

ENTHÜLLT: ACTIVE DIRECTORY SICHERHEITSCHECK



Während Microsoft Active Directory die Verwaltung des Zugriffs auf wichtige Systeme in einem Unternehmen vereinfacht, bleibt die Absicherung eine große Herausforderung. ENTHÜLLTE Schwachstellen in diesem sich ständig verändernden Pool aus Benutzern, Gruppen, Richtlinien und App-Berechtigungen können Ihre Identitätsresilienzstrategie gefährden.

Hier erfahren Sie, worauf Sie beim Schutz achten sollten:

- 01 Schützen Sie AD – es ist ein primäres Angriffsziel.**

Durch die Ausnutzung von Schwachstellen können Angreifer privilegierte Konten kompromittieren, autorisierte Benutzer imitieren und sich unbemerkt durch Infrastruktur, Arbeitsstationen und Anwendungen bewegen. Wenn AD nicht geschützt wird, erhalten Angreifer einen zentralen Zugangspunkt, um den Zugriff auf geschäftskritische Ressourcen zu kontrollieren oder zu unterbrechen. Wahre Identitätsresilienz beginnt mit der Erkenntnis, dass der Schutz von AD keine Option ist – sondern eine Notwendigkeit.
- 02 Führen Sie häufige Sicherungen durch.**

Sie benötigen vollständige Backups des gesamten AD – regelmäßig, automatisch und extern gespeichert – mit integrierten Prozessen für langfristige Aufbewahrung.
- 03 Automatisierte Forest-Wiederherstellung verkürzt die Wiederherstellungszeit.**

Die Wiederherstellung eines AD-Forest ist komplex und kann bei manueller Durchführung Tage oder Wochen dauern. Im Katastrophenfall zählt jede Minute – je länger die Wiederherstellung dauert, desto größer ist die Beeinträchtigung des Geschäftsbetriebs. Eine Lösung, die die Wiederherstellung auf Forest-Ebene automatisiert, beschleunigt den Prozess, reduziert menschliche Fehler und ermöglicht eine schnellere und zuverlässigere Wiederherstellung.
- 04 Eine unternehmensgerechte Lösung stärkt die Identitätsresilienz.**

Eigenentwickelte und manuelle Wiederherstellungsprozesse sind zeitaufwendig, komplex und fehleranfällig. Moderne Bedrohungen erfordern eine speziell entwickelte Cyber-Resilienzplattform, die eine vereinfachte Verwaltung, mehrschichtige Sicherheit mit Verschlüsselung, unveränderliche Backups und automatisierte Wiederherstellung bietet.
- 05 Granulare Wiederherstellung spart Zeit und stärkt die Resilienz.**

Nicht jede Störung erfordert eine vollständige Wiederherstellung. Eine schnelle, granulare Wiederherstellung ermöglicht es Ihnen, nur das wiederherzustellen, was fehlt, beschädigt oder falsch konfiguriert ist – das reduziert Ausfallzeiten und macht eine vollständige Wiederherstellung überflüssig.
- 06 Erstellen Sie Ihren Notfallwiederherstellungsplan und testen Sie ihn, bevor er gebraucht wird.**

Ein gut dokumentierter und regelmäßig getesteter Wiederherstellungsplan ist entscheidend, um Ihre AD-Umgebung schnell in einen gesunden, vor dem Angriff bestehenden Zustand zurückzubringen. AD-Wiederherstellungstests schaffen Vertrauen in den Prozess und geben IT- und Sicherheitsteams die Möglichkeit, in ruhigen Zeiten für Krisensituationen zu üben.

Lassen Sie Ihre Identitätsinfrastruktur nicht ENTHÜLLT.
Erfahren Sie, wie Commvault Cloud Ihrem Unternehmen helfen kann, **Identitätsresilienz aufzubauen** und Ihre wertvollsten digitalen Ressourcen zu schützen.