Zerto Cyber Resilience Vault

Die Lösung für schnelle Air-Gapped-Wiederherstellung

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 beiden Aspekten Priorität einräumen, um Ransomware schnell zu erkennen, darauf zu reagieren und sich davon zu erholen.

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, möglicherweise etwa die Einführung von Data Vaults. In der EU lenkt der Digital Operational Resilience Act (DORA) die Aufmerksamkeit auf Sicherheit und Business Continuity. In den USA hat die US-Börsenaufsichtsbehörde SEC strenge Anforderungen für Aktiengesellschaften eingeführt, einschließlich der Benennung von Verantwortlichen für ihre Cyberresilienz Strategie. Noch nie war der Bedarf an einem umfassenden und entschiedenenAnsatz 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 aus alten Kopien 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, auf einen All-in-One-Cyber-Wiederherstellungs-Vault zu vertrauen, 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

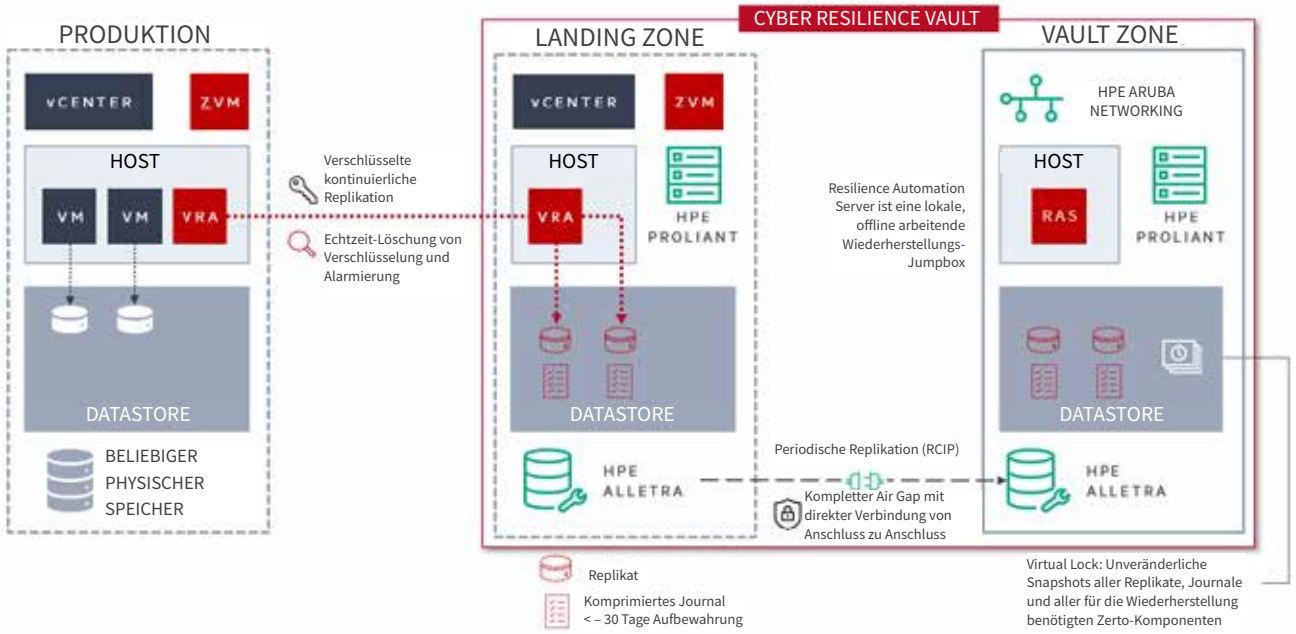
Durch die nahezu synchrone Streaming-Datenreplikation wird jeder Schreibvorgang in der Produktion geschützt und verdächtige Anomalien werden sofort erkannt und gemeldet.

Isolieren und sperren

Der separierte Vault wird durch einen Air Gap offline isoliert und verwahrt unveränderliche Datenkopien auf sicherer, hochleistungsfähiger Hardware von HPE.

