COHESITY

FICHE INFO

5 moyens par lesquels les ransomwares rendent vos sauvegardes inutiles

Présentation

Votre solution de sauvegarde et restauration doit protéger votre organisation, or les programmes malveillants sophistiqués tels que Locky et Crypto en ont désormais après vos données sauvegardées. Les attaques par ransomware, plus fréquentes et plus répandues aujourd'hui, sont aussi plus précises. Elles ne se contentent pas de verrouiller vos données et de les conserver jusqu'à ce que vous payiez une rançon, mais compromettent le système même conçu pour les protéger. Selon Cybersecurity Ventures, les ransomwares étaient en passe d'attaquer une entreprise toutes les 11 secondes d'ici la fin 2021. C'est pourquoi il est important de garder ces cinq conseils à l'esprit lorsque vous concevez votre stratégie de protection des données sauvegardées, afin d'éviter le pire, et de répondre rapidement en cas d'attaque par ransomware.

Les ransomwares en chiffres

- Une attaque par ransomware toutes les 11 secondes[1]
- 10,5 milliards de dollars de préjudices d'ici 2025[1]
- Une hausse de 1 070 % des attaques par ransomware entre juillet 2020 et juin 2021[2]
- 10 à 15 fois plus de dommages financiers que de demandes de rançon[3]

1. Les attaques par ransomware sophistiquées font de votre police d'assurance (vos sauvegardes), une responsabilité

Les cybercriminels s'attaquent maintenant de façon agressive aux données sauvegardées, et ce, dans le but de prendre le plein contrôle, ou pire, de détruire ce que vous considérez depuis longtemps comme votre assurance de continuité d'activité. Leurs attaques plus élaborées pénètrent dans un environnement primaire à partir d'un point d'accès et visent directement vos sauvegardes, qui stockent aujourd'hui 80 % des données d'entreprise, en supprimant ou en compromettant tout ce qui s'y trouve, avant de prendre le contrôle de l'environnement de production. Vous devez vous doter d'une défense multicouche pour protéger vos sauvegardes des ransomwares. Les données sauvegardées originales doivent être inaltérables et la copie « gold » des données ne doit jamais être montée par un système externe. Des règles telles que l'écriture non-réinscriptible (WORM), le chiffrement de données, la tolérance aux pannes intégrée et une isolation des données moderne incorporées à votre solution de sauvegarde procurent une couche supplémentaire de protection contre les attaque par ransomware.

> Les développeurs de ransomware sont conscients que les sauvegardes constituent une défense efficace et modifient leurs programmes malveillants pour les localiser et les éliminer.
>
> **CSO Magazine**

2. La multiplication des surfaces d'attaque expose les sauvegardes aux attaques par ransomware

IDC rapporte que 64,2 ZB de données ont été créées ou copiées en 2020, et estime que plus de 175 zettabytes de données existeront d'ici 2025. Pour protéger des données de plus en plus volumineuses, les entreprises ont toujours eu recours à de multiples produits ponctuels (par exemple, des serveurs de médias et des serveurs maîtres, un stockage cible, etc.) pour la sauvegarde, et comme ces produits créent des silos tentaculaires, occupant les sites et les multiclouds, ils élargissent la surface d'attaque de votre organisation, rendant vos données sauvegardées plus accessibles aux cybercriminels. Pour prévenir l'intrusion des ransomwares, il est essentiel de commencer par réduire la surface d'attaque de votre entreprise, et se pencher sur la fragmentation massive des données. Il vous faut aussi savoir quelles sont ces données et où elles sont localisées. Une solution unifiée qui renforce la visibilité dans l'ensemble de votre infrastructure, vos charges de travail et vos emplacements de stockage arme plus efficacement votre organisation contre les ransomware.

[1] Cybersecurity Ventures

[2] Rapport d'enquête Fortinet sur les ransomware 2021

[3] Gartner : Comment se préparer aux attaques par ransomwares, novembre 2020

3. Les informations d'identification de l'utilisateur compromises sont une aubaine pour le ransomware qui peut alors se multiplier

Les identifiants volés sont le Graal pour les assaillant par ransomware car ils procurent un accès permanent à toute une partie d'un environnement informatique, y compris aux sauvegardes, et permettent aux cybercriminels d'exfiltrer les données pour en tirer encore plus profit. Selon le Rapport Verizon d'enquêtes sur les violations de données de 2021, les informations d'identification compromises étaient le type de données le plus courant dans les violations intentionnelles cette année, impliquées dans 61 % des violations. Les organisations qui s'appuient sur un système de sauvegarde moderne avec un contrôle strict des accès utilisateurs, incluant un accès basé sur les rôles (RBAC), une authentification multifactorielle (MFA) et des capacités de surveillance continue, peuvent plus facilement contrer les attaques par ransomware, évitant les temps d'arrêt et les impacts négatifs sur la productivité qui vont avec.

4. Le manque de visibilité et de détection précoce donne aux assaillants une longueur d'avance

Les attaquants par ransomware prospèrent grâce aux données sombres. Ils peuvent verrouiller les sauvegardes et s'attaquer aux systèmes de production pour subtiliser et vendre vos données sur le dark web. La détection précoce grâce à une solution de gestion des données de nouvelle génération est un bon départ pour ralentir les malfaiteurs. En revanche, pour découvrir les attaques par ransomware par exfiltrations, il vous faudra une détection en temps quasi réel, qui utilise l'intelligence artificielle et le Machine Learning (IA / ML). Un système automatisé, qui intègre des alertes, permet d'assurer une détection plus rapide des attaques.

5. La longueur des cycles de restauration aggrave vos problèmes liés aux ransomwares

Si votre entreprise s'appuie sur des produits d'ancienne génération qui nécessitent une sauvegarde synthétique complète et qu'elle est victime d'une attaque par ransomware, votre équipe informatique peut passer des jours (voire des semaines !) en mode restauration. Un récent rapport du Ponemon Institute estime le coût moyen d'une seule attaque par ransomware à 5 millions de dollars, principalement en raison de la perte de productivité, des temps d'arrêt des systèmes et du vol d'informations. Vous avez besoin d'une solution de sauvegarde et restauration qui répond rapidement aux attaques et vous permet de localiser une copie propre de votre fichier dans l'ensemble de votre empreinte de données, y compris dans les clouds publics. Vous avez également besoin d'une capacité de restauration massive instantanée pour restaurer des centaines de machines virtuelles, des bases de données et un grand volume de données non-structurées instantanément, à n'importe quel point dans le temps.

Mettez fin à la cyber-extorsion, et défendez vos données contre les ransomwares

Si vous voulez réduire votre exposition aux cyber-risques et avoir la confiance nécessaire pour refuser les demandes de paiement des ransomwares, faites en sorte que vos sauvegardes et vos solutions de gestion des données soient cyber-résilientes. Seule une approche globale de défense contre les ransomwares inclut la protection de vos sauvegardes contre les menaces, l'arrêt des intrusions avec une visibilité complète, et une détection précoce ainsi que la réduction des temps d'arrêt et la perte de données avec une restauration rapide, propre et à grande échelle.

Téléchargez le livre électronique ici pour en savoir plus sur la défense de vos données.

COHESITY

Cohesity.com | +1 855 926 4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110, États-Unis

9100003-006-FR 1-2022