7 wichtige Gründe für Microsoft 365 Backup

Warum Unternehmen ihre Microsoft 365-Daten sichern müssen

Einführung

Haben Sie die Kontrolle über Ihre Microsoft 365-Daten? Haben Sie Zugriff auf alle benötigten Objekte? Die reflexartige Antwort ist in der Regel „Natürlich“ oder „Microsoft kümmert sich darum“. Aber sind Sie sich da wirklich sicher?

Microsoft kümmert sich um eine ganze Menge. Das Unternehmen bietet seinen Kunden erstklassigen Service, indem es die Infrastruktur von Microsoft 365 verwaltet und die Verfügbarkeit für Ihre Benutzer sicherstellt. Die Verantwortung für Ihre Daten überlässt Microsoft jedoch IHNEN. Unternehmen unterliegen häufig dem Irrglauben, dass Microsoft ihre Daten standardmäßig sichert. Eine Microsoft 365-Standardlizenz bietet jedoch keine umfassendes Backup Ihrer Daten. Es könnte nachteilige Folgen haben, wenn Sie Ihre Vorgehensweise nicht ändern und diese Verantwortung nicht selbst wahrnehmen.

Letztendlich müssen Sie sicherstellen, dass Sie Zugriff auf und Kontrolle über Ihre Daten in Exchange Online, SharePoint Online, OneDrive for Business und Microsoft Teams haben. Und selbst wenn Sie keine Backup-Infrastruktur verwalten möchten, gibt es Backup-Services, die sich ohne manuellen Verwaltungs- oder Wartungsaufwand schnell bereitstellen lassen. Denken Sie an sofortigen Zugriff auf anpassbare Datensicherung, blitzschnelle Wiederherstellung und die Gewissheit, stets die Kontrolle zu haben. Denken Sie dann daran, was Sie riskieren, wenn Sie dies alles nicht haben.

Dieser Report untersucht die Risiken, denen Sie ausgesetzt sind, wenn Sie keinen Backup-Plan für Microsoft 365 haben. Wir sprechen darüber, wie Backup-Lösungen für Microsoft 365, insbesondere cloudbasierte Backup-Services, Lücken hinsichtlich der langfristigen Aufbewahrung und der Datensicherung schließen. Dies ist für moderne Unternehmen von wirklich kritischer Bedeutung.

> „Sun Chemical ist ein wirklich globales Unternehmen: Jeden Tag verlassen sich Mitarbeiter weltweit auf Microsoft 365-Anwendungen, um kritische Daten auszutauschen. Veeam Data Cloud for Microsoft 365 schützt diesen essenziellen Teil unserer Umgebung. Die Lösung hilft unseren Mitarbeitern, produktiver zu arbeiten, und bietet uns eine zusätzliche Ebene der Cyberresilienz.“

Stuart Hudson
Global IT Infrastructure Senior Manager
Strategic Infrastructure Programs — AP, Sun Chemical

Der große Irrglaube in Bezug auf Microsoft 365

Dieser Unterschied zwischen der angenommenen Verantwortung von Microsoft und der tatsächlichen Verantwortung der Unternehmen selbst für Microsoft 365-Daten führt dazu, dass sich Unternehmen nicht um die Sicherung und langfristige Aufbewahrung ihrer Daten kümmern. Die Resilienz- und Aufbewahrungsfunktionalität, die Microsoft in einer Microsoft 365-Standardlizenz bereitstellt, unterscheidet sich häufig von dem, was Benutzer annehmen. Sie müssen also unter Umständen genau prüfen, wie viel Kontrolle Sie neben den standardmäßigen Sicherheitsvorkehrungen von Microsoft 365 über Ihre Daten haben, und wie gut Sie tatsächlich darauf zugreifen können.

