



6 Gründe für Microsoft Entra ID Backup



Einführung

Microsoft Entra ID (ehemals Azure Active Directory) spielt eine entscheidende Rolle im modernen Identity and Access Management (IAM). Aufgrund seiner Bedeutung ist es aber auch ein bevorzugtes Ziel für Cyberkriminelle. Angesichts von unglaublichen 600 Millionen Angriffen auf Microsoft Entra ID jeden Tag sind die Risiken heute komplexer und größer und stellen Unternehmen weltweit vor große Herausforderungen.

Die Bedrohungen sind ebenso vielfältig wie gefährlich. Ob Phishing, bei dem Benutzer zur Herausgabe von Anmeldedaten verleitet werden, oder Credential-Stuffing-Angriffe, bei denen gestohlene Daten ausgenutzt werden — die Bedrohungsakteure lassen nicht locker. Die Folgen sind katastrophal:



Die Mitarbeiter verlieren den Zugang zu wichtigen Systemen, wodurch die Produktivität zum Erliegen kommt.



Die Kunden können nicht auf Services zugreifen, was zu Frustration und einer potenziellen Kundenabwanderung führt.



Ausfallzeiten und Maßnahmen zur Wiederherstellung verschlingen Ressourcen, behördliche Bußgelder erhöhen die Belastung noch zusätzlich.



Nachrichten über eine Sicherheitsverletzung verbreiten sich schnell. Dies schwächt das Vertrauen von Kunden, Partnern und Stakeholdern.



Datenschutzverletzungen führen oft zu Verstößen gegen Vorschriften wie die DSGVO oder HIPAA, was hohe Strafen zur Folge hat.



Die Wiederherstellung nach einem Angriff ist keine leichte Aufgabe. Es braucht Zeit, Ressourcen und eine klare Strategie, um den Betrieb wiederaufzunehmen und das Vertrauen zurückzugewinnen. Microsoft bietet zwar robuste Sicherheitsfunktionen, doch gemäß dem Shared Responsibility Model ist es Aufgabe der Unternehmen, ihre Daten zu schützen. Sicherheitsbedrohungen sind nur ein Grund, warum Sie Microsoft Entra ID-Daten schützen müssen. In diesem E-Book nennen und erläutern wir viele weitere.

1

Sicherheitsbedrohungen

Das allgegenwärtige Risiko von Cyberangriffen erfordert robuste Verteidigungsmaßnahmen zum Schutz vor unbefugtem Zugriff und potenziellen Verstößen.

2

Compliance

Ordnungsgemäße Verfahren für die Datenverwaltung sorgen für Compliance mit lokalen, nationalen und globalen Standards.

3

Versehentliche Löschungen und Fehlkonfigurationen

Menschliches Versagen kann zu massiven Datenverlusten und erheblichen Unterbrechungen führen.

4

Einschränkungen des Papierkorbs

Für eine vollständige Datenwiederherstellung reicht es nicht aus, sich auf integrierte Tools wie den Papierkorb zu verlassen.

5

Effiziente Wiederherstellung

Die Minimierung von Ausfallzeiten und die Sicherstellung einer schnellen Wiederherstellung nach einem Datenverlust sind für die Aufrechterhaltung des Geschäftsbetriebs von entscheidender Bedeutung.

6

Hybride Umgebungen

Um die Komplexität von hybriden IT-Umgebungen zu bewältigen, müssen Sie sich sowohl auf lokale als auch auf Cloud-Umgebungen einstellen.

1. Sicherheitsbedrohungen

Microsoft Entra ID ist ein wesentlicher Bestandteil des Identity and Access Management (IAM) in Microsoft 365, Azure und zahlreichen anderen Plattformen. Von den Benutzern oftmals unbemerkt, ist die Verwendung dieses Diensts bei jeder Anmeldung entscheidend. Doch gerade diese Unsichtbarkeit macht Microsoft Entra ID zu einem bevorzugten Ziel für Cyberkriminelle.

