CARBONITE

L'importance de protéger les données d'Office 365

Développer une stratégie de protection efficace pour les données Microsoft Office 365

Développer une stratégie de protection efficace pour les données Microsoft Office 365

Les applications « SaaS » (logiciels fournis sous forme de service) destinées à favoriser la productivité comme Microsoft Office 365 sont tout simplement indispensables dans le monde mobile d'aujourd'hui – l'intérêt de pouvoir accéder facilement à des documents depuis n'importe quel appareil et de collaborer plus efficacement est évident. Cependant, de nombreuses organisations pensent que l'acquisition d'Office 365 les dispense d'effectuer des sauvegardes. Selon un rapport publié récemment par « Enterprise Strategy Group », une entreprise sur quatre pense qu'il n'est pas nécessaire de sauvegarder les données d'Office 365.

Cette fausse idée vient probablement du fait que Microsoft Office 365 offre une certaine protection contre la perte de données. Certaines organisations pensent que comme les données sont hébergées dans le cloud, elles sont automatiquement sauvegardées. D'autres encore croient que la synchronisation des fichiers Microsoft OneDrive remplace la sauvegarde. Toutes ces idées sont fausses. La sauvegarde est aussi importante avec Office 365 que lors du déploiement d'applications Microsoft sur site.

Dans ce livret électronique, nous allons voir quelles sont les causes les plus fréquentes de perte de données dans Office 365, pourquoi il ne faut pas compter seulement sur la Corbeille ou sur One Drive, et quelles sont les mesures à prendre pour protéger les données Office 365 essentielles de votre organisation.

Risques liés à Office 365

Les politiques de protection des données de Microsoft ne garantissent pas une restauration complète et rapide des données Office 365 supprimées ou corrompues. En bref, Microsoft se contente de garantir que vos données ne seront pas perdues. Mais Microsoft ne donne aucune garantie concernant leur restauration.

C'est évidemment un problème. L'incapacité de récupérer des informations commerciales critiques peut vous faire perdre des revenus et des clients et entacher votre réputation. Qui plus est, si votre entreprise est soumise à des obligations de conservation de données, une perte de données peut même avoir des conséquences juridiques.

Comme nous l'avons mentionné plus haut, les données Office 365 sont tout aussi vulnérables que les données hébergées sur site. Passons en revue les risques les plus courants :

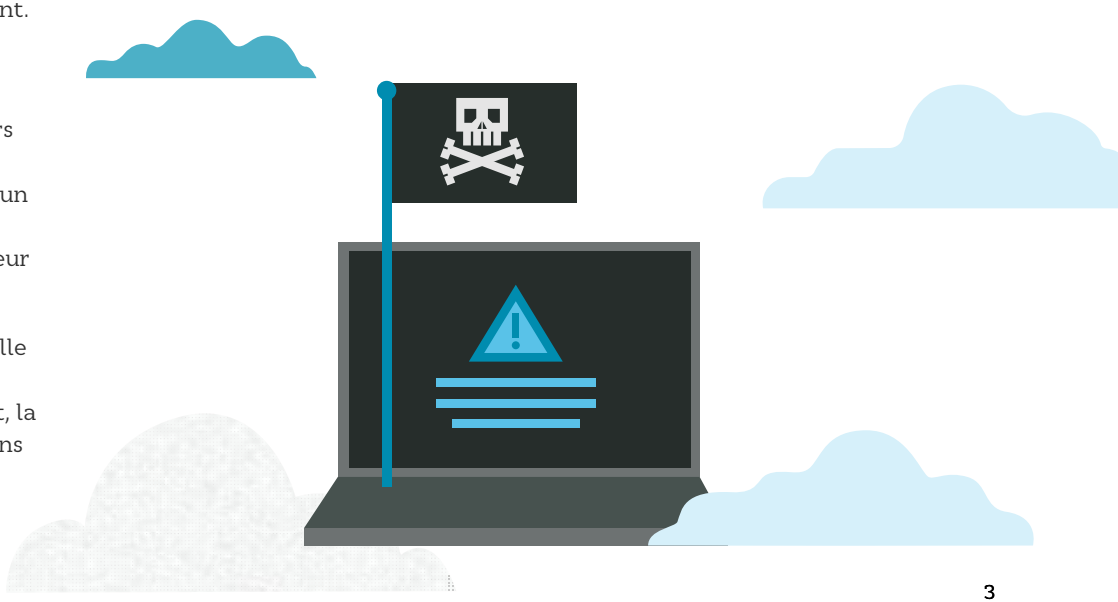
Suppression accidentelle :
Le principal risque est la suppression accidentelle : un employé supprime un fichier ou un dossier par erreur. Il est facile de supprimer des données et des conversations dans SharePoint, Groups ou Teams, ou d'écraser certaines versions de données existantes. Une telle suppression de données n'est pas catastrophique si elle est décelée immédiatement. Il suffit d'aller récupérer les documents dans la Corbeille. Mais les fichiers supprimés ne sont conservés dans la Corbeille que temporairement.

