VERITAS

Verbesserte Datenwiederherstellung mit Air Gaps und Isolierung

Wie Sie mit sicheren Kopien Ihrer Daten die Auswirkungen von Cyberangriffen neutralisieren können.

Whitepaper | Mai 2023

Warum sollten Sie einen Datentresor erstellen?

Cybersicherheit steht für Unternehmensführer weiterhin an erster Stelle. Digitale Bedrohungen werden immer raffinierter und nutzen ständig ausgefeiltere Techniken, um größtmöglichen Schaden anzurichten. Laut Gartner werden bis 2025 40 Prozent aller Vorstände über einen eigenen Cybersicherheitsausschuss verfügen, der für zusätzliche Berichte und Strategieerwartungen zu Richtlinien, deren Umsetzung und Wiederherstellung zuständig ist[1]. Das exponentielle Wachstum der Cyberkriminalität kostet Unternehmen Millionen von Dollar und Stunden, die sie unbedingt einsparen oder wiedererlangen wollen. 2022 geschah alle 15 Sekunden ein Cyberangriff[2]. Es ist somit ein Wettlauf gegen die Zeit, um sicherzustellen, dass Sie über eine Strategie verfügen, die Ihr Risiko reduziert, Unsicherheiten beseitigt und Ihnen maximale Kontrolle über Ihre Umgebung gibt.

Das Vertrauen in einen Ausfallsicherheits- und Wiederherstellungsplan entsteht durch die Implementierung eines zuverlässigen Cybersicherheitsrahmens mit der richtigen Technologie und den richtigen Prozessen. Verfügen Sie über einen Reaktionsplan für Cybersicherheitsvorfälle, den Sie Ihrem Vorgesetzten und dem oberen Management mit gutem Gewissen vorlegen können? Laut Gartner[3] werden bis 2025 70 % der CEOs eine Kultur der Resilienz gegen Cyberkriminalität fordern. Jetzt ist es an der Zeit, Cybersicherheitstrends und die entscheidenden Komponenten eines erfolgreichen Wiederherstellungsplans zu verstehen. Versetzen Sie sich in die Lage, Ransomware-Angriffe im Keim zu ersticken, und weisen Sie gegenüber Ihrem Vorstand nach, dass Sie die richtigen Tools zur Wiederherstellung implementiert haben.

Was ist ein Air Gap und warum ist es so wichtig?

Cyberangriffe werden immer ausgefeilter und Hacker nehmen dabei nicht nur Ihren primären Datenspeicher ins Visier, sondern auch den Backup-Speicher. Dies müssen Sie unbedingt in Ihrer Disaster-Recovery-Strategie berücksichtigen. In den meisten Fällen bleiben Hacker eine ganze Weile unerkannt im System, bis sie auf Ihre Primär- und Backup-Daten zugreifen und diese kompromittieren können. Wenn der Zugriff gelingt, richten sie meist großen Schaden an.

Laut dem National Institute of Standards and Technology (NIST) ist ein Air Gap eine Schnittstelle zwischen zwei Systemen, an der (a) sie nicht physisch verbunden sind und (b) keine logische Verbindung automatisiert ist (d. h. Daten nur manuell, unter menschlicher Kontrolle übertragen werden)[4]. In der Vergangenheit waren Air Gaps der Goldstandard zum Schutz von Betriebstechnik wie Thermostaten oder Haushaltsgeräten. Da mittlerweile fast alles über ein kabelloses oder kabelgebundenes Netzwerk verbunden ist, sind strenge Air-Gap-Prozesse von entscheidender Bedeutung, damit Sie über eine intakte Datenkopie für die Wiederherstellung verfügen.

In vernetzten Umgebungen können Hacker nahezu jeden Einstiegspunkt ausnutzen – selbst ein System, bei dem alle kabellosen und kabelgebundenen Signale deaktiviert sind. In den geschlossensten Systemen für hochsichere Daten deaktivieren einige IT-Abteilungen alle USB-Anschlüsse und verwenden einen Faradayschen Käfig, um sämtliche kabellose Übertragungen zu blockieren und elektromagnetische Lecks zu verhindern.