Microsoft 365 bietet Geo-Redundanz, was häufig als Backup-Funktionalität missverstanden wird. Geo-Redundanz schützt Daten bei einem Standort- oder Hardwareausfall, sodass die Benutzer bei einem Ausfall ihrer Infrastruktur weiterarbeiten können und häufig gar nichts von diesen Problemen bemerken. Bei Backups hingegen wird eine historische Kopie der Daten erstellt und an einem Standort gespeichert, der nicht mit der Produktivumgebung identisch ist. Dies stellt sicher, dass eine Kopie Ihrer Daten vorhanden ist — unabhängig davon, was innerhalb von Microsoft 365 geschieht — und dass die Daten stets wiederhergestellt werden können.

Backups (und nicht die Geo-Redundanz) sind die letzte Verteidigungslinie eines Unternehmens. Es ist jedoch nicht nur wichtig, dass es Backups gibt — es muss auch sichergestellt sein, dass Sie direkt auf sie zugreifen können und die Kontrolle über sie haben. Wenn Daten verloren gehen, versehentlich gelöscht werden oder Angriffen ausgesetzt sind, müssen Sie diese schnell wiederherstellen können.

Microsoft 365 basiert auf dem Modell der gemeinsamen Verantwortung

Die Wahrnehmung

Microsoft kümmert sich um alles.

Die Realität

Microsoft kümmert sich um die Infrastruktur, aber die Daten bleiben in der Verantwortung des Kunden.

Verfügbarkeit von Microsoft 365

Schutz und langfristige Aufbewahrung von Microsofts 365-Daten

> "Ihre Daten und Identitäten gehören bei jeder Art von Cloudbereitstellung Ihnen."

Quelle: Gemeinsame Verantwortung in der Cloud, Microsoft

7 Gründe, warum ein Backup-Plan für Microsoft 365 von kritischer Bedeutung ist

Microsoft 365 ist eine zuverlässige und leistungsstarke Software-as-a-Service (SaaS)-Plattform, die den Anforderungen zahlreicher Unternehmen vollständig gerecht wird. Microsoft 365 stellt die Verfügbarkeit von Anwendungen sicher, damit Ihre Benutzer stets produktiv sein können. Eine umfassende Backup-Lösung kann Sie jedoch vor zahlreichen weiteren Sicherheitsbedrohungen schützen, bietet Sicherheit und robusten Datenschutz.

Sie oder Ihr Vorgesetzter sind vielleicht der Meinung, dass Daten „im Notfall auch aus dem Papierkorb wiederhergestellt werden können". Und genau damit liegen Sie falsch — wie übrigens viele andere Benutzer auch. Die Zeitspanne von einem Datenschutzverstoß bis zu seiner Entdeckung kann ungefähr 140 Tage betragen — eine erschreckend lange Zeit. Sehr wahrscheinlich werden Sie daher erst bemerken, dass etwas fehlt, wenn es für eine Wiederherstellung über den Papierkorb zu spät ist — und das ist noch nicht einmal Ihr größtes Problem.

Quelle: [7 Schritte zu einer ganzheitlichen Sicherheitsstrategie, Microsoft]

In unseren Gesprächen mit Hunderten von IT-Professionals weltweit, die zu Microsoft 365 migrierten, ergaben sich im Bereich Datensicherung sieben wichtige Schwachstellen:

1. Versehentliche Löschung

2. Aufbewahrungsrichtlinie — Lücken und Ungenauigkeiten

3. Interne Sicherheitsbedrohungen

4. Externe Sicherheitsbedrohungen

5. Gesetzliche Bestimmungen und Compliance-Anforderungen

6. Management von hybriden E-Mail-Bereitstellungen und Migration zu Microsoft 365

7. Teams-Datenstruktur

1. Versehentliche Löschung

Angenommen, Sie löschen einen Benutzer. Ob Sie dies beabsichtigt haben oder nicht, diese Löschung wird im gesamten Netzwerk repliziert, ebenso wie die Löschung des OneDrive for Business-Kontos und des Postfachs. Wenn keine alternativen Lösungen genutzt werden, schützen die nativen Papierkörbe und Versionsverläufe von Microsoft 365 nur eingeschränkt vor Datenverlusten. Daher kann ein ansonsten einfacher Backup-Job zu einem großen Problem werden, wenn Microsoft 365 Daten unwiderruflich in allen Speicherregionen löscht oder wenn der Aufbewahrungszeitraum abgelaufen ist.

