VEEAM

7 wichtige Gründe für die Sicherung von Microsoft 365

Warum Unternehmen ihre Microsoft 365-Daten sichern müssen

Einleitung

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

Doch sind Sie sich da wirklich sicher?

Microsoft stellt Kunden eine Vielzahl von Funktionen und Services zur Verfügung. Der Schwerpunkt liegt dabei jedoch auf dem Management der Microsoft 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 Kontrolle über Ihre Daten in Exchange Online, SharePoint Online, OneDrive for Business und Microsoft Teams haben.

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

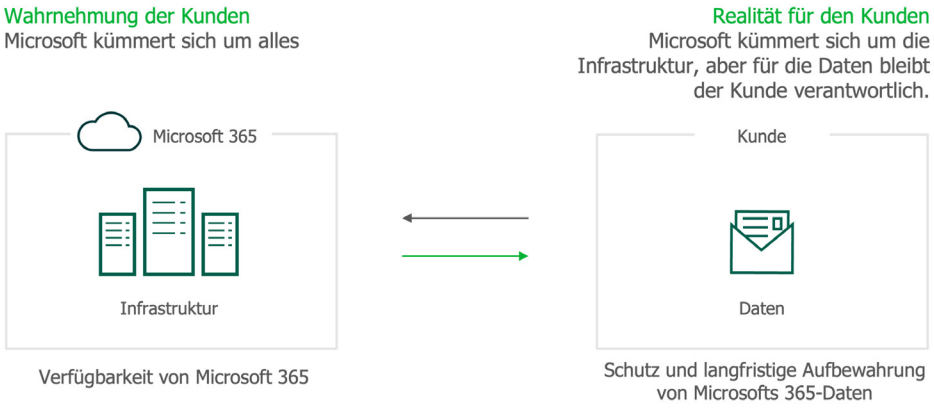
> „Als unsere Mitarbeiter während der Pandemie im Homeoffice arbeiteten, ist das Volumen der Microsoft 365-Daten deutlich angestiegen, vor allem in Teams. Wir hatten die beruhigende Gewissheit, dass wir diese Daten schnell wiederherstellen können.“
>
> **— Aleh Sadaunichy,**
> Infrastructure Solutions Architect,
> Staples Solutions

Der große Irrglaube

Viele Unternehmen gehen davon aus, dass die Verantwortung für ihre Microsoft 365-Daten bei Microsoft liegt, und verkennen deshalb, dass sie sich selbst um die Sicherung und langfristige Aufbewahrung kümmern müssen. Häufig überschätzen Anwender, in welchem Umfang Microsoft Backup- und Wiederherstellungsfunktionen bereitstellt. Sie sollten deshalb genau prüfen, wie viel Kontrolle Sie tatsächlich über Ihre Daten haben und wie gut Sie darauf zugreifen können. Die standardmäßigen Sicherheitsvorkehrungen von Microsoft 365 reichen in aller Regel nicht aus.

Dass Microsoft 365 die georedundante Speicherung an zwei unterschiedlichen Standorten ermöglicht, wird oft mit einem Backup verwechselt. 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 nur bei einem Standort- oder Hardwareausfall. Sollte also einmaldie Infrastruktur ausfallen, merken Ihre Anwender oft gar nichts davon und können ohne Unterbrechung weiterarbeiten.

Microsoft kümmert sich um die Infrastruktur, doch für ihre Daten sind Kunden selbst verantwortlich.



