Sechs gute Gründe für Office 365-Backups

Warum Unternehmen ihre Office 365-Daten sichern müssen

VEEAM

Einführung

Haben Sie die Kontrolle über Ihre Office 365-Daten? Können Sie auf alle nötigen Objekte zugreifen? Reflexartig kommt dann oft die Erwiderung: „Natürlich" oder „Microsoft kümmert sich darum".

Aber Hand aufs Herz: Sind Sie sich da wirklich sicher?

Microsoft übernimmt tatsächlich in vielen Aspekten die Verantwortung und bietet seinen Kunden damit auch einen beachtlichen Service. Doch im Fokus steht dort die Verwaltung der Office 365-Infrastruktur und das Sicherstellen der vereinbarten Dienstverfügbarkeit. Worum SIE sich kümmern müssen, sind Ihre Daten. Der Irrglaube, Microsoft erstelle vollständige Backups von den Daten seiner Nutzer, ist weitverbreitet und kann geschäftsschädigende Folgen haben. Es gilt also, sich der eigenen Verantwortung in dieser Hinsicht bewusst zu werden.

Am Ende ist es an Ihnen, dafür zu sorgen, dass Sie jederzeit auf Ihre Exchange Online-, SharePoint Online-, OneDrive for Business- und Microsoft Teams-Daten zugreifen können und die Kontrolle über diese behalten.

In diesem Report erfahren Sie, was passiert, wenn Sie Ihre Office 365-Daten nicht sichern, und wie Backup-Lösungen für Microsoft Office 365 die Lücken bei der langfristigen Aufbewahrung und der Datensicherheit schließen.

„Die Backup- und Aufbewahrungsrichtlinie von Office 365 bereitete uns Sorgen, deshalb entschieden wir uns für ein Backup-System für Office 365-Daten."

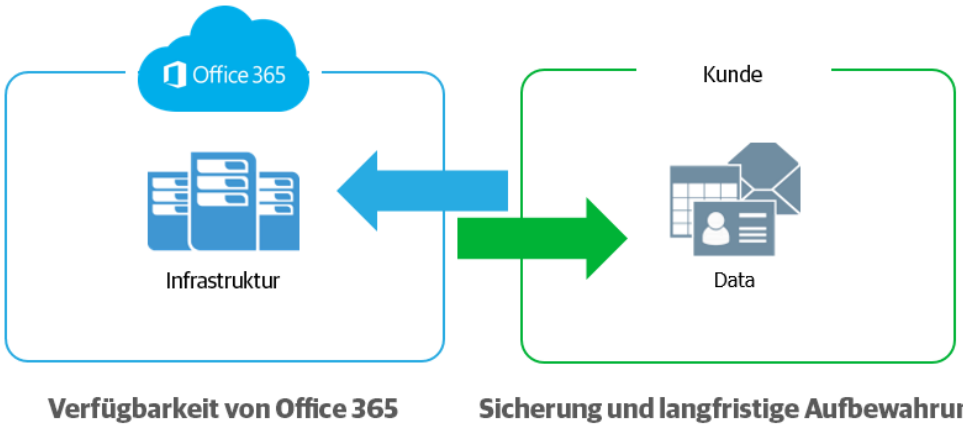
– **Karen St.Clair,** IT-Managerin,
Columbia Power & Water Systems

Das große Office 365-Missverständnis

Immer wieder wird Microsofts Verantwortung zugeschrieben, was tatsächlich in der des Nutzers liegt: die Sicherung und langfristige Aufbewahrung von Office 365-Daten. Zwischen der von Microsoft gewährleisteten Sicherung und Wiederherstellbarkeit und dem, was dies dem Nutzer tatsächlich bringt, klafft eine Lücke. Anders gesagt, sollten Sie trotz den diesbezüglichen Standardfunktionen in Office 365 gründlich prüfen, ob Sie tatsächlich das gewünschte Maß an Kontrolle über Ihre Daten besitzen und wie umfangreich Ihr Zugriff auf die Daten wirklich ist.

Microsoft Office 365 ist georedundant organisiert, und das verwechseln viele mit Backups. Zur Auffrischung: Ein Backup ist das Kopieren vorhandener Daten, wobei diese Kopie an einem anderen als dem ursprünglichen Speicherort dieser Daten hinterlegt wird. Allerdings muss der direkte Zugriff auf und die Kontrolle über solche Backups gegeben sein – nur dann können verlorene Daten schnell wiederhergestellt werden, beispielsweise nach einem Hackerangriff. Georedundanz schützt dagegen vor Standort- oder Hardwareausfällen. Nicht verfügbare Infrastrukturen werden von anderen Standorten vertreten, sodass Nutzer produktiv bleiben können – oft ohne überhaupt etwas von Verfügbarkeitsproblemen zu bemerken.

