LÖSUNGSÜBERSICHT

InfiniBox® Data Defense: Unabhängig von der Art der Bedrohung – Ransomware, Naturkatastrophe, Systemausfall, menschliches Versagen – InfiniBox hält Ihnen den Rücken frei.

DIE HERAUSFORDERUNG

Daten sind heutzutage einer größeren Gefahr ausgesetzt als je zuvor. Naturkatastrophen kommen immer häufiger vor, und einfaches menschliches Versagen kann dazu führen, dass große Mengen Ihrer wertvollen Daten völlig unbrauchbar werden. Heutzutage steht bei CEOs, CIOs und CSOs auch Cybercrime, wie Ransomware und Malware, ganz oben auf der Liste der Bedrohungen.

Wenn sich das für Sie dramatisch und gefährlich anhört, liegt das daran, dass es das auch ist – oder zumindest sein kann, wenn Sie unvorbereitet sind. Die meisten Unternehmen betreiben den üblichen Datenschutz (wie Backups), um ihre Daten vor diesen Bedrohungen zu schützen. Viele setzen auch auf Business Continuity Planning, damit ihre Daten trotz Störungen und Angriffen zuverlässig und verfügbar bleiben. Diese Planungen werden durch die zunehmende Verbreitung von Ransomware und Malware zusätzlich erschwert.

Selbst fortschrittliche Unternehmen sind sich nicht immer sicher, ob sie ihre Daten ausreichend geschützt haben. Um die neuesten Standards des modernen Datenschutzes, einschließlich der Daten- und Cybersicherheit, sicherzustellen, liefern InfiniBox und InfiniBox SSA von Infinidat die Infinisafe®-Referenzarchitektur. Mit Hilfe dieser Referenzarchitektur können Sie die passenden Verfahren mit den passenden Tools und Technologien so einrichten, dass Ihre Daten jederzeit sicher, verfügbar und zuverlässig sind.

In dieser Lösungsübersicht untersuchen wir eine der häufigsten und größten Bedrohungen für Daten: Cybercrime und Ransomware.

> *„... Cybercrime ist inzwischen ein so ernstes Problem, dass in jüngsten Umfragen von Fortune im Mai 2021 und von KPMG im März 2021 Risiken für die Cybersicherheit als die größte Bedrohung für Unternehmen genannt wurden."*

Cybercrime nimmt exponentiell zu

- Es geht nicht mehr darum, OB, sondern WANN Sie angegriffen werden und wie oft. Sie können davon ausgehen, dass sich Cyberattacken auch gegen Ihr Unternehmen richten werden, und Sie sollten darauf vorbereitet sein.
- Cybercrime bleibt nicht auf eine einzige Angriffsart beschränkt. Zu den gängigsten Arten gehören Phishing-Betrug, Online-Diebstahl von geistigem Eigentum und Internet-Betrug (der berüchtigte „UN-Generalsekretär" bietet dem glücklichen Empfänger zig Millionen Euro an).
- Anspruchsvolle Malware-Angriffe wie Advanced Persistent Threat (APT) erfordern zwar mehr Ressourcen, sind aber äußerst lukrativ. APT-Hacker zielen auf datenreiche Netzwerke mit wertvollen Daten, große Geldsummen und das Potenzial für eine maximale öffentliche Bloßstellung ab, sollte ein Angriff erfolgreich sein.[1]
- In der Tat ist Cybercrime inzwischen ein so ernstes Problem, dass in jüngsten Umfragen von Fortune im Mai 2021[2] und von KPMG im März 2021[3] Risiken für die Cybersicherheit als die größte Bedrohung für Unternehmen genannt wurden.
- Es gibt eindeutige Belege dafür, dass Cyberangriffen eine monatelange Planung vorausgeht. Im Durchschnitt haben Eindringlinge schon mehr als 9 Monate vor der Attacke mit der Unterwanderung der Unternehmensumgebung begonnen.

