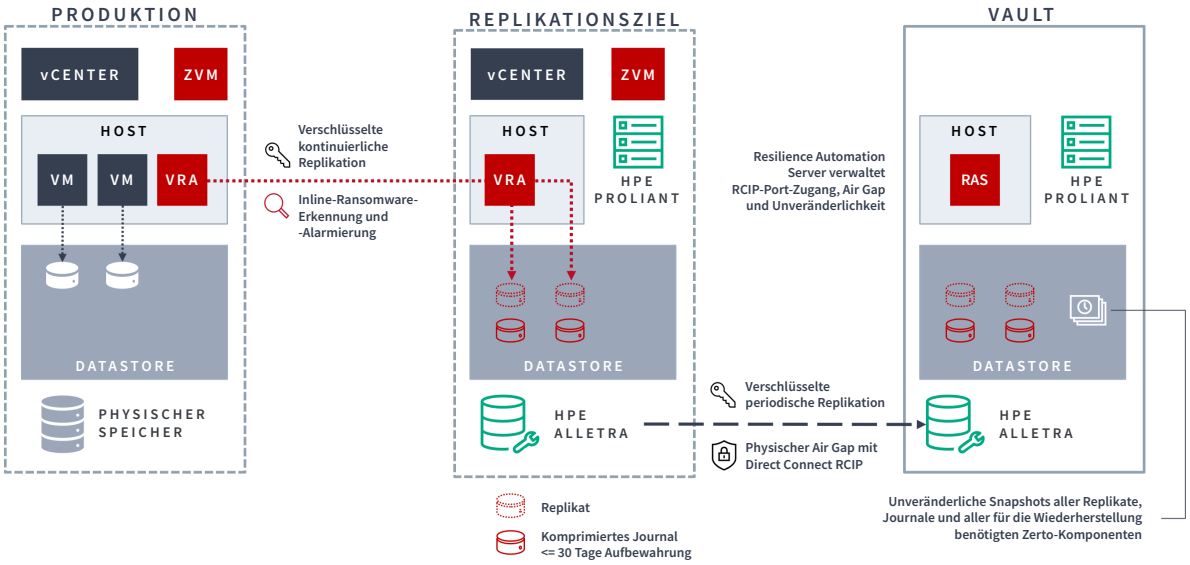
Isolieren und sperren

Der separierte Vault wird durch einen Air Gap physisch isoliert und verwahrt unveränderliche Datenkopien auf sicherer, hochleistungsfähiger und FIPS-validierter Hardware.



Testen und wiederherstellen

Identifizieren Sie mühelos saubere Wiederherstellungspunkte und stellen Sie schnell ganze Multi-VM-Anwendungen auf Hochleistungsspeicher wieder her – und das alles unter Wahrung der VM-übergreifenden Konsistenz, selbst bei tausenden von VMs.



So funktioniert‘s

Der Kern dieser Cyberresilienz-Lösung basiert auf HPE Alletra, HPE ProLiant und Zerto, mit drei wichtigen Infrastrukturkonzepten, die an den oben erwähnten Säulen ausgerichtet sind.

1 Replikationsziel

Diese sicher mit dem Produktionsstandort gekoppelte vSphere-basierte Landing Zone kann lokal oder remote sein und auch als herkömmliches DR-Ziel dienen, wenn sie sich außerhalb des Standorts befindet. Die Zone dient als Replikationsziel für Continuous Data Protection (CDP) mit Zerto. Die CDP-Replikation von Zerto verwendet keine Agenten, d. h. es gibt nichts innerhalb einer geschützten VM, das durch Malware deaktiviert oder gekapert werden könnte. Jeder Schreibvorgang auf geschützten VMs wird verschlüsselt, komprimiert und an das Replikationsziel gesendet, wo er in einem dynamischen CDP-Journal gespeichert wird – einem Streaming-Protokoll mit Tausenden von Wiederherstellungspunkten mit VM-übergreifender Konsistenz und Einhaltung der Schreibreihenfolge. Das Journal hat einen benutzerdefinierten Verlauf von einer Stunde bis zu 30 Tagen und ist die erste und beste Option für die Wiederherstellung nach einem Ransomware-Angriff.

Die Journale und alle zugehörigen Replikate sind an virtuelle Appliances geknüpft, die auf HPE ProLiant ausgeführt werden, wobei die Datenspeicher auf HPE Alletra vLUNs liegen. Da die Schreibvorgänge für das Journal gespiegelt werden, werden sie zugelich anhand der Echtzeit-Verschlüsselungserkennung von Zerto überprüft, um eine frühzeitige Warnung vor möglichen Infektionen sicherzustellen. Als zusätzliche Sicherheitsmaßnahme prüft HPE InfoSight, welches in HPE Alletra enthalten ist, alle Daten auf Anomalien.