Bedrohungsakteure entwickeln ihre Taktiken ständig weiter. Sie müssen nur einmal erfolgreich sein, während die Verteidiger jedes Mal alles richtig machen müssen. Die Angreifer sind geschickt und wenden Taktiken wie Phishing und Credential Stuffing an, um mithilfe von gestohlenen Passwörtern in Konten einzudringen. Ransomware ist zwar anders, aber ebenso zerstörerisch. Sie sperrt Unternehmen aus ihren Cloud-Umgebungen aus und legt den Betrieb lahm.

In einer idealen Welt würden sich Unternehmen dafür entscheiden, Sicherheitsverletzungen von vornherein zu verhindern. Viele Strategien zur Risikominimierung sind sehr effektiv und Ressourcen wie Tools für proaktives Monitoring und Bedrohungsanalyse sind ungemein nützlich.

Allerdings ist keine Verteidigung narrensicher. Daher sind Sicherung und Wiederherstellung unerlässlich. Eine robuste Backup-Strategie stellt sicher, dass Sie, wenn Angreifer Ihre Verteidigungsmaßnahmen durchbrechen, schnell wieder auf wichtige Identitätsdaten zugreifen können. Ob es um die Wiederherstellung nach einem Ransomware-Angriff, das Rückgängigmachen von versehentlichen Löschungen oder die Eindämmung von Insider-Bedrohungen geht — Backups sind Ihr Sicherheitsnetz.

In Bezug auf Microsoft Entra ID ist Redundanz keine Übertreibung, sondern eine Überlebensstrategie. Wenn Identitätsdaten gesichert werden und leicht wiederherstellbar sind, schützen sich Unternehmen damit vor den lähmenden Auswirkungen eines Verlusts dieser Daten.

2. Compliance

Die Compliance mit gesetzlichen Vorschriften ist für die meisten Unternehmen unerlässlich, da Gesetze wie die DSGVO und HIPAA die strikte Einhaltung der Anforderungen in Bezug auf Datenschutz, Sicherheit und Transparenz verlangen. Es steht viel auf dem Spiel: Bei fehlender Compliance drohen Strafen in Höhe von **bis zu 4 % des Jahresumsatzes** oder **20 Millionen EUR**, wobei der höhere Betrag maßgeblich ist.

Im Zusammenhang mit Microsoft Entra ID ist die Compliance mit Vorschriften von der ordnungsgemäßen Verwaltung der Benutzer- und Gruppenberechtigungen abhängig. Fehlkonfigurationen oder unbefugte Änderungen können sensible Daten offenlegen, wodurch es zu Datenschutzverletzungen und Compliance-Verstößen kommen kann. Wenn ein Administrator beispielsweise versehentlich zu viele Berechtigungen erteilt oder eine kritische Benutzergruppe löscht, können sensible Daten in die falschen Hände geraten und die Behörden können auf den Plan gerufen werden.

Um die Vorschriften einzuhalten, benötigen Unternehmen robuste Sicherheitskontrollen, einschließlich Verschlüsselung, Zugriffsverwaltung und Audit-Protokollierung. Eines der wichtigsten Compliance-Instrumente ist dabei jedoch eine umfassende Backup-Lösung.

Backups sorgen dafür, dass Ihre Microsoft Entra ID-Daten stets sicher und wiederherstellbar sind und den regulatorischen Vorgaben entsprechen. Sie können Fehlkonfigurationen oder nicht autorisierte Änderungen schnell erkennen und die korrekten Einstellungen wiederherstellen. Dadurch minimieren Sie das Risiko einer fehlenden Compliance mit Vorschriften und einer Offenlegung von Daten.



3. Versehentliche Löschungen und Fehlkonfigurationen

Stellen Sie sich vor, ein Administrator löscht versehentlich eine wichtige Benutzergruppe oder konfiguriert die Zugriffskontrollen in Microsoft Entra ID falsch. Plötzlich sind legitime Benutzer von wichtigen Systemen ausgesperrt oder — schlimmer noch — unbefugte Benutzer erhalten Zugriff darauf. In einem so zentralen System wie Microsoft Entra ID kann selbst ein kleiner Fehler weitreichende Folgen haben.

