rubrik

Langs Building Supplies stoppe une attaque de ransomware grâce à une solution de sauvegarde nouvelle génération

RÉSULTATS

- 25 minutes pour écrire un script de restauration des fichiers sur la machine virtuelle à partir du snapshot le plus récent
- 1 heure pour confiner la menace et reprendre des activités normales
- Aucune donnée perdue

LES DÉFIS

- Attaque de ransomware sur le système via un lien envoyé par e-mail
- Un serveur de fichiers de production infecté par CryptoLocker
- 15 000 fichiers chiffrés

LA SOLUTION

- Architecture API-first
- Recherche de fichiers globale et en temps réel
- Gestion des données convergée pour la sauvegarde et la restauration

« Disposer d'une solution de gestion optimale me permet de réaliser mes tâches quotidiennes sans m'inquiéter de perdre des données. Je sais que tout est sous contrôle », explique Matthew Day, responsable TCI et support chez Langs Building Supplies, un fabricant et fournisseur leader de produits pour le secteur de la construction basé à Stapylton, dans l'État du Queensland en Australie. Son entreprise a récemment été frappée par une attaque de ransomware. Grâce à l'efficacité de son infrastructure de sauvegarde, elle a su déjouer la menace et restaurer ses données sans payer aucune rançon.

LA MENACE CROISSANCE DU RANSOMWARE

Le ransomware est un type spécial de malware. Son principe est le suivant : un pirate retient les données des utilisateurs en otage jusqu'à ce qu'une rançon lui soit versée. Plusieurs formes de ransomware exploitent une cryptographie forte pour chiffrer les données de la victime, via une clé de chiffrement connue uniquement par le pirate. Après un délai imparti, le pirate supprime la clé de chiffrement et les données de la victime sont ainsi perdues à jamais. Cependant, même si la victime paie le pirate avant ce délai, ce dernier n'a aucune obligation de fournir la clé de chiffrement à la victime. Le nombre d'attaques de ransomware augmente de façon exponentielle. Depuis le 1er janvier, on rapporte en moyenne plus de 4 000 attaques de ransomware par jour, soit une augmentation de 300 % par rapport aux 1 000 attaques par jour en 2015[1]. Les victimes sont habituellement issues de secteurs où l'ordinateur est utilisé pour des activités critiques. Elles ne sont généralement pas dotées des toutes dernières technologies sur l'ensemble du système et finissent par payer la rançon afin de récupérer l'accès à leurs données. Par le passé, il n'y avait aucun moyen efficace de contourner ces attaques alors que leur fréquence ne fait qu'augmenter.

EXPÉRIENCE DE LANGS BUILDING SUPPLIES

Début juin, après qu'un salarié de Langs Building Supplies ait cliqué sur le lien d'un e-mail, un serveur de fichiers de production s'est trouvé infecté par CryptoLocker. L'équipe informatique a été avertie 10 minutes après le début de l'attaque, grâce à des outils de surveillance étudiant les taux de modifications élevées sur les structures des données. De ce fait, seulement 15 000 fichiers sur plusieurs millions ont été renommés en « .encrypted », une extension de fichier qui empêche l'accès auxdits fichiers sans la clé du pirate.

ATTAQUE DE RANSOMWARE CONFINÉE GRÂCE À UNE SOLUTION DE GESTION DE DONNÉES NOUVELLE GÉNÉRATION

Après avoir reçu l'alerte du système de surveillance, M. Day a pu isoler le bureau VDI infecté et ainsi empêcher l'attaque de s'étendre au reste de l'infrastructure de l'entreprise. « Nous avons pu écrire un script pour restaurer sur la machine virtuelle la version la plus récente des fichiers, conservée dans notre système de sauvegarde. Environ une heure après, tous nos fichiers étaient de nouveau disponibles sur le serveur. Aucune perte à déplorer », raconte M. Day.

[1] Source : rapport sur les menaces de sécurité Internet de Symantec, 2016

Certains aspects clés de la solution de gestion de données de Langs Building Supplies ont permis d'éviter une situation potentiellement préjudiciable :

1. **Technologie moderne :** « Même si elle nécessite encore votre intervention sur certains points, une technologie moderne fonctionne de la manière et aux moments que vous avez choisis. Notre appliance de sauvegarde convergée est d'une réelle aide pour la gestion de nos données. Elle gère et protège facilement nos machines virtuelles, applique nos politiques de protection aussi globalement ou granulairement que nous le souhaitons et recherche parmi nos données protégées pour restaurer des machines virtuelles, des objets ou des fichiers spécifiques. »

2. **Interface de programmation et API :** « La recherche d'un fichier çà et là via l'IU est simple. Par contre, rechercher des milliers de fichiers peut vite devenir chronophage. Grâce à l'interface de programmation qui permet d'élaborer des flux de travail personnalisés pour des services tiers, nous automatisons et orchestrons encore davantage la gestion de notre environnement. Grâce aux API RESTful de Rubrik, nous avons pu écrire un script pour rechercher et restaurer les fichiers infectés, et ainsi éviter d'avoir à faire cette pénible exploration et récupération à la main. »

3. **Incréments perpétuels :** « Grâce à l'approche d'incréments perpétuels, nous pouvons faire des snapshots plus souvent puisque moins de données doivent être déplacées vers notre système de sauvegarde. Cela nous a permis de découvrir le moment précis auquel nos fichiers ont été renommés et de récupérer la version juste avant que l'attaque ne se produise. »

4. **Restauration rapide :** restaurez rapidement vos machines virtuelles et applications en montant directement sur Rubrik. M. Day explique : « Nos serveurs de production ont été remis en état de fonctionnement en une heure ».

« Grâce à Rubrik, nous avons évité tout dommage financier potentiel à long terme. Les systèmes en place ont prouvé qu'ils pouvaient parer à ces éventualités. Il faut néanmoins former les utilisateurs, établir des politiques de groupe et aussi disposer de disques de sauvegarde déconnectés, gérés par des systèmes parfaitement séparés de votre environnement de production afin qu'aucune attaque ne puisse les atteindre. C'est précisément là que Rubrik entre en jeu », détaille M. Day.

La meilleure façon de limiter une attaque de ransomware est d'instaurer une défense en profondeur, en alliant la sécurité à la protection des données. Comme M. Day l'explique, « il y aura toujours des failles. C'est pourquoi vous avez besoin d'une gestion de données robuste. Il faut toujours aller de l'avant et non pas s'arrêter sur le passé. Puisque nous avions anticipé cette défaillance, la menace n'a eu l'effet que d'un inconvénient mineur. Le jour suivant, c'était comme s'il ne s'était rien passé ».

LANGS BUILDING SUPPLIES

« Disposer d'une solution de gestion optimale me permet de réaliser mes tâches quotidiennes sans m'inquiéter de perdre des données. Je sais que tout est sous contrôle. »

Matthew Day, responsable TCI et support chez Langs Building Supplies

rubrik

Siège global
299 South California Ave. #250
Palo Alto, CA 94306
États-Unis

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik propose la plateforme de Cloud Data Management, leader du secteur, qui renforce la protection, la gestion et la sécurisation des données des entreprises, partout. Les entreprises qui figurent au classement Fortune 500 font confiance à la plateforme unique Rubrik pour la protection, la recherche et l'analyse des données, mais aussi l'archivage et la gestion de la conformité, ou encore la gestion de la copie des données. C'est ainsi qu'elles peuvent bénéficier d'un accès instantané aux données et d'un coût total de possession (TCO) réduit de moitié, mais aussi consacrer infiniment moins de temps à la gestion quotidienne (de l'ordre de quelques minutes).