Microsoft kümmert sich um die Infrastruktur, aber für die Daten bleibt der Kunde verantwortlich



„Office 365: Es sind Ihre Daten. Ihre Verantwortung. Die Kontrolle liegt in Ihrer Hand."

– Office 365 Trust Center

Sechs Gründe, warum Office 365-Backups ein Muss sind

Die zuverlässige und hochleistungsfähige Software-as-a-Service-Plattform Microsoft Office 365 kommt der Arbeitsweise vieler Unternehmen sehr entgegen. Obwohl die von Office 365 gewährleistete Anwendungsverfügbarkeit und Betriebszeit ununterbrochene Produktivität ermöglicht, gibt es noch andere Bedrohungen als Hardwareausfälle. Deshalb sollten Sie über Office 365-Backups nachdenken.

Wahrscheinlich denken Sie oder Ihre Vorgesetzten, dass der Papierkorb schon ausreichen wird. Hier liegen Sie aber, wie viele andere übrigens auch, falsch. Durchschnittlich dauert es von der Datenmanipulation bis zu deren Entdeckung 140 Tage[1]. Das ist viel zu lange. Mit großer Sicherheit werden Sie erst dann bemerken, dass etwas fehlt, wenn der Papierkorb längst geleert ist.

Im Gespräch mit Hunderten IT-Profis aus der ganzen Welt, die auf Office 365 umgestellt haben, kristallisierten sich in Bezug auf die Datensicherung sechs Schwachstellen heraus:

Versehentliche Löschung

Lückenhafte Aufbewahrungs-richtlinie und Verwirrung

Interne Sicherheits-risiken

Externe Sicherheits-risiken

Rechtliche Bestimmungen und Compliance-Anforderungen

Verwaltung von Hybrid-E-Mail-Bereitstellungen und -Migrationen in Office 365

[1] https://discover.office.com/6-steps-to-holistic-security/chapter1/

Nummer 1: Versehentliche Löschung

Wenn Sie einen Nutzer löschen, ob absichtlich oder aus Versehen, wird diese Änderung auf das gesamte Netzwerk angewendet. Auch die private SharePoint-Website des Nutzers und seine OneDrive-Daten werden gelöscht.

Die Papierkorbfunktion und der Versionsverlauf in Office 365 schützen nur bedingt vor Datenverlust, denn sobald die Daten endgültig aus allen Office 365-Speicherregionen gelöscht sind oder der Aufbewahrungszeitraum vorüber ist, stehen Sie trotz ordnungsgemäßem, wiederherstellungsfähigem Backup vor einem großen Problem.

Beachten Sie, dass Office 365 zwei Arten der Löschung kennt: die vorläufige und die unwiderrufliche. Unter das vorläufige Löschen fällt beispielsweise das Leeren des Ordners „Gelöschte Elemente". Das Ergebnis dieses Vorgangs wird auch als „endgültig gelöscht" bezeichnet. Allerdings ist das Wort „endgültig" etwas irreführend gewählt, da sich das gelöschte Element immer noch im Postfach „Wiederherstellbare Elemente" befindet.

Nummer 2: Lückenhafte Aufbewahrungsrichtlinie und Verwirrung

Dem gegenüber steht das unwiderrufliche Löschen eines Elements aus der Postfachdatenbank. Ein solcherart gekennzeichnetes Element lässt sich tatsächlich nicht mehr wiederherstellen.

Die Digitalisierung beschleunigt das Geschäftsleben und die Weiterentwicklung diesbezüglicher Richtlinien, darunter Aufbewahrungsrichtlinien, mit denen IT-Teams kaum Schritt halten können – ganz zu schweigen davon, sie souverän anzuwenden. Ähnlich wie beim vorläufigen und unwiderruflichen Löschen bietet Office 365 nur beschränkte Backup- und Aufbewahrungsrichtlinien. Sie sollen einen momentanen Datenverlust abfedern, jedoch keine umfassende Backup-Lösung darstellen.

Für seine Postfachobjekte bietet Microsoft keine Wiederherstellung auf einen bestimmten Zeitpunkt an. Im Katastrophenfall ist also eine Backup-Lösung erforderlich, um die Daten auf einen spezifischen Stand kurz vorher zurückzusetzen und einen größeren Schlamassel zu verhindern.

