

Kostenloser Leitfaden

Microsoft Teams: Schluss mit Datenverlusten

6 Punkte, die Sie beachten müssen,
damit Ihre Teams-Daten sicher bleiben

Inhalt

Einführung	3
Cloud-Migration: Neue Vorteile – und neue Datenschutzprobleme	3
Kostspielige, dauerhafte Datenverluste in Microsoft Teams	4
5 Gründe, warum der Schutz von Microsoft Teams-Daten unverzichtbar ist	5
I. Microsoft erwartet, dass Sie Ihre Daten sichern	5
II. Der Schutz und die Verwaltung der Daten sind hochkomplex	6
III. Die Benutzer sind das schwache Glied in der Kette	7
IV. Backups in der Microsoft-Domäne reichen nicht aus	7
V. Ein Verlust von Teams-Daten kann teuer werden	8
6 Punkte, die Sie beachten müssen, um Ihre Teams-Daten zu schützen	9

Einführung

Microsoft hat sich zum Ziel gesetzt, Teams zu einer digitalen Plattform zu machen, die für Unternehmen so wichtig ist wie der Internetbrowser und so unersetzlich wie ein Betriebssystem. Dies hat Microsoft CEO Satya Nadella bekannt gegeben und erklärt, dass Microsoft zu diesem Zweck in Teams sämtliche Tools zusammenführen will, die Mitarbeiter brauchen, um Geschäftsabläufe erfolgreich zu gestalten.

Um dieses Ziel zu erreichen, möchte Microsoft möglichst viele Nutzer möglichst schnell für Teams gewinnen und wird diesen Dienst um eine Vielzahl neuer Funktionalitäten erweitern. Die neuen Funktionen und Features werden kontinuierlich hinzugefügt. Für die Arbeitsabläufe und die Leistung der Nutzer ist das von Vorteil – für die Unternehmen allerdings bedeutet es weniger Kontrolle über die Plattform. Dies kann zu erheblichen Problemen hinsichtlich Datenschutz und Compliance führen, vor allem dann, wenn keine geeignete Datenschutzstrategie und Backup-Lösung vorhanden ist.

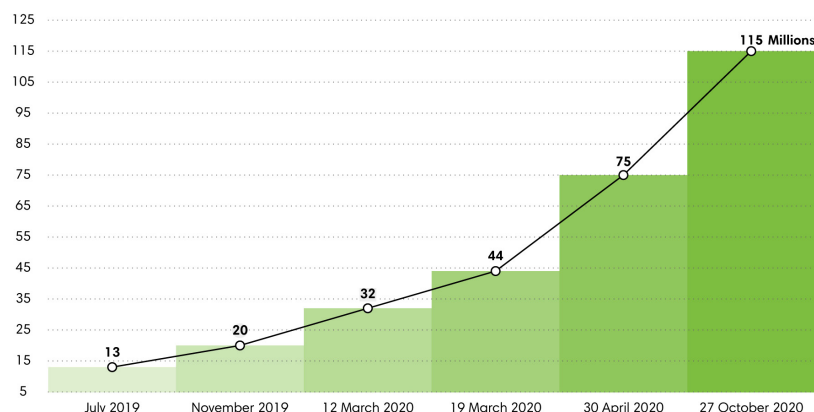
Microsoft Teams hilft Unternehmen, mit den neuen Anforderungen durch vermehrte Remote-Arbeit Schritt zu halten. Bei der Einführung müssen Unternehmen jedoch beachten, dass mit der zunehmenden Datendemokratisierung und Verlagerung von Daten in die Cloud auch die Notwendigkeit wächst, die Daten zuverlässig zu schützen.

Dieses Whitepaper zeigt die Fallstricke auf, denen sich Unternehmen aussetzen, wenn sie Microsoft Teams nutzen und sich bei der Sicherung, Archivierung und Verwaltung ihrer Daten ausschließlich auf Microsoft 365 verlassen. Sie erfahren, wie wichtig es ist, Drittanbieter-Lösungen zur Datensicherung und -verwaltung in Betracht zu ziehen, um kostspielige Datenverluste zu vermeiden und Geschäftskontinuität zu gewährleisten.