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

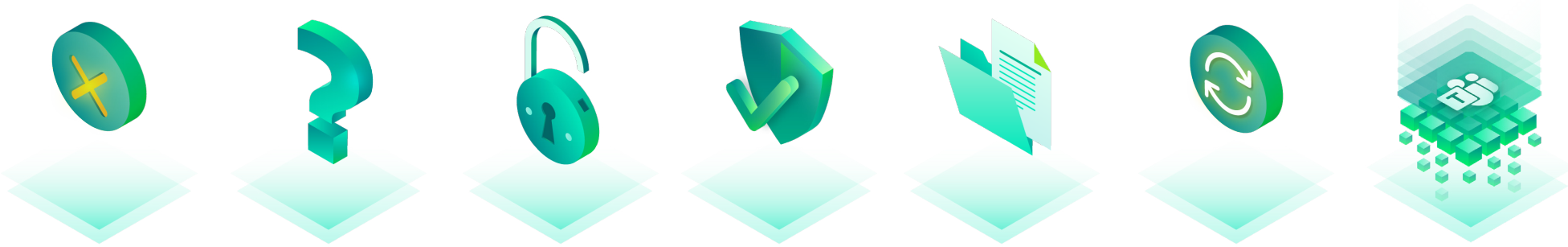
Quelle: https://learn.microsoft.com/de-de/azure/security/fundamentals/shared-responsibility

Warum die Sicherung von Microsoft 365 so wichtig ist – 7 Gründe

Microsoft 365 ist eine zuverlässige und leistungsstarke SaaS-Plattform (Software-as-a-Service), die den Anforderungen zahlreicher Unternehmen voll und ganz gerecht wird. Mit Microsoft 365 können Sie sich auf die Verfügbarkeit Ihrer Anwendungen verlassen, sodass Ihre Nutzer ohne Unterbrechungen produktiv sein können. Mit einem Microsoft 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 ein Datenverlust entdeckt wird, vergehen durchschnittlich 140 Tage[1] – ein erschreckend langer Zeitraum. Mit hoher Wahrscheinlichkeit werden Sie erst dann bemerken, dass etwas fehlt, wenn die Aufbewahrungsdauer für Papierkorb-Inhalte bereits abgelaufen ist.

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



Versehentliche Löschung

Lückenhafte und unpräzise Aufbewahrung-srichtlinien

Interne Sicherheits-bedrohungen

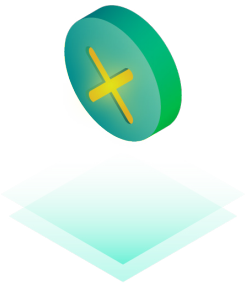
Externe Sicherheits-bedrohungen

Gesetzliche Bestimmungen und Compliance-Anforderungen

Verwaltung von hybriden E-Mail-Deployments und Umstellung auf Microsoft 365

Datenstruktur in Teams

[1] – http://info.microsoft.com/rs/157-GQE-382/images/EN-GB-CNTNT-eBook-Security-HolisticVision.pdf



Schwachstelle 1 Versehentliche Löschung

Wenn Sie einen Benutzer löschen (möglicherweise versehentlich), gilt diese Löschung im gesamten Netzwerk. Auch sein OneDrive for Business-Konto und sein Postfach werden gelöscht.

Die Papierkorbfunktion und der Versionsverlauf in Microsoft 365 schützen nur bedingt vor Datenverlust, denn sobald die Daten endgültig aus allen Microsoft 365-Speicherregionen gelöscht sind oder der Aufbewahrungszeitraum endet, ist eine einfache Wiederherstellung nicht mehr möglich.

Die Microsoft 365-Plattform kennt zwei Arten von Löschvorgängen: das vorläufige Löschen (Soft Delete) und das endgültige Löschen (Hard Delete). Ein Beispiel für das vorläufige Löschen ist das Leeren des Ordners „Gelöschte Elemente“. Zwar wird dieser Vorgang auch als „endgültig gelöscht“ bezeichnet, doch in diesem Fall bedeutet das nicht wirklich dauerhaft, da sich die Daten weiterhin im Ordner „Wiederherstellbare Elemente“ befinden.

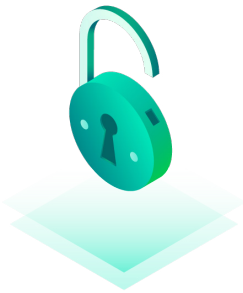
Beim tatsächlichen endgültigen Löschen, dem Hard Delete, wird ein Element so gekennzeichnet, dass es vollständig aus der Postfachdatenbank entfernt wird. Eine Wiederherstellung ist dann nicht mehr möglich.