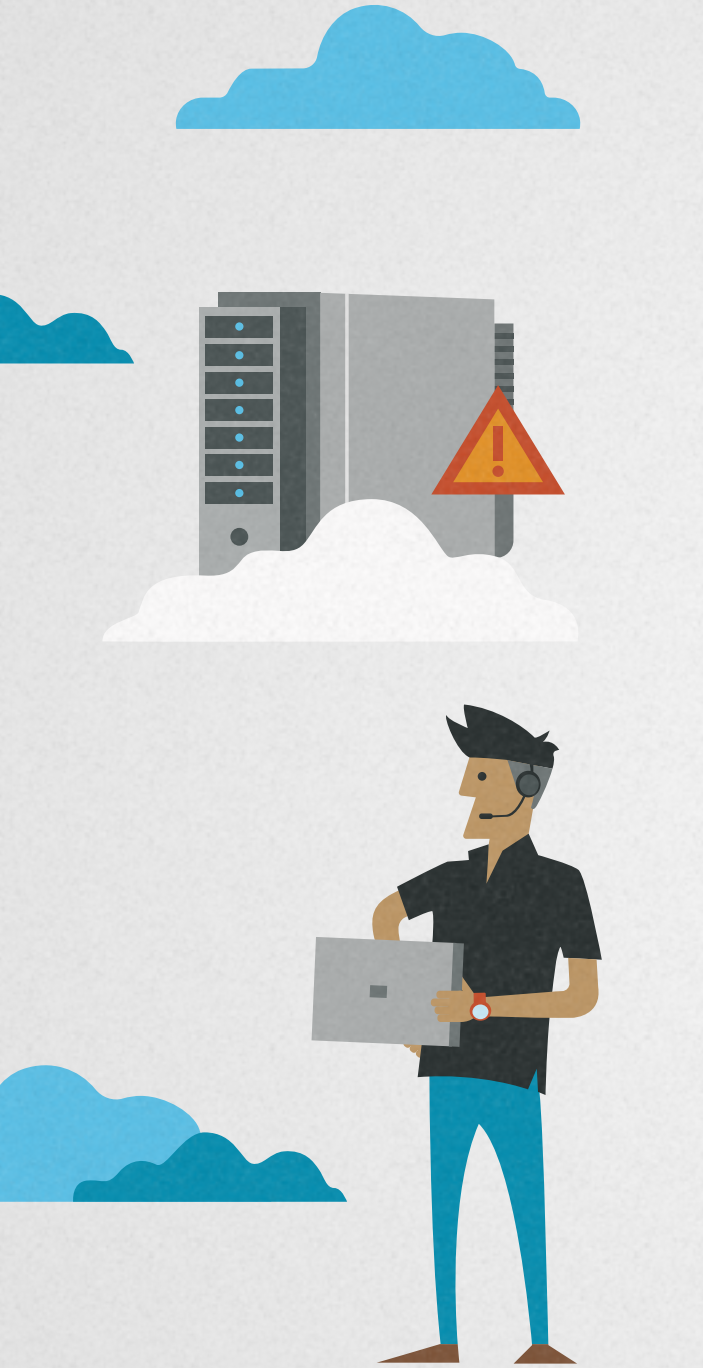
Suppression intentionnelle :
Dans certains cas, la suppression de données n'est pas accidentelle. Des employés mécontents peuvent volontairement supprimer leurs propres fichiers ou des fichiers se trouvant dans des dossiers partagés avant de quitter l'entreprise. Une personne extérieure peut également accéder à des fichiers et dossiers Office 365 au moyen d'un ordinateur portable volé protégé par un mot de passe facile à deviner. Dans le pire des cas, un administrateur mondial d'Office 365 peut effacer des comptes d'utilisateur avant de quitter l'entreprise et empêcher les autres administrateurs d'y accéder.

