RANSOMWARE : QUESTIONS COURANTES

SECTION 1 : TOUR D'HORIZON DES RANSOMWARE

Qu'est-ce qu'un ransomware ?

Un ransomware est une sorte de logiciel malveillant conçu pour bloquer l'accès au système d'un ordinateur ou chiffrer les fichiers ou autres données d'un utilisateur. Le cybercriminel impliqué peut alors exiger une rançon (généralement sous la forme d'une devise virtuelle difficile à tracer, telle que les bitcoins), en échange (mais il n'existe aucune garantie !) des instructions expliquant comment accéder de nouveau au système et aux fichiers. Les ransomware sont souvent utilisés contre des particuliers. Toutefois, les professionnels (y compris les grosses entreprises) sont également devenus des cibles potentielles.

Pourquoi devrais-je me sentir concerné par les ransomware ?

Les ransomware représentent une menace grandissante. De fait, les nouvelles variantes de programmes malveillants se comptent par millions chaque année. C'est pourquoi une stratégie pour lutter contre cette forme de cybercriminalité est absolument nécessaire.

Comment les ransomware se propagent-ils ?

Les ransomware accèdent aux systèmes informatiques par le maillon le plus faible d'un réseau, lequel correspond généralement aux comptes de messagerie des utilisateurs ou aux sites de réseaux sociaux. Le plus souvent, les criminels s'en prennent aux utilisateurs via des e-mails de phishing ou des liens douteux. Dès que l'utilisateur clique sur un lien malveillant ou ouvre une pièce jointe infectée, le programme malveillant se propage dans tout le système. Une fois ouverts, les fichiers infectés par un programme malveillant sont capables de contourner rapidement la sécurité du réseau d'une organisation. Les ordinateurs des utilisateurs sont également des cibles potentielles de ces fichiers infectés. Lorsque ces fichiers sont synchronisés ou stockés sur une plate-forme de collaboration à laquelle d'autres utilisateurs ont accès, les programmes malveillants peuvent alors également se propager d'un ordinateur à un autre.

Comment les ransomware sont-ils détectés ?

Les attaques perpétrées par les ransomware ne sont généralement détectées qu'une fois le système infecté par le programme malveillant. Bien souvent, un message s'affiche sur l'écran d'ordinateur de l'utilisateur pour l'informer que celui-ci a été verrouillé et/ou que ses fichiers ont été chiffrés.

Que puis-je faire pour me protéger des ransomware ?

Les listes blanches, le filtrage, la mise en quarantaine, les antivirus, et les analyses du système sont autant de méthodes permettant de prévenir les attaques de ransomware. Toutefois, les cybercriminels sont ingénieux et persévérants, et il suffit d'un clic pour que votre système soit infecté. La meilleure façon de vous protéger des ransomware consiste à disposer d'une sauvegarde fiable vous permettant de restaurer vos fichiers non infectés. Les sauvegardes doivent être régulières et sûres afin de vous garantir une restauration des données correspondant à un point dans le temps antérieur à l'attaque.

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

La synchronisation et la sauvegarde sont deux choses différentes. Toutes les modifications effectuées dans les fichiers sources, y compris le code du ransomware, sont synchronisées rapidement dans le Cloud et sont donc partagées avec tous les autres utilisateurs ayant accès à ces fichiers. En outre, les services de synchronisation permettant la gestion des versions ou comprenant une corbeille impliquent que l'utilisateur sélectionne un par un les fichiers individuels à restaurer contrairement à un snapshot intégral effectué à un point dans le temps. Les services de sauvegarde permettent quant à eux de restaurer en quelques clics des fichiers spécifiques ou liés à une date en particulier. Par conséquent, les services de synchronisation fournissent un accès pratique aux fichiers, tandis que les services de sauvegarde offrent un niveau de restauration bien plus complet en cas de sinistre. De plus, les services de synchronisation peuvent, de manière involontaire, servir de vecteur à la propagation de malwares sur plusieurs ordinateurs et périphériques.

