Commvault

eBOOK

Vier Dinge, die Sie beim Active Directory-Schutz beachten sollten

Spezielle Sicherheit und Wiederherstellbarkeit für Ihre Microsoft AD- und Entra ID-Daten

eBOOK

Commvault

Die Schlüssel zum Königreich

Als weit verbreitetes Authentifizierungswerkzeug für kleine, mittlere und große Unternehmen sind Microsoft Active Directory (AD) und Entra ID die Torwächter der Autorisierungsprozesse für Netzwerke, Anwendungen und Umgebungen. Benutzerkontenattribute wie Namen, Adressen, Telefonnummern, Passwörter und mehr werden gruppiert, was den Administratoren eine vereinfachte Kontrolle über den Benutzerzugang bietet. Während AD das Leben der Verwaltung des Zugangs zu Schlüsselsystemen vereinfacht, kann dessen Sicherung besonders herausfordernd sein. Es steuert einen ständig wechselnden Pool von Benutzern, Gruppen, Richtlinien und App-Berechtigungen. Ein einziger Fehltritt—sei es eine Fehlkonfiguration, ein kompromittiertes Passwort oder ein inaktives Konto—kann es einem böswilligen Akteur ermöglichen, Berechtigungen zu erhöhen und kritische Anwendungen und Daten zu stehlen, zu beschädigen oder den Zugang zu verweigern, was letztendlich zu ungeplanten Ausfallzeiten von Produktionsservices führt.

Mit Active Directory im Zentrum der sicheren Authentifizierung und Dienste ist der Schutz und die Sicherung dieser Daten heute für Unternehmen von entscheidender Bedeutung. Die Fähigkeit zu wissen, was sich in der Umgebung geändert hat und diese Änderungen rückgängig zu machen, ist von größter Wichtigkeit.

Eine Datenschutzlösung für Active Directory kann helfen, das Risiko von Datenverlust zu mindern und Ihr Unternehmen schnell wieder online zu bringen.

Hier sind vier Dinge, die Sie beachten sollten, um Ihre AD-Daten sicher und geschützt zu halten:

#1

HÄUFIGE BACKUPS

Best Practices sollten nicht nur für Unternehmensdaten und Datenbanken gelten, sondern auch für AD. Häufige, automatisierte Backups ersparen Ihnen die Qualen, die mit dem Verlust von Domäneninformationen und mehr einhergehen. Obwohl die Verwendung von Tombstone zur vorübergehenden Wiederherstellung gelöschter Elemente hilfreich sein kann, ist die Abhängigkeit von dieser Methode riskant, da die Lebensdauer von Tombstones begrenzt ist. Ein vollständiges und häufiges Backup des gesamten Active Directory ist am besten. Backup als Service-Lösung ermöglicht häufige Backups, sichere Off-Site-Speicherung und vereinfachtes Management—mit integrierten Best Practices für langfristige Aufbewahrung.

#2

EIGENE LÖSUNGEN BAUEN—KÖNNEN VS. SOLLTEN

Sicher, es gibt Möglichkeiten, Skripte und andere installierbare Dienste, die Ihnen helfen, Active Directory zu schützen, aber sollten Sie es selbst bauen? Eigenentwickelte Lösungen mögen lohnend erscheinen, sind jedoch zeitintensiv in der Wartung, erfordern zusätzliche Patches und belasten die IT zusätzlich.

Stattdessen bietet die Wahl einer unternehmensgerechten und sicheren Datenschutzlösung, die als SaaS bereitgestellt wird, die Notwendigkeit einer internen Entwicklung und Unterstützung kann mit einer speziellen Datenschutzlösung für Active Directory erheblich reduziert werden. Mit nur wenigen Klicks können Sie innerhalb von Minuten durch vereinfachtes Management, mehrschichtige Sicherheit mit Verschlüsselung und Schutz vor Ransomware geschützt sein.

#3

WIEDERHERSTELLENDE ATTRIBUTE

Anstrengungen in die Organisation einer Active Directory-Struktur, um sicherzustellen, dass die richtigen Elemente in den richtigen Organizational Units (OUs) mit den entsprechenden Berechtigungen sind. Eine spezielle Datenschutzlösung ermöglicht eine granulare Wiederherstellung, indem nur die fehlenden, beschädigten oder falsch konfigurierten Objektattribute wiederhergestellt werden. Diese Granularität kann Geschäftssysteme oder Benutzer schnell wieder online bringen, ohne dass eine vollständige Wiederherstellung der gesamten Active Directory-Umgebung erforderlich ist.