Mit Auto Image Replication (AIR) können Sie gesicherte Daten zwischen Backup-Domänen replizieren, die sich am selben oder an verschiedenen Standorten befinden können, einschließlich der öffentlichen Cloud. AIR ermöglicht außerdem die Aufbewahrung von Offline-Air-Gap-Kopien Ihrer Backups, wodurch die Gefahr des Datenzugriffs durch unbeabsichtigte Quellen weiter reduziert wird. Da die Datenmenge in Ihren eigenen Rechenzentren und in der öffentlichen Cloud zunimmt, ist es wichtig, über eine Backup- und Recovery-Lösung zu verfügen, die eine Air-Gap-Struktur nutzt. Auf diese Weise haben Sie immer eine letzte als funktionierend bekannte Kopie kritischer Daten.

Cloud-Daten und Air-Gap-Konzept

Die Cloud-First-Strategie nimmt zu: 85 % der Unternehmen geben an, dass sie bis 2025 darauf umgestellt haben werden, wobei 94 % davon einen Multi-Cloud-Ansatz wählen[5]. Wir haben einen starken Anstieg beschleunigter Cloud-Migrationen beobachtet, was zu einer Menge an verschiedenen Tools und Entscheidungsbefugnissen führen kann. So wie Sie Ihr primäres Daten-Repository mit verschiedenen Public-Cloud-Optionen diversifizieren und optimieren, sollten Sie auch bei Ihrem Datenwiederherstellungsansatz vorgehen, damit Sie im Ernstfall schnell wieder betriebsbereit sind.

Als bestmögliche Option empfehlen wir eine Isolated Recovery Environment (IRE). In einer IRE bereitgestellte Air-Gap-Lösungen generieren eine sichere Kopie Ihrer kritischen Daten. Bei Bedarf können Administratoren auf einen sauberen Satz von Dateien zugreifen, um die Auswirkungen eines Ransomware-Angriffs in einer Multi-Cloud-Umgebung zu neutralisieren.

Isolated Recovery Environment

Herkömmliche Netzwerkisolationslösungen unterbrechen physisch oder logisch die Konnektivität zwischen Standorten und machen so jegliche eingehende oder ausgehende Kommunikation unmöglich. Dies schränkt die Datenübertragung in die isolierte Umgebung ein und gefährdet die RTOs und RPOs, falls die Tertiärkopie benötigt wird. Im Allgemeinen wird dies als Replikationsdaten-„Push" von der Quelle zum Ziel bezeichnet. Die Quelldomäne verarbeitet einen Replikationsauftrag unabhängig und sendet ihn an eine Zieldomäne. Dieser herkömmliche Ansatz begrenzt die Zeit, die für die Replikation kritischer Daten in einer sicheren Umgebung zur Verfügung steht, wenn die Verbindung unterbrochen oder blockiert ist.

Im Gegensatz dazu initiiert das „Pull"-Replikationsmodell die Replikationsanforderung vom Ziel. Veritas bietet die IRE-Lösung von NetBackup an, die die Datenverschiebung optimiert, indem sie ein Pull-Replikationsmodell anwendet, bei dem die Anforderung zur Datenübertragung vom Medienserver-Deduplizierungspool (MSDP) der IRE kommt. Die umgekehrte Verbindung ermöglicht eine bessere Kontrolle des Datenflusses, um die Umgebung weiter logisch und physisch zu sichern. Replikationen zur IRE können jetzt vollständig von der IRE aus gesteuert werden, einschließlich der Unterstützung eines bestimmten Fensters, wie im IRE-Air-Gap-Zeitplan definiert.

Die NetBackup-IRE ist während der Datenübertragung aufgrund mehrerer Sicherheitsebenen (einschließlich Intrusion Prevention-Mechanismen und Datenverschlüsselung während der Übertragung und im Ruhezustand) undurchdringlich. Während ihrer gesamten Reise sind die Daten sicher, unabhängig davon, wo sie sich befinden. Der Speicher wird nicht beeinträchtigt und es besteht kein Risiko, dass böswillige oder unbefugte Benutzer Daten lesen oder modifizieren. Veritas bietet Datenisolationsoptionen vor Ort und in der Cloud mit NetBackup Recovery Vault: einem nahtlosen Cloud-Storage-as-a-Service mit Air Gap zum Schutz vor Ransomware, optimiert für Skalierung und Gewährleistung der Datenportabilität bei vorhersehbaren Kosten.