Nummer 3: Interne Sicherheitsrisiken

Eine Backup-Lösung für Office 365 schließt etwaige Lücken in der Aufbewahrungsrichtlinie und sorgt für Flexibilität bei der Wiederherstellung. Für den schnellen, einfachen und bequemen Datenzugriff in problematischen Situationen stehen dann kurzfristige Backups und Langzeitarchive sowie eine granulare bzw. zeitpunktspezifische Wiederherstellung zur Auswahl.

Beim Wort „Sicherheitsbedrohung" denken die meisten an Hacker und Computerviren. Allerdings sind Unternehmen auch Gefahren aus den eigenen Reihen ausgesetzt, und zwar öfter, als vielen bewusst ist. Das Risiko sind die eigenen Mitarbeiter, die in böswilliger Absicht oder einfach unvorsichtig handeln.

Der Zugriff auf Dateien und Kontaktdaten geht durch viele Hände, da fehlt manchmal der Überblick, wer wozu berechtigt ist. Werden wichtige Daten gelöscht, kann Microsoft nicht wissen, ob dies durch einen regulären Nutzer geschieht oder jemanden, der die Kündigung erhalten hat und vor seinem Ausscheiden noch Ärger machen will.

Nummer 4: Externe Sicherheitsrisiken

Hinzu kommen die unbeabsichtigt eingeschleppten Bedrohungen durch das Herunterladen präparierter Dateien oder das Eingeben von Benutzernamen und Passwörtern auf seriös anmutenden Phishing-Websites.

Ein weiteres Problem ist die Beweismanipulation. Angenommen, ein Mitarbeiter löscht gezielt belastende E-Mails oder Dateien, damit die Rechts-, Compliance- oder Personalabteilung sie nicht zu fassen bekommt.

Schadsoftware und Viren wie Ransomware haben weltweit schon so einige Unternehmen schwer geschädigt. Nicht nur der Ruf der betroffenen Organisation ist dann in Gefahr, sondern auch Interna und Kundendaten.

Externe Bedrohungen werden vorranging über E-Mails und deren Anhänge eingeschleust, und das mitunter trotz sorgfältiger Schulung der Mitarbeiter. Die Methoden werden immer raffinierter, und die präparierten Nachrichten wirken oft täuschend echt. Die begrenzten Backup- und Wiederherstellungsfunktionen von Exchange Online reichen nicht aus, um gezielte

Nummer 5: Rechtliche Bestimmungen und Compliance-Anforderungen

Angriffe abzufedern. Durch regelmäßige Backups und deren Aufbewahrung an einem separaten Speicherort ist schon viel getan, die Datenintegrität zu wahren und eine schnelle Wiederherstellung zu unterstützen.

Im Rahmen von Rechtsprozessen kann es mitunter nötig sein, bestimmte E-Mails, Dateien und andere Arten von Daten zu präsentieren. Niemand rechnet ernsthaft damit, selbst in diese Situation zu kommen, doch wie heißt es? Sag' niemals nie … Für genau diesen Fall bietet Microsoft die „Aufbewahrung für juristische Zwecke", allerdings handelt es sich dabei nur um ein kleines Sicherheitsnetz, keine solide Backup-Lösung, auf die Sie sich im juristischen Ernstfall blind verlassen können. Wenn Sie zum Beispiel versehentlich einen Nutzer löschen, wird auch dessen Postfach, private SharePoint-Website und OneDrive-Konto aus der Aufbewahrung gelöscht.

Rechts-, Konformitäts- und Zugriffsvorschriften unterscheiden sich je nach Branche und Land, und bei Nichteinhaltung drohen Bußgelder, Vertragsstrafen und juristische Auseinandersetzungen. So etwas möchte wohl jeder vermeiden.

Nummer 6: Verwaltung von Hybrid-E-Mail-Bereitstellungen und -Migrationen in Office 365

Unternehmen und Organisationen, die von einem lokalen Exchange-System auf Office 365 Exchange Online umsteigen, benötigen dafür in der Regel einen gewissen Übergangszeitraum. Einige behalten sogar einen kleinen Teil des bisherigen Systems, weil sie sich davon noch mehr Flexibilität und Kontrolle versprechen. Solche hybriden E-Mail-Deployments sind häufig anzutreffen, stellen jedoch zusätzliche Anforderungen an die Verwaltung.

Die richtige Backup-Lösung für Office 365 sollte hybriden E-Mail-Deployments gegenüber offen sein und auch Exchange-Daten so behandeln, sodass die Datenquelle als Faktor irrelevant wird.

Des Weiteren sollte sie Ihnen die Datenspeicherung an jedem beliebigen Ort ermöglichen: vor Ort, in cloudbasiertem Objektspeicher (z. B. AWS S3 oder Azure Blob) oder bei einem Managed Serviceprovider.

