VEEAM

1 + 1 = 3
HPE + Veeam
Better Together

Descriptif de solution

Protégez vos données contre les menaces par ransomware

Cette meilleure pratique de disponibilité des données est conçue pour assurer que toutes les entreprises se préparent efficacement à éviter les pertes de données et les temps d'arrêt potentiels dus aux attaques de ransomware. En suivant les meilleures pratiques de l'industrie, les responsables IT peuvent éviter de payer les rançons demandées et mettre en place une solution de disponibilité des données en béton pour leurs opérations quotidiennes en tirant parti de HPE et des logiciels Veeam®.

La prolifération des attaques par ransomware

Les attaques par ransomware continuent à se généraliser dans de nombreux secteurs en exploitant les exigences réglementaires et de conformité, les réseaux vulnérables et les mauvaises pratiques de sauvegarde. Alors que la menace s'amplifie, de plus en plus de secteurs d'activités et d'entreprise sont pris pour cible. Même avec des solutions et pratiques de sécurité renforcées, les réseaux sont régulièrement pénétrés. Selon l'Institute for Critical Infrastructure Technology (ICIT), 2016 et 2017 seront des années au cours desquelles les ransomwares feront des ravages dans les entreprises. Les menaces de ransomware sont en hausse avec « presque 40 % d'entreprises attaquées ».[1]

Risques métier et informatiques des ransomware

Les attaques par ransomware constituent plus que des risques de sécurité. Les entreprises victimes des ransomwares se trouvent confrontées à des problèmes techniques et financiers ainsi qu'à des dommages affectant la marque dont elles pourraient ne jamais se remettre.

Effondrement financier

Le montant de la rançon, la perte d'un temps IT précieux et le temps d'arrêt potentiel des applications stratégiques peuvent causer un préjudice permanent à l'activité.

Revers informatiques

Les pirates gardent le contrôle et l'accès du réseau de la victime pour de futures attaques et extorsions possibles. Les responsables IT font face à des menaces répétées et consacrent davantage de ressources à la prévention des ransomwares, volant du temps aux pratiques IT cruciales essentielles à l'activité.

Une image de marque endommagée

De nombreuses entreprises ne signalent pas les attaques par ransomware afin d'éviter de compromettre leur réputation, de perdre des clients et des parts de marché. Pourtant, les sociétés qui paient des rançons ou ne sauvegardent pas leurs données sont finalement les victimes d'attaques encore plus spectaculaires qui causent des dommages sévères à leur identité de marque et à leur réputation sur le marché.

Étude de cas : une défense efficace contre les ransomwares au moyen de Veeam

En Angleterre, la Bedford School a été victime d'attaques par ransomware par l'intermédiaire d'un virus CryptoLocker qui a infecté l'ordinateur d'un membre de la faculté et chiffré tous les fichiers. L'école manquait des ressources nécessaires pour payer l'énorme rançon exigée et ne pouvait se permettre le temps d'arrêt supplémentaire de ses réseaux.

L'équipe informatique de Bedford avait suivi la règle de sauvegarde du 3-2-1. Elle n'a payé aucune rançon et n'a perdu aucune capacité réseau. Veeam l'a aidée à restaurer rapidement chaque fichier chiffré.

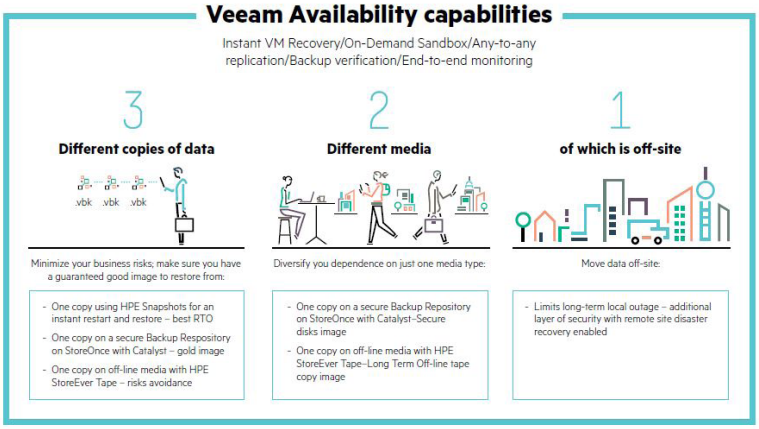
« Aucune méthode ou aucun outil ne protégera entièrement votre entreprise d'une attaque par ransomware. Mais les plans d'urgence et d'assainissement sont essentiels à la reprise et à la continuité de l'activité — et ces plans doivent être testés régulièrement. »