Dank des unkomplizierten Veritas-Workflows können Sie jedes NetBackup – lokal oder in der Cloud – in ein IRE-Framework umwandeln, das Ransomware-Resilienz mit drei Schlüsselprinzipien bietet:

- **Schutz**: Integrieren Sie ganz einfach isolierte Wiederherstellungsfunktionen, die auch Multi-Faktor-Authentifizierung (MFA) und rollenbasierte Zugriffskontrolle (RBAC) gemäß der Zero-Trust-Sicherheitsstrategie von Veritas unterstützen.
- **Erkennung**: NetBackup IT Analytics umfasst Anomalieerkennung, die Ransomware in Echtzeit identifizieren kann. Die integrierte Malware-Scan-Funktion von NetBackup prüft Dateien vor der Wiederherstellung und lässt sich anhand von Anomalie-Bewertungen priorisieren.
- **Wiederherstellung**: Orchestrieren Sie die Wiederherstellung eines gesamten Datensatzes in einer isolierten Umgebung, in der Cloud oder lokal, einschließlich der Möglichkeit, eine Vielzahl von RPO- und RTO-Anforderungen zu verwalten.

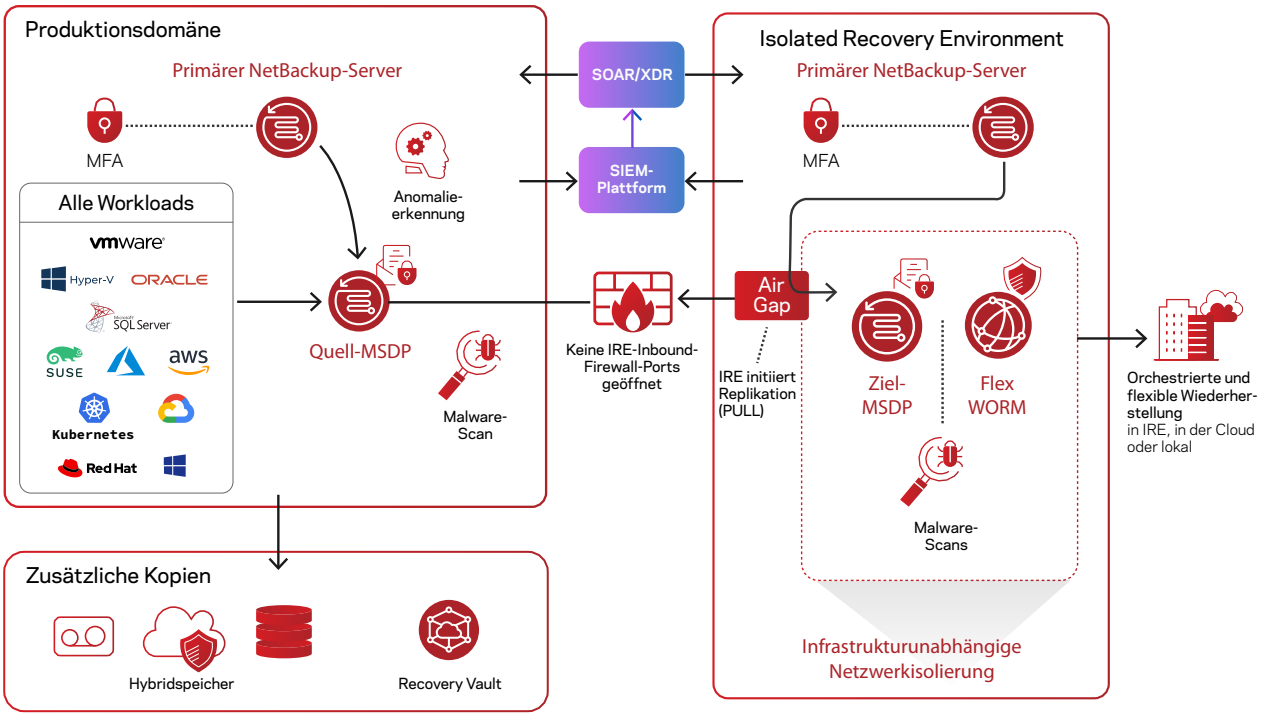

Abbildung 1: NetBackup – Isolated Recovery Environment

Eine isolierte Umgebung bietet eine weitere Ebene der Ausfallsicherheit zur Bekämpfung von Ransomware und Malware.

Erhöhter Schutz durch Zero Trust

Eine Zero-Trust-Richtlinie verbessert Ihren Schutz noch weiter. Die Einführung einer unternehmensweiten Zero-Trust-Mentalität verringert nachweislich das Risiko eines verheerenden Angriffs.