Ransomware

Ransomware ist eine Form von Malware. Doch im Gegensatz zu risikoreichen und lukrativen APT-Angriffen können Hacker Ransomware direkt und problemlos im Darkweb kaufen. Ein Großteil davon ist sehr billig, und einige findige Anbieter „vermieten" sogar Ransomware, was zur Entstehung von Cybercrime-as-a-Service (CaaS) geführt hat.[4]

[1] „What is an Advanced Persistent Threat?" Kaspersky
[2] „Fortune 500 CEO survey"
[3] „KPMG 2021 CEO Outlook Pulse Survey"
[4] „Revealed: The Supermarkets that Will Sell You Malware for $50", Forbes

Ransomware-Angriffe schleusen Software ein, die automatisch alle Dateien und Datenträger verschlüsselt, auf die sie zugreifen kann. Wenn die Ransomware einen vernetzten Computer angreift, breitet sich der Verschlüsselungsprozess auf das Netzwerk aus und wirkt sich auf alle primären und sekundären Speicher, einschließlich Backups und Archive, aus. In vielen Fällen wird der sekundäre Speicher tatsächlich zuerst angegriffen, was die Wiederherstellungsmöglichkeiten beschränkt und die Position des Angreifers stärkt. Die Hacker verlangen anschließend von den Geschädigten eine Zahlung als Gegenleistung für die Herausgabe des Entschlüsselungscodes.

Warum sollte man das geforderte Geld nicht zahlen?

Viele Geschädigte zahlen lieber das Lösegeld in der Hoffnung, den Schlüssel zu erhalten, als ihre Daten zu verlieren.

Das ist häufig ein aussichtsloses Unterfangen. Der von Sophos veröffentlichte Bericht **State of Ransomware 2021** enthüllt die Ergebnisse der Untersuchungen des Unternehmens zu Ransomware-Zwischenfällen: 92 % der Unternehmen, die in den letzten 12 Monaten Lösegeld gezahlt haben, konnten nicht alle ihre Daten wiederherstellen. Die durchschnittliche Menge der wiederhergestellten Daten aller Befragten lag bei 65 %, das heißt, dass einige von ihnen ihre Daten teilweise, einige vollständig und einige überhaupt nicht wiederherstellen konnten. Der Bericht von Sophos zeigt außerdem, dass sich die durchschnittlichen Kosten für die Wiederherstellung von Daten in der ersten Hälfte des Jahres 2021 gegenüber 2020 bereits verdoppelt haben. Am Ende können die Kosten für die Wiederherstellung in die Millionen gehen.

> *„Ich war äußerst beeindruckt von der Leistung, der Kosteneffizienz und der Verwaltung des Systems, das OFFSITE eingerichtet hat … Die Funktionalität für unveränderliche Snapshots von Infinidat stellt einen großen Mehrwert zum Schutz der Daten vor Ransomware dar.“*
>
> — **Chief Technology Officer**, OFFSITE

Zudem legen die Regierungen vieler Staaten weltweit Regeln, Vorschriften und Gesetze für die Zahlung von Lösegeld und die Meldung von derartigen Vorfällen fest. Unternehmen müssen über die Anforderungen in ihrer konkreten Region auf dem Laufenden bleiben.

DIE LÖSUNG

Das leistungsstarke Speichersystem InfiniBox von Infinidat bietet eine KI-gesteuerte „Set-it-and-forget-it“-Lösung mit beispielloser 100-prozentiger Verfügbarkeit, unübertroffener Leistung und deutlich niedrigeren Gesamtbetriebskosten. Durch getrennte Verwaltungs- und Datenebenen wird ein leistungsstarker Datenschutz in die Systemarchitektur integriert.

Die Abwehrfunktionen von InfiniBox ermöglichen einen besseren Schutz der Daten durch Snapshots/unveränderliche Snapshots, Replikation, Verschlüsselung und Zugriffsverwaltungskontrollen, eine schnellere Erkennung von Bedrohungen durch Alarmschwellenwerte für die Speicherpoolkapazität und eine schnelle Wiederherstellung dank lokaler und replizierter Snapshots.

InfiniSafe: Referenzarchitektur für InfiniBox-Lösungen

Zu wissen, wie eine gegen Cyberattacken widerstandsfähige Umgebung für Ihren Primärspeicher aufgebaut wird, ist wichtiger denn je. Unternehmen benötigen eine mehrschichtige Strategie, um ihre wichtigsten Datenbestände auch weiterhin schützen zu können. Mit der InfiniSafe-Referenzarchitektur werden einfach zu implementierende Methoden definiert, mit denen Sie den Schutz vor Cyberangriffen erhöhen können. Die Lösung basiert auf vier Säulen:

