

Comment renforcer la protection des données Microsoft 365 dans six domaines majeurs

Si vous utilisez Microsoft 365, vous pouvez compter sur un accès fiable à ses applications, avec un haut niveau de disponibilité. Microsoft est réputé pour sa capacité à assurer la disponibilité de son infrastructure cloud. En revanche, l'éditeur n'assume aucune responsabilité quant à la protection des données Microsoft 365. Microsoft recommande d'ailleurs très explicitement à ses utilisateurs de déployer leurs propres applications ou services de sauvegarde tiers pour assurer la protection de leurs données. Pour reprendre les termes du contrat de services Microsoft : « Nous mettons tout en œuvre pour assurer la disponibilité permanente des Services. Toutefois, aucun service en ligne n'est à l'abri d'interruptions et de pannes, et Microsoft n'est en aucun cas responsable des perturbations ou éventuelles pertes occasionnées. En cas de panne, **vous risquez de ne pas pouvoir récupérer Votre Contenu ou Vos Données** que vous stockez. **Nous vous recommandons de sauvegarder régulièrement Votre Contenu et Vos Données** que vous stockez sur les Services ou que vous stockez **en utilisant des Applications et Services Tiers**. »

Malgré cela, de nombreuses entreprises s'imaginent encore que Microsoft offre une protection complète et une rétention à long terme des données Microsoft 365, alors qu'elles ne sont en réalité pas protégées contre les problèmes de pertes de données les plus courants ou les plus graves (suppressions accidentelles, attaques de malware, etc.). Cette idée reçue peut causer à de nombreuses entreprises de mauvaises surprises du fait de cette faille dans la protection des données. Les responsables informatiques doivent prendre conscience qu'il est de leur responsabilité de protéger les données Microsoft 365 de leur entreprise et d'implémenter une solution de sauvegarde complète pour se protéger contre les sources de pertes de données les plus courantes.

Toutes les entreprises doivent renforcer la protection de leurs données Microsoft 365 dans six domaines majeurs

1. Suppressions accidentelles de données

Risque pour les données : au cours d'une journée de travail, les collaborateurs suppriment régulièrement des profils utilisateur Microsoft 365, des e-mails et des pièces jointes Exchange Online, des fichiers OneDrive Entreprise et des contenus Teams et SharePoint Online. Ces suppressions peuvent être accidentelles, ou délibérées puis regrettées, mais elles peuvent dans tous les cas entraîner la perte de données importantes.

Niveau de protection assuré par Microsoft : les suppressions de ce type sont répliquées au niveau du réseau. L'ancienneté des ressources aggrave le problème : les données plus anciennes risquent d'être définitivement supprimées et irrécupérables. Les suppressions plus récentes de ressources moins anciennes sont moins problématiques ; en effet, les fichiers et les e-mails supprimés de façon réversible peuvent être récupérés à court terme dans la Corbeille ou le dossier Éléments supprimés.

2. Failles des règles de rétention

Risque pour les données : tout changement ou inadaptation des priorités dans les règles de rétention des données Microsoft 365 peut entraîner une suppression définitive des données. Pour remédier à ce problème, il faut vérifier et mettre à jour régulièrement les règles de rétention.

Niveau de protection assuré par Microsoft : les clients Microsoft 365 sont responsables de la gestion des règles de rétention. Cela étant, si pour quelque raison que ce soit, une suppression définitive se produit en raison de l'obsolescence des règles de rétention existantes, Microsoft n'a pas la possibilité de récupérer la ressource supprimée.

3. Menaces de sécurité internes

Risque pour les données : les données et les ressources Microsoft 365 doivent être protégées non seulement contre les suppressions ordinaires non malveillantes, mais aussi contre toute altération ou destruction malveillante des données par des collaborateurs, sous-traitants ou partenaires mal intentionnés.

Niveau de protection assuré par Microsoft : à l'exception des suppressions de ressources relativement récentes, Microsoft ne dispose d'aucune protection contre la destruction ou l'altération malveillante en interne des données Microsoft 365.

4. Menaces de sécurité externes

Risque pour les données : les données Microsoft 365 sont exposées à la destruction ou à l'altération par différents malwares, le plus souvent des ransomwares, qui chiffrent les données des utilisateurs et les prennent en otage contre rançon payée en ligne.

Niveau de protection assuré par Microsoft : Microsoft offre des protections relativement limitées contre les attaques de malware, telles que les ransomwares, et une capacité très limitée à restaurer la version antérieure à l'attaque des fichiers chiffrés ou altérés par des malwares.

5. Migration depuis Microsoft Office sur site

Risque pour les données : si votre entreprise décide d'effectuer une migration de la suite d'applications Microsoft Office traditionnelle sur site vers les services Microsoft 365 dans le cloud, elle doit généralement remplacer l'ancienne solution de protection des données par une nouvelle, prenant en charge le cloud. Les deux solutions de sauvegarde sont souvent incompatibles, ce qui empêche de restaurer les anciennes données dans le nouvel environnement.

Niveau de protection assuré par Microsoft : Microsoft ne propose aucune solution pour résoudre les problèmes de pertes de données survenant pendant la migration entre Office et Microsoft 365. Rares sont les solutions de protection des données d'autres éditeurs qui intègrent une fonctionnalité de sauvegarde pour Office et Microsoft 365 : ces solutions couvrent l'un ou l'autre, mais pas les deux.

6. Problèmes juridiques et de conformité

Risque pour les données : les obligations réglementaires et les problèmes juridiques peuvent augmenter les coûts engendrés par les pertes de données non protégées décrites ci-dessus. La perte définitive de données Microsoft 365 peut exposer votre entreprise à des problèmes importants : amendes réglementaires nationales ou sectorielles ; sanctions pénales ; pertes de revenus et chute du cours des actions ; perte de confiance des clients ; atteinte à l'image de marque.

Niveau de protection assuré par Microsoft : compte tenu de tous les risques de pertes de données associés décrits ci-dessus, Microsoft peut difficilement protéger les entreprises qui utilisent Microsoft 365 contre les différents risques de non-conformité et vulnérabilités juridiques. Par exemple, après une attaque de ransomware, une société qui stocke dans SharePoint Online les données personnelles de ses clients résidents de l'Union européenne risque de ne pas pouvoir répondre aux demandes de copies de ces données, et donc de contrevenir au RGPD.

Protection de vos données Microsoft 365

Si vous utilisez Microsoft 365, vous devez compléter les fonctions de protection des données proposées par Microsoft avec Acronis Cyber Protect, la solution de sauvegarde la plus fiable et la plus facile à utiliser. Les sauvegardes rapides, la restauration fiable à une date donnée et les options flexibles de restauration et de stockage dans le cloud, ainsi que la fonctionnalité de recherche rapide d'Acronis Cyber Protect, vous aident à protéger les données Microsoft 365 critiques de votre entreprise dans un paysage des menaces en constante évolution.

Microsoft garantit la résilience de sa propre infrastructure cloud, mais la protection de vos données vous incombe. Des dirigeants d'entreprise et des responsables des technologies du monde entier font confiance à Acronis Cyber Protect pour protéger leurs données Microsoft 365 et préserver la continuité de leurs activités.

Pour en savoir plus sur Acronis Cyber Protect, démarrez dès aujourd'hui votre évaluation gratuite de 30 jours.

DÉMARRER