#4

RANSOMWARE PASSIERT

Active Directory ist ein primäres Ziel für Ransomware-Angriffe, da es ein zentrales Element des zentralisierten Managements ist. Angreifer können blinde Flecken ausnutzen, um privilegierte Konten zu kompromittieren, autorisierte Benutzer nachzuahmen und Infrastruktur, Arbeitsstationen und Anwendungen stillschweigend zu durchqueren. Das Versäumnis, AD zu schützen, ermöglicht es Angreifern, die Kontrolle zu übernehmen und den Zugang zu kritischen Geschäftsressourcen zu unterbrechen. Daher ist es für Unternehmen von entscheidender Bedeutung, den AD-Schutz in ihre Sicherheits- und Ransomware-Reaktionsstrategien einzubeziehen. Die Bekämpfung von Ransomware erfordert einen mehrschichtigen Ansatz zur Datensicherheit, wobei die Bereitschaft zur Wiederherstellung eine entscheidende Rolle spielt.

50% der Organisationen erlebten in den letzten zwei Jahren einen Active Directory-Angriff.[1]

SCHLIESSEN DER DATENWIEDERHERSTELLUNGSLÜCKE

Moderne Unternehmen benötigen robusten, speziellen Schutz ihrer kritischen Microsoft AD- und Entra ID-Daten. Optimiert, um den Anforderungen heutiger Unternehmen gerecht zu werden, bieten speziell entwickelte Lösungen für AD unübertroffene Einfachheit.

Vorteile des speziellen Schutzes umfassen

- Luftgekapselte, isolierte Datenbackups
- Robuste Werkzeuge für Wiederherstellung und Compliance
- Fortgeschrittene Benutzerkontrolle, um schädliche und unerwünschte Änderungen rückgängig zu machen
- Mehrschichtige Sicherheit und frühzeitige Bedrohungserkennung zum Schutz vor Ransomware

COMMVAULT® CLOUD, ANGETRIEBEN DURCH METALLIC AI

Commvault Cloud bietet branchenführende Sicherheit und Schutz für Active Directory- und Entra-ID-Daten—bewährt, um Ihr Unternehmen sicher, konform und wiederherstellbar vor Bedrohungen zu halten. Die Plattform minimiert die Datenexposition, fördert die Sichtbarkeit von Bedrohungen und ermöglicht ein selbstbewusstes Reagieren mit der fortschrittlichsten Plattform für Datenresilienz der Branche. Sie schützt die gesamte Datenumgebung über eine einzige Oberfläche, schützt kritische Objekte und ermöglicht eine schnelle Wiederherstellung versehentlich oder böswillig

gelöschter Objekte. Zusätzlich verwendet sie virtuelle luftgekapselte Backup-Kopien, Zero-Trust-Zugangskontrollen und KI-gestützte Erkennung, um Datenkopien zu isolieren und gegen Cyberangriffe zu verteidigen.

Schützen Sie Ihr hybrides Verzeichnis, indem Sie kritische Microsoft AD- und Entra ID-Objekte schützen, einschließlich Gruppenrichtlinienobjekte, Benutzer, Gruppen, bedingte Zugriffsrichtlinien, Rollen und mehr.

Interaktive Vergleiche identifizieren alle Änderungen am Domänen- oder Mandantenbereich, sodass Sie versehentlich oder böswillig gelöschte Objekte schnell wiederherstellen oder überschriebene Attribute im gesamten Verzeichnis zurücksetzen können.

Virtuell luftgekapselte Backup-Kopien, Zero-Trust-Zugangskontrollen und Früherkennungsfähigkeiten isolieren Datenkopien für fortschrittlichen Schutz vor Ransomware.

VORTEILE

Risiken durch Ransomware mindern, Datenkonformität sicherstellen und schnell wiederherstellen mit integriertem Cloud-Speicher von Commvault.

Optimieren Sie den Betrieb
mit automatisierten und hochfrequenten Backups

Inhalte bewahren
mit unveränderlichen und manipulationssicheren Datenkopien

Daten vergleichen und schnell wiederherstellen mit Optionen
für Wiederherstellung am ursprünglichen Ort und an einem anderen Ort

Sandbox-Umgebungen
für Entwicklung und Tests säen, replizieren und behalten

Risiken mindern
durch Datenisolation, losgelöst von Quellumgebungen

Cyberangriffe minimieren
mit KI-gestützter Erkennung, Überwachung und Datenverteidigung

SLA-Konformität aufrechterhalten
mit unbegrenztem Speicher und eingebauter Aufbewahrung

Schützen Sie alles
mit einer Einzellösung, die mehrere Plattformen abdeckt

NÄCHSTE SCHRITTE

Das Schützen von Active Directory mag überwältigend erscheinen, aber Sie müssen es nicht alleine tun. Kontaktieren Sie Commvault, um mehr darüber zu erfahren, wie wir helfen können.

Melden Sie sich noch heute für eine 30-tägige kostenlose Testversion an.

1 EMA Research Report – The Rise of Active Directory Exploits

Um mehr zu erfahren, besuchen Sie **commvault.com**