Auf der Microsoft 365-Plattform gibt es zwei Arten von Löschvorgängen: vorläufiges („weiches“) Löschen und endgültiges („hartes“) Löschen. Ein Beispiel für vorläufiges Löschen ist das Leeren des Ordners „Gelöschte Elemente“. Die auf diese Weise gelöschten Elemente werden auch als „dauerhaft gelöscht“ bezeichnet. Die Löschung ist in diesem Fall allerdings nicht wirklich dauerhaft, da sich diese Elemente weiterhin im Ordner „Wiederherstellbare Elemente“ befinden. Beim endgültigen Löschen wird ein Objekt so gekennzeichnet, dass es vollständig aus der Postfachdatenbank entfernt wird. Eine Wiederherstellung ist dann wirklich und endgültig nicht mehr möglich. Bei Verwendung einer Backup-Lösung als Failsafe-Mechanismus sind Datenverluste aufgrund einer versehentlichen Löschung jedoch ausgeschlossen.

2. Aufbewahrungsrichtlinie — Lücken und Ungenauigkeiten

Im unserem dynamischen digitalen Zeitalter unterliegen Richtlinien kontinuierlichen Änderungen. Es ist alles andere als einfach, den Überblick über immer wieder neue Aufbewahrungsrichtlinien zu behalten, ganz zu schweigen davon, diese korrekt zu handhaben. Wie beim vorläufigen und endgültigen Löschen stellt Microsoft 365 nur eingeschränkte Sicherungs- und Aufbewahrungsrichtlinien bereit, mit denen sich Datenverluste nur in bestimmten Situationen vermeiden lassen. Diese Richtlinien sollen auch keine umfassende Backup-Lösung darstellen.

Eine bestimmte Art der Wiederherstellung, die Wiederherstellung von Postfachelementen auf einen bestimmten Zeitpunkt, ist mit einer Microsoft 365-Standardlizenz nicht möglich. Bei einem katastrophalen Vorfall bietet eine Backup-Lösung die Möglichkeit, ein Rollback auf einen früheren, bestimmten Zeitpunkt durchzuführen und so den Geschäftsbetrieb aufrechtzuerhalten. Mehr noch: Mit einer Backup-Lösung, die speziell auf Microsoft 365 zugeschnitten ist, gibt es keine Lücken bei der Aufbewahrungsrichtlinie oder fehlende Flexibilität bei der Wiederherstellung. Ob kurzfristige Backups oder langfristige Archivierung, granulare Wiederherstellung oder Wiederherstellung auf einen bestimmten Zeitpunkt — die gesamte Funktionalität ist direkt verfügbar, sodass Daten schnell, einfach und zuverlässig wiederhergestellt werden können.

3. Interne Sicherheitsbedrohungen

Wenn der Begriff „Sicherheitsbedrohungen“ fällt, denken die meisten Menschen an Hacker und Computerviren. Dabei sind Unternehmen auch Gefahren von innen ausgesetzt — und dies häufiger, als oft angenommen wird. Mitarbeiter können durch vorsätzliches oder unbeabsichtigtes Verhalten eine Bedrohung darstellen. Der Zugriff auf Dateien und Kontaktdaten ändert sich so schnell, dass Sie manchmal den Überblick über die Benutzer verlieren, denen Sie am meisten vertrauen.