Veritas IRE basiert auf dem Container-basierten Multi-Tenant-WORM-Speicher (Write Once Ready Many) der Flex-Appliances mit gehärtetem Betriebssystem und einer Zero-Trust-Architektur. Durch die Stärkung Ihres Identitäts- und Zugriffsmanagements (IAM) mit MFA und RBAC für Benutzer, Tools und Computer beschränken Sie den Zugriff auf hochsensible Daten und Backups. Er sollten nur Benutzern vorbehalten sein, die ihn wirklich benötigen. Auch eine gute Passworthygiene hat oberste Priorität.

Sie können den Zugriff auf sensible Bereiche mit strengen IAM-Kontrollen, Berechtigungskontrollen, Härtung und sicherer Hardware verhindern – alles basierend auf den Zero-Trust-Ansatz. Wenn es zu einer Kompromittierung kommt, verringert sich die Angriffsfläche bzw. der Explosionsradius, da es mehrere Sicherheitsebenen gibt, die die Auswirkungen minimieren. Sobald sich Cyberkriminelle in Ihren Systemen eingenistet haben, bewegen sie sich häufig nach allen Seiten auf der Suche nach geschäftskritischen Daten, vertraulichen Informationen und Backup-Systemen.

Anomalieerkennung und Malware-Scans

Durch vollständige Transparenz, intelligente Anomalieerkennung und Malware-Scans wissen Sie genau, wo sich alle Ihre Daten befinden, während Sie gleichzeitig die betriebliche Komplexität reduzieren und das Kostenmanagement optimieren. Die KI-gestützte Anomalieerkennung von Veritas identifiziert ungewöhnliche Daten und Benutzeraktivitäten in Ihrer gesamten Umgebung und warnt Sie nahezu in Echtzeit, falls etwas Verdächtiges gefunden wurde. Sie stellt sicher, dass Ihre Daten jederzeit wiederhergestellt werden können, und ermöglicht es Ihnen, bei einem Ransomware-Angriff sofort Maßnahmen zu ergreifen, Backups mit Malware zu isolieren und die Auswirkungen auf Ihre Backup-Daten einzudämmen. Sie können entweder vollständige Images wiederherstellen, die geprüft und als sicher validiert wurden, oder nur einzelne Dateien. Sollte eine zur Wiederherstellung markierte Datei infiziert sein, können Sie sie aus einem nicht infizierten Backup wiederherstellen. Auf diese Weise lassen sich Daten sicher und effektiv wiederherstellen, ohne dass das Risiko einer erneuten Infektion des Zielcomputers besteht.

