Les données Microsoft 365 face aux ransomwares

De l'importance des backups

Barracuda

Le paysage des ransomwares

Les attaques par ransomware font couler beaucoup d'encre depuis plusieurs années, et ce à juste titre. En effet, les pertes financières qu'elles ne cessent de causer aux entreprises, tous secteurs confondus, ainsi que leur impact sur la réputation de ces dernières, s'avèrent considérables. Implacables, les auteurs de ces attaques s'emparent des données de leurs victimes et les chiffrent (mettant ainsi leurs systèmes hors d'état de fonctionner), leur extorquent de l'argent pour rétablir l'accès et les font chanter en les menaçant de rendre publiques les données volées.

Année après année, le montant des rançons ne cesse d'augmenter : selon le Rapport trimestriel sur la menace ransomware de Coveware, ces paiements ont atteint une moyenne de 258 143 $ au troisième trimestre 2022, un record à ce jour, soit une hausse de 13,2 % par rapport au trimestre précédent. Mais le vrai problème, c'est le coût de reprise après une attaque par ransomware, qui a atteint une moyenne de 1,85 million de dollars en 2021. Les chiffres pour l'année 2022 ne sont pas encore disponibles, mais ils risquent d'être encore plus élevés..

Les comptes Microsoft 365 sont sans conteste une cible de choix pour les ransomwares

Outre l'impact financier sur leurs victimes, les attaques par ransomware font peser un risque plus grave encore : la perte de données. Les entreprises qui utilisent Microsoft 365 au quotidien sont particulièrement concernées par ce problème. Sachant qu'environ 54 % des attaques sont menées par e-mail et que Microsoft 365 compte plus de 354 millions d'utilisateurs avec licence, les comptes Outlook sont une cible de choix. Les attaques par phishing (hameçonnage) qui consistent, par exemple, à fournir une fausse page de connexion pour tenter d'obtenir les identifiants des utilisateurs, visent quotidiennement les boîtes mail professionnelles.

En outre, des chercheurs ont récemment découvert une possible faille qui permettrait aux pirates de chiffrer les fichiers stockés dans SharePoint et OneDrive et de rendre leur récupération impossible sans une clé de déchiffrement. Au vu des vulnérabilités présentes dans les comptes Microsoft 365, les acteurs malveillants multiplient les tactiques pour pénétrer le réseau, chiffrer les données confidentielles et demander une rançon. Les entreprises se voient alors confrontées au dilemme de payer la rançon ou de subir les conséquences de l'attaque. La meilleure solution pour prévenir ce risque est le backup sécurisé, qui vous permettra de restaurer vos données Microsoft 365 sans devoir payer une lourde rançon.

Face à la menace ransomware, il devient indispensable pour les entreprises de sauvegarder toutes leurs données et de tester régulièrement leurs backups afin de garantir la disponibilité des informations sensibles et la poursuite de l'activité, même en cas d'attaque. Par ailleurs, une solution de backup efficace saura vous protéger contre divers autres types de malwares et vous éviter la perte de fichiers au quotidien ou la suppression accidentelle de vos données, qui peuvent perturber vos systèmes ou entraîner des conséquences plus graves encore pour votre équipe informatique.

Le choix d'une solution de backup tierce se révèle indispensable pour Microsoft 365

Malgré le risque évident que font peser les attaques par ransomware sur les entreprises, avec des conséquences désastreuses sur les données, 67 % des responsables informatiques s'en remettent à Microsoft pour sauvegarder leurs données Microsoft 365 et choisissent de ne mettre en place aucune procédure de backup, formelle ou non. Le fait de croire que Microsoft se charge de sauvegarder les données témoigne simplement d'une mauvaise compréhension des stratégies de rétention de l'entreprise. Microsoft ne sauvegarde pas vos données et décline toute responsabilité en cas de perturbation ou de perte de données liées à une interruption de service. L'absence de sauvegarde constitue un risque majeur dont bon nombre d'entreprises n'ont pas connaissance.