Microsoft bietet keine Möglichkeit, zwischen einem normalen Benutzer und einem Mitarbeiter zu unterscheiden, der entlassen wurde und vielleicht versucht, kritische Unternehmensdaten zu löschen. Dazu kommen unwissentlich entstehende Bedrohungen durch das Herunterladen infizierter Dateien oder das Eingeben von Benutzernamen und Passwörtern auf Websites, die Mitarbeiter für vertrauenswürdig halten. Ein weiteres schwerwiegendes Beispiel ist die Manipulation von Beweisen. Angenommen, ein Mitarbeiter löscht gezielt belastende E-Mails oder Dateien, damit die Rechts-, Compliance- oder Personalabteilung sie nicht zu sehen bekommt. Wenn Ihre Microsoft 365-Daten zuverlässig geschützt sind, sowohl extern als auch in der Cloud, kommen zusätzliche Schutzebenen hinzu, um diese internen Bedrohungen zu bekämpfen und dafür zu sorgen, dass Ihre Daten sicher und wiederherstellbar bleiben.

4. Externe Sicherheitsbedrohungen

Und dann gibt es natürlich noch externe, böswillige Bedrohungen. Malware und Viren, wie zum Beispiel Ransomware, haben Unternehmen weltweit großen Schaden zugefügt. Dies gefährdet nicht nur den Ruf der betroffenen Unternehmen, sondern auch die Sicherheit und Vertraulichkeit von internen Daten und Kundendaten.

Externe Bedrohungen schleichen sich häufig über E-Mails und Anhänge ein. Es reicht nicht immer aus, die Benutzer darüber aufzuklären, worauf sie achten müssen, insbesondere wenn infizierte Nachrichten oft sehr überzeugend erscheinen. Die eingeschränkten Funktionen von Exchange Online in den Bereichen Sicherung und Wiederherstellung bieten keinen ausreichenden Schutz vor schwerwiegenden Angriffen. Regelmäßige Backups, insbesondere solche, die extern und in der Cloud über einen Backup-Service verwaltet werden, stellen sicher, dass eine separate, nicht infizierte und schnell wiederherstellbare Kopie Ihrer Daten vorhanden ist — dies ist weit mehr, als die eingeschränkten Sicherungs- und Wiederherstellungsfunktionen von Exchange Online leisten. Außerdem wurden führende Backup-Service-Lösungen in Microsoft 365 Backup Storage integriert, sodass Unternehmen nach einem Ransomware-Angriff auch große Datenvolumina schnell wiederherstellen können.

5. Gesetzliche Bestimmungen und Compliance-Anforderungen

Manchmal müssen Sie im Rahmen von Gerichtsverfahren unerwartet E-Mails, Dateien oder andere Arten von Daten abrufen. Eine solche Situation tritt meist völlig unerwartet ein. Microsoft 365 bietet zwar einige integrierte Sicherheitsnetze (Litigation Hold und Retention), doch diese sind alles andere als eine zuverlässige Backup-Lösung und werden Ihr Unternehmen nicht vor rechtlichen Konsequenzen bewahren.

Wenn Sie beispielsweise vor der Implementierung einer gesetzlichen Aufbewahrungsfrist E-Mails oder Dokumente versehentlich löschen, können Sie diese mit einem zuverlässigen Backup-Service wiederherstellen und Ihre gesetzlichen Verpflichtungen erfüllen. Gesetzliche Anforderungen, Compliance-Anforderungen und Zugriffsbestimmungen variieren von Branche zu Branche und von Land zu Land — aber Bußgelder, Strafen und Rechtsstreitigkeiten sind drei Dinge, die auf Ihrer To-Do-Liste häufig fehlen.

Und wenn Sie einfach nicht die nötigen Kapazitäten haben, um bei Änderungen von Gesetzen, Vorschriften und Anforderungen auf dem Laufenden zu bleiben, und daher nicht wissen, wo Sie anfangen sollen, kann ein Backup-Service Sie dabei unterstützen. Dank Monitoring- und Reporting-Funktionalitäten können Sie die Compliance und die Einhaltung gesetzlicher Vorschriften sicherstellen. Und angesichts der Schnelligkeit und Unkompliziertheit, mit der Backup-Services bereitgestellt werden können, erhalten Sie innerhalb weniger Minuten ein Gefühl der Sicherheit, was die Erfüllung dieser Anforderungen betrifft.