Cloud-Migration: Neue Vorteile – und neue Datenschutzprobleme

Immer mehr Unternehmen nutzen cloudbasierte Lösungen wie Microsoft 365, um zahlreichen geschäftlichen Anforderungen gerecht zu werden. So verzeichnete etwa die Chat- und Kollaborationsplattform Microsoft Teams allein im Jahr 2020 einen **sprunghaften Anstieg der Benutzerzahlen um mehr als 50 Prozent**. Angesichts neuer Anforderungen am Arbeitsplatz beschleunigen die Unternehmen ihre Digitalisierungsprozesse, um Agilität und Flexibilität auf ein neues Level zu bringen.

Zahl der weltweit täglich aktiven Benutzer (daily active users, DAU) von Microsoft Teams (in Millionen):



Ein Umstieg auf die Cloud bringt klare Vorteile, aber auch Herausforderungen, und viele Unternehmen versäumen es, eine dedizierte Datenschutzstrategie umzusetzen. Darauf zu bauen, dass der SaaS-Anbieter die Daten gegen Verlust schützt, ist keine Datenschutzstrategie. Es ist ein Spiel mit dem Feuer, das die Geschäftskontinuität gefährden kann, weil SaaS-Anbieter nicht für die Sicherung Ihrer Daten verantwortlich sind.

Kostspielige, dauerhafte Datenverluste in Microsoft Teams

Ob Malware, Ransomware oder menschliches Versagen – Ursachen für potenziell dauerhafte Datenverluste gibt es viele. Und wenn Daten verlorengehen und keine Backup-Lösung vorhanden ist, um sie zu lokalisieren und wiederherzustellen, kann das für ein Unternehmen nicht nur kostspielig, sondern potenziell fatal sein:

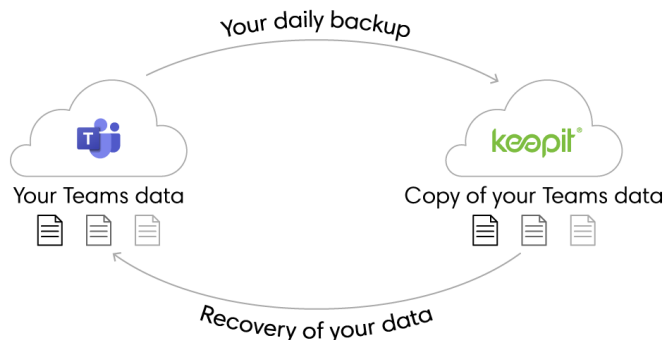
Heimtückischer Angriff

Ein Unternehmen in Carlsbad, Kalifornien, erlitt schwere Betriebsstörungen aufgrund unwiederbringlich verlorener Daten in seinem Microsoft Tenant, nachdem ein IT-Dienstleister 1.200 der 1.500 Microsoft-Benutzerkonten des Unternehmens absichtlich gelöscht hatte. Zwei Tage war das Unternehmen komplett lahmgelegt, weil die Mitarbeiter nicht mehr auf Exchange, SharePoint und Teams zugreifen und nicht mit den externen Anbietern und Kunden kommunizieren konnten. Kontaktlisten konnten nicht wiederhergestellt werden, Mitarbeiter erhielten keine Einladungen zu Besprechungen und hatten keinen Zugriff auf wichtige Ordner. Die IT-Abteilung brauchte drei Monate, um die Probleme zu beheben, die das Unternehmen 567.000 Dollar kosteten.

Menschliches Versagen

Neben böswilligen Angriffen ist auch menschliches Versagen ein erhebliches Risiko bei Kollaborationsplattformen. So könnten etwa Daten versehentlich gelöscht oder überschrieben werden. Die KPMG, eines der weltweit größten Wirtschaftsprüfungsunternehmen, erlitt einen massiven Datenverlust in Teams, als ein Mitarbeiter versehentlich 145.000 private Chatverläufe löschte, obwohl er eigentlich nur das Konto eines einzelnen Benutzers aus einer aktiven Aufbewahrungsrichtlinie hatte entfernen wollen. Das Ergebnis: eine dauerhafte Löschung von Daten ohne Wiederherstellungsmöglichkeit, die weitreichende Auswirkungen auf das Unternehmensnetzwerk hatte.