Lorsque des fichiers importants sont perdus à la suite d'une suppression accidentelle ou intentionnelle, la productivité s'en trouve forcément altérée. C'est plus qu'un simple inconvénient. Lorsque les employés ne peuvent pas travailler normalement, la perte de revenus est inévitable. Et si votre organisation est soumise à des obligations de conservation de données, il peut même y avoir des conséquences juridiques.

Logiciels de rançon (et autres logiciels malveillants) :
De nombreuses organisations croient, à tort, que les données Office 365 sont à l'abri des logiciels de rançon et autres types de logiciels malveillants. C'est totalement faux. Un logiciel de rançon peut verrouiller les fichiers Office 365 dans le cloud et bloquer un grand nombre d'utilisateurs. Voilà comment : un utilisateur télécharge par inadvertance un logiciel de rançon sur son ordinateur portable qui va infecter ses fichiers locaux. Si cet utilisateur a activé la synchronisation OneDrive, les fichiers infectés sont immédiatement copiés dans le cloud. Et cela ne s'arrête pas là. Les logiciels de rançon sont conçus pour se diffuser sur les réseaux via les fichiers et dossiers partagés. L'application OneDrive étant conçue pour favoriser la collaboration, elle peut être particulièrement vulnérable face à ce type d'attaque.

Problèmes liés à la personnalisation :
Si la personnalisation d'Office 365 offre de nombreux avantages, les conceptions, solutions, flux de travail, marques personnalisées et autres modifications apportées aux sites destinés aux utilisateurs peuvent provoquer des incidents techniques. En cas d'erreur, il peut être nécessaire d'annuler la personnalisation. Selon le système concerné, la perte de données peut entraîner des heures, voire des jours, d'arrêt.





OneDrive n’est pas un système de sauvegarde

Beaucoup de gens pensent que OneDrive remplace la sauvegarde étant donné que l’application enregistre une copie des fichiers utilisateur dans le cloud de Microsoft. Cependant, en utilisant OneDrive comme système de sauvegarde, vous risquez de perdre des données. Voici pourquoi : si un fichier est supprimé ou infecté sur un appareil local, ce changement est automatiquement répercuté dans OneDrive. Autrement dit, le fichier est automatiquement supprimé ou infecté sur tous les appareils synchronisés.

Le système de conservation de fichiers d’Office 365 permet aux organisations de sélectionner les fichiers à conserver ainsi que leur durée de conservation. Les politiques de conservation peuvent être notamment basées sur la date de création ou de dernière modification des fichiers, le type de fichier ou des mots-clés. Elles peuvent aider les organisations à respecter leurs obligations réglementaires en matière de conservation des données et réduire les risques en cas de litige ou de faille de sécurité. Toutefois, les paramètres de conservation d’Office 365 varient selon les applications et certaines d’entre elles, comme Microsoft Teams, n’intègrent aucune fonctionnalité de conservation.

OneDrive permet de restaurer des fichiers à partir de la Corbeille. Mais cette dernière n’offre pas – loin s’en faut – tous les avantages d’une véritable sauvegarde :

- Les versions de fichier ne constituent pas des points de récupération immuables et distincts. Ainsi, si un fichier actif est supprimé, toutes les versions précédentes dudit fichier sont supprimées également. Par ailleurs, les fichiers supprimés définitivement de la Corbeille ne peuvent pas être récupérés.
- Les données utilisateur ne peuvent pas être gérées de manière centralisée. Autrement dit, la Corbeille ne permet pas au service informatique de contrôler les sauvegardes et les récupérations.
- Elle n’enregistre pas de points de récupération réguliers pour les fichiers, les dossiers et les utilisateurs. De ce fait, toute restauration importante devra se faire manuellement et prendra un temps considérable. Par exemple, pour restaurer des fichiers à la suite d’une attaque par un logiciel de rançon, l’utilisateur devra rechercher manuellement les points de récupération adéquats et restaurer les fichiers un par un.