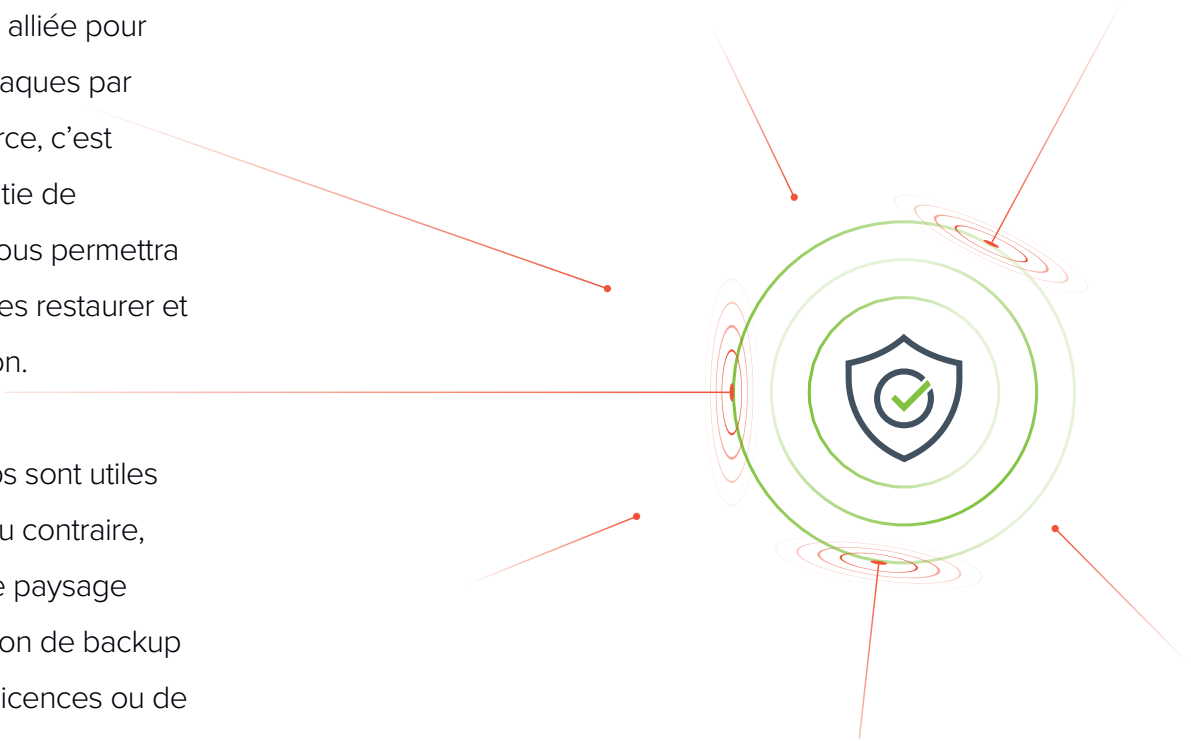
Microsoft 365 propose, en effet, toute une série de stratégies de rétention. Sachez toutefois que par défaut, la durée maximale de conservation est de 90 jours, et que l'accord indique bien qu'il ne s'agit pas d'une option infaillible. Microsoft recommande de confier la

Contrat de services :

« Nous mettons tout en œuvre pour assurer la disponibilité permanente des services. Toutefois, ils ne sont pas offerts avec un niveau de qualité de service garanti et aucun service en ligne n'est à l'abri d'interruptions et de pannes. En cas de panne ou d'interruption du service, vous pouvez temporairement ne pas être en mesure de récupérer votre contenu. » Nous vous recommandons de sauvegarder régulièrement votre contenu et les données que vous stockez en utilisant des applications et des services tiers.

sauvegarde de vos données à un fournisseur tiers - leur politique de rétention par défaut n'est pas une sauvegarde et n'est pas conçue pour restaurer de gros volumes de données pour une utilisation dans un environnement de production.

Une véritable solution de backup sera votre meilleure alliée pour protéger les données de votre entreprise face aux attaques par ransomware. Investir dans une solution de backup tierce, c'est souscrire une assurance ransomware. Véritable garantie de récupération en cas d'attaque par ransomware, elle vous permettra de revenir à une version propre de vos données, de les restaurer et de reprendre votre activité, le tout sans payer la rançon.