Die Quintessenz: Die beiden oben beschriebenen Datenverlustszenarien hätten sich leicht beheben lassen, wenn die betroffenen Unternehmen eine spezielle Cloud-Datenschutzlösung wie Keepit implementiert hätten, die Cloud-Daten sichert und unabhängig vom Grund des Datenverlusts eine intelligente Suche und schnelle Wiederherstellung ermöglicht.



Haben Sie kürzlich Microsoft Teams implementiert? Wir haben fünf Gründe zusammengestellt, warum eine Datenschutzstrategie für Ihre Microsoft Teams-Daten so wichtig ist. Anschließend geben wir Empfehlungen zum Schutz Ihrer Teams-Daten.

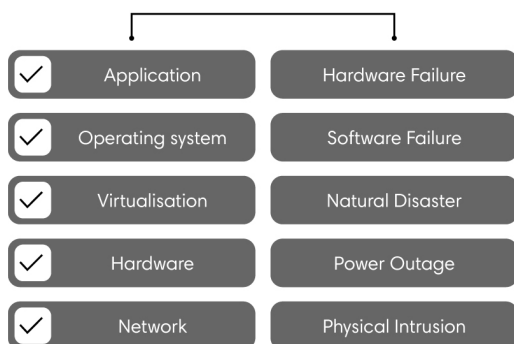
5 Gründe, warum der Schutz von Microsoft Teams-Daten unverzichtbar ist

I. Microsoft erwartet, dass Sie Ihre Daten sichern

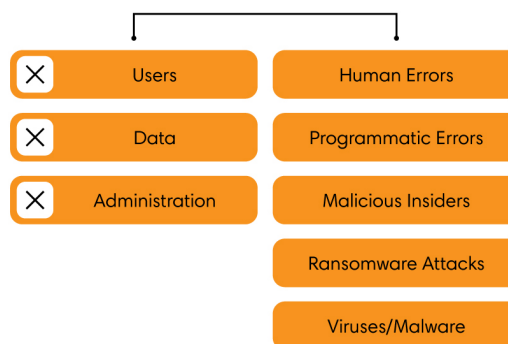
Der wichtigste Grund, warum Sie Ihre Teams-Daten sichern sollten, liegt eigentlich auf der Hand: Microsoft erwartet es von Ihnen. **Microsoft ist dafür verantwortlich, dass die Infrastruktur für den Dienst verfügbar ist**, nicht aber für die Sicherung Ihrer Daten. Unternehmen übersehen oft, dass Microsoft weder für die Sicherung von Teams-Daten zuständig ist, noch eine Wiederherstellung der Daten oder den Schutz vor Datenverlusten garantiert (siehe das nachfolgend dargestellte Modell der gemeinsamen Verantwortung).

Ausfälle und Unterbrechungen der Infrastruktur von Microsoft können die Geschäftskontinuität erheblich gefährden — vor allem dann, wenn Daten in Ihrem Microsoft 365-Konto verlorengehen oder anderweitig kompromittiert werden. Auch Backups in Azure sind betroffen, wenn Microsoft-Server ausfallen.

SaaS Provider's Responsibility:



Your Data - Your Responsibility:



II. Der Schutz und die Verwaltung der Daten sind hochkomplex

Microsoft Teams stützt sich auf eine Reihe von Microsoft 365- und Azure-Diensten, darunter SharePoint. Eine Schwierigkeit bei Teams-Backups ist die Art und Weise, wie die erzeugten Daten gespeichert sind – nämlich über zahlreiche Komponenten von Microsoft 365 verstreut (s. Unten). Um Teams-Daten zu schützen, brauchen Sie eine Backup-Lösung, die Microsoft 365 vollständig abdeckt. Noch komplexer wird die Sicherung von Teams durch die zahlreichen neuen Funktionen und Änderungen an der Microsoft-Architektur. Datenschutz und Datenverwaltung sind anspruchsvolle Aufgaben, und die umfangreichen Teams-Erweiterungen, die Microsoft plant, werden sie vermutlich nicht einfacher machen.