Schwachstelle 2 Lückenhafte und unpräzise Aufbewahrungsrichtlinien

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 Microsoft 365 nureingeschränkte Sicherungs- und Aufbewahrungsrichtlinien, mit denen sich Datenverlust nur in bestimmten Situationen vermeiden lässt. Diese Richtlinien eignen sich nicht als umfassende Backup-Lösung.

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

Mit einer Backup-Lösung für Microsoft 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.



Schwachstelle 3 Interne Sicherheitsbedrohungen

Bei Sicherheitsbedrohungen denken die meisten an Hacker und Computerviren. Dabei sind Unternehmen auch Gefahren von innen ausgesetzt — und das häufiger, als man denkt. Die eigenen Mitarbeiter können durch vorsätzliches oder unbeabsichtigtes Handeln eine Bedrohung darstellen.

Dateien und Kontaktdaten gehen durch viele Hände, sodass manchmal der Überblick fehlt, wer Zugriff hatte. Microsoft bietet keine Möglichkeit, zwischen einem normalen Anwender und einem Mitarbeiter zu unterscheiden , der entlassen wurde und aus Frust versucht, wichtige Unternehmensdaten zu löschen. Hinzu kommen die unbeabsichtigt eingeschleppten Bedrohungen durch das Herunterladen infizierter Dateien oder das Eingeben von Benutzernamen und Passwörtern auf Phishing-Websites.

Ein weiteres Beispiel ist das Manipulieren von Beweismaterial. Ein Mitarbeiter könnte etwa gezielt belastende E-Mails oder Dateien löschen, damit die Rechts-, Compliance- oder Personalabteilung nicht mehr darauf zugreifen kann.

Schwachstelle 4 Externe Sicherheitsbedrohungen

Malware und Viren, so zum Beispiel Ransomware, haben Unternehmen weltweit bereits großen Schaden zugefügt. Nicht nur der Ruf des betroffenen Unternehmens steht auf dem Spiel, auch Kunden- und interne Daten sind gefährdet.

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.Die eingeschränkten Sicherungs- und Wiederherstellungsfunktionen von Exchange Online bieten keinen ausreichenden Schutz vor gezielten Angriffen. Durch regelmäßige Backups können Sie sicherstellen, dass eine separate, nicht infizierte Kopie Ihrer Daten zur Verfügung steht, aus der bei Bedarf schnell wiederhergestellt werden kann.

Schwachstelle 5
Gesetzliche Bestimmungen und Compliance-Anforderungen

Im Rahmen von Gerichtsverfahren kann es mitunter nötig sein, kurzfristig bestimmte E-Mails, Dateien und andere Arten von Daten abzurufen. Eine solche Situation tritt meist völlig unerwartet ein. Microsoft bietet dafür ein gewisses Sicherheitsnetz (Litigation Hold und Retention). Das ist jedoch keine zuverlässige Backup-Lösung, die Ihr Unternehmen im Ernstfall vor rechtlichen Konsequenzen bewahren würde. Wenn Sie beispielsweise E- Mails oder Dokumente versehentlich löschen, bevor Sie die Aufbewahrung für juristische Zwecke anwenden können, sind Sie mit einer Backup-Lösung in der Lage, diese wiederherzustellen und Ihren rechtlichen Pflichten nachzukommen.

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

Schwachstelle 6
Verwaltung von hybriden E-Mail-Deployments und Umstellung auf Microsoft 365

Für die Umstellung von einem lokalen Exchange-System auf Microsoft 365 Exchange Online benötigen Unternehmen in der Regel eine gewisse Übergangszeit. Manche behalten sogar einen Teil ihrer bisherigen Systeme bei, um von zusätzlicher Flexibilität und Kontrolle zu profitieren. Solche hybriden E-Mail-Umgebungen sind relativ weit verbreitet, bringen jedoch zusätzliche Herausforderungen für die Verwaltung mit sich.