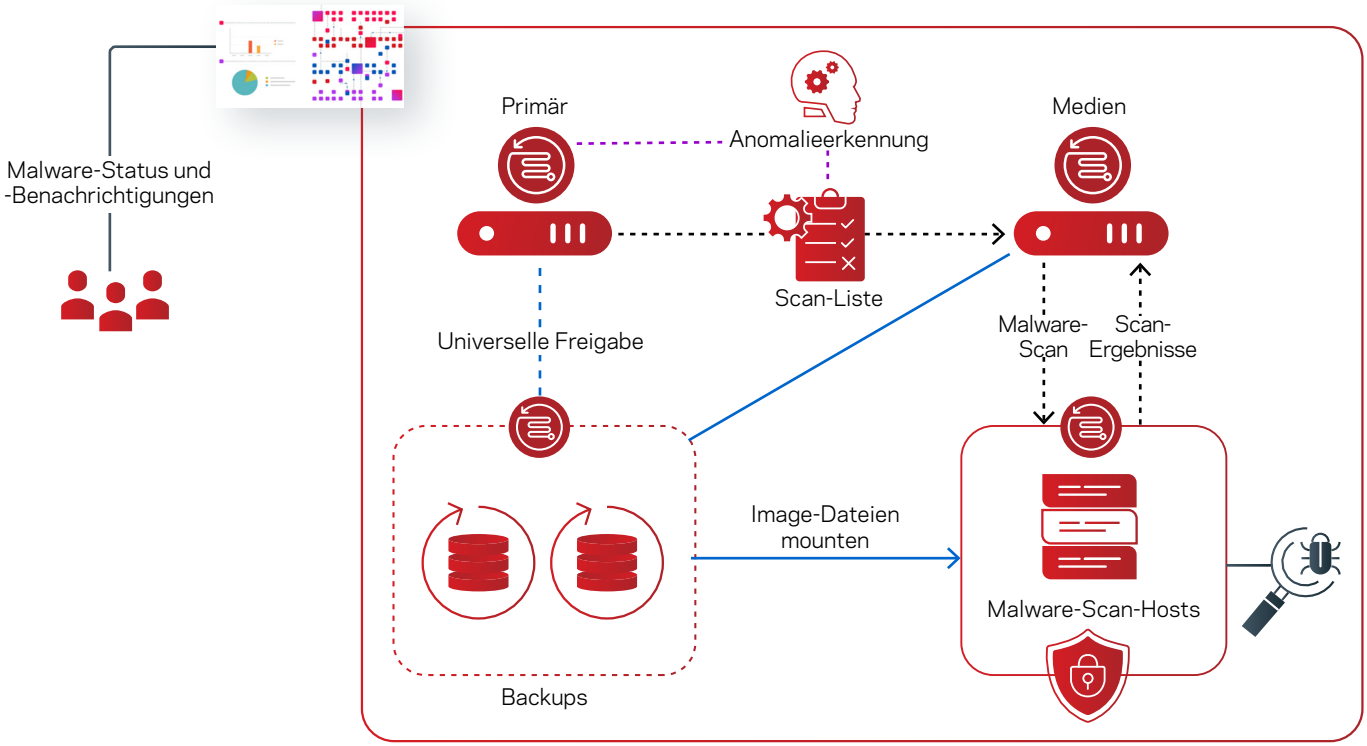

Abbildung 2: In NetBackup integrierter Malware-Scan

Wiederherstellung mit unveränderlichem und unlöschbarem Speicher

Unveränderliche und unlöschbare Speicher gewährleisten, dass niemand oder nichts Daten in einem bestimmten Zeitraum (oder überhaupt) ändern, verschlüsseln oder löschen kann. Sie verhindern auch Datenmanipulationen und unbefugten Zugriff. Als Teil Ihrer IRE-Strategie bietet NetBackup Recovery Vault eine cloudbasierte, unveränderliche und unlöschbare Speicherlösung, die je nach Bedarf vergrößert oder verkleinert werden kann.

Wiederherstellung ohne Risiko mit IRE

Reduzieren Sie Risiken, beseitigen Sie Unsicherheiten und behalten Sie die Kontrolle mit NetBackup Isolated Recovery Environment. Besuchen Sie Veritas.com oder kontaktieren Sie unser Team für weitere Informationen dazu, wie unsere Lösung Ransomware Resilience in Ihrer Multi-Cloud-Umgebung gewährleisten kann.

Schließen Sie die Lücken in Ihrer Strategie für Ausfallsicherheit.
Weitere Informationen >

1. www.gartner.com/en/newsroom/press-releases/2021-01-28
2. www.sonicwall.com/resources/white-papers/2023-sonicwall-cyber-threat-report/
3. www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022
4. csrc.nist.gov/glossary/term/air_gap
5. www.gartner.com/en/newsroom/press-releases/2021-11-10

Über Veritas

Veritas Technologies ist ein weltweit führender Anbieter im Bereich Multicloud-Datenmanagement. Über 80.000 Kunden – darunter 95 Prozent der Fortune 100 – vertrauen darauf, mit Lösungen von Veritas den Schutz, die Wiederherstellbarkeit und Compliance ihrer Daten zu gewährleisten. Veritas steht für skalierte, zuverlässige Produkte, welche die Widerstandsfähigkeit bieten, die seine Kunden im Fall von Cyberangriffen wie Ransomware benötigen. Kein anderer Anbieter erreicht Veritas' Leistungsfähigkeit mit Unterstützung für mehr als 800 Datenquellen, über 100 Betriebssystemen, über 1.400 Speicherzielen und über 60 Clouds im Rahmen eines einzigen, einheitlichen Ansatzes. Mithilfe der Cloud Scale Technology setzt Veritas heute seine Strategie für autonomes Datenmanagement um, die den betrieblichen Aufwand reduziert und gleichzeitig einen größeren Mehrwert bietet. Weitere Informationen finden Sie unter veritas.com/de/de und folgen Sie uns auf Twitter unter @veritastechllc.

VERITAS

Veritas (Deutschland) GmbH
Theatinerstr. 11, 8. Etage
80333 München
Tel.: 0800-724 40 75
veritas.com/de/de

Die weltweiten Kontaktinformationen finden Sie hier:
veritas.com/de/de/company/contact

V1626 05/23