Barracuda

Backup und Archivierung für Microsoft 365

White Paper

Zusammenfassung

Die beiden sich ergänzenden Prozesse für Datensicherung und Informationsarchivierung werden häufig nicht klar voneinander abgegrenzt. In diesem White Paper werden die Konzepte verglichen und die jeweils dadurch erfüllten Anforderungen erläutert. Außerdem wird darauf eingegangen, warum Unternehmen auch nach dem Wechsel zu Microsoft 365 weiterhin eine Backup- und eine Archivierungslösung benötigen. Darüber hinaus erfahren Sie hier, warum es nicht ratsam ist, eine einzige Lösung für beide Prozesse einzusetzen.

Vergleich zwischen Backup und Archivierung

In Backups und Archiven werden jeweils Kopien von Daten aus der Produktionsumgebung gespeichert, allerdings für jeweils unterschiedliche Anwendungsfälle. Daher ist für jeden Vorgang eine eigene Lösung erforderlich.

Ein Backup (eine Sicherungskopie) ermöglicht die Wiederherstellung, wenn Daten verloren gegangen sind, beschädigt wurden oder nicht mehr zugänglich sind. Es dient also in erster Linie als Maßnahme zur Datenwiederherstellung. Bei einer Sicherung werden mehrere Kopien gespeichert, die jeweils mit einer bestimmten Datenrevision verknüpft sind, sodass die Wiederherstellung eines bekannten fehlerfreien Zustands zu einem bestimmten Zeitpunkt möglich ist.

Ein Archiv ermöglicht die Einhaltung rechtlicher und geschäftlicher Datenaufbewahrungsrichtlinien sowie das eDiscovery. Ein Archiv umfasst eine einzelne Kopie in einem sicheren unveränderlichen Speicher für einen begrenzten Zeitraum, sodass Endbenutzer weiterhin auf bisherige Geschäftsdaten zugreifen können.

Diese Tabelle enthält eine Zusammenfassung der wichtigen Unterschiede zwischen Backup und Archivierung:

Funktion	Backup	Archivierung
Hauptzweck	Schutz aktueller Daten und von Revisionsdaten	Beibehaltung historischer Daten
Ermöglicht	Point-in-Time-Datenwiederherstellung	Datenaufbewahrung und Discovery
Geschäftliche Anforderung	Wiederherstellung von Daten von einem bestimmten Zeitpunkt nach Verlust, Beschädigung oder unbeabsichtigter Löschung	Vollständige und akkurate Nachweise zur Erfüllung rechtlicher, gesetzlicher und unternehmensweiter Verpflichtungen
Benutzer	Administratoren (IT)	Geschäftsanwender (Rechtsabteilung, HR usw.)
Inhalt	Mehrere Point-in-Time-Kopien von Daten (Revisionen)	Eine einzelne vollständig indizierte Kopie aller Daten
Optimiert für	Point-in-Time-Wiederherstellung der Produktionsumgebung	Aufbewahrung, Suche, Abruf, Analyse und Export auf Elementebene
Datenverschiebung	Quelldaten verbleiben an Ort und Stelle	Quelldaten können gelöscht werden
Suche	Suche nach Point-in-Time-Revisionen und allgemeinen Metadaten	Volltextsuche in Dateien, Anhängen und Metadaten (Verwalter, Stichwörter usw.) plus eDiscovery-Funktion
Aufbewahrungsrichtlinien	In erster Linie basierend auf dem Alter der wiederherzustellenden Daten	In erster Linie basierend auf Alter, Speicherort, Inhalt und Metadaten. Umfasst Vorrang der gesetzlichen Aufbewahrungsfrist.

Um Daten effektiv zu schützen und aufzubewahren, benötigen Unternehmen sowohl eine Backup- als auch eine Archivierungsstrategie. Sie können zwar versuchen, eine Sicherungslösung als Archiv (und umgekehrt) zu verwenden, wie dieses Dokument aber erläutert, ist dieser Ansatz aufgrund erheblicher Einschränkungen und Nachteile nicht ratsam.

Backups dienen der Wiederherstellung

Der Hauptzweck von Backup ist es, die Wiederherstellung zu ermöglichen, wenn die ursprüngliche Datenversion aufgrund von unbeabsichtigter oder versehentlicher Löschung verloren geht oder Dateien beschädigt wurden und nicht mehr verwendet werden können.

Ein Sicherungssystem erfasst dazu regelmäßig Kopien der Daten, um mehrere Revisionen zu erstellen. Jede dieser Revisionen spiegelt die Daten zu einem bestimmten Zeitpunkt wider und kann nach Bedarf wiederhergestellt werden.

