Sauvegardes : 5 conseils pour prévenir les attaques de ransomware

Compte tenu de l'augmentation de la fréquence et de l'ampleur des attaques de ransomware, ce n'est pas surprenant. Le premier paiement de rançon – vers 1989 – a pavé le chemin pour que les pirates informatiques du monde entier commencent à chiffrer et verrouiller les données de victimes peu méfiantes pour les conserver jusqu'à ce que les propriétaires aient payé le prix fixé pour les récupérer.

Quelques chiffres :

– Une attaque de ransomware se produit toutes les 14 secondes

– 700 % de croissance depuis 2016

– 35 % des criminels ont obtenu une rançon

– 2 G$ de pertes financières

– 11 G$ en pertes financières, de productivité et de temps d'arrêt

Aujourd'hui, les analystes estiment qu'une attaque de ransomware visant les entreprises se produit toutes les 14 secondes – ce qui représente un coût global de plusieurs milliards de dollars pour les organisations.

C'est la raison pour laquelle il est important de garder ces cinq considérations à l'esprit lors de l'élaboration d'une stratégie de prévention, détection et réaction vis-à-vis d'une attaque de ransomware visant les sauvegardes.

1 – Les attaques par ransomware font des sauvegardes une responsabilité

Les cybercriminels ciblent désormais avec insistance les sauvegardes pour détenir un contrôle total sur les données, ou pire, pour détruire l'unique plan de repli des entreprises pour assurer leur continuité d'affaires. Les attaques les plus sophistiquées s'insinuent au sein d'un environnement primaire à partir d'un terminal et se dirigent directement vers les sauvegardes, où 80 % des données d'entreprise sont désormais stockées, supprimant ou compromettant tout pour ensuite revenir vers l'environnement de production et s'y attaquer.

Pour empêcher les ransomware d'attaquer l'environnement de sauvegarde, il est nécessaire d'établir une défense à plusieurs niveaux. Les sauvegardes d'origine doivent être conservées dans un état immuable (lecture seule) et ne doivent jamais être rendues accessibles pour éviter qu'elles ne soient montées par un système externe. De plus, l'authentification multifacteur (MFA = multi-factor authentication) et l'écriture en lecture unique (WORM = write once read many) pour

l’instantané sont des fonctions indispensables.

2 – L’extension de la surface d’attaque expose les sauvegardes aux attaques de ransomware

IDC estime que 175 zettaoctets de données existeront d’ici 2025. Cette croissance et la fragmentation massive des données – à savoir la prolifération croissante des données de sauvegarde dans différents silos tentaculaires – se sont combinées pour élargir la surface d’attaque des entreprises. En conséquence, les données de sauvegarde sont devenues plus accessibles aux cybercriminels.

Pour empêcher le succès des tentatives d’attaque de type ransomware, il faut d’abord réduire la surface d’attaque de l’entreprise et comprendre à la fois le type de données hébergées et déterminer leur emplacement. Une solution unifiée pour la gouvernance de l’infrastructure, des flux et des sites de sauvegarde protège les entreprises contre les malwares en éliminant la fragmentation massive des données.

3 – Des attaques sur les sauvegardes facilitées par une surveillance intermittente

Les cybermenaces ne proviennent pas toujours de l’extérieur de l’organisation ; elles peuvent aussi provenir de l’interne. Il peut par exemple s’agir d’un employé mécontent qui essaie de modifier ou de supprimer un grand volume de données. S’appuyer exclusivement sur des données de sauvegarde pour détecter de tels comportements est insuffisant.
C’est pourquoi l’organisation doit être en mesure de détecter une attaque en temps réel.

Il faut donc disposer d’une solution capable de surveiller, de détecter automatiquement des taux de changements et de générer des alertes à partir d’une analyse permanente des fichiers et des journaux d’audit, sans qu’il soit nécessaire d’y prêter une attention particulière.
La solution de sauvegarde adéquate protégera votre entreprise contre les cyberattaques de manière automatisée chaque seconde, chaque jour.

4 – Des points d'entrée dans les clouds publics pour les criminels

Le cloud devient un point d'entrée pour les cyber-attaquants, ce qui met également données de sauvegarde en danger. McAfee estime en effet qu'un utilisateur de cloud public sur quatre a été victime de vol de données. Il faut retenir que les données dans le cloud ne sont pas à l'abri des ransomwares. Le cloud public peut s'avérer rentable pour les stratégies de sauvegarde, mais il rime également avec une visibilité globale réduite sur les données.

Pour garder une longueur d'avance sur les ransomwares, il est essentiel de disposer d'une solution de sauvegarde et de restauration qui offre un tableau de bord unique et centralisé. Être capable de voir, d'administrer et d'agir rapidement sur les données de sauvegarde – qu'elles résident sur site ou dans les clouds publics – contribue à protéger l'entreprise des attaques de ransomware.

5 – Les longs cycles de sauvegarde et de restauration ajoutent à la pénibilité de la demande de rançon

Si votre entreprise s'appuie sur des sauvegardes complètes synthétiques et si elle est victime d'une attaque de ransomware, les responsables informatiques peuvent consacrer des jours (voire des semaines !) à restaurer les systèmes. Un récent rapport du Ponemon Institute évalue à 5 millions de dollars le coût moyen d'une attaque de ransomware en raison principalement de la perte de productivité, de la panne système et du vol d'informations.

Il est essentiel que la solution de sauvegarde et de restauration permette de répondre rapidement aux attaques, de localiser et de supprimer rapidement les fichiers infectés où qu'ils se trouvent dans l'infrastructure de gestion des données – y compris les clouds publics. Il faut qu'elle dispose également de capacités de restauration de masse instantanée de manière à restaurer des centaines de machines virtuelles instantanément, à l'échelle et à n'importe quel moment du passé.

Prévenir, détecter et réagir rapidement aux menaces de ransomware

Les organisations veulent n'avoir à déplorer aucune perte de données à la suite de cyberattaques et par ailleurs souhaitent pouvoir refuser les demandes de paiement de la rançon en toute sérénité. Pour cela, il leur faut protéger leurs données en adoptant une approche complète de prévention, de détection et de réponse aux attaques.