Teams data	Location	Backup Situation
Personal and group chat messages	Azure CosmosDB	Backed up with Keepit
Channel conversations	Azure CosmosDB	Backed up with Keepit
GIFs used in Teams messages	Teams CDN	Backed up with Keepit
Documents shared in personal and group chats	OneDrive for Business	Backed up with Keepit
Documents shared in Teams channels (Files)	Document libraries and folders in SharePoint Online sites	Backed up with Keepit via SharePoint Online.
Private channels	Separate set of SharePoint Online sites	Backed up with Keepit
Email sent to Teams channels via connector	Azure CosmosDB and SharePoint Online	Backed up with SharePoint Online (messages posted to channels are not backed up)
Messages posted to channels via Office connectors	Azure CosmosDB	No backup API available
Teams calendar	User and group mailboxes (Exchange Online)	Backed up with Exchange Online data
Teams meeting recordings	Stream	No Stream backup API available
Teams Wiki	SharePoint Online	Backed up with Keepit
Teams compliance records	Exchange Online mailboxes	Backed up with Exchange Online data
Planner	Azure	Planner backup API is available
Teams audit data	Office 365 audit log	Can be extracted with Search-UnifiedAuditLog (PowerShell)
Third-party apps	Teams app store and third-party repositories	Responsibility of third-party apps
Teams membership and group object	Azure Active Directory	Backed up with Keepit
Teams policies and settings	Azure	Some data can be backed up by reading policies and settings with PowerShell
Teams usage data	Microsoft Graph	Can be read from the Graph

III. Die Benutzer sind das schwache Glied in der Kette

Ransomware gilt seit langem als der mit Abstand größte Risikofaktor für Datenverluste. Doch Insider-Bedrohungen und menschliches Versagen sind ebenfalls bedeutende Risiken, die Unternehmen im Zeitalter der Digitalisierung und Daten-Demokratisierung von Daten einkalkulieren müssen. Microsoft hat in einem neueren Bericht festgestellt, dass **im Zeitraum von 12 Monaten mehr als 53 Prozent der Unternehmen einen Insider-Angriff gemeldet hatten** und dass Insider-Bedrohungen für die meisten Unternehmen zu einem echten Problem werden.



Doch nicht nur die zunehmenden Insider-Bedrohungen stellen ein Risiko dar, sondern auch reine Fehler und Irrtümer. Zwar sind die Mitarbeiter durch die Nutzung neuer Tools immer besser mit der Technik vertraut, doch sind sie sich der Auswirkungen ihrer Handlungen auf die Sicherheit nicht immer voll bewusst.

Microsoft Teams ermöglicht den Benutzern einfache Zugriffe, um effektive Kooperation und erhöhte Produktivität zu fördern. Dies bedeutet allerdings auch, dass es leicht zu Datenverlusten durch menschliches Versagen und Insider-Angriffe kommen kann. Teams-Benutzer haben Zugang zu geschäftskritischen Daten wie Channel-Chats, Dateien, Plänen, Kalendern und Unterhaltungen. Dieser einfache Zugriff kann jedoch auch zu Datenverlusten durch versehentliches Überschreiben und Löschen führen. Eine Wiederherstellung über Microsoft allein kann in solchen Fällen unmöglich oder zumindest zeitaufwändig und teuer sein. alone may be impossible, or, in the best-case, time-consuming and expensive.

IV. Backups in der Microsoft-Domäne reichen nicht aus

Wenn Unternehmen eine Strategie zur Datensicherung und Wiederherstellung entwickeln, sollten sie die 3-2-1-Backup-Strategie beachten. Diese besagt, dass von Daten mindestens drei Kopien existieren sollten: Zwei davon sollten auf verschiedenen Arten von Speichermedien gespeichert werden und eine an einem externen Standort.