Mit der richtigen Backup-Lösung für Microsoft 365 sind Sie in dieser Hinsicht gut aufgestellt. Sie sollte alle Exchange-Daten gleich behandeln, sodass der Ursprung irrelevant wird.

Sie haben damit außerdem die Möglichkeit, den Speicherort für Ihre Daten flexibel zu wählen – ob in der lokalen Umgebung, auf Cloud-Objektspeicher wie AWS S3 oder Azure Blob oder bei einem Managed Serviceprovider.

Schwachstelle 7 Datenstruktur in Teams

Durch die Umstellung auf das Arbeiten im Homeoffice hat sich die Zahl der Nutzer von Microsoft Teams innerhalb kürzester Zeit vervielfacht. Microsoft Teams wird nun in zahlreichen Unternehmen eingesetzt, um die Produktivität zu steigern. Die Anwendung besteht aus einer Benutzeroberfläche, in der Microsoft 365-Dienste wie SharePoint Online und OneDrive for Business zentral zusammengeführt werden. Die Teams in den Unternehmen können so in Echtzeit miteinander kommunizieren und zusammenarbeiten.

Sie müssen die Daten der einzelnen Dienste sichern, aber das ist noch nicht alles. Teams hat auch eigene Einstellungen, Konfigurationen und Mitgliederinformationen, die geschützt werden und wiederherstellbar sein müssen. Eine Backup-Lösung, die auch Microsoft Teams unterstützt, ermöglicht nicht nur den Schutz Ihrer Daten, sondern auch der Einstellungen und Verknüpfungen zwischen den Anwendungen.

Für immer mehr Projekte und Initiativen werden Teams-Umgebungen genutzt. Dabei darf nicht vergessen werden, nach Projektabschluss eine Kopie der Projektdateien zu speichern, um gesetzliche Aufbewahrungsvorschriften und Compliance-Vorgaben zu erfüllen. Sehr häufig jedoch werden diese Teams-Daten versehentlich gelöscht oder nicht den Vorschriften entsprechend aufbewahrt, sodass der Zugriff auf wichtige Dateien und Dokumente nicht mehr möglich ist.

Backups unterstützen darüber hinaus auch kurzfristige Szenarien. Wenn ein Mitarbeiter beispielsweise nach einer unangemessenen Äußerung in einer Teams-Unterhaltung die entsprechende Nachricht löscht, könnte der Chat mit einem Backup wiederhergestellt und der Personalabteilung zur Prüfung bereitgestellt werden. Externe Backup-Lösungen bieten nicht nur Schutz vor unvorhergesehenen Ereignissen, sondern auch eine Vielzahl von Möglichkeiten zur Wiederherstellung nicht auffindbarer oder versehentlich gelöschter Teams-Daten oder -Channels.

Wie häufig treten diese Situationen ein?