Testen und wiederherstellen

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



So funktioniert‘s

Der Kern der Lösung ist HPE Alletra Storage, HPE ProLiant Compute, HPE Aruba Networking und Zerto, mit zwei wichtigen Infrastrukturzonen, die an den oben erwähnten Säulen ausgerichtet sind.

1 Landing Zone

Die sicher mit dem Produktionsstandort gekoppelte VMware vSphere-basierte Landing Zone kann lokal oder remote sein und auch als herkömmliches DR-Ziel dienen, wenn sie sich außerhalb des Standorts befindet. Die Landing 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 die Landing Zone 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. Die Verschlüsselungsanalyse ist auch über API verfügbar, um eine weitere Bewertung und Visualisierung mit Ihrem bestehenden Sicherheitslösungs-Stack zu ermöglichen.

2 Vault Zone

Der Vault selbst, der sich physisch an demselben Standort wie die Landing Zone befindet, umfasst auch HPE ProLiant und HPE Alletra. Die isolierte Vault Zone oder der Reinraum ist durch einen Air Gap vollständig 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 in der Landing Zone und HPE Alletra in der Vault Zone nutzen Direct Connect Remote Copy over IP (RCIP) für die Punkt-zu-Punkt-Replikation aller Daten von der Landing Zone, 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). Schlussendlich ist der Resilience Automation Server (RAS) innerhalb der Vault Zone ein leichtgewichtiger Server, der wichtige Services ausführt und mittels der nativen Services in HPE Aruba und HPE Alletra wichtige Maßnahmen zur Cyberresilienz steuert.

3 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, die Landing Zone 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 produktionstaugliche All-Flash-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 Zerto Cyber Resilience Vault zum sichersten Reinraum, in dem die Wiederherstellung erfolgen kann. Hier eine grobe Zusammenfassung des Wiederherstellungsprozesses:

- **Wiederaufbau des Wiederherstellungsstandorts:** Innerhalb des isolierten Vaults wird ein unveränderlicher Snapshot verwendet, um das VMFS unter Beibehaltung der UUID-Signaturen erneut bereitzustellen.
- **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.
- **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 oder Stunden anstatt von 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 Leistung durch Design

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

- Vollständiger Air Gap für einen isolierten, unverbundenen Vault
- Zero-Trust-Architektur
- Abgesicherte virtuelle Linux-Appliances
- Integrierte Prinzipien der geringsten Privilegien
- Unveränderliche Offsite- und Offline-Datenkopien
- Manipulationssicherer NTP-Schutz
- Inline-Echtzeit-Erkennung von Verschlüsselung
- Skalierbar auf mehr als 10.000 VMs pro vCenter
- Chiffriertext-, zeit- und verschlüsselungsbasierte Passwörter
- Garantierte Verfügbarkeit von 100 % für den Landing Zone-Speicher
- All-Flash-Arrays der nächsten Generation zur temporären Ausführung anspruchsvollster Anwendungen nach der Wiederherstellung
- KI-gestützter, selbstheilender Speicher
- Silicon Root of Trust für sämtliche Hardware
- Dezentralisierte Verwaltung zur Beseitigung einzelner Kompromittierungspunkte

Die Lösung für echte Cyberresilienz

Mit dem Zerto Cyber Resilience Vault haben Unternehmen jetzt eine sichere und leistungsstarke Lösung, um der Bedrohung durch Ransomware zu begegnen. Die einzigartige, dezentrale Architektur von Zerto ermöglicht eine schnelle Air-Gapped-Wiederherstellung selbst nach dem schlimmsten Angriff.

- Minimieren Sie die Ausfallzeit nach einem Angriff und vermeiden Sie direkte oder indirekte Umsatzeinbußen.
- Unterstützen Sie die Erfüllung von Compliance-Anforderungen gemäß Vorschriften wie HIPAA, DORA, 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 Cyber-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 Kundinnen und 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, softwarebasierte Lösung nutzt 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