6. Management von hybriden E-Mail-Bereitstellungen und Migration zu Microsoft 365

Unternehmen, die Microsoft 365 einführen, benötigen in der Regel ein Übergangszeitfenster zwischen lokalem Exchange und Microsoft 365 Exchange Online. Dieses Setup, bei dem ein Teil des E-Mail-Systems lokal verbleibt und der Rest zu Microsoft 365 Exchange Online verschoben wird, bietet zusätzliche Flexibilität und Kontrolle und ist in der Tat weit verbreitet. Im Gegenzug bedeutet dies jedoch auch zusätzliche Managementkomplexitäten, insbesondere im Hinblick auf Backups. Der Umgang mit mehreren Umgebungen erfordert sorgfältige Überwachung, damit Daten reibungslos fließen und geschützt sind.

Hier ist ein Backup-Service für Microsoft 365 von unschätzbarem Wert. Der richtige Backup-Service für Microsoft verarbeitet hybride E-Mail-Bereitstellungen effizient und behandelt Exchange-Daten aus lokalen Systemen und Microsoft 365 gleich. Der Quellspeicherort wird irrelevant, der Backup-Prozess wird vereinfacht, und die Notwendigkeit der Verwaltung mehrerer getrennter Systeme wird beseitigt.

7. Teams-Datenstruktur

Häufiger als je zuvor nutzen Menschen Teams, um gemeinsam an Projekten und besonderen Initiativen zu arbeiten, und dies in einem immer höheren Tempo. Nach Abschluss eines Projekts benötigen Sie jedoch eine Kopie des Projekts, um gesetzliche Aufbewahrungsvorschriften und Compliance-Vorgaben zu erfüllen. Dies ist der Punkt, an dem Unternehmen oft Probleme haben. Häufiger als Ihnen lieb sein kann werden diese Teams-Umgebungen jedoch versehentlich gelöscht, oder es werden falsche Aufbewahrungsfristen angewendet, sodass Dateien und wichtige Dokumente nicht mehr verfügbar sind.

Mit einem Backup-Service für Microsoft 365 ist dies nie der Fall. Ihre Daten sind immer da, egal, wer oder was sie löscht. Dies kann sogar in kurzfristigen Szenarien hilfreich sein. Wenn ein Mitarbeiter beispielsweise in einem Teams-Gespräch etwas Unangemessenes sagt und die entsprechende Nachricht dann löscht, sind Backups leicht zu beschaffen. Teams-Daten können mit nur wenigen Klicks stets wiederhergestellt werden, sodass sie durch die Personalabteilung überprüft werden können.

Mehr als alles andere ist wichtig, wie gut Sie Ihren Backups vertrauen können. Die Gewissheit, dass es vorhanden sind und ordnungsgemäß geschützt werden, bietet nicht nur Schutz vor dem Unbekannten, sondern auch eine Vielzahl von Möglichkeiten für die Wiederherstellung von fehlenden oder versehentlich gelöschten Teams-Daten oder -Kanälen. Mit einem Backup-Service speziell für Microsoft Teams stellen Sie sicher, dass Ihre Daten jederzeit verfügbar sind, egal wann auch immer, passiert.

Bonus-Grund: Identitäts- und Zugriffsverwaltung

Entra ID (ehemals Azure Active Directory) fungiert als Rückgrat von Microsoft 365, indem es alle Identitäts- und Zugriffsverwaltungsservices miteinander verbindet und Benutzerkonten und -gruppen den Zugriff auf die Ressourcen ermöglicht, zu deren Nutzung sie berechtigt sind. Die Bedeutung von Entra ID kann gar nicht hoch genug eingeschätzt werden. Deshalb haben Bedrohungsakteure erkannt, dass der schnellste Weg, ein Unternehmen in die Knie zu zwingen, darin besteht, auf Entra ID zu zielen, wobei die Zahl der Angriffe mittlerweile bei täglich 600 Millionen liegt.