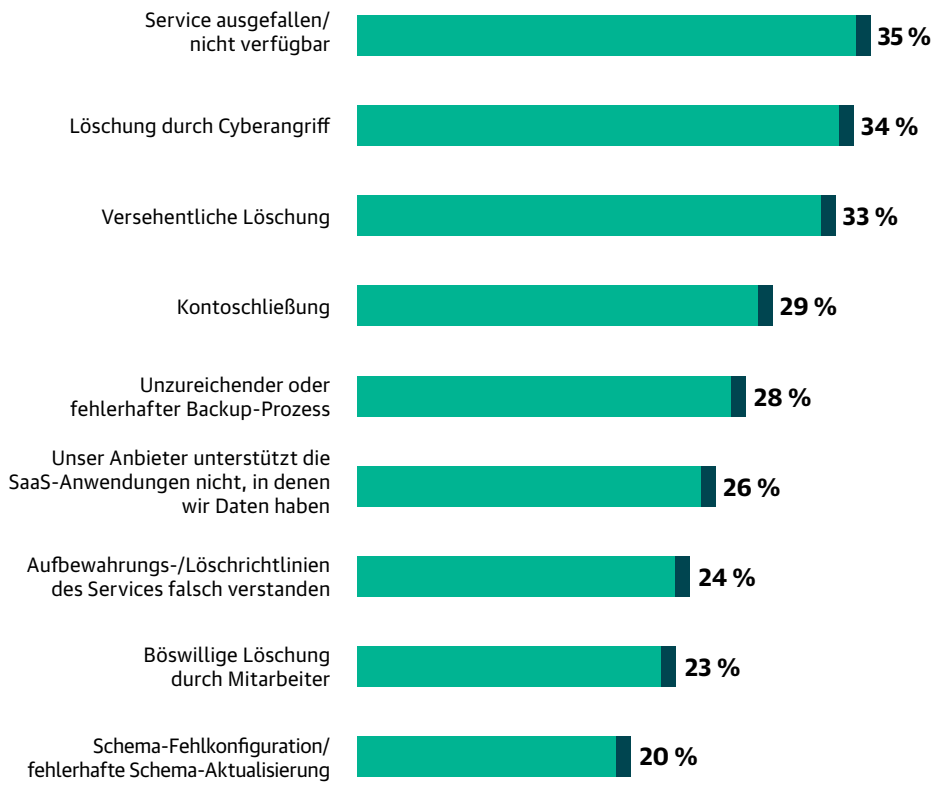
Sie wissen nun, warum die Sicherung Ihrer Microsoft 365-Daten so wichtig ist. Doch vermutlich fragen Sie sich, wie häufig diese sieben Schwachstellen tatsächlich auftreten. Die Antwort lautet leider: viel zu oft.

In einer aktuellen ESG-Umfrage gaben 53 % der IT-Professionals an, dass ihre Unternehmen schon einmal von Datenverlust oder -beschädigung in ihren SaaS-Anwendungen betroffen waren. Im Balkendiagramm rechts sehen Sie, wie oft die häufigsten Datenverlustszenarien in den befragten Unternehmen aufgetreten sind.

Die erschreckende Realität: Obwohl immer wieder Daten verloren gehen, werden 59 % der Unternehmen nicht aktiv, um ihre SaaS-Daten zu schützen. Arbeiten auch Sie in einem solchen Unternehmen? Falls ja, wissen Sie nun nach der Lektüre dieses Reports, warum der Schutz von Microsoft 365-Daten für Ihr Unternehmen unverzichtbar ist.

Quelle: ESG, SaaS Data Protection: A Work in Progress, 2022

Was sind die häufigsten Ursachen von Datenverlust oder -beschädigung bei den in Ihrem Unternehmen eingesetzten SaaS-Anwendungen? (Prozentsatz der Umfrageteilnehmer, N = 398, drei Antworten möglich)



Fazit

Wenn Sie genau hinsehen, werden Sie wahrscheinlich Sicherheitslücken entdecken, die Ihnen bisher entgangen sind.

Mit Microsoft 365 treffen Sie eine gute Wahl. Mit der richtigen Backup-Lösung haben Sie zusätzlich uneingeschränkten Zugriff auf Ihre Microsoft 365-Daten sowie vollständige Kontrolle darüber und können Datenverlust verhindern.

Falls Ihnen die Ressourcen fehlen, um Ihre Microsoft 365-Umgebung selbst zu sichern und zu verwalten, können Sie Backup-as-a-Service (BaaS) über einen Managed Serviceprovider nutzen, der kompetent und zügig eine Lösung für Sie implementiert. Wählen Sie dafür einen BaaS-Partner aus, der Ihren Backup- und Disaster-Recovery-Aufgabenstellungen gerecht werden kann.

Stellen Sie diesen Report gerne auch Ihren Kollegen zur Verfügung:
Report weiterleiten