Ransomware : Foire aux questions

L'avantage Mozy

Simple

Gérez de manière transparente la sauvegarde, la synchronization et l'accès mobile dans les environnements de serveurs et multi-utilisateurs à partir d'une console Web unique.

Sécurisé

Vos données sont protégées grâce à un chiffrement d'entreprise, à des datacenters très avancés et à Dell EMC, une entreprise conçue pour durer.

Économique

Réalisez des économies : aucun matériel à acheter et frais supplémentaires minimes.

Contactez Mozy

mozyemeasales@dell.com
0800 91 71 34
www.mozy.fr/pro

Section 1 : Présentation du ransomware

Qu'est-ce qu'un ransomware ?

Un ransomware est une forme de logiciel malveillant conçue soit pour bloquer l'accès au système d'un ordinateur, soit pour crypter les fichiers ou les autres données d'un utilisateur. Le cybercriminel exige ensuite une rançon (normalement sous forme d'une devise virtuelle, telle que Bitcoin, qui est difficile à suivre), après quoi le coupable peut (il n'y a aucune garantie !) fournir des instructions expliquant comment regagner l'accès au système et aux fichiers. Le ransomware vise normalement les invididus ; cependant, les sociétés - dont les entreprises - sont désormais des cibles.

En quoi dois-je me sentir concerné par le ransomware ?

Le ransomware est une menace en plein essor ; de fait, ce sont des millions de nouvelles variantes malveillantes qui apparaissent chaque jour. Il est indispensable de mettre en place un plan de lutte contre cette forme de cyber-criminalité.

Comment le ransomware se propage-t-il ?

Le ransomware obtient un accès au système informatique au moyen du lien le plus faible d'un réseau, normalement l'e-mail ou un site de réseau social d'un utilisateur. La plupart du temps, les criminels visent les utilisateurs informés au moyen d'e-mails d'hameçonnage et les liens Web suspects. Une fois qu'un utilisateur clique sur un lien malveillant ou ouvre une pièce jointe infectée, le maliciel se propage dans le système. Une fois ouvert, les fichiers infectés par un logiciel malveillant peuvent rapidement contourner la sécurité de réseau d'une organisation. Le logiciel malveillant peut également résider au sein de fichiers sur les ordinateurs d'utilisateurs finaux. Si ces fichiers-là sont synchronisés ou conservés dans une plateforme de collaboration où d'autres utilisateurs peuvent y accéder, le logiciel malveillant peuvent également se répandre d'ordinateur en ordinateur.

Comment le ransomware se détecte-t-il ?

Une attaque de ransomware est normalement détectée uniquement après l'infection du système par le logiciel malveillant. Souvent, un message s'affiche sur l'écran de l'ordinateur de l'utilisateur lui signalant que son ordinateur a été verrouillé et que ses fichiers sont cryptés.

Que puis-je faire pour me protéger contre le ransomware ?

Vous pouvez utiliser des listes blanches, filtres, méthodes de mise en quanrantaine, antivirus et balayages de système dans le but d'empêcher le ransomware. Cependant, les criminels sont ingénieux et tenaces ; il ne suffit que d'un clic pour qu'une infection se produise. La meilleure façon de vous protéger contre le ransomware est d'avoir une sauvegarde fiable capable de vous rendre vos fichiers non infectés. Les sauvegardes devraient s'effectuer de façon régulière et fiable afin d'assurer que vous pouvez restaurer vos données à un point connu dans le temps avant l'attaque.

Pourquoi la synchronisation ne représente-t-elle pas une bonne méthode de sauvegarde ?

La synchronisation n'est pas une sauvegarde. Toutes les modifications apportées au fichier source, y compris le ransomware, sont rapidement synchronisés avec le cloud et avec tous les autres utilisateurs qui ont accès au fichier. En outre, les services de synchronisation qui offrent la création de versions ou des corbeilles exigent que l'utilisateur sélectionne des fichiers individuels à restaurer un par un, par rapport à un instantané d'un point dans le temps intégral, alors qu'un service de sauvegarde permet la restauration de fichiers précis ou de tous les fichiers d'une date précise avec quelques clics. Ainsi, un service de synchronisation offre un accès pratique aux fichiers, mais un service de sauvegarde fournit une expérience de restauration bien plus compréhensive en cas de catastrophe. De plus, un servicce de synchronisation peut involontairement servir de véhicule de propagation de logiciels malveillants parmi plusieurs ordinateurs et appareils.

