ConversationalGeek

Infografik zur Microsoft Teams-Datensicherung

Von Brien M. Posey, Microsoft MVP

#1 Sorgen Sie dafür, dass Ihre *Microsoft Teams-Daten gesichert werden*

Auch wenn es sich eigentlich von selbst verstehen sollte, lautet der wichtigste Ratschlag: Sorgen Sie dafür, dass Ihre Microsoft Teams-Daten (und die Daten in Ihren übrigen Microsoft 365-Anwendungen) auch tatsächlich gesichert werden.

Der Einsatz von Drittanbieter-Anwendungen für die Sicherung von Microsoft 365-Daten ist von 27 % im Jahr 2020 um 18 % auf 45 % im Jahr 2021 gestiegen

Laut einer Studie von Netwrix sind Benutzerfehler mit 50 % die häufigste Ursache für Datenverlust
https://hostingtribunal.com/blog/data-loss-statistics/#gref

In 35 % der Fälle ist Datenverlust laut Netwrix auf Hardwareausfälle zurückzuführen.
https://hostingtribunal.com/blog/data-loss-statistics/#gref

#2 Nutzen Sie eine *Backup-Lösung*, die auf die Anforderungen von Teams zugeschnitten ist

Im Gegensatz zu Anwendungen wie Exchange Online oder SharePoint Online speichert Teams Daten nicht zentral, sondern verteilt diese auf verschiedene Microsoft 365-Anwendungen. Zwar sollten alle Backup-Anwendungen von Microsoft 365 in der Lage sein, auch Teams-Daten zu sichern, doch könnte sich die Wiederherstellung dieser Daten als äußerst kompliziert erweisen, wenn die Anwendung Microsoft Teams nicht ausdrücklich unterstützt.

Laut Tech Radar hatte Microsoft Stand Juli 2021 250 Millionen aktive Teams-Nutzer monatlich. Dies ist eine Steigerung von über 100 Millionen gegenüber den 145 Millionen, die Stand April des selben Jahres gemeldet wurden.
https://www.techradar.com/news/microsoft-teams-now-has-250-million-monthly-active-users

"Mehr als 500.000 Unternehmen nutzen Microsoft Teams als Standard-Plattform für Messaging."
https://www.businessofapps.com/data/microsoft-teams-statistics

#3 Nutzen Sie das *richtige Tool* für die Sicherung Ihrer Daten

Eine weitere Best Practice für die Datensicherung in Microsoft Teams ist die Wahl eines geeigneten Tools. Einige Funktionalitäten von Microsoft 365, etwa Aufbewahrungsrichtlinien und das Beweissicherungsverfahren, lassen sich als Pseudo-Backup nutzen. Diese Tools dienen jedoch zu Compliance-Zwecken und nicht zur Datensicherung. Somit gewährleisten sie auch keinen angemessenen Schutz für Microsoft Teams-Daten.

60%

Laut einer Studie von Avast sind 60 % aller Backups unvollständig. Dies ist im Wesentlichen auf die Nutzung veralteter Backup-Technologien zurückzuführen.
https://invenioit.com/continuity/disaster-recovery-statistics

37%

37 % aller KMU waren bereits von Datenverlust in der Cloud betroffen.
https://invenioit.com/continuity/disaster-recoverystatistics

#4 Setzen Sie bei der Datensicherung auf einen *hybriden Ansatz*

Unser vierter Ratschlag lautet: Setzen Sie bei der Sicherung Ihrer Daten auf einen hybriden Ansatz. Statt Microsoft 365-Daten und Daten in Ihren lokalen Microsoft Office-Anwendungen separat zu sichern, empfiehlt es sich, mit einer einzigen Anwendung beide Umgebungen gleichzeitig zu schützen.

Anstelle von lokalen Anwendungen werden für die Datensicherung immer häufiger cloudbasierte Lösungen genutzt, die von einem Serviceprovider verwaltet werden. Lag ihr Anteil 2020 noch bei 29 %, wird er Schätzungen zufolge bis 2023 auf 46 % steigen.

Die meisten Unternehmen gehen davon aus, dass sie in den kommenden zwei Jahren die Zahl ihrer physischen Server schrittweise verringern, ihre virtualisierte Infrastruktur weiter ausbauen und auf eine Cloud-First-Strategie setzen werden. Die Hälfte aller produktiven Workloads wird somit bis 2023 in der Cloud ausgeführt.

https://solutionsreview.com/backup-disasterrecovery/veeam-data-protection-report-2021-shows-58-of-backups-are-failing

#5 Berücksichtigen Sie bei der *Backup-Planung* Ihre SLA

Best Practice Nummer 5 ist, bei der Planung der Datensicherung Ihre Service Level Agreements (SLAs) zu berücksichtigen. Wichtig sind dabei vor allem angemessene RPOs und RTOs für Ihre Microsoft Teams-Umgebung. Die RPOs bestimmen, wie häufig Daten gesichert werden, und entscheiden somit über den maximal möglichen Datenverlust zwischen zwei Backups. Die RTOs geben an, wie lange die Wiederherstellung eines Backups maximal dauern sollte.

80%

In 80 % aller Unternehmen gibt es eine „Verfügbarkeitslücke" zwischen der tatsächlichen und der eigentlich angestrebten Dauer für die Wiederherstellung von Anwendungen.

76%

In 76 % dieser Unternehmen besteht zudem eine Lücke zwischen der Häufigkeit der Datensicherung und dem tolerierbaren Datenverlust.

