Sechs wichtige Gründe für die Sicherung von Office 365

Warum Unternehmen ihre
Office 365-Daten sichern sollten

VEEAM

Einführung

Haben Sie Ihre Office 365-Daten unter Kontrolle? Haben Sie uneingeschränkten Zugriff auf alle benötigten Elemente? Diese Fragen werden meist reflexartig mit „Natürlich!“ oder „Darum kümmert sich ja Microsoft“ beantwortet.

Doch sind Sie wirklich sicher?

Microsoft stellt Kunden eine Vielzahl von Funktionen und Services zur Verfügung. Der Schwerpunkt liegt dabei jedoch auf dem Management der Office 365-Infrastruktur und deren Verfügbarkeit für Ihre Anwender. Die Verantwortung für Ihre Daten liegt hingegen bei Ihnen. Viele Unternehmen gehen davon aus, dass ihre Daten mit Microsoft vollständig gesichert sind. Dieser Irrglaube kann verheerende Folgen haben, wenn sie deshalb den Schutz ihrer Daten vernachlässigen.

Letztlich müssen Sie selbst sicherstellen, dass Sie Zugriff auf und die Kontrolle über Ihre Daten in Exchange Online, SharePoint Online und OneDrive for Business haben.

Dieses Whitepaper beschreibt die Gefahren, denen Sie sich aussetzen, wenn Sie Ihre Office 365-Umgebung nicht sichern. Sie erfahren außerdem, warum Backup-Lösungen für Microsoft Office 365 auch die langfristige Sicherung und Aufbewahrung ermöglichen und somit eine Lücke füllen.

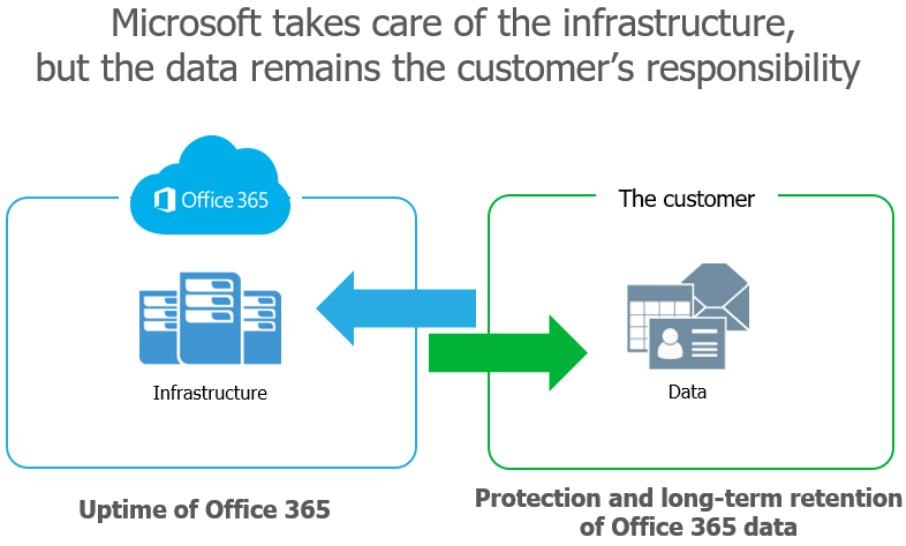
„Die Sicherungs- und Aufbewahrungsrichtlinien in Office 365 wurden unseren Anforderungen nicht gerecht. Microsoft kümmert sich um unsere Daten, doch auch der Schutz historischer E-Mail-Daten ist für uns wichtig. Deshalb haben wir uns für eine Lösung entschieden, mit der wir unsere Daten in Office 365 zuverlässig sichern können.“

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

Der große Irrglaube im Hinblick auf Office 365

Viele Unternehmen gehen davon aus, dass die Verantwortung für ihre Office 365-Daten bei Microsoft liegt, und verkennen deshalb, dass sie sich selbst um die Sicherung und langfristige Aufbewahrung ihrer Daten kümmern müssen. Die Backup- und Wiederherstellungsfunktionen, die Microsoft bereitstellt, entsprechen häufig nicht dem, was die Anwender erwarten. Sie müssen also unter Umständen genau prüfen, wie viel Kontrolle Sie neben den standardmäßigen Sicherheitsvorkehrungen von Office 365 über Ihre Daten haben und wie gut Sie tatsächlich darauf zugreifen können.

Microsoft Office 365 ermöglicht die georedundante Speicherung an zwei unterschiedlichen Standorten in einer Region, was von vielen Anwendern mit einem Backup verwechselt wird. Bei einem Backup wird eine historische Kopie von Daten erstellt und an einem anderen Ort gespeichert. Noch wichtiger ist jedoch, dass Sie direkten Zugriff auf und direkte Kontrolle über dieses Backup haben. Nur so können die Daten schnell wiederhergestellt werden, wenn sie verloren gehen, versehentlich gelöscht werden oder böswilligen



Angriffen zum Opfer fallen. Die georedundante Speicherung hingegen schützt Ihre Daten bei einem Standort- oder Hardwareausfall. Sollte also Ihre Infrastruktur oder ein System ausfallen, können Ihre Anwender weiterarbeiten und merken oft gar nichts von diesen Problemen.