Die Auswirkungen dieser Fehlkonfigurationen und Löschungen sind tiefgreifend. Kritische Systeme können unzugänglich werden, was zu Ausfallzeiten und Produktivitätsverlusten führt und kostspielige Wiederherstellungsprozesse erforderlich macht. Darüber hinaus können diese Fehler das Vertrauen von Kunden und Partnern in ein Unternehmen schwächen und so möglicherweise Auswirkungen auf langfristige Geschäftsbeziehungen haben.

Doch es gibt auch eine gute Nachricht: Eine umfassende Backup-Lösung kann aus einer Katastrophe ein kleines Problem machen. Mithilfe von Backups können versehentliche Löschungen oder Fehlkonfigurationen innerhalb von Minuten korrigiert werden. Ob es um die Wiederherstellung einer gelöschten Benutzergruppe oder um die Rückkehr zu einer sicheren Konfiguration vor einem Fehler geht — ordnungsgemäße Backups sorgen dafür, dass sich Fehler nicht zu Krisen ausweiten.

Fehler werden passieren, das liegt in der Natur des Menschen. Doch mit einer robusten Backup-Strategie lassen sich die Folgen solcher Fehler besser vermeiden als je zuvor.



4. Einschränkungen des Papierkorbs

Nicht nur die Aufbewahrungszeit ist kurz, auch der Umfang des nativen Papierkorbs von Microsoft Entra ID ist begrenzt. Datentypen wie Rollenzuweisungen und Richtlinien für den bedingten Zugriff werden überhaupt nicht aufbewahrt — sie sind nach dem Löschen sofort unzugänglich, es gibt also keine zweite Chance. Auch die Beschränkung der wiederherstellbaren Datenmenge stellt eine Einschränkung dar. Der Papierkorb von Microsoft Entra ID ist eine hilfreiche Funktion, aber bei Weitem keine vollständige Lösung. Für bestimmte Datentypen bietet er zwar ein Wiederherstellungsfenster von bis zu 30 Tagen, doch das reicht in der Praxis nicht aus. Laut Microsoft Defense Report 2024 beträgt die durchschnittliche Zeit bis zur Erkennung von Vorfällen 207 Tage, also weit mehr als die Aufbewahrungsdauer im Papierkorb. Wenn Sie bemerken, dass Daten fehlen, ist es oft schon zu spät, sie wiederherzustellen.

Mit dem Papierkorb verhält es sich so: Wenn die Aufbewahrungsfrist abgelaufen ist oder Daten aufgrund von manuellen Löschungen oder dauerhaftem Entfernen den Papierkorb umgehen, ist eine Wiederherstellung mit den nativen Tools von Microsoft nicht mehr möglich. Eine spezielle Backup-Lösung ist die einzige Chance, diese Lücken zu schließen und den Schutz über die integrierten Schutzmechanismen von Microsoft hinausgehend auszuweiten. Auf diese Weise schaffen Sie ein zuverlässiges Sicherheitsnetz zum Schutz vor versehentlichen oder vorsätzlichen Datenverlusten und stellen sicher, dass nahezu alle Arten von Identitätsdaten wiederhergestellt werden können.

5. Effiziente Wiederherstellung

Sicherheitsverletzungen beginnen nicht immer mit einem Knall. Viele fangen mit kleinen, unbemerkten Änderungen an — einer nicht autorisierten Anpassung von Berechtigungen, der Löschung einer Sicherheitsgruppe oder einer kleinen Änderung der Einstellungen. Es ist entscheidend, diese Veränderungen frühzeitig erkennen zu können, damit sie sich nicht zu ernsthaften Bedrohungen ausweiten.

