

Warum es so wichtig ist, Microsoft 365 und Entra ID zu sichern

Früher wusste jeder, dass Backups wichtig sind, und jedes Unternehmen hatte sein eigenes Rechenzentrum im Keller, um seine Daten zu schützen. Wir hörten beängstigende Geschichten über Menschen, die wichtige Daten verloren, weil sie keine Sicherungskopien erstellt oder nicht überprüft hatten, ob die Sicherungskopien funktionierten. Wir erkannten, dass Datenverluste schlecht für das Geschäft und die Kontinuität wären.

Dann wurde die Cloud eingeführt und uns wurde versprochen, dass wir keine Backups mehr brauchen würden. Viele Technikexperten dachten, die Cloud würde uns schützen. Sie glaubten, dass Software-as-a-Service-Anbieter (SaaS) unsere Daten für uns sichern würden. Aber wie so oft gab es Einschränkungen im Kleingedruckten.

Ist eine Sicherung von Microsoft 365 und Entra ID erforderlich?

Viele Unternehmen sind immer noch der Meinung, dass Anbieter wie Microsoft auch für den Schutz ihrer Daten verantwortlich oder teilweise verantwortlich sind. Sie denken, dass SaaS-Anbieter wie Microsoft alles schützen.

Die bittere Wahrheit ist, dass Microsoft nicht für die Sicherung der Daten verantwortlich ist, die Sie auf ihrer Plattform speichern.

Wenn Sie sich bei der Sicherung Ihrer Daten auf einen SaaS-Anbieter verlassen, entstehen unerwünschte Lücken in Ihrer Sicherheitsstrategie, die sich nachteilig auf die Fähigkeit Ihrer Organisation auswirken können, den Geschäftsbetrieb wie gewohnt fortzusetzen.

1 von 3 

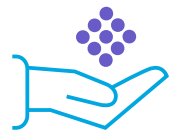
glaubt, dass SaaS-Anbieter für den Schutz ihrer Daten in der Cloud verantwortlich sind

45 %



glauben, dass SaaS-Anbieter teilweise für die Sicherung ihrer Daten in der Cloud verantwortlich sind

22 %



wissen, dass sie selbst für ihre Daten in der Cloud verantwortlich sind

Quelle: [Enterprise Strategy Group, 2022](#)

Was ist nicht abgedeckt?

Lokales Active Directory-Backup

Objekte, die nicht im lokalen AD vorhanden sind

- Rollen
- Lizenzen
- Richtlinien für bedingten Zugriff
- Anwendungen und Dienstprinzipien

Natives Entra ID-Backup

Vorläufig gelöschte Objekte

- Benutzer- und Gastkonten
- Microsoft 365-Gruppen
- Microsoft Entra-Anwendungen (App-Anmeldungen)

Bleiben nur 30 Tage im Papierkorb

Endgültig gelöschte Objekte

- Sicherheitsgruppen
- Verteilergruppen
- Dienstprinzipien (Unternehmensanwendungen)
- Richtlinien für bedingten Zugriff
- Geräte (Intune)

Keine Aufbewahrung



Die Bedeutung eines Backups für Microsoft 365 und Entra ID

„Sie sollten davon ausgehen, dass Sie irgendwann Opfer eines Ransomware-Angriffs werden. Einer der wichtigsten Schritte, die Sie zum Schutz Ihrer Daten und zur Vermeidung von Lösegeldzahlungen unternehmen können, ist ein zuverlässiger Sicherungs- und Wiederherstellungsplan für Ihre geschäftskritischen Informationen.“
– Microsoft: Lernen Sie die Grundlagen der Azure-Sicherheit kennen



M365



Entra ID

Es gibt zahlreiche Beispiele aus der Praxis, bei denen Schäden entstanden sind, nachdem Microsoft 365 und Entra ID absichtlich oder unabsichtlich in die Hände von Kriminellen gelangt sind.

- Bevor sie ihre SaaS-Daten sicherte, verlor eine Organisation 2,5 Millionen Dollar an einem einzigen Tag, weil ein Microsoft Entra-Mandant zusammen mit all seinen Microsoft Cloud Services durch Ransomware verschlüsselt wurde.
- Aufgrund einer fehlerhaften Richtlinie für den bedingten Zugriff wurden alle Administratoren einer Organisation von ihrem Microsoft Entra-Mandanten ausgesperrt und konnten nicht auf Microsoft Cloud Services zugreifen. Sie hatten kein Notfallkonto und konnten auch kein Support-Ticket bei Microsoft erstellen, um das Problem zu beheben.

Unternehmen haben oft nur begrenzte Einblicke in die Verwendung ihrer Identitäten. Sie werden nicht überwacht oder geprüft, sodass es schwierig ist, zu erkennen, ob sie manipuliert wurden.

Haben Sie darüber nachgedacht, was passiert, wenn Ihre Entra-ID-Umgebung verschlüsselt wird und Sie keinen Zugriff auf den Schlüssel für den Microsoft-Mandanten Ihrer Organisation und all Ihre Identitäten, Richtlinien und Konfigurationen haben? Würden Sie es merken, wenn Ihre Identitäten manipuliert worden wären?

Verbessern Sie die Geschäftskontinuität mit Arcserve SaaS Backup

Genau wie im Jahr 2002 liegt es immer noch in unserer eigenen Verantwortung, unsere wichtigen Daten zu sichern. Der einzige Unterschied besteht heute darin, dass sich die meisten unserer wertvollen Daten in der Cloud befinden und über eine Vielzahl von isolierten SaaS-Anwendungen verteilt sind.

Arcserve SaaS Backup unterstützt Unternehmen bei der Sicherung von Daten, die in SaaS-Diensten wie Microsoft 365, Entra ID, Salesforce, Google Workspace und Zendesk gespeichert sind.

Im Falle eines Datenverlusts oder einer vollständigen Katastrophe stellen wir sicher, dass Sie Ihre Daten sofort wiederherstellen und den Betrieb ohne Unterbrechung wie gewohnt fortsetzen können.

Arcserve SaaS Backup bietet die umfassendste Abdeckung von Microsoft 365 und Entra ID auf dem Markt, die sicherstellt, dass Ihre gesamte Microsoft Cloud vollständig geschützt ist, sodass Sie jederzeit einsatzbereit bleiben.

Unternehmen Sie den nächsten Schritt, um Ihre SaaS-Daten vollständig zu schützen

Arcserve ist weltweit einer der Top-5-Anbieter von Datensicherungslösungen und einer einheitlichen Plattform für die Datenausfallsicherheit. Unabhängig von Standort und Komplexität bietet das Unternehmen eine Komplettserie von Best-in-Class-Lösungen zum Verwalten, Sichern und Wiederherstellen aller Daten-Workloads für KMU bis hin zu großen Unternehmen an.

Sie erreichen uns unter info@arcserve.com



Produktinformationen



Kostenlose Testversion