- **Unveränderliche Snapshots**
- **Logisches Remote Air Gapping**
- **Abgeschirmte forensische Umgebung**
- **Nahezu sofortiges Recovery**

Von entscheidender Bedeutung ist es, gesperrte und unveränderliche Kopien Ihrer Daten zu erstellen. Diese können als logisch getrennt und isoliert angesehen werden (Air Gap). Wichtig ist jedoch, diesen Schutz wie beim Disaster Recovery um ein Best Practice-Replikationsverfahren zu erweitern, bei dem eine zweite unveränderliche Kopie erstellt wird. Danach müssen Sie die Daten in dieser Kopie testen bzw. validieren. Eine abgeschirmte Umgebung (auch Zero-Trust-Umgebung) ist von der Produktion abgetrennt und wird nur zu bestimmten Zeitpunkten aktiviert, wenn Sie sich vom einwandfreien Zustand von Daten überzeugen müssen. Sie können die Tools und Anwendungen nutzen, die sich am besten für die Validierung bzw. das Testen der Daten eignen. Nachdem Sie die Daten zu diesen Zeitpunkten validiert haben, verfügen Sie schließlich über die Möglichkeit, diese Daten innerhalb von Sekunden bis Minuten wiederherzustellen. Die Funktionen unserer InfiniBox-Lösungen bietet Ihnen all dies, ohne proprietäre Anforderungen, oder eine Bindung an einen bestimmten Vendor oder ein bestimmtes Toolset.

Snapshots: Das Kernstück für Datenschutz und Business Continuity

Der Snapshot-Mechanismus von Infinidat, InfiniSnap®, erweitert wichtige Datensicherungsfunktionen, ohne die Skalierbarkeit oder Leistung zu beeinträchtigen. InfiniSnap verwendet einen nicht sperrenden Redirect-on-Write-Mechanismus, der Snapshots und unveränderliche Snapshots erstellt und bei Bedarf eine schnelle Wiederherstellung ermöglicht.

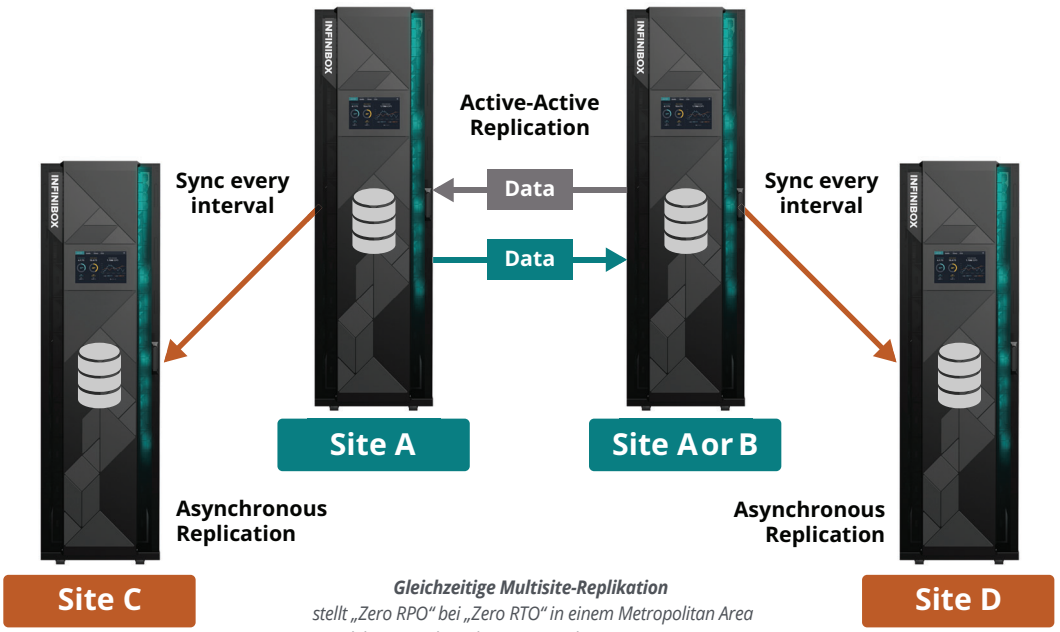
Snapshots können schreibgeschützt oder beschreibbar sein, und in jedem Datensatz können bis zu 1.000 Snapshots gespeichert werden. Die mit InfiniSnap erstellten Snapshots ermöglichen unveränderbare Snapshots für Volumes, Dateisysteme und Konsistenzgruppen. Snapshot Directory ermöglicht es Endanwendern, versehentlich gelöschte oder geänderte Dateien einfach zu suchen, auszuwählen und wiederherzustellen.