2 Cyber Resilience Vault

Der Vault selbst, der sich an demselben Standort wie das Replikationsziel befindet, umfasst auch HPE ProLiant und HPE Alletra. Der isolierte Vault oder Reinraum ist durch einen Air Gap physisch separiert und hat keine Verbindung zum Internet oder zum Produktionsnetzwerk. Da keine zentrale Steuerungsebene vorhanden ist, gibt es bei dem Vault keinen ungeschützten Verwaltungs-Port und keinen einzelnen Kompromittierungspunkt. HPE Alletra am Wiederherstellungsstandort und HPE Alletra im Vault nutzen Direct Connect Remote Copy over IP (RCIP) für die Punkt-zu-Punkt-Replikation aller Daten vom Wiederherstellungsstandort, einschließlich der von Zerto erstellten Journale und Replikate. Dieser Ansatz kombiniert die Vorteile synchroner Replikation (z. B. extrem geringe RPOs und hohe Leistung) und traditioneller asynchroner Ansätze (z. B. höhere Latenztoleranz und geringerer Speicherverbrauch).

3 Vault-Automatisierung

Der Resilience Automation Server (RAS) innerhalb des Vault ist eine leichtgewichtige VM, die mittels nativer Switch- und Array-Services von HPE wichtige Maßnahmen zur Cyberresilienz steuert, darunter:

- Aktivieren und Deaktivieren von RCIP auf HPE Alletra, um einen vollständig isolierten Vault zu erhalten.
- Zufallsgenerierung der Replikations-Ports, um die Vorhersagbarkeit des Datenverkehrs zu verringern.
- Erstellung unveränderlicher Snapshots mit der Virtual Lock-Technologie von HPE Alletra (nicht einmal der technische Support von HPE kann diese manipulationssicheren Retention Locks auflösen).
- Wiederherstellung des Zerto Virtual Manager, der Journale und Replikate, um ein sauberes Zerto-Deployment innerhalb des Vault sicherzustellen, falls alles andere außerhalb des Vault kompromittiert wird.
- Protokollierung aller Aktivitäten innerhalb des Vault zur Erstellung eines Auditprotokolls.

Wiederherstellungsprozess

Diese Zerto-Architektur deckt eine Vielzahl von Infektionsszenarien ab, darunter:

Infektion auf Datei-/Ordner-/VM-Ebene: Wenn sich der Radius der Ransomware auf Dateien und Ordner auf einer VM beschränkt, können diese fast sofort an ihrem Ursprungsort wiederhergestellt werden, und zwar von einem Zerto-Journal-Zeitstempel, der nur 5–15 Sekunden vor der Infektion liegt. Wenn eine oder mehrere VMs mit Ransomware verschlüsselt sind, ermöglicht Zerto nahezu sofort und ohne Zwischenschritte die Wiederherstellung in der Produktionsumgebung (z. B. Storage vMotion). Diese Wiederherstellung kann auch für alle VMs gelten, die einen Multi-VM-Anwendungs-Stack bilden. Dies beinhaltet, dass für die Wiederherstellung derselbe saubere Point-in-Time-Checkpoint verwendet wird, im Abstand von Sekunden mit eingehaltener Schreibreihenfolge, anstelle von Zeitstempeln, die über ein nächtliches Backup-Fenster gestaffelt sind.

Kontamination des gesamten Workloads: Wenn alle VMs am Produktions- bzw. Ursprungsort infiziert wurden, der Wiederherstellungsort aber noch aktiv und nicht betroffen ist, kann ein vollständiges Failover sicherstellen, dass der Betrieb innerhalb von Minuten wieder aufgenommen werden kann. Da es sich bei HPE Alletra um eine erstklassige produktionstaugliche Top-Tier-Speicherlösung handelt, die für unternehmenskritische Workloads entwickelt wurde, können Anwendungen von diesem sekundären Standort aus ausgeführt werden, ohne dass es zu Leistungseinbußen kommt und ohne dass eine zusätzliche Migration auf einen zusätzlichen Standby-Speicher erforderlich ist, der für die Ausführung von Unternehmens-Workloads geeignet ist.