Cela dit, ce serait une erreur de croire que les backups sont utiles uniquement en cas d'attaque par ransomware. Bien au contraire, la sauvegarde s'impose comme une évidence dans le paysage informatique. Dans le cas de Microsoft 365, une solution de backup efficace vous permettra non seulement de gérer vos licences ou de procéder à une restauration croisée des utilisateurs et des données, mais aussi de répondre aux exigences de conformité. Nécessaire bien avant l'apparition des ransomwares, la sauvegarde s'avère plus que jamais indispensable pour se protéger contre cette menace omniprésente aux effets potentiellement dévastateurs.

Comment protéger vos utilisateurs et vos données Microsoft 365 contre les attaques par ransomware

En plus de sauvegarder vos données, vous devez impérativement mettre en place une solution de protection des e-mails pour Microsoft 365 afin de pouvoir déjouer les attaques par ransomware. Une solution de protection des e-mails efficace propose les fonctionnalités nécessaires pour bloquer les spams et les malwares, empêcher le piratage de compte et répondre aux incidents.

Il est également indispensable de sensibiliser et de former régulièrement vos équipes. En effet, ces dernières doivent être capables de repérer une tentative de phishing susceptible d'introduire un ransomware et d'y répondre. Elles doivent savoir, par exemple, à qui la signaler. Souvent, les violations de données sont rendues possibles par l'incapacité à reconnaître un e-mail suspect ou une mauvaise compréhension des enjeux. La formation doit être au cœur de votre stratégie de cybersécurité. Sensibiliser vos collaborateurs aux règles d'hygiène informatique, comme la protection des mots de passe, est indispensable mais insuffisant. Compte tenu du nombre important de violations de données, vos identifiants sont susceptibles d'avoir été compromis. C'est pourquoi il devient nécessaire de mettre en œuvre une solution de sécurité supplémentaire telle que l'authentification multifacteur ou l'accès zero trust.

Malheureusement, se prémunir contre les ransomwares ne suffit pas. Vous devez tout de même mettre en œuvre une solution de backup tierce qui soit sécurisée et fiable, que vous testerez régulièrement afin de garantir l'accès à vos données en cas d'attaque. Pour être efficace, votre solution de backup (qui est votre dernière ligne de défense) doit proposer des fonctionnalités telles que le chiffrement à grande échelle, l'authentification multifacteur, le contrôle d'accès basé sur les rôles, les données immuables et la purge différée.

Barracuda Cloud-to-Cloud Backup

Une protection de Microsoft 365 flexible et facile à utiliser

Sauvegardez vos données Teams, Exchange, SharePoint et OneDrive et trouvez et récupérez les données exactes dont vous avez besoin, rapidement et facilement, grâce à une fonction de recherche avancée.

Ransomware Protection

Votre sauvegarde constitue votre dernière ligne de défense contre les ransomwares et autres menaces. Il vous faut donc une solution de backup sécurisée qui allie contrôle d'accès basés sur les rôles, chiffrement et multiplication des copies de données.

Cloud native

Vos données Microsoft 365 sont déjà sur le cloud. En les sauvegardant de manière sécurisée et chiffrée sur le même réseau, vous gagnez en performance et en évolutivité.

Découvrez Barracuda Cloud-to-Cloud Backup et profitez de notre essai gratuit sans engagement.

Barracuda

Barracuda en quelques mots

Notre mission est de renforcer la sécurité de tous. Chez Barracuda, nous pensons que chaque entreprise mérite un accès à des solutions de sécurité de niveau professionnel cloud-first, abordables, intuitives et facilement déployables. Nous protégeons vos e-mails, réseaux, données et applications à l'aide de solutions innovantes capables de s'adapter au parcours de nos clients, et de se développer en conséquence. Plus de 200 000 entreprises partout dans le monde ont choisi Barracuda pour veiller à leur sécurité pendant qu'elles prospèrent. Pour en savoir plus, rendez-vous sur fr.barracuda.com.

Barracuda

Abonnez-vous au blog de Barracuda, Threat Spotlight, pour vous tenir informé(e) tous les mois.