Der Schlüssel zur Vermeidung dieser Probleme liegt in einer schnelleren Erkennung von Änderungen. Administratoren müssen in der Lage sein, Probleme zu erkennen und zu lösen, bevor sie eine größere Reaktion erfordern. Mithilfe der granularen Wiederherstellungsoptionen sind Unternehmen in der Lage, genau die benötigten Objekte wiederherzustellen — von einem einzelnen Benutzerkonto bis hin zu einer vollständigen Verzeichnisstruktur — und das auf effiziente Weise ohne unnötige Ausfallzeiten.

Wie sieht nun eine effiziente Wiederherstellung für Microsoft Entra ID aus? Es handelt sich um eine Kombination aus folgenden Elementen:

- **Metadatenvergleich:** Vergleichen Sie vor der Wiederherstellung die Produktionskonfigurationen mit den Backup-Wiederherstellungspunkten. Dies stellt sicher, dass Sie genau wissen, was sich geändert hat, und in der Lage sind, nur das Nötige wiederherzustellen.
- **Wiederherstellung auf Objektebene:** Mit Funktionalitäten für eine granulare Wiederherstellung auf Objektebene können Sie bestimmte Elemente wiederherstellen, ohne Ihre restliche Umgebung zu beeinträchtigen.
- **Regelmäßige Backups:** Stellen Sie sicher, dass alle Änderungen und Konfigurationen in regelmäßigen Abständen in einem sicheren Repository gespeichert werden. Dies schafft ein zuverlässiges Sicherheitsnetz und ermöglicht eine schnelle und genaue Wiederherstellung, wenn Probleme auftreten.
- **Umsetzbare Wiederherstellungspläne:** Stellen Sie klare, schrittweise Prozesse für die Wiederherstellung von Systemen bereit, damit Ihr Unternehmen eine schnelle, sichere und nahtlose Wiederherstellung durchführen kann.

Zusammen bilden diese Elemente eine umfassende Wiederherstellungsstrategie, die Ausfallzeiten minimiert, Risiken reduziert und dafür sorgt, dass Ihre Microsoft Entra ID-Umgebung sicher und zugänglich bleibt.



6. Hybride Umgebungen

Die Verwaltung von Identitäten über ein lokales Active Directory (AD) und Microsoft Entra ID hinweg in einer hybriden Umgebung bringt sowohl Flexibilität als auch Komplexität mit sich. Da Benutzer ständig zwischen Cloud- und lokalen Systemen synchronisieren, können versehentliche Löschungen, Fehlkonfigurationen oder Synchronisierungsprobleme den Zugriff unterbrechen und Sicherheitsrisiken verursachen. Wenn ein Benutzer entfernt wird — sei es bewusst oder versehentlich —, ist es entscheidend für die Business Continuity, dass nicht nur seine Identität, sondern auch seine Beziehungen und Berechtigungen wiederhergestellt werden können.

Microsoft Entra Connect und andere Synchronisierungstools konzentrieren sich darauf, Identitätsdaten zwischen AD und Entra ID konsistent zu halten, sie sind jedoch nicht für eine vollständige Wiederherstellung vorgesehen. Wenn ein synchronisierter Benutzer gelöscht wird, wird er von Entra Connect möglicherweise ohne seine ursprünglichen Rollen, Gruppenmitgliedschaften und Lizenzen wiederhergestellt. Administratoren sind dann gezwungen, die Identität des Benutzers manuell zu rekonstruieren. Dieser Prozess ist zeitaufwendig und erhöht das Risiko unvollständiger Wiederherstellungen oder einer Fehlausrichtung von Berechtigungen.

Bei der Verwaltung hybrider Identitäten geht es nicht nur darum, Benutzer aktiv zu halten, sondern sie mit den richtigen Zugriffs-, Rollen- und Sicherheitseinstellungen wiederherzustellen. Ohne eine geeignete Backup-Strategie können IT-Teams Stunden damit verbringen, Zugriffsprobleme nach einer Löschung oder einem Synchronisierungsfehler manuell zu beheben.