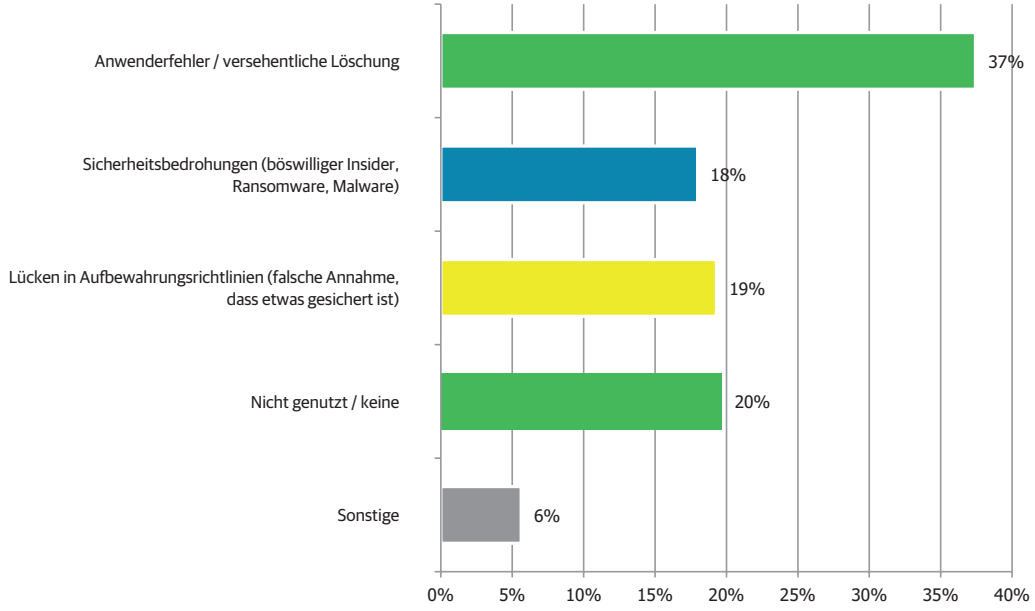
Wie oft treten diese Gründe auf?

Ihnen dürfte nun hinreichend klar sein, weshalb Office 365-Backups ein Muss sind. Und sicher fragen Sie sich, wie häufig die sechs Arten von Vorfällen in der Praxis tatsächlich sind. Die Antwort lautet leider: viel zu häufig.

Mehr als 1.000 IT-Profis wurden gefragt, welche Art des Datenverlusts sie in der Cloud bereits erlebt haben. Am häufigsten wurden Anwenderfehler / versehentliche Löschung, Sicherheitsbedrohungen und Aufbewahrungslücken genannt. Sie machen 18 bis 37 % der Fälle aus[2].

Fatalerweise sind geschätzt 76 % der in Office-Dokumenten enthaltenen sensiblen Clouddaten nicht durch Backups abgesichert[2]. IDC geht sogar davon aus, dass sechs von zehn Unternehmen ihre Office 365-Daten immer noch nicht absichern[3]. Arbeiten Sie in einem solchen Unternehmen? Wenn ja, dann gibt Ihnen dieser Report hoffentlich genügend Argumente an die Hand, um die Verantwortlichen von einer Office 365-Backup-Lösung zu überzeugen.

FRAGE 14: Welche Arten von Datenverlust haben Sie bereits in der Cloud erlebt? (Alle zutreffenden Antworten auswählen)



Teilnehmer = 1.579

[2]Veeam-Kundenumfrage, September 2019
[3]IDC: „Why a Backup Strategy for Microsoft Office 365 is Essential", 2019

Fazit

Wenn Sie genau hinschauen, werden Sie wahrscheinlich Sicherheitslücken entdecken, die Ihnen bisher nicht aufgefallen sind.

Mit der Entscheidung für Office 365 haben Sie bereits unternehmerisches Denken bewiesen. Jetzt ist es Zeit für eine Backup-Lösung, die Ihnen sowohl vollen Zugriff auf Ihre Office 365-Daten als auch die volle Kontrolle darüber verschafft, damit Sie so weit wie möglich gegen Datenverlust abgesichert sind.

Wenn Ihnen dieser Report eine Hilfe war, können Sie ihn sehr gern Kollegen zusenden: Report weiterleiten

Mehr über Office 365-Backups erfahren Sie hier:
https://go.veeam.com/wp-why-backup-office-365-data-de

VEEAM

Cloud-Daten

Mit Backups rundum geschützt

Mehr erfahren: veeam.com/de