Section 2 : Ransomware et Mozy

Comment les données Mozy sont-elles protégées contre une attaque de ransomware ?

Les données client de Mozy sont conservées dans le cloud Dell EMC, qui est isolé de l'environnement du client. De plus, le cloud Dell EMC est un environnement de non exécution, ce qui signifie que les programmes, y compris les virus, ne peuvent pas s'exécuter dans le cloud et ne peuvent pas infecter les fichiers qui y sont conservés.

Quel est le procédé de restauration de données non infectées avec Mozy ?

Une fois que vous aurez identifié tous les utilisateurs affectés, éliminé le logiciel malveillant et déterminé le moment auquel l'infection s'est produite, vous pouvez restaurer les données d'une sauvegarde réalisée avant l'infection.

Et si ma sauvegarde Mozy contient le logiciel malveillant ?

Le cloud Dell EMC est un environnement de non exécution, ce qui signifie que les programmes, y compris les virus, ne peuvent pas s'exécuter dans le cloud et ne peuvent pas infecter les fichiers qui y sont conservés. En outre, Mozy conserve jusqu'à un an de versons de fichiers, ce qui signifie que si vous avez identifié le point d'infection (utilisateur et fichier) et le moment auquel le maliciel s'est présenté dans l'ordinateur, Mozy peut restaurer tous les fichiers d'un utilisateur précis depuis le moment juste avant l'introduction du logiciel malveillant. Par exemple, si le logiciel malveillant s'est présenté le 2 juin, vous pouvez restaurer les fichiers de la sauvegarde du 1er juin. Ce procédé est parfois nommé « rollback » (restauration rapide).

Section 2 : Ransomware et Spanning

Comment le ransomware peut-il infecter les données dans Google Drive ou OneDrive Entreprise ?

La plupart des organisations utilisent les services de synchronisation de déploiement commercial de Google Drive ou OneDrive sur leurs points d'extrémités (ordinateurs portables), afin de pouvoir facilement accéder, modifier puis synchroniser les modifications de fichiers dans le cloud et pour tous les autres utilisateurs qui ont un accès partagé aux fichiers. Lorsque le ransomware attaque un point d'extrémité, les fichiers qui sont cryptés par le ransomware sont synchronisés dans le cloud et propagés parmi d'autres utilisateurs de votre organisation, ou pire, vos partenaires ou clients en dehors de votre organisation.

Comment les données dans Spanning Backup sont-elles protégées contre une attaque de ransomware ?

Les données client conservées dans Spanning Bakup sont isolées de l'environnement du client. Toutes les données sont conservées dans l'environnement cloud conforme

à la norme SSAE SAE SOC 2 et sont isolées dans un environnement de non exécution, ce qui signifie que les programmes, y compris les virus et les logiciels malveillants, ne peuvent pas exécuter et infecter les fichiers qui y sont conservés.

Quel est le procédé de restauration de données non infectées avec Spanning ?

Une fois que vous aurez identifié tous les utilisateurs affectés, éliminé le logiciel malveillant et déterminé le moment auquel l'infection s'est produite, vous pouvez restaurer les données directement dans Office 365 ou Google Apps de n'importe quelle sauvegarde de point dans le temps dans Spanning Backup. Une fois les données restaurées, elles peuvent ensuite être synchronisées avec les points d'extrémité. De plus, les organisations peuvent élire de suspendre les services de synchronisation pendant que l'infection est toujours présente et autoriser les utilisateurs à modifier des documents uniquement dans les services cloud tels que Google Docs et les versions en ligne de Word, Excel et PowerPoint d'Office 365.

05/17, Brochure, H16431-FR