— James Trainor,
Ancien directeur adjoint
de la cyberdivision du FBI

Cette citation permet aux utilisateurs de comprendre que les ransomwares ne constituent qu'une partie du paysage de menaces qui pénétreront finalement dans leur réseau. La meilleure solution consiste à protéger la cible de ces attaques : leurs données.
fbi.gov/news/stories/incidents ofransomware-on-the-rise

[1] « Les menaces de ransomware sont en hausse avec "presque 40 % d'entreprises attaquées". » The Guardian, août 2016

Hewlett Packard
Enterprise



La solution anti-ransomware de HPE et Veeam

Cette solution de disponibilité des données de Veeam et HPE est conçue pour combattre toute tentative d'attaque par ransomware par les pirates. En suivant la meilleure pratique du 3-2-1 de Veeam, les entreprises peuvent s'assurer de l'intégrité et de la disponibilité de leurs données. Le diagramme ci-dessus illustre la règle du 3-2-1 ainsi que les principales recommandations en vigueur dans le secteur d'activité.

Tirer parti de la règle du 3-2-1 pour lutter contre les ransomwares

L'objectif de la règle du 3-2-1 est de fournir aux clients une solution de protection des données qui maximise le temps de fonctionnement des applications et la disponibilité des données. En exécutant correctement les meilleures pratiques de la sauvegarde 3-2-1, les responsables IT peuvent protéger leurs données. Voici nos directives :

- Maintenez 3 (trois) copies de vos données — la donnée primaire et deux copies — pour éviter de perdre des données à cause d'une sauvegarde endommagée.
- Stockez ces copies de sauvegarde sur 2 (deux) types de supports différents tels que bande, disque, stockage secondaire ou cloud.
- Conservez 1 (une) copie hors site — sur bande ou dans le cloud — pour parer aux aléas locaux ou aux infections par ransomware à l'intérieur du réseau.

Synthèse

La solution de disponibilité des données est une solution entièrement intégrée composée des technologies existantes. Elle permet non seulement aux entreprises de rétablir rapidement une exploitation normale après les attaques par ransomware, mais elle offre aussi une solution de disponibilité des données de niveau entreprise pour les opérations quotidiennes. Cette solution de meilleure pratique est à la fois flexible et abordable et peut être rapidement mise en œuvre par un partenaire Veeam certifié.

En savoir plus :

Comment suivre la règle du 3-2-1 de la sauvegarde avec Veeam Backup & Replication™ sur le blog.

a00000445enw, janvier 2017

Aperçu des solutions Veeam et HPE

Les solutions phares du marché de Veeam et HPE offrent aux entreprises de toutes tailles tous les outils pour combattre les attaques et protéger leurs données.

- Restauration rapide des données // Les snapshots de baie de stockage HPE et la restauration rapide et granulaire des machines virtuelles (VMs) permettent d'outrepasser les bases de données, applications, fichiers et systèmes d'exploitation (SE) chiffrés par les ransomwares. Effectuez des restaurations rapides et évitez les temps d'arrêt des applications grâce à une intégration éprouvée à HPE 3PAR StoreServ, Store Virtual, StoreOnce et StoreOnce Catalyst.
- Verrouillage des infrastructures // Les ransomwares ne peuvent infecter ce qu'ils ne voient pas. HPE le permet grâce à l'intégration à StoreOnce Catalyst qui rend les images de sauvegarde invisibles aux ransomwares et la restauration possible. Une protection supplémentaire est offerte par la bande hors ligne et les copies asynchrones répliquées à distance.
- Environnement de test // Testez et supprimez les objets vérolés rapidement avant de restaurer vos VMs en production avec Veeam On-Demand Sandbox™ et Veeam SureBackup.
- Facilité d'utilisation // Tirez parti de l'audit des sauvegardes intégré pour vous assurer que vos VMs critiques sont protégées par l'outil de monitoring, de reporting et de capacity planning de Veeam ONE™.

Ces capacités sont disponibles en standard avec l'intégration de Veeam Availability Suite™ et des stockages HP. Cette solution ne nécessite aucun script spécial et tire parti des produits standards de HPE et de Veeam.

Hewlett Packard
Enterprise

En savoir plus :