„Mit Office 365 gehören Ihre Daten Ihnen! Sie sind der Besitzer. Sie haben die Kontrolle."

– Das Office 365 Trust Center

Sechs Gründe, warum die Sicherung von Office 365 so wichtig ist

Microsoft Office 365 ist eine zuverlässige und leistungsstarke SaaS-Plattform (Software-as-a-Service), die den Anforderungen zahlreicher Unternehmen voll und ganz gerecht wird. Mit Office 365 können Sie sich auf die Verfügbarkeit Ihrer Anwendungen verlassen, sodass Ihre Nutzer ohne Unterbrechungen produktiv sein können. Mit einem Office 365-Backup sind Sie jedoch auch gegen andere Sicherheitsbedrohungen gewappnet.

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 im Übrigen viele Nutzer. Bis eine Datenschutzverletzung entdeckt wird, vergehen durchschnittlich 140 Tage.[1] Dieser Zeitraum ist alarmierend lang. Es ist sehr wahrscheinlich, dass Sie den Verlust von Daten erst dann bemerken, wenn es zu spät für eine Wiederherstellung aus dem Papierkorb ist.

Wir haben uns mit vielen Hundert IT-Professionals auf der ganzen Welt unterhalten, die bereits auf Office 365 umgestellt haben, und dabei sechs Schwachstellen im Hinblick auf die Datensicherung identifiziert:

Versehentliche Löschung

Lückenhafte und unpräzise Aufbewahrungsrichtlinien

Interne Sicherheitsbedrohungen

Externe Sicherheitsbedrohungen

Gesetzesvorschriften und Compliance-Anforderungen

Management von hybriden E-Mail-Anwendungen und Migration auf Office 365

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

Schwachstelle 1: Versehentliche Löschung

Wenn Sie einen Benutzer löschen (möglicherweise versehentlich), gilt diese Löschung im gesamten Netzwerk. Auch seine persönliche SharePoint-Website und seine OneDrive-Daten werden gelöscht.

Die nativen Papierkörbe und Versionshistorien in Office 365 bieten nur eingeschränkten Schutz vor Datenverlust. So kann aus einer einfachen Wiederherstellung aus einem ordnungsgemäßen Backup ein großes Problem werden, wenn Office 365 die Daten unwiderruflich an allen Standorten gelöscht hat oder der Aufbewahrungszeitraum überschritten wurde.

Die Office 365-Plattform kennt zwei Arten von Löschvorgängen: das vorläufige Löschen und das endgültige Löschen. Ein Beispiel für das vorläufige Löschen ist das Leeren des Ordners „Gelöschte Elemente“, mit dem die Elemente dauerhaft gelöscht werden. In diesem Fall jedoch nicht wirklich dauerhaft, da sie sich weiterhin im Postfach „Wiederherstellbare Elemente“ befinden.

Schwachstelle 2 Lückenhafte und unpräzise Aufbewahrungsrichtlinien

Beim endgültigen Löschen wird ein Element so gekennzeichnet, dass es vollständig aus der Postfachdatenbank entfernt wird. Eine Wiederherstellung ist dann nicht mehr möglich.

Im schnelllebigen digitalen Zeitalter werden Richtlinien regelmäßig geändert. Es ist alles andere als einfach, den Überblick über immer wieder neue Aufbewahrungsrichtlinien zu behalten, ganz zu schweigen davon, diese zu verwalten. Wie beim vorläufigen und endgültigen Löschen bietet Office 365 nur eingeschränkte Sicherungs- und Aufbewahrungsrichtlinien, mit denen sich Datenverlust nur in bestimmten Situationen vermeiden lässt. Diese Richtlinien eignen sich nicht für den Einsatz als umfassende Backup-Lösung.

Auch die Wiederherstellung von Postfachelementen auf einen bestimmten Zeitpunkt wird von Microsoft nicht unterstützt. Bei einem katastrophalen Ausfall bietet eine Backup-Lösung die Möglichkeit, ein Rollback auf einen früheren Zeitpunkt durchzuführen und so den Geschäftsbetrieb aufrechtzuerhalten.

Schwachstelle 3 Interne Sicherheits-bedrohungen

Mit einer Backup-Lösung für Office 365 sind Sie vor lückenhaften Aufbewahrungsrichtlinien und mangelnder Flexibilität bei der Wiederherstellung gefeit. Ganz gleich, ob Sie Daten kurzzeitig sichern oder langfristig archivieren, eine granulare Wiederherstellung oder die Wiederherstellung auf einen bestimmten Zeitpunkt durchführen möchten – eine solche Lösung enthält alle benötigten Features für eine schnelle, einfache und zuverlässige Wiederherstellung.