Die meisten Sicherungskopien werden nur einige Tage oder Wochen lang beibehalten und anschließend durch neueren Kopie ersetzt. Häufig wird jedoch eine Version längere Zeit (z. B. eine Woche oder einen Monat) beibehalten, damit Daten auch von einem früheren Zeitpunkt wiederhergestellt werden können. Insbesondere für E-Mail-Daten werden Sicherungslösungen in der Regel dazu eingesetzt, die neuesten Daten zu schützen, da diese meist am relevantesten für Endbenutzer sind.

Gründe für ein Backup von Microsoft 365

Der häufigste Grund für Datenverlust in einer SaaS-Umgebung wie Microsoft 365 ist das versehentliche Löschen durch Benutzer. Jedoch können Daten auch auf andere Weise verloren gehen. Anwendungs- oder Verarbeitungsfehler können dazu führen, dass Daten verloren gehen oder überschrieben werden. Zudem besteht immer das Risiko, dass Mitarbeiter mit Zugriff auf Daten diese mit böswilliger Absicht löschen. Eine Bedrohung, die in letzter Zeit an Bekanntheit gewonnen hat, ist Ransomware, die Daten verschlüsselt, sodass sie nicht mehr zugänglich sind.

Microsoft 365 selbst stellt in erster Linie sicher, dass die Service- und Datenverfügbarkeit nicht unterbrochen wird. Microsoft stellt Kunden aber auch zwei Optionen für die Datenwiederherstellung zur Verfügung:

1. Papierkorb: Vor Kurzem von Benutzern gelöschte Daten können aus dem Papierkorb (bei OneDrive) bzw. aus den Ordnern „Gelöschte Elemente“ und „Wiederherstellbare Elemente“ (bei Exchange Online) wiederhergestellt werden. Diese unterliegen aber den unten aufgeführten Aufbewahrungszeiträumen, nach denen Daten endgültig gelöscht werden und nicht mehr verfügbar sind.

MICROSOFT-LÖSUNG	WIEDERHERSTELLUNGSFEATURE	AUFBEWAHRUNGSZEITRAUM
SharePoint Online	Papierkorb für Website	93 Tage
	Endgültiger Papierkorb	93 Tage
Exchange Online	Gelöschte Elemente	Konfigurierbar
	Wiederherstellbare Elemente	Bis zu 30 Tage
OneDrive for Business	Papierkorb	93 Tage
	Endgültiger Papierkorb	93 Tage

2. Versionsverwaltung für Dokumente: Wenn das Feature der Versionsverwaltung für Dokumente aktiviert ist, behält OneDrive for Business eine bestimmte Anzahl vorheriger Versionen jedes geänderten Dokuments bei, sodass Endbenutzer jede dieser vorherigen Versionen wiederherstellen können. Dieses Feature bietet jedoch keinen Schutz vor unbeabsichtigtem oder versehentlichem Löschen, da alle Versionen eines Dokuments beim Löschen der aktuellen Version entfernt werden.

Unternehmen, die Microsoft 365 einsetzen, sollten sich über die erheblichen Einschränkungen beider dieser Optionen bewusst sein:

- Diese Optionen gelten für individuelle Elemente und eignen sich daher nicht für die Wiederherstellung größerer Datenmengen wie ganze Ordner oder Posteingänge
- Eine Point-in-Time-Wiederherstellung kann bei beiden dieser Optionen nur mit beträchtlichem zusätzlichen Arbeits- und Rechenaufwand durchgeführt werden.

Ein weiterer Problembereich mit Microsoft 365 ist die Beibehaltung von Daten, wenn ein Mitarbeiter aus einem Unternehmen austritt. Alle von einem Benutzer in Exchange Online gespeicherten Daten werden 30 Tage nach Löschen des jeweiligen Kontos gelöscht. Diese Daten müssen also zunächst gesichert werden. E-Mail-Daten können längere Zeit beibehalten werden, wenn eine Aufbewahrungsrichtlinie vor der Löschung des Kontos angewendet wird. Dieses Premium-Feature ist allerdings nur ab Microsoft 365 E3-Plänen verfügbar.

Daher setzen nun immer mehr Unternehmen Sicherungslösungen von Drittanbietern mit Microsoft 365 ein. Diese Lösungen bieten eine zusätzliche Schutzschicht sowie viel längere Aufbewahrungszeiträume und umfassendere Widerherstellungsoptionen.