SECTION 2 : RANSOMWARE ET MOZY

Comment les données Mozy sont-elles protégées contre les attaques des ransomware ?

Les données des clients Mozy sont stockées dans le Cloud EMC, lequel se trouve à part de leur environnement. En outre, le Cloud EMC est un environnement non exécutable, ce qui signifie que les programmes, y compris les virus, ne peuvent y être exécutés. Cela empêche toute infection des fichiers qui y sont stockés.

Quel est le processus de restauration des données non infectées avec Mozy ?

Après avoir identifié tous les utilisateurs concernés, éliminé le programme malveillant et défini le moment où l'infection a eu lieu, les données peuvent être restaurées à partir d'une sauvegarde spécifique, effectuée avant l'infection.

Que se passe-t-il si le programme malveillant fait partie de ma sauvegarde Mozy ?

Le Cloud Mozy est un environnement non exécutable, ce qui signifie que les programmes, y compris les virus, ne peuvent y être exécutés. Cela empêche toute infection des fichiers qui y sont stockés. En outre, Mozy conserve les versions des fichiers pour les 90 derniers jours, ce qui signifie que si vous avez identifié le point d'infection (utilisateur et fichier) et le moment auquel le programme malveillant a été introduit dans l'ordinateur, Mozy est capable de restaurer tous les fichiers de l'utilisateur donné au point dans le temps se situant juste avant l'infection par le programme malveillant. Par exemple, si le programme malveillant a été introduit le 2 juin, les fichiers peuvent être restaurés à partir de la sauvegarde du 1er juin. Cette méthode est parfois appelée « retour arrière ».

SECTION 3 : RANSOMWARE ET SPANNING

Dans quelle mesure les données de Google Drive ou OneDrive Entreprise sont-elles susceptibles d'être infectées par un ransomware ?

La plupart des organisations qui s'appuient sur Google Drive ou OneDrive Entreprise déploient des services de synchronisation sur les postes des utilisateurs (ordinateurs portables), afin de leur faciliter l'accès, la modification et la synchronisation des fichiers dans le Cloud qui deviennent ainsi visibles à tous ceux qui les partagent. Lorsqu'un ransomware s'attaque à un poste, par exemple un ordinateur portable, les fichiers chiffrés par ce dernier sont synchronisés avec le Cloupoint de terminaisond et sont diffusés auprès d'autres utilisateurs de l'organisation, ou pire encore, auprès de partenaires ou de clients extérieurs à l'entreprise.

Comment les données de Spanning sont-elles protégées contre les attaques de ransomware ?

Les données client stockées dans Spanning Backup sont isolées de l'environnement de ce dernier. Toutes les données sont stockées dans le Cloud Spanning conforme à SSAE SOC 2 et isolées dans un environnement non exécutable, ce qui signifie que les programmes, y compris les virus et programmes malveillants, ne peuvent y être exécutés et infecter les fichiers qui y sont stockés.

Quel est le processus de restauration des données non infectées avec Spanning ?

Après avoir identifié tous les utilisateurs concernés, éliminé le malware et défini le moment où l'infection a eu lieu, les données peuvent être restaurées directement dans Office 365 ou Google Apps à partir de n'importe quelle sauvegarde à un point dans le temps de Spanning Backup. Une fois les données restaurées, celles-ci peuvent être resynchronisées avec les postes. En outre, les organisations peuvent choisir d'interrompre les services de synchronisation tant que l'infection est présente et autoriser les utilisateurs à modifier les documents des services Cloud tels que Google Docs et Office 365 uniquement via les versions en ligne de Word, Excel et PowerPoint.

CONTACTEZ NOUS

Pour en savoir plus sur la façon de prévenir un sinistre suite à l'attaque d'un ransomware grâce à la protection des données des postes, rendez-vous sur Mozy. Pour plus d'informations sur la protection de vos données SaaS, rendez-vous sur Spanning.