ConversationalGeek

Infographie sur la sauvegarde Microsoft Teams

Par Brien M. Posey, Microsoft MVP

#1 Veillez à *sauvegarder Microsoft Team*

Même si c'est une évidence, la première meilleure pratique à adopter est de bien sauvegarder Microsoft Teams (et les autres applications Microsoft 365).

Augmentation de 18% des sauvegardes tierces pour Office 365 (de 27 % en 2020 à 45 % en 2021)
http://vee.am/DPR21report

50 % des pertes de donnée sont imputables à une erreur humaine (le principal problème, selon Netwrix Research).
https://hostingtribunal.com/blog/data-loss-statistics/#gref

35 % des pertes de donnée sont imputables à une défaillance matérielle, d'après Netwrix Research
https://hostingtribunal.com/blog/data-loss-statistics/#gref

#2 Adoptez une *solution de sauvegarde* conçue pour Teams

Contrairement à Exchange Online ou SharePoint Online, par exemple, Teams ne stocke pas l'intégralité de ses données au même endroit. Les données Microsoft Teams sont en effet réparties entre plusieurs applications Microsoft 365. Bien que toute application de sauvegarde Microsoft 365 soit normalement capable de sauvegarder les données Teams, le processus de restauration risque d'être très compliqué si cette application n'est pas spécialement conçue pour prendre en charge Microsoft Teams.

Selon TechRadar, Microsoft a annoncé en juillet 2021 que le nombre d'utilisateurs actifs mensuels de Teams s'établissait à 250 millions, soit une hausse de plus de 100 millions par rapport aux 145 millions comptabilisés en avril de la même année.
https://www.techradar.com/news/microsoft-teams-now-has-250-million-monthly-active-users

"Plus de 500 000 entreprises utilisent Microsoft Teams comme plateforme de messagerie par défaut"
https://www.businessofapps.com/data/microsoft-teams-statistics

#3 Utilisez l'*outil approprié*

Troisième meilleure pratique en matière de sauvegarde Microsoft Teams : utiliser l'outil approprié. Certaines fonctionnalités de l'écosystème Microsoft 365, comme les stratégies de rétention et la conservation pour litige, peuvent faire office de pseudo-sauvegardes. Néanmoins, ces fonctionnalités existent pour des raisons de conformité, et non de protection des données. Elles ne protègent donc pas les données Microsoft Teams de manière adéquate.

60%
Selon Avast, « 60 % des sauvegardes sont incomplètes », ce qui est essentiellement dû à l'utilisation de technologies obsolètes
https://invenioit.com/continuity/disaster-recovery-statistics

37%
37 % des PME ont perdu des données dans le cloud
https://invenioit.com/continuity/disaster-recoverystatistics

#4 Adoptez une *approche hybride* des sauvegarde

Quatrième meilleure pratique : adopter une approche hybride de vos sauvegardes. Au lieu de sauvegarder Microsoft 365 séparément de vos applications Microsoft Office locales, mieux vaut faire appel à une seule application de sauvegarde capable de protéger les deux environnements à la fois.

Les solutions de sauvegarde sur site sont peu à peu abandonnées au profit de solutions cloud gérées par un fournisseur de services (29 % en 2020 contre 46 % en 2023, selon les prévisions).

La plupart des entreprises prévoient de réduire progressivement le nombre de serveurs physiques, de maintenir et consolider leur infrastructure virtualisée, mais aussi de déployer des stratégies « cloud-first ». Résultat, la moitié des workloads de production seront hébergés dans le cloud d'ici 2023.

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

#5 *Planifiez vos sauvegardes* en mettant l'accent sur les contrats de niveau de service

La cinquième meilleure pratique consiste à planifier les sauvegardes en mettant l'accent sur les contrats de niveau de service (SLA). Plus spécifiquement, vous devez tenir compte du délai optimal de reprise d'activité (RPO) et des objectifs de temps de restauration (RTO) de votre environnement Microsoft Teams. Le RPO détermine la fréquence à laquelle les sauvegardes sont créées, et donc le volume maximal de données qui risque d'être perdues entre les sauvegardes. Le RTO correspond au temps nécessaire pour restaurer une sauvegarde.

80%
80 % des entreprises reconnaissent qu'il existe un « écart de disponibilité » entre le délai de restauration réel des applications et le délai attendu.

