ConversationalGeek

Infografica per il backup di Microsoft Teams

Di: Brien M. Posey, Microsoft MVP

#1 Assicurati di *eseguire il backup di Microsoft Teams*

Sebbene possa sembrare del tutto ovvio, la best practice più importante per i backup di Microsoft Teams è assicurarsi di eseguire effettivamente il backup di Microsoft Teams (e di tutte le altre applicazioni di Microsoft 365).

18%: aumento del backup di terze parti per Office 365, passando dal 27% nel 2020 al 45% nel 2021.
http://vee.am/DPR21report

Il 50% dei dati persi può essere attribuito a un errore umano: è il motivo numero uno secondo Netwrix Research.
https://hostingtribunal.com/blog/data-loss-statistics/#gref

Il 35% della perdita di dati può essere attribuito a un guasto hardware, secondo Netwrix Research.
https://hostingtribunal.com/blog/data-loss-statistics/#gref

#2 Adotta una *soluzione di backup* che comprenda veramente Teams

A differenza di applicazioni come Exchange Online o SharePoint Online, Teams non archivia tutti i dati in un'unica posizione. Al contrario, i dati di Microsoft Teams sono disseminati in una varietà di diverse applicazioni Microsoft 365. Sebbene qualsiasi applicazione di backup di Microsoft 365 dovrebbe essere in grado di eseguire il backup dei dati di Teams, il processo di ripristino potrebbe essere estremamente difficile a meno che l'applicazione non sia stata progettata specificamente per supportare Microsoft Teams.

Secondo Tech Radar, Microsoft ha rivelato a luglio 2021 di avere 250 milioni di utenti mensili attivi su Teams. Si tratta di un incremento di oltre 100 milioni dai 145 milioni segnalati ad Aprile dello stesso anno.
https://www.techradar.com/news/microsoft-teams-now-has-250-million-monthly-active-users

"Oltre 500.000 organizzazioni utilizzano Microsoft Teams come piattaforma di messaggistica predefinita"
https://www.businessofapps.com/data/microsoft-teams-statistics

#3 Usa lo *strumento corretto* per l'attività da svolgere

Una terza best practice per i backup di Microsoft Teams consiste nell'assicurarsi di utilizzare lo strumento corretto per l'attività da svolgere. All'interno dell'ecosistema Microsoft 365 sono presenti funzionalità, come le policy di retention e il blocco per controversia legale, che possono fungere da pseudo-backup. Tuttavia, questi strumenti esistono per scopi di conformità, non per la protezione dei dati. Pertanto, non proteggono adeguatamente i dati di Microsoft Teams.

60%
Secondo Avast, il "60% dei backup non è completo". Ciò è in gran parte dovuto all'utilizzo di tecnologie di backup obsolete da parte delle aziende
https://invenioit.com/continuity/disaster-recovery-statistics

37%
Il 37% delle PMI ha perso i dati nel cloud
https://invenioit.com/continuity/disaster-recoverystatistics

#4 Adotta un *approccio ibrido* ai backup

La quarta best practice prevede l'adozione di un approccio ibrido ai backup. Anziché eseguire il backup di Microsoft 365 separatamente dalle applicazioni Microsoft Office on-premises, è preferibile utilizzare un'unica applicazione di backup in grado di proteggere contemporaneamente entrambi gli ambienti.

Il backup sta passando da soluzioni on-premises a soluzioni basate sul cloud gestite da un provider di servizi, con una traiettoria che va dal 29% nel 2020 al 46% previsto entro il 2023.

Nei prossimi due anni, la maggior parte delle aziende prevede di ridurre gradualmente i propri server fisici, mantenere e rafforzare la propria infrastruttura virtualizzata e adottare strategie "cloud-first". Ciò significa che la metà dei carichi di lavoro in produzione sarà in hosting nel cloud entro il 2023.

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

#5 Mantieni gli SLA all'*avanguardia della pianificazione dei backup*

La quinta best practice consiste nel mantenere gli Accordi sul livello di servizio (SLA) in primo piano nella pianificazione del backup. In particolare, è necessario considerare gli obiettivi Recovery Point Objective (RPO) e Recovery Time Objective (RTO) appropriati per l'ambiente di Microsoft Teams. L'RPO definirà la frequenza con cui vengono creati i backup, determinando così la quantità massima di dati che potrebbero essere potenzialmente persi tra un backup e l'altro. L'RTO riguarda il tempo necessario per ripristinare un backup.