Veeam Data Cloud for Microsoft Entra ID

Die Herausforderungen bei der Sicherung von Microsoft Entra ID liegen auf der Hand: Menschliches Versagen, Cyberbedrohungen und Compliance-Anforderungen schaffen beständig neue Risiken. Ohne eine robuste Backup-Strategie kann selbst ein kleiner Fehler zu Ausfallzeiten, Produktivitätsverlusten und Sicherheitsverletzungen führen.

Microsoft Entra ID ist das Rückgrat der digitalen Identität Ihres Unternehmens und muss daher unbedingt geschützt werden. Mit **Veeam Data Cloud for Microsoft Entra ID** können Sie den Datenschutz vereinfachen und sicherstellen, dass Ihre Identitätsinfrastruktur sicher, konform und stets verfügbar ist.

Diese SaaS-Backup-Lösung bietet folgende Vorteile:



Umfassende Sicherung und Wiederherstellung:

Schutz für Benutzer, Gruppen, Anwendungsregistrierungen und verschiedene andere Objekte



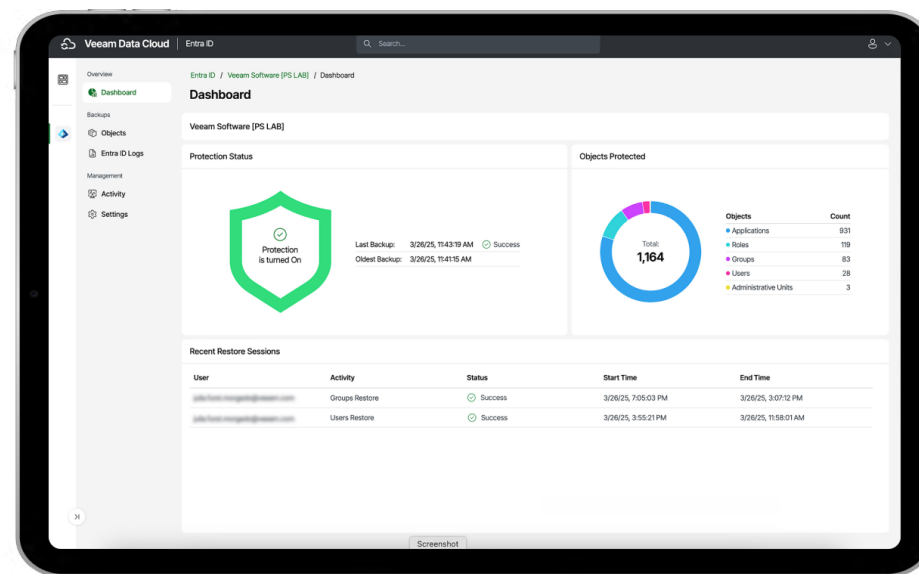
Unbegrenzter Speicher:

Dank der in die SaaS-Backup-Lösung integrierten unbegrenzten Speicher können Sie problemlos skalieren.



Nahtlose Benutzererfahrung:

Eine moderne, einheitliche Benutzeroberfläche, die auf Benutzerfreundlichkeit ausgelegt ist.



Microsoft Entra ID ist zu wichtig, um nicht geschützt zu werden. Die Risiken sind real, doch die Lösung ist es auch. Veeam bietet die Sicherheit, Resilienz und Gewissheit, die moderne Unternehmen benötigen, um dafür zu sorgen, dass ihre Identitätsinfrastruktur dauerhaft geschützt, konform und stets verfügbar ist.

→ [Demo anfordern](#)

→ [Kontakt zum Vertrieb](#)

Erfahren Sie mehr über den Schutz für Microsoft 365

Sichern Sie Microsoft 365 und Entra ID gemeinsam



Die Themen dieses Reports:

- Verantwortlichkeiten Ihres Unternehmens in Microsoft 365
- Gründe, weshalb der Schutz von Microsoft 365-Daten heute so wichtig ist
- Erkennen von Sicherheitslücken in Ihrem Unternehmen
- Die Vorteile der Nutzung eines Backup-Service gegenüber anderen Methoden



→ [7 wichtige Gründe für Microsoft 365 Backup](#)