- **Unveränderliche Snapshots:** Unveränderliche Snapshots können innerhalb eines festgelegten Aufbewahrungszeitraums weder geändert noch gelöscht werden. Administratoren können das Ablaufdatum der Sperre zwar verlängern, aber nicht verkürzen. Die Funktion für unveränderliche Snapshots ermöglicht auch versteckte Snapshots als Backup-Images, wodurch Snapshots noch besser vor Angriffen geschützt sind.
- **Erkennung von Bedrohungen:** Die Verschlüsselung durch Ransomware erhöht die Dateigröße, wodurch sich auch die Größe der Snapshots der Daten erhöht. Administratoren können Schwellenwerte für die Kapazitätsnutzung festlegen. So werden sie alarmiert, wenn das Snapshot-Volumen plötzlich über die durchschnittlichen Parameter hinaus wächst. Wird ein Angriff erkannt, können Administratoren schnell auf die Daten zugreifen, sie prüfen und den letzten guten Snapshot schnell wiederherstellen.

Replikation: Sicherstellung von Business Continuity

Durch die Replikation werden die Möglichkeiten von Snapshots zum Schutz und zur Wiederherstellung gefährdeter Daten erweitert. InfiniBox unterstützt mehrere Replikationstypen für die Anforderungen unterschiedlicher Umgebungen.

- **Asynchrone Replikation:** Ermöglicht ein Recovery Point Objective (RPO) von 4 Sekunden. Die Verwendung einer IP-Infrastruktur reduziert Kosten und Komplexität.
- **Synchrone Replikation:** Ermöglicht ein RPO von 0 Sekunden mit einer Latenzzeit von unter 400 Mikrosekunden für unternehmenskritische Anwendungen. Sollte es zu Verzögerungen oder einem Ausfall des WAN kommen, wechselt die synchrone Replikation der InfiniBox wieder in den asynchronen Modus. Sobald das WAN wiederhergestellt wurde, repliziert die Engine sämtliche fehlenden Daten automatisch und die synchrone Replikation wird ohne I/O-Unterbrechungen fortgesetzt.
- **Aktiv/Aktiv-Replikation:** InfiniBox-Systeme ermöglichen das gleichzeitige Lesen und Schreiben in Konsistenzgruppen über größere Entfernungen hinweg. Die Volumes sind externe Abbilder, die als Multipfade zum selben Volume erscheinen. Die synchrone Replikation hält die Volumes jederzeit konsistent. Es gibt keine Master-Slave-Beziehung und keine zusätzlichen Roundtrips, um Schreib-Updates für ein Volume durchzuführen. Ein externer Lightweight-„Zeuge“ kann bei Bedarf auf einem eigenständigen Knoten oder sogar einer virtuellen Maschine in einer Cloud gespeichert werden.
- **Gleichzeitige Multisite-Replikation:** InfiniBox kann gleichzeitig Konsistenzgruppen von Hauptreplikationsstandorten zu einem anderen Standort in einem Metronetz replizieren. Von dort aus können die Benutzer eine asynchrone Replikation an einen dritten Standort vornehmen.



Gleichzeitige Multisite-Replikation *stellt „Zero RPO“ bei „Zero RTO“ in einem Metropolitan Area Network bereit, während Daten asynchron mit „Near-Zero RPO“ an einen dritten oder vierten Standort repliziert werden.*

INFINIDAT

Verschlüsselung: Schutz verschlüsselter Daten

Ransomware kann verschlüsselte Dateien nochmals verschlüsseln, weshalb Snapshots und Replikation die erste Verteidigungslinie darstellen. Je stärker die Verschlüsselung ist, desto schwieriger ist es für Hacker, sie erneut zu verschlüsseln.