76%
Dans 76 % de ces entreprises, il existe un écart entre la fréquence à laquelle les données sont sauvegardées et le volume de données qu'elles peuvent se permettre de perdre.

#6 Ne négligez pas la *restauration granulaire*

Bien souvent, les entreprises ne s'assurent pas que la solution de sauvegarde qu'elles utilisent pour Microsoft Teams offre des fonctionnalités de restauration granulaire. Or, bien qu'il soit important de pouvoir restaurer une équipe entière (voire plusieurs), il est également crucial de pouvoir restaurer un fichier ou une conversation au sein d'une équipe.

Pour 44 % des administrateurs SaaS et 47 % des administrateurs de sauvegarde, la meilleure qualité de la restauration, granularité comprise, est la principale raison de protéger les données d'Office 365.
https://www.youtube.com/watch?v=RIHm8-0LUJs

70 % des entreprises du classement Fortune 500 ont acheté Office 365 en 2020.
https://hostingtribunal.com/blog/microsoft-statistics/#gref

#7 Utilisez la sauvegarde pour étoffer les *fonctionnalités d'eDiscovery*

MIcrosoft 365 intègre depuis longtemps des fonctionnalités d'eDiscovery qui permettent aux entreprises de localiser des données spécifiques dans l'écosystème Microsoft 365 en réponse à une citation à comparaître. Bien que les fonctionnalités natives d'eDiscovery soient utiles, il est souvent plus efficace d'utiliser un logiciel de sauvegarde dans le processus de discovery.

Selon un sondage sur la disruption en matière d'eDiscovery, « au moins 58 % des sondés ont utilisé à plusieurs reprises la technologie d'eDiscovery à des fins autres que des plaintes ou des réclamations ». Force est donc de constater que l'eDiscovery ne se cantonne plus aux litiges juridiques.

$12.9 Billion
Le marché de l'eDiscovery devrait se développer et représenter 12,9 milliards de dollars d'ici 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 Protégez Teams *contre les ransomwares*

Une autre meilleure pratique consiste à protéger vos données Microsoft Teams contre les ransomwares. Contrairement à la croyance populaire, les données stockées dans Microsoft 365 peuvent être chiffrées par des ransomwares. Le fait que de nombreuses personnes continuent à télétravailler en utilisant leurs appareils personnels augmente considérablement le risque d'attaque par ransomware. Une sauvegarde efficace constitue la meilleure défense contre les pertes de données liées aux ransomwares.

Selon le Ponemon Institute, seulement 45 % des entreprises jugent suffisante la part de leur budget consacrée à la cybersécurité.

Selon IDC, 69% des entreprises ont été victimes d'attaques par un logiciel malveillant au cours des 12 derniers mois, 39 % d'entre elles impliquant des ransomwares.

*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 Assurez-vous que votre *stockage* est gage de *flexibilité*

Lorsque vous choisissez une application de sauvegarde pour Microsoft Teams, vous devez vous assurer qu'elle vous laisse le choix du stockage, quel qu'il soit. Vous pourrez ainsi sélectionner le tier de stockage répondant aux exigences de votre entreprise en termes de performances, de résilience et de coût. La flexibilité du stockage donne également aux entreprises la possibilité d'écrire des sauvegardes vers un stockage inaltérable pour les protéger des attaques par ransomware.

CNA Financial a battu un triste record mondial en versant une rançon de 40 millions de dollars en 2021.

Selon une enquête réalisée par Sophos en 2021, "7 % des entreprises interrogées avaient subi une attaque de ransomware l'année précédente".

*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 Privilégiez la *simplicité d'utilisation*

Certaines applications de sauvegarde ont la réputation d'être extrêmement difficiles à configurer et à utiliser, ce qui augmente les risques d'erreur humaine. Si une entreprise choisit une application de sauvegarde simple et intuitive, les échecs de sauvegarde ou de restauration imputables à une erreur humaine sont généralement moins nombreux.

Selon la FEMA, 40 à 60 % des petites entreprises ne réussissent pas à se relever d'une perte de données
https://hostingtribunal.com/blog/data-loss-statistics/#gref

58%
Selon une enquête réalisée en 2021, 58 % des sauvegardes ne peuvent pas être restaurées

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