Die Notwendigkeit, Entra ID zu schützen, geht über Cybersecurity-Bedrohungen hinaus. Die Herausforderungen, mit denen Unternehmen konfrontiert sind, spiegeln die in den vorangegangenen Abschnitten genannten wider — komplexe Compliance-Anforderungen, Papierkorbbeschränkungen, versehentliche Löschungen und inkorrekte Konfigurationen von Richtlinien. Der Schutz der Identität Ihres Unternehmens liegt letztendlich in Ihrer Verantwortung. Ein wichtiger Teil des Schutzes von Microsoft 365-Daten ist die Gewährleistung eines umfassenden Schutzes für Ihre Entra ID-Benutzer, -Gruppen, -Anwendungsregistrierungen und andere zugehörige Objekte.

Quelle: Microsoft Digital Defense Report 2024

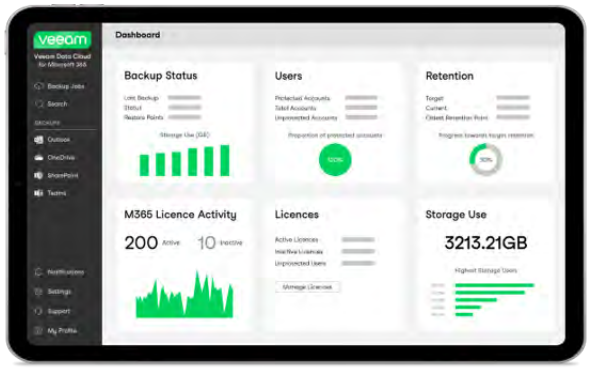
Fazit

Nehmen Sie sich einen Moment Zeit, um Ihre aktuelle Sicherheitslage zu bewerten. Möglicherweise gibt es Lücken, die Ihnen nicht bewusst waren. Mit der Bereitstellung von Microsoft 365 haben Sie bereits eine gute Entscheidung getroffen. Kombinieren Sie diese Lösung jetzt mit einem Backup-Service, der Ihnen den vollständigen Zugriff und die vollständige Kontrolle über Ihre Daten bietet. So vermeiden Sie unnötige Risiken, was Datenverluste betrifft.

Sie müssen nicht mehr die Zeit, das Geld und die Ressourcen investieren, die mit einer Softwarelösung verbunden sind. Mit **Veeam Data Cloud *for Microsoft 365*** erhalten Sie einen All-in-One-Service, der Ihnen auch unbegrenzten Speicherplatz bietet. Sie können aus drei Plänen wählen, um Ihre Ziele in den Bereichen Backup und Disaster Recovery zu erreichen. Unabhängig davon, ob Sie eine schnelle und skalierbare Sicherung und Wiederherstellung, Kontrolle und Flexibilität oder eine Kombination aus beidem benötigen — Veeam arbeitet mit Microsoft zusammen, um sicherzustellen, dass Ihre Daten stets sicher, wiederherstellbar und skalierbar sind. So können die Anforderungen Ihres Unternehmens erfüllt werden.

Stellen Sie diesen Report gern auch Ihren Kollegen zur Verfügung:
Leiten Sie den Report weiter.

Veeam Data Cloud *for Microsoft 365*:
Resiliente Datensicherung leicht gemacht



- Zuverlässige, branchenführende Backup-Technologie für Microsoft 365
- Umfassender Backup-Service mit unbegrenztem Speicherplatz
- Unterstützt von Microsoft 365 Backup Storage

→ Demo anfordern

→ Kontakt

→ **Interessieren Sie sich für den Entra ID-Schutz? Lesen Sie das Whitepaper *6 Gründe für Microsoft Entra ID Backup*.**