Wenn Sie Microsoft einschließlich Teams nutzen, haben Sie bereits zwei Kopien an verschiedenen Orten, da Microsoft mehrere Kopien Ihrer Produktionsdaten an getrennten Orten speichert. Wenn jedoch Ihre Produktionsdaten bei Microsoft beschädigt werden, nicht mehr zugänglich sind oder verlorengehen, müssen Sie eine dritte Kopie außerhalb der Microsoft-Domäne haben, damit Sie die Daten schnell wiederherstellen können. Diese dritte Kopie sollte bei einem unabhängigen Cloud-Backup-Anbieter wie Keepit gespeichert werden, der eine private, herstellerneutrale Cloud mit mehreren gespiegelten Datenzentren bietet. So ist gewährleistet, dass Sie jederzeit auf alle Ihre Daten zugreifen können.

Auch die Analysten von IDC konstatieren, dass ein Backup bei einem Dienstleister außerhalb der Domäne des Datenanbieters vorgehalten werden muss, damit die Daten optimal geschützt sind.

3 
Copies of data
(1 primary and 2 backups)

2 
Copies Stored
(At separate locations)

1 
Off-site Storage
(Secure Private Cloud)

V. Ein Verlust von Teams-Daten kann teuer werden

Was Datenverluste kosten, ist über die Jahre gut dokumentiert worden. Von Wetterkatastrophen bis hin zu verheerenden Malware-Angriffen – die IT-abteilung muss ständig zwischen Budgetbeschränkungen und realen Risiken für die Geschäftskontinuität abwägen. Zum Glück sind unternehmensweite Datenverluste eher die Ausnahme. Doch wird in fast allen Unternehmen in den nächsten Monaten ein Szenario eintreten, bei dem Daten nicht verfügbar sind. Ob Datenverluste nun auf menschliches Versagen, Infrastrukturausfälle oder böswillige Angriffe zurückgehen – Unternehmen müssen davor geschützt sein:

Energie, Öl und Gas

Was, wenn Ihre teuerste Bohrinself in der Nordsee wegen eines Ausfalls der Microsoft Cloud stillsteht? Wichtige seismische Daten, die bei Microsoft gespeichert sind, sind nicht verfügbar, und die Plattform-Techniker können mit den Bohrungen nicht beginnen. Wie hoch sind die Kosten für die Bohrinself, das Team und die Tausende nicht geförderter Barrel Öl, wenn die Arbeit ruht? Es liegt in Ihrer Verantwortung, die Daten in der Public Cloud zu schützen.

Finanzdienstleistungen

Was, wenn Ihre Devisenhändler feststellen, dass ihre Modelle zu Handelsbeginn nicht verfügbar sind? Die Modelle wurden am Vorabend für den heutigen Handel erstellt und im Teams-Konto der Devisenhändler freigegeben. Wenn Teams ausfällt, wie lange wird die Wiederherstellung dauern, wenn die Daten in Ihrem alten Rechenzentrum gesichert sind? Bietet Ihr IT-Team ein SLA für Datenverfügbarkeit, sodass Ihre Händler arbeiten können, oder entgeht ihnen heute das Geschäft? Was kostet Sie ein verlorener Tag auf dem Devisenmarkt und was sind die Folgen für das IT-Team?

Pharma

Nie waren die größten Pharmaunternehmen in der Öffentlichkeit bekannter als heute. Tagtäglich wird die Welt über die Fortschritte bei der Entwicklung von Impfstoffen, über Studien und Produktionsdaten informiert. Was, wenn ein Ransomware-Angriff auf einen Microsoft Tenant inklusive Teams plötzlich die Produktionsanlage eines wichtigen Spritzenherstellers zum Stillstand bringt? Wie schnell würde der Name dieses Herstellers weltweit in die Schlagzeilen geraten, und mit welchen kurz- und langfristigen finanziellen Auswirkungen müsste er rechnen?