Probleme bei Nutzung eines Backups als Archiv:

Bei Verwendung eines Backups als Archivierungslösung entstehen mehrere Probleme:

- Ein Backup erfasst alle Daten zu einem bestimmten Zeitpunkt, allerdings keine flüchtigen Daten wie neue E-Mail-Nachrichten, die unter Umständen vor der nächsten Sicherung geändert oder gelöscht werden. Dementsprechend kann ein Backup nicht komplett konforme Datenaufbewahrung und eDiscovery für eine Organisation unterstützen.

- Aufgrund gesetzlicher Anforderungen und geschäftlicher Vorschriften müssen Unternehmen in der Regel eine Reihe Aufbewahrungsrichtlinien für unterschiedliche Informationsarten durchsetzen. Diese basieren häufig auf dem Dateninhalt selbst oder den mit den einzelnen Datenelementen verknüpften Metadaten. Dank der Indizierung unterstützt die Archivierung zahlreiche richtlinienbasierte Aufbewahrungsregeln für die höchsten Anforderungen, während die Aufbewahrungsrichtlinien in Sicherungslösungen diese granulare Kontrolle normalerweise nicht bereitstellen.

- Archivierungslösungen unterstützen Such- und Abruffunktionen und indizieren daher alle Dateninhalte und Metadaten. Gleichzeitig ermöglichen erweiterte Verfahren wie die Volltextsuche und das Daten-Tagging es Geschäftsanwendern, Discovery-Aufgaben einfach ohne Beteiligung der IT auszuführen. Sicherungslösungen dagegen sind für Administratoren konzipiert, die auf Dateiebene oder höher arbeiten. Da die Daten hierbei in der Regel nicht vollständig indiziert werden, kann die Nutzung eines Backups für eDiscovery-Zwecke eine hoch komplexe und zeitaufwendige Aufgabe für die IT-Abteilung sein.

- Backup-Lösungen behalten mehrere Point-in-Time-Revisionen bei, damit Unternehmen Wiederherstellungspunktziele erreichen können. Das Durchsuchen mehrerer Revisionen gibt allerdings mehrere Versionen individueller Datenelemente zurück, die dann abgestimmt werden müssen, um eine einzelne akkurate und prüfbare Ergebnismenge für eDiscovery bereitzustellen. Ein Archiv liefert dagegen eine einzelne prüfbare Kopie jedes Datenelements.

- Da Endbenutzer nicht auf Sicherungslösungen zugreifen können, kann es erheblichen andauernden Arbeitsaufwand für die IT-Abteilung bedeuten, den Endbenutzern Zugriff auf ihre historischen Daten zu ermöglichen. Im Gegensatz dazu können Endbenutzer mit Archivierungslösungen ihre eigenen archivierten Daten durchsuchen und abrufen sowie einzelne Elemente nach Bedarf wiederherstellen, ohne dass die IT-Abteilung daran beteiligt ist.

Archivierung dient der Discovery

Der Hauptzweck der Archivierung ist die langfristige Aufbewahrung aktueller und historischer Daten, damit das Unternehmen rechtlichen und anderen eDiscovery-Anfragen zu diesen Daten nachkommen sowie seine Compliance- und Geschäftsanforderungen zu Datenaufbewahrung und -löschung erfüllen kann.

Dazu erfasst und sichert ein Archivierungssystem eine Kopie jedes erstellten Datenelements. Eine E-Mail muss beispielsweise erfasst werden, sobald die Nachricht gesendet oder empfangen wird und bevor ein Endbenutzer sie ändern oder löschen kann.

Das Archiv wird mit der Zeit immer größer und enthält jedes Datenelement, das je in dieser Zeit vorhanden war, selbst wenn es in der Zwischenzeit aus dem ursprünglichen Speicherort gelöscht wurde. Aufbewahrungsrichtlinien sorgen dafür, dass die Archivkopie jedes Datenelements so lange wie nötig beibehalten und nach dem erforderlichen Zeitraum gelöscht wird.

Endbenutzer können ihre eigenen archivierten Daten jederzeit durchsuchen und abrufen. Auditoren und Administratoren erhalten gleichzeitig zahlreiche erweiterte Such- und Exportfeatures, mit denen sie komplexe unternehmensweite eDiscovery-Anforderungen erfüllen können.