Standortübergreifende Infektion: Wenn sowohl die Produktions- als auch die Wiederherstellungsstandorte ausgefallen sind – z. B. im Falle verschlüsselter Hosts und schneller lateraler Bewegungen trotz Netzwerksegmentierung –, wird der in diesem Leitfaden beschriebene Zerto Cyber Resilience Vault zum sichersten Reinraum, in dem die Wiederherstellung erfolgen kann. Hier eine grobe Zusammenfassung des Wiederherstellungsprozesses:

1. Wiederaufbau des Wiederherstellungsstandorts: Innerhalb des isolierten Vaults wird ein unveränderlicher Snapshot verwendet, um das VMFS unter Beibehaltung der UUID-Signaturen erneut bereitzustellen.
2. Wiederherstellung von Zerto: Aufgrund der Resilienz von Zerto können die virtuellen Manager und Data Mover ohne manuelle Neukonfiguration oder Einrichtung online gehen und den Betrieb wieder aufnehmen.
3. Wiederherstellung von Daten: Wählen Sie mithilfe des Zerto-Journals einen der Tausenden verfügbaren Wiederherstellungspunkten aus, um alle VMs in der von Ihnen ausgewählten Boot-Reihenfolge wiederherzustellen. Die Orchestrierungs-Engine von Zerto in Kombination mit der erstklassigen Leistungsfähigkeit von HPE Alletra ermöglichen ein RTO von Minuten anstatt von Stunden, Tagen oder Wochen. Multi-VM-Anwendungs-Stacks werden schnell zum genau gleichen Zeitpunkt wiederhergestellt, wodurch der manuelle Konfigurationsaufwand nach der Wiederherstellung minimiert wird.

Sicherheit durch Design trifft auf Performance durch Design

Der Zerto Cyber Resilience Vault kombiniert Sicherheit und Performance, um die heutigen gesetzlichen und Compliance-Anforderungen zu erfüllen:

- Vollständiger physischer Air Gap für einen isolierten, unverbundenen Vault
- Zero-Trust-Architektur
- FIPS 140-2-validiert
- Abgesicherte virtuelle Linux-Appliances
- Integrierte Prinzipien der geringsten Privilegien
- Unveränderliche Offsite/Offline-Kopien, die mit einem nicht entfernbaren Virtual Lock gesichert sind
- Manipulationssicherer NTP-Schutz
- Inline-Erkennung von Ransomware in Echtzeit
- Skalierbar auf 10.000 VMs pro vCenter
- Verschlüsselung bei der Speicherung und auf dem Übertragungsweg
- Chiffriertext-, zeit- und verschlüsselungsbasierte Passwörter
- Garantierte Verfügbarkeit von 99,9999 % für den Wiederherstellungs-/DR-Standortspeicher
- Produktionstaugliche Arrays zur Ausführung anspruchsvollster Anwendungen
- KI-gestützter, selbstheilender Speicher
- Silicon Root of Trust für sämtliche Hardware
- Dezentralisierte Verwaltung zur Beseitigung einzelner Kompromittierungspunkte

Die Lösung für echte Cyberresilienz

Mit dem Cyber Resilience Vault von Zerto erhalten Unternehmen sichere, hochgradig anpassbare Optionen, um eine maßgeschneiderte Lösung für ihren Betrieb zu entwickeln. Die einzigartigen flexiblen Architekturen von Zerto ermöglichen Ihnen eine schnelle Wiederherstellung nach Ransomware-Angriffen.

- Minimieren Sie die Ausfallzeit nach einem Angriff und vermeiden Sie direkte oder indirekte Umsatzeinbußen.
- Erfüllen Sie Compliance-Anforderungen gemäß Vorschriften wie HIPAA, DSGVO, SOX, oder FISMA/NIST SP 800-34.
- Geringere Komplexität dank einer Lösung aus einer Hand, die Best-of-Breed-Produkte für jeden einzelnen Schritt der Wiederherstellungskette umfasst.

Kontaktieren Sie uns, um eine Demo zu sehen, Informationen zu unseren Paketpreisen zu erhalten und zu erfahren, was Ransomware-Resilienz für Ihr Unternehmen bedeuten kann.

KONTAKT

Über Zerto

Zerto, ein Unternehmen von Hewlett Packard Enterprise, ermöglicht es seinen Kunden, einen Always-On-Betrieb zu managen, indem es den Schutz, die Wiederherstellung und die Mobilität von On-Premises- und Cloud-Anwendungen vereinfacht. Zerto beseitigt die Risiken und Komplexitäten, die mit der Modernisierung und Cloud-Einführung in privaten, öffentlichen und hybriden Umgebungen verbunden sind. Die einfache Softwarelösung basiert auf Continuous Data Protection (CDP), um Ransomware-Resilienz, Disaster Recovery und Multi-Cloud-Mobilität sicherzustellen. Zerto genießt das Vertrauen von über 9.500 Kunden weltweit und unterstützt Angebote für Amazon, Google, IBM, Microsoft, Oracle und mehr als 350 Managed Service Provider. **www.zerto.com**

RITM0090405