- **Validiert nach den Federal Information Processing Standards (FIPS) 140-2:** Das National Institute of Standards and Technology (NIST) hat dem kryptografischen Modul von Infinidat die Validierung nach FIPS 140-2 erteilt. Der Standard zertifiziert InfiniBox für den Einsatz in einer Reihe von IT-Projekten der US-Regierung und behördlich regulierter Branchen.
- **Standardmäßige Self Encrypting Drives (SEDs) mit AES-256-Verschlüsselung:** InfiniBox verwendet standardmäßige Self Encrypting Drives (SEDs) mit FIPS 140-2-konformer AES-256-Verschlüsselung, den stärksten von den Laufwerken unterstützten Authentifizierungsschlüsseln.
- **Key Derivation Functions (KDF):** Infinidat verwendet die von der US-Regierung zugelassene KDF-Technologie, die global eindeutige Schlüssel für jedes Laufwerk erzeugt. Unser Pluggable Key Manager ermöglicht die externe Schlüsselverwaltung über das Key Management Interoperability Protocol (KMIP).
- **Integration mit Drittlösungen:** Ermöglicht eine umfassende Integration mit allen Verschlüsselungsprodukten wie Thales, VMware, Oracle TDE oder Microsoft TDE ohne spezielle Programmierung oder hohe Kosten.

Zugriffsmanagement: Kein unbefugter Zugriff

Cyberkriminelle können auf verschiedenen Wegen in ein Netzwerk eindringen. Am wertvollsten sind dabei die Zugangsdaten von Administratoren. InfiniBox ist bereits so eingestellt, dass Cyberkriminelle gar nicht erst so weit kommen können: Der gesamte Zugriff erfolgt über die API, und die API verhindert jede Änderung von Snapshots, selbst mit Administrator-Zugangsdaten.

Dank der InfiniBox-Zugangsverwaltung können Angreifer nicht voranschreiten.

- **Role-Based Access Control (RBAC):** RBAC wird in der Systemsteuerungsebene ausgeführt, um lokale Konten und Domänen-/LDAP-Gruppen zu schützen. Durch zugewiesene Gruppenrollen können Benutzer die vollständige Kontrolle, die Kontrolle über einen begrenzten Kapazitätspool oder nur Leseberechtigungen erhalten. Benutzer können lokale Konten deaktivieren oder sperren, so dass sie nur verwendet werden können, wenn Techniker von Infinidat Wartungsarbeiten durchführen. Die Sitzungsauthentifizierung schützt den Verwaltungszugang zusätzlich.
- **Host-Authentifizierung:** iSCSI verwendet CHAP zur Authentifizierung von Hosts auf der Datenebene. CHAP erfordert eine mehrstufige Host-Authentifizierung, um zu verhindern, dass ein Host auf die Daten eines anderen Hosts zugreifen kann.
- **Integration der Zugriffsverwaltung von Drittanbietern:** Infinidat lässt sich mit professionellen externen Lösungen für die Verwaltung privilegierter Zugriffe wie CyberArk integrieren.
- **Zugriff von Verwaltungsstationen und Audits:** Die Zugriffsverwaltung umfasst auch den Zugriff von Verwaltungsstationen über eine sichere Verbindung, während Prüfprotokolle alle Vorgänge aufzeichnen, mit denen die Konfiguration/der Status oder die Komponenten eines Geräts geändert werden. Das Auditing protokolliert auch den Administrator, der die Änderungen an der Konfiguration vornimmt.

SCHLUSSFOLGERUNG

Der Schutz Ihrer Daten ist entscheidend für den Erfolg Ihres Unternehmens. Die umfangreichen Unternehmensfunktionen von InfiniBox ebnen den Weg zu einer umfassenden Daten- und Cybersicherheit und machen Speicherlösungen zu einem Teil der gesamten Cybersicherheitsstrategie Ihres Unternehmens.

Mit einer Investition in InfiniBox profitieren Sie nicht nur von überlegener Leistung, 100-prozentiger Verfügbarkeit, einfacher Bedienung und deutlich niedrigeren Gesamtbetriebskosten, sondern vereiteln auch Ransomware-Angriffe. Cyberkriminelle machen ihre Profite mit der Ahnungslosigkeit ihrer Opfer. Sie rechnen nicht damit, leistungsstarke Datenschutzmaßnahmen vorzufinden.

Wehren Sie diese Angriffe mit unveränderlichen Snapshots, leistungsstarker Replikation, ausgeklügelter Verschlüsselung und starkem Zugriffsmanagement von InfiniBox ab, und zwar mit einem All-inclusive-Modell, das auf Ihr Speicherbudget, Ihre Mitarbeiter und Ihre Unternehmensziele zugeschnitten ist.