80%
L'80% delle organizzazioni riconosce di avere un "divario di disponibilità" tra la velocità con cui sono in grado ripristinare le applicazioni e la velocità con cui è necessario farlo.

76%
Il 76% delle stesse organizzazioni presenta un divario tra la frequenza con cui viene eseguito il backup dei dati e la quantità di dati che possono permettersi di perdere.

#6 Non trascurare la *granularità del ripristino*

Una delle best practice spesso trascurate per il backup di Microsoft Teams consiste nell'assicurarsi che la soluzione di backup in uso consenta funzionalità di ripristino granulare. Sebbene sia importante poter ripristinare un intero team (o anche più di uno), è altrettanto importante poter ripristinare un file o una chat all'interno di un team.

Il 44% degli amministratori SaaS e il 47% degli amministratori di backup cita un ripristino migliore, inclusa la granularità, come motivo principale per proteggere i dati di Office 365.
https://www.youtube.com/watch?v=RIHm8-0LUJs

Il 70% delle aziende Fortune 500 ha acquistato Office 365 nel 2020
https://hostingtribunal.com/blog/microsoft-statistics/#gref

#7 Usa il backup per aumentare le tue *capacità di eDiscovery*

Microsoft 365 include da tempo funzionalità di eDiscovery che consentono a un'organizzazione di individuare dati specifici dall'ecosistema Microsoft 365 in risposta a una citazione. Sebbene le funzionalità native di eDiscovery siano utili in alcune circostanze, è spesso più efficace utilizzare il software di backup nel processo di rilevamento.

Un sondaggio sui problemi dell'eDiscovery ha rilevato che "almeno il 58% degli utenti aveva utilizzato la tecnologia di eDiscovery per questioni che non riguardavano reclami o controversie 'almeno in diverse occasioni'", dimostrando che l'eDiscovery non è più limitata solamente alle controversie.

$12,9 miliardi
Si prevede che il mercato dell'eDiscovery crescerà fino a 12,9 miliardi di dollari entro il 2025

*https://ediscoverytoday.com/2020/08/31/here-are-some-disruptivestats-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 Difendi Teams *dal ransomware*

Un'altra best practice consiste nell'assicurarsi di proteggere dal ransomware i dati di Microsoft Teams. Contrariamente alla credenza popolare, i dati archiviati in Microsoft 365 possono essere crittografati dal ransomware. Il fatto che così tante persone lavorino ancora in remoto sui dispositivi personali aumenta notevolmente il rischio di un'infezione da ransomware. Un buon backup è la difesa migliore dalla perdita di dati correlata al ransomware.

Secondo l'istituto Ponemon, solo il 45% delle aziende ritiene di avere un budget adeguato per la sicurezza informatica

Secondo IDC, il 69% delle organizzazioni aveva subito attacchi malware andati a segno nei precedenti 12 mesi, il 39% dei quali riguardava il ransomware

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

#9 Assicurati che il tuo *Storage* offra la *flessibilità*

Quando si seleziona un'applicazione di backup per Microsoft Teams, è importante assicurarsi che la soluzione ti offra la libertà di scegliere il tuo storage, indipendentemente da dove si trova. In questo modo, le organizzazioni possono scegliere un tier di storage che offra le prestazioni e la resilienza di cui l'azienda ha bisogno al miglior costo possibile. La flessibilità dello storage offre inoltre alle organizzazioni la possibilità di scrivere i backup su storage immutabile, se lo desiderano, proteggendo così i backup dagli attacchi ransomware.

CAN Financial ha stabilito un record mondiale nel 2021 quando la società ha pagato un riscatto di 40 milioni di dollari.

Un sondaggio del 2021 di Sophos ha rilevato che "il 7% delle organizzazioni degli intervistati è stato colpito dal ransomware nell'ultimo anno"

*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 Focalizzati sulla *facilità d'uso*

Alcune applicazioni di backup hanno la reputazione di essere eccessivamente complesse da configurare e utilizzare. Il problema è che la complessità aumenta le probabilità di errore umano. Se un'organizzazione seleziona un'applicazione di backup intuitiva e facile da usare, può ridurre le probabilità che si verifichino errori di backup o ripristino a causa di un errore umano.

Secondo la FEMA, il 40-60% delle piccole imprese non riaprirà mai dopo un evento di perdita di dati
https://hostingtribunal.com/blog/data-loss-statistics/#gref

58%
Secondo uno studio del 2021, il 58% dei backup non riesce quando si tenta il ripristino

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