Gründe für eine Archivierung von Microsoft 365

Microsoft hat die Compliance-Features in Microsoft 365 verbessert und bietet zudem ein Archivpostfach in Exchange Online. Es gelten aber nach wie vor einige Einschränkungen. Aufgrund dieser Einschränkungen und der Verwendung der „In-Place-Archivierung" anstelle eines separaten eigenen Archivs eignet sich Microsoft 365 in den meisten Fällen nicht für Unternehmen mit speziellen Anforderungen an Datenaufbewahrung, Richtliniendurchsetzung und E-Discovery. Beachten Sie zudem, dass die Archivierungs- und Compliance-Features nur in den kostspieligeren Microsoft 365 E3- und E5-Plänen verfügbar sind.

Datensicherheit: Microsoft 365 behält alle Daten (einschließlich archivierter Daten) zusammen mit transienten Daten in der Betriebsumgebung bei, wo sie geändert oder gelöscht werden können. Lösungen von Drittanbietern verwenden im Gegensatz dazu den bewährten „Best Practice"-Ansatz, bei dem eine separate unveränderliche Kopie jeder E-Mail außerhalb der betrieblichen E-Mail-Umgebung in einem eigenen sicheren Repository beibehalten wird.

Datenaufbewahrung: Aufbewahrungsrichtlinien für E-Mails in Microsoft 365 gelten nur für Alter oder Speicherort. Sie bieten nicht die Flexibilität oder Granularität, die viele Unternehmen zum Erfüllen ihrer Compliance-Anforderungen benötigen, wie z. B. Regeln für Verwalter oder Inhalt.

Datenbeibehaltung: Aufbewahrungsrichtlinien in Microsoft 365 verwenden einen komplexen Prozess mit mehreren Ordnern, um E-Mail-Daten vor Änderungen oder Löschung zu schützen. Die Unterordner für Discovery-Aufbewahrung und Versionen im Ordner „Wiederherstellbare Elemente" werden zum Speichern der Originalkopien von gelöschten oder geänderten Elementen verwendet, während unveränderte Elemente im Posteingang oder Archivpostfach des Benutzers verbleiben. Das bedeutet, dass die Originalkopien von E-Mails auf mehrere Ordner verteilt sein können, wobei ein Postfach mehrere Versionen derselben E-Mail enthalten kann. So können Sie also nur schwer sicherstellen und nachweisen, dass Sie eine vollständige und akkurate Kopie jeder gesendeten oder empfangenen E-Mail beibehalten.

Aufgrund dieser und weiterer Einschränkungen eignet sich Microsoft 365 in den meisten Fällen nicht für Unternehmen mit speziellen Anforderungen an Datenaufbewahrung, Richtliniendurchsetzung und eDiscovery. Daher implementieren viele Organisationen nun Archivierungslösungen von Drittanbietern zur Ergänzung von Microsoft 365.

Probleme bei Nutzung eines Archivs zur Wiederherstellung:

Einige Unternehmen können sich dazu verleiten lassen, im Archiv gespeicherte Daten als Sicherungslösung zu verwenden. Dieser Ansatz bringt aber mehrere Einschränkungen mit sich und ist somit ungeeignet und problematisch:

- Ein Archiv erfasst eine Kopie aller in einem bestimmten Zeitraum erstellten Datenelemente in einer einzigen Version. Ein Backup erfasst dagegen jede Revision eines Datenelements im aktuellen Kontext zu diesem Zeitpunkt. Eine Point-in-Time-Wiederherstellung aus einem Archiv kann unter Umständen nur mit beträchtlichem zusätzlichen Arbeits- und Rechenaufwand durchgeführt werden.

- Die Verzeichnisstruktur für die Daten jedes Benutzers im Archiv basiert auf historischen Informationen und spiegelt möglicherweise nicht die aktuelle Live-Nutzung wider, sodass Daten nur schwer am richtigen Speicherort wiederhergestellt werden können.

- Ein Archiv behält (entsprechend den Aufbewahrungsrichtlinien der Organisation) eine Kopie aller Daten bei, mit denen ein Benutzer im jeweiligen Zeitraum gearbeitet hat. Diese umfasst Elemente, die gezielt gelöscht wurden und nur bei spezifischer Anforderung wiederhergestellt werden sollten.

- Ein Archiv ist für Suche und Abruf optimiert, sodass Endbenutzer individuelle Elemente wiederherstellen können. Es eignet sich aber wahrscheinlich nicht für die Wiederherstellung größerer Datenmengen wie ganze Ordner oder Postfächer.

Backups und Archive sollten sich ergänzen

Wie weiter oben erläutert übernehmen Sicherung und Archivierung unterschiedliche Funktionen für unterschiedliche Zwecke. Sie ergänzen sich jedoch, und die Funktionen einer Lösung können zu einem effizienteren Betrieb der jeweils anderen beitragen.