Datenverfügbarkeit ist kein Nice-to-have, sondern essenziell. Unternehmen weltweit implementieren cloudbasierte Daten-Backup-Dienste, um Datenverfügbarkeit rund um die Uhr zu gewährleisten. Eine Verfügbarkeit, die sicher, erschwinglich und garantiert ist.

6 Punkte, die Sie beachten müssen, um Ihre Teams-Daten zu schützen

Wenn Sie mit Microsoft Teams in die Cloud gehen, eröffnen sich vielfältige neue Möglichkeiten für Ihre Geschäftsabläufe. Doch mit neuen Möglichkeiten gehen oft auch neue Herausforderungen einher. Machen Sie sich diese Herausforderungen bewusst und stellen Sie sich die Frage, wie Sie Ihre Microsoft Teams-Daten schützen können. Um stets die Kontrolle über Ihre Teams-Daten zu behalten, sollten Sie eine echte Drittanbieter-Lösung für Datensicherung und Datenmanagement wählen.

Tools für Datensicherung und Datenmanagement weisen erhebliche Unterschiede auf. Deshalb haben wir sechs Punkte zusammengestellt, die Sie bei der Wahl einer Datenschutzlösung berücksichtigen sollten:



Zentralisieren Sie Ihren Datenschutz

Viele Unternehmen nutzen eine ganze Reihe von SaaS-Anwendungen, deren Daten abgesichert werden müssen. Wenn Sie eine zentrale Lösung zum Schutz all Ihrer SaaS-Daten einsetzen, ist das praktischer und effizienter, als für jede SaaS-Anwendung eine eigene Lösung zu verwalten und zu bezahlen.



Sicherheit und Datenverfügbarkeit Sind Essenz

Suchen Sie nach einer Backup-Lösung, die Ihre Teams-Daten außerhalb der Microsoft-Domäne sichert und gewährleistet, dass Sie jederzeit Zugriff auf eine externe Kopie der Daten haben – auch bei einem Ausfall der Microsoft-Cloud. Nur so sind Sie gegen einen Verlust Ihrer Teams-Daten geschützt, denn Microsoft sichert Ihre Daten nicht für Sie.



Einfachheit ist Trumpf

Microsoft Teams-Daten selbst zu sichern ist schwierig. Sehen Sie sich deshalb nach einem Anbieter um, der das Schwierige leicht macht. Um Ihr IT-Team zu entlasten und Personalkosten zu sparen, sollten Sie eine einfache, intelligente Lösung wählen, die sich intuitiv integrieren lässt und durchgehend läuft.



Bleiben Sie vorschrittkonform

Die meisten Unternehmen brauchen eine Lösung für Datenmanagement und Datensicherung, mit der sie spezifische Daten (und bestimmte Versionen von Daten) leicht lokalisieren, archivieren und an ihre Rechtsabteilung übermitteln können, um gegenüber Prüfern nachzuweisen, dass die Daten vorschrittkgemäß gespeichert und geschützt sind.



Denken Sie in die Zukunft

Microsoft Teams wird ständig um neue Funktionen erweitert. Um sicherzustellen, dass Ihre Datenschutzlösung Ihren heutigen und künftigen Anforderungen gerecht wird, sollten Sie sich bei der Anbieterwahl informieren, wie gut der Dienstleister Teams abdeckt und wie er die Abdeckung längerfristig weiterentwickeln und ausbauen will.



Planbarkeit zählt

Wählen Sie eine Lösung, die Cloud-Schutz für eine breite Palette von SaaS-Anwendungen ermöglicht und Ihren Datenaufbewahrungsrichtlinien gerecht wird. Zudem sollte die Lösung eine kalkulierbare Preisgestaltung bieten, damit Sie keine unangenehmen und kostspieligen Überraschungen erleben, wenn Ihr Backup-Bedarf wächst.

Sehen Sie sich jetzt die dedizierte Backup- und Recovery lösung an, die Keepit für Microsoft 365 einschließlich Teams bietet:

<https://www.keepit.com/services/backup-microsoft-office-365/microsoft-teams/>