Mit dem Begriff „Sicherheitsbedrohung" werden meist Hacker-Angriffe und Viren assoziiert. Dabei sind Unternehmen auch Gefahren von innen ausgesetzt — und das häufiger, als man denkt. Mitarbeiter können durch vorsätzliches oder unbeabsichtigtes Verhalten eine Bedrohung darstellen.

Schwachstelle 4 Externe Sicherheits-bedrohungen

Der Zugriff auf Dateien und Kontakte ändert sich so schnell, dass es schwierig ist, die Personen im Blick zu behalten, denen Sie das größte Vertrauen entgegenbringen. Microsoft bietet keine Möglichkeit, zwischen einem normalen Anwender und einem Mitarbeiter zu unterscheiden, der entlassen wurde und aus Frust versucht, wichtige Unternehmensdaten zu löschen. Manche Anwender gefährden zudem das Unternehmen, ohne es zu wissen, indem sie infizierte Dateien herunterladen oder versehentlich Benutzernamen und Kennwörter auf vermeintlich vertrauenswürdigen Websites eingeben.

Ein weiteres Beispiel ist das Manipulieren von Beweisen, etwa wenn ein Mitarbeiter gezielt belastende E-Mails oder Dateien löscht, damit diese nicht von der Rechts-, Compliance- oder Personalabteilung gegen ihn verwendet werden können.

Schwachstelle 5 Gesetzesvorschriften und Compliance-Anforderungen

Malware und Viren, so zum Beispiel Ransomware, haben Unternehmen weltweit großen Schaden zugefügt. Sie gefährden nicht nur das Ansehen eines Unternehmens, sondern auch den Schutz und die Sicherheit von internen Daten und Kundendaten.

Diese externen Bedrohungen werden durch E-Mails und Anhänge in Unternehmen eingeschleust. Nicht immer reicht es aus, die Anwender für die Gefahren zu sensibilisieren – insbesondere dann, wenn infizierte Nachrichten täuschend echt wirken.

Schwachstelle 6 Management von hybriden E-Mail-Anwendungen und Migration auf Office 365

Die eingeschränkten Sicherungs- und Wiederherstellungsfunktionen von Exchange Online bieten keinen ausreichenden Schutz vor schwerwiegenden Angriffen. Durch regelmäßige Backups können Sie sicherstellen, dass eine separate, nicht infizierte Kopie Ihrer Daten zur Verfügung steht, die eine schnelle Wiederherstellung ermöglicht.

Im Zuge von Rechtsverfahren müssen mitunter E-Mails, Dateien oder andere Datentypen abgerufen werden. Diese Situation tritt meist völlig unerwartet ein. Microsoft hat Office 365 mit einigen Sicherheitsnetzen versehen (ein Beispiel ist das Beweissicherungsverfahren), doch auch diese stellen keine solide Backup-Lösung dar, mit der Ihr Unternehmen in einem Gerichtsverfahren alle erforderlichen Nachweise erbringen kann. Wenn Sie beispielsweise versehentlich einen Benutzer gelöscht haben, werden auch das archivierte Postfach, die persönliche SharePoint-Website und das OneDrive-Konto dieses Benutzers gelöscht.

Die Gesetzesvorschriften, Compliance-Anforderungen und Zugriffsregelungen sind von Branche zu Branche und von Land zu Land unterschiedlich. Bußgelder, Strafen und Rechtsstreitigkeiten gilt es jedoch in jedem Fall zu vermeiden.

Für die Umstellung von einem lokalen Exchange-System auf Office 365 Exchange Online benötigen Unternehmen Zeit. Manche behalten sogar einen Teil ihrer bisherigen Systeme, um von zusätzlicher Flexibilität und Kontrolle zu profitieren. Solche hybriden E-Mail-Umgebungen sind relativ weit verbreitet, bringen jedoch zusätzliche Herausforderungen im Hinblick auf das Management mit sich.

Mit der richtigen Backup-Lösung für Office 365 sind Sie in dieser Hinsicht gut aufgestellt, indem Sie Exchange-Daten sowohl in lokalen als auch in cloudbasierten Systemen sichern.

Zusammenfassung

Machen Sie den ersten Schritt und überprüfen Sie Ihre Umgebung auf Sicherheitslücken, die Ihnen bislang vielleicht noch gar nicht bewusst waren.

Durch die Implementierung von Microsoft Office 365 profitiert Ihr Business bereits von zahlreichen Vorteilen. Mit der richtigen Backup-Lösung haben Sie zusätzlich uneingeschränkten Zugriff auf Ihre Office 365-Daten sowie vollständige Kontrolle und können das Risiko von Datenverlust vermeiden.

Erfahren Sie mehr über die Sicherung von Office 365:
https://www.veeam.com/de/backup-microsoft-office-365.html


VEEAM