#6 Achten Sie auf *granulare Wiederherstellungsoptionen*

Häufig wird im Hinblick auf die Microsoft Teams-Datensicherung vergessen sicherzustellen, dass die eingesetzte Backup-Lösung auch granulare Wiederherstellungsoptionen bietet. Sie müssen nicht nur in der Lage sein, ein gesamtes Team (oder auch mehrere Teams) wiederherzustellen, sondern auch einzelne Dateien oder Chats eines Teams.

44 % der SaaS-Administratoren und 47 % der Backup-Administratoren führen als primären Grund für die Sicherung von Office 365-Daten eine bessere Wiederherstellbarkeit und insbesondere granulare Wiederherstellungsmöglichkeiten an.
https://www.youtube.com/watch?v=RIHm8-0LUJs

70 % der Fortune 500-Unternehmen haben 2020 Lizenzen für Microsoft 365 erworben.
https://hostingtribunal.com/blog/microsoft-statistics/#gref

#7 Nutzen Sie Backups zur Erweiterung Ihrer *e-Discovery-Funktionen*

Microsoft 365 beinhaltet seit Langem e-Discovery-Funktionen, mit denen Unternehmen in ihrer Microsoft 365-Landschaft nach Daten suchen können, die für eine Gerichtsverhandlung benötigt werden. Zwar sind diese nativen e-Discovery-Funktionen nützlich, doch ist der Einsatz von Backup-Software zum Auffinden der benötigten Daten oft effektiver.

Laut einer Umfrage zur Veranstaltung „Disruption in eDiscovery" hatten mindestens 58 % der Teilnehmer e-Discovery-Technologie bereits mehrfach für andere Szenarien als rechtliche Ansprüche und Rechtsstreitigkeiten genutzt. Dies zeigt, dass e-Discovery nicht mehr ausschließlich im Zusammenhang mit Gerichtsverfahren zum Einsatz kommt.

$12.9 Billion

Prognosen zufolge wird der Umsatz mit e-Discovery-Lösungen bis 2025 auf 12,9 Mrd. USD steigen.

**https://ediscoverytoday.com/2020/08/31/here-are-some-disruptivests-in-discovery-ediscovery-trends*
***https://www.prnewswire.com/newsreleases/global-12-9-billion-ediscovery-market-forecast-to-2025---focus-on-proactive-governance-withdata-analytics-and-the-emergence-of-new-content-sources-301231643.html*

#8 Schützen Sie Teams-Daten vor *Ransomware*

Eine weitere Empfehlung lautet, den Schutz Ihrer Microsoft Teams-Daten vor Ransomware zu gewährleisten. In Microsoft 365 gespeicherte Daten können entgegen landläufiger Meinung von Ransomware verschlüsselt werden. Da nach wie vor sehr viele Mitarbeiter im Homeoffice sind und dort ihre privaten Geräte nutzen, steigt die Gefahr einer Ransomware-Infektion. Eine zuverlässige Datensicherung ist der beste Schutz vor Datenverlust nach einem Ransomware-Angriff.

Laut einer Untersuchung des Ponemon Institute sind nur 45 % der Unternehmen der Auffassung, dass ihr Budget für Cybersicherheit angemessen ist.

IDC zufolge sind 69 % aller Unternehmen in den vergangenen zwölf Monaten Opfer eines Malware-Angriffs geworden. In 39 % dieser Fälle handelte es sich um Ransomware-Attacken.

**https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf)*
***https://www.veeam.com/de/why-backup-office-365.html*

#9 Gewährleisten Sie die *Flexibilität* Ihrer *Storage-Systeme*

Bei der Wahl einer Backup-Anwendung für Microsoft Teams sollten Unternehmen sicherstellen, dass die Lösung Wahlfreiheit in Bezug auf das Storage-System bietet – unabhängig davon, wo es sich befindet. So können sie einen Storage-Tier wählen, der ihren Anforderungen an Performance und Stabilität bei möglichst geringen Kosten gerecht wird. Eine flexible Wahl des Storage-Systems bietet Unternehmen zudem die Möglichkeit, Backups auf Immutable Storage zu speichern und so vor Ransomware-Angriffen zu schützen.

CAN Financial zahlte 2021 ein Lösegeld in Rekordhöhe von 40 Millionen USD.

Eine Umfrage von Sophos hatte 2021 ergeben, dass 7 % aller befragten Unternehmen in den vergangenen zwölf Monaten von Ransomware-Angriffen betroffen waren.

**https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5).*
***https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-ofransomware-2021-wp.pdf?cmp=120469*

#10 Achten Sie auf *Benutzerfreundlichkeit* der Lösung

Manche Backup-Anwendungen sind für ihre komplizierte Konfiguration und Nutzung berüchtigt. Das Problem dabei ist, dass Komplexität die Fehleranfälligkeit erhöht. Mit einer intuitiven und benutzerfreundlichen Backup-Anwendung verringert sich die Wahrscheinlichkeit, dass infolge von Benutzerfehlern Backups oder Wiederherstellungen fehlschlagen.

Laut FEMA geben 40 bis 60 % aller kleinen Unternehmen ihr Geschäft nach einem Datenverlust auf
https://hostingtribunal.com/blog/data-loss-statistics/#gref

Einer Studie von 2021 zufolge lassen sich 58 % aller Backups nicht erfolgreich wiederherstellen.

58%

**https://www.continuitycentral.com/index.php/news/technology/6092-survey-finds-that-58-percent-ofdata-backups-fail-when-restoration-is-attempted*

ConversationalGeek

Im Auftrag von Veeam