Die Speicherung von Daten in einem Archiv ist die beste Möglichkeit, eine sichere Kopie aller historischen Informationen beizubehalten. Außerdem können Unternehmen dadurch ihre Geschäftsanforderungen im Hinblick auf Compliance und Discovery erfüllen.

Eine Archivierung älterer oder inaktiver Daten, bei der diese aus dem Betriebsspeicher entfernt werden, verbessert zudem die Leistung von Sicherungsprozessen. Da die zu sichernde Datenmenge verringert wird, können Backups schneller erstellt werden. Darüber hinaus können Daten aufgrund der geringeren Datenmenge einfacher wiederhergestellt werden.

Barracuda-Lösungen für Sicherung und Archivierung mit Microsoft 365

Barracuda Cloud-to-Cloud Backup

Diese Lösung schützt Exchange Online- und OneDrive for Business-Daten, indem diese direkt in Barracuda Cloud Storage gesichert werden. Sie können Barracuda Cloud-to-Cloud Backup als Add-on für eine lokale Barracuda Backup-Appliance oder als eigenständiges Abonnement ohne Appliance verwenden.

Für Exchange Online schützt Barracuda Cloud-to-Cloud Backup alle E-Mail-Nachrichten, einschließlich aller Anhänge, sowie die vollständige Ordnerstruktur der Postfächer aller Benutzer. In OneDrive for Business werden alle Dateien in der Document Library, einschließlich der gesamten Ordnerstruktur, geschützt.

Barracuda Cloud Archiving Service

Die cloudbasierte Archivierung ermöglicht es Microsoft 365-Kunden, strenge Compliance-Vorschriften zu erfüllen und eDiscovery-Anfragen mühelos und effektiv zu bearbeiten. Der Barracuda Cloud Archiving Service gewährleistet, dass E-Mails sicher in einem separaten Repository gespeichert werden – so lange wie nötig und ohne Risiko für Änderung oder Löschung.

Essentials for Office 365

Barracuda Essentials für Microsoft 365 kombiniert Cloud-to-Cloud Backup und Cloud Archiving Service mit dem Barracuda Email Security Service und bietet so eine integrierte mehrschichtige Sicherheits-, Archivierungs- und Sicherungslösung für Microsoft 365. Microsoft 365-Kunden können sich auf umfassenden Schutz von E-Mails, Daten und Cloud-Infrastrukturen mit Barracuda Essentials verlassen.

Fazit

Auch in Microsoft365 sind Sie noch immer für Ihre Daten verantwortlich. Obwohl Microsoft Ihre Daten so effektiv wie möglich verwaltet, müssen Sie sich letztendlich um den Schutz, die Sicherung und die Compliance dieser Daten kümmern – genauso wie vor dem Wechsel zu Microsoft 365. Daher müssen Sie effektive Backup- und Archivierungslösungen implementieren.

Sie haben in diesem Dokument gelernt, dass Backup- und Archivierungslösungen jeweils eigene Merkmale und Features aufweisen, um zwei unterschiedliche Anforderungen zu erfüllen.

Auch wenn einige Unternehmen versucht sein können, ihr Archiv als Backup (oder umgekehrt) zu verwenden, stellt dies wegen der vielen damit verbundenen Probleme keinen effektiven Ansatz dar. Unternehmen sollten also sowohl eine Archivierungs- als auch eine Backup-lösung implementieren.

Minimieren Sie Verwaltungs- und Supportaufwand durch die Wahl eines etablierten Anbieters wie Barracuda und einer integrierten Lösung wie Essentials für Microsoft 365. Damit erhalten Sie sowohl Backup und Archivierung als auch E-Mail-Sicherheit.

Über Barracuda Networks

Barracuda ist bestrebt, die Welt zu einem sichereren Ort zu machen und überzeugt davon, dass jedes Unternehmen Zugang zu Cloud-fähigen, unternehmensweiten Sicherheitslösungen haben sollte, die einfach zu erwerben, zu implementieren und zu nutzen sind. Barracuda schützt E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die im Zuge der Customer Journey wachsen und sich anpassen. Mehr als 200.000 Unternehmen weltweit vertrauen Barracuda, damit diese sich auf ein Wachstum ihres Geschäfts konzentrieren können. Für weitere Informationen besuchen Sie www.barracuda.com.

Barracuda

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
USA

t: 1-408-342-5400
1-888-268-4772 (USA & Kanada)
e: info@barracuda.com
w: barracuda.com