Encore une fois, c’est plus qu’un simple inconvénient. En cas de problème, il faut intervenir manuellement, ce qui monopolise l’attention du service informatique et/ou des employés. Comme nous l’avons évoqué précédemment, tout arrêt de l’activité entraîne une perte de revenus.

Développer une stratégie de protection des données Office 365

Votre stratégie de protection d'Office 365 doit commencer par la formation des employés. La plupart des cyberattaques proviennent de sites de « phishing » ou malveillants. C'est pourquoi il est important que les employés sachent identifier les e-mails de « phishing » et puissent prévenir les services compétents s'ils reçoivent un e-mail suspect.
Par ailleurs, il est essentiel d'élaborer et de mettre en œuvre des directives pour une utilisation sûre d'Internet.
Enfin, expliquez aux employés pourquoi il est important de définir des mots de passe complexes, et apprenez-leur à en créer et à les gérer.

La protection antivirus est un autre aspect crucial. Les virus et logiciels malveillants pouvant facilement contaminer les données stockées dans le cloud à partir d'une machine locale, il est essentiel de prendre des mesures de sécurité informatique pour assurer la protection d'Office 365. Les logiciels de rançon sont constamment mis à jour pour rester indétectables ; assurez-vous donc de mettre votre logiciel antivirus à jour également. Certaines solutions antivirus sont basées dans le cloud et sont donc fréquemment mises à jour. Ce type de solution peut alléger les tâches de gestion.

La sauvegarde est la meilleure façon de se protéger contre la suppression de fichiers accidentelle ou intentionnelle, d'autres erreurs commises par les utilisateurs, les logiciels de rançon et la corruption de données. Les outils natifs de Microsoft offrent un certain degré de protection, mais les solutions de sauvegarde tierces vous garantissent une restauration rapide de vos données et le respect des obligations en matière de conservation et de souveraineté pour toutes les données Office 365.

Tous les outils de sauvegarde d'Office 365 ne se valent pas. En réalité, la plupart d'entre eux n'assurent pas la protection de toute la suite de produits – par exemple, rares sont ceux qui protègent Microsoft Teams. D'autres produits ne permettent pas d'effectuer de récupération granulaire ou de restaurer les autorisations. En conclusion, lorsque vous choisissez une solution de sauvegarde pour Office 365, vérifiez qu'elle offre bien la protection dont vous avez besoin. Carbonite Backup for Office 365 protège toute la suite Microsoft Office 365, y compris Teams, OneDrive, Exchange, SharePoint, le Planificateur et Skype Entreprise.

Certains outils de sauvegarde d'Office 365 possèdent des fonctions qui peuvent vous aider à remplir vos obligations en matière de gouvernance et de conformité, comme le RGPD. Carbonite Backup for Office 365 offre par exemple un tableau de bord dédié à la confidentialité qui permet aux utilisateurs d'accéder à des fonctions relatives au droit à l'oubli et au traitement des demandes d'accès aux données personnelles, ainsi que des fonctions d'audit et de purge des données.

Enfin, la mise en œuvre d'une stratégie de sauvegarde d'Office 365 peut également contribuer à réduire les coûts de conservation. Si votre organisation doit conserver les données utilisateur pendant une durée spécifique, la gestion des licences Office 365 des anciens employés peut vite devenir onéreuse. Carbonite Backup for Office 365 permet de conserver leurs fichiers et e-mails pour un coût bien inférieur à celui d'une licence Microsoft.

Contactez-nous pour en savoir plus sur Carbonite Backup for Office 365 :

+33 14 777 0500
SalesFR@carbonite.com
www.carbonite.fr

W131-0919_EMEA_FR