5 types d'attaques de ransomware qui touchent la sauvegarde… et comment les éviter

Les solutions de sauvegarde et de récupération sont conçues pour protéger votre organisation, mais les programmes malveillants sophistiqués tels que Locky et Crypto en ont désormais après vos données de sauvegarde. Ce n'est pas surprenant quand on connaît l'augmentation de la fréquence et de l'étendue des attaques de ransomware. Le premier paiement de ransomware, aux alentours de 1989, a ouvert la voie aux pirates du monde entier qui ont commencé à verrouiller les données de cibles peu méfiantes et à les séquestrer jusqu'au versement de la rançon. Si l'on en croit les analystes, une attaque de ransomware a lieu toutes les 14 secondes sur une entreprise, ce qui coûte des milliards aux organisations mondiales. C'est pourquoi il est important de garder ces cinq conseils à l'esprit lorsque vous concevez votre stratégie de prévention, de détection et de réponse rapide aux attaques qui touchent vos sauvegardes :

Les ransomware en chiffres

- Une attaque toutes les 14 secondes
- Croissance de 700 % depuis 2016
- 35 % des pirates sont payés
- 2 milliards de dollars de pertes financières
- 11 milliards de dollars de pertes en considérant l'aspect financier, la productivité et les temps d'arrêt

1. Les attaques de ransomware sophistiqués font de votre assurance (vos sauvegardes) une responsabilité

Les cybercriminels ont développé des tactiques agressives pour les données de sauvegarde des clichés instantanés, 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 depuis un point de terminaison et visent directement vos sauvegardes, qui stockent aujourd'hui 80 % des données d'entreprise, y supprimant ou corrompant tout, avant de passer à votre environnement de production. Vous avez besoin d'une défense multicouche pour protéger vos sauvegardes. Les tâches de sauvegarde originales ne doivent pas être modifiables ni accessibles afin qu'elles ne soient pas montées par un système externe. Par ailleurs, l'authentification multifacteur (MFA) et les capacités de disques non réinscriptibles (WORM) pour la capture sont des fonctionnalités indispensables.

> "
>
> 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. Multiplier les points d'accès expose les sauvegardes aux attaques

La croissance exponentielle des données (IDC estime qu'il en existera plus de 175 zettaoctets d'ici 2025) et la fragmentation de masse des données (la prolifération des données de sauvegarde dans des silos de plus en plus étendus) ont augmenté les points d'attaque des organisations. En conséquence, vos données de sauvegarde sont plus accessibles pour les cybercriminels. Empêcher la réussite des ransomware passe en premier lieu par la réduction du nombre de points d'accès de votre entreprise et la connaissance de vos données et de leur lieu de stockage. En utilisant une solution unifiée pour connecter l'infrastructure, les charges de travail et les emplacements de stockage, vous armez votre organisation contre les ransomware en éliminant la fragmentation de masse des données.

3. Facilitation des attaques aux sauvegardes par la surveillance intermittente

Les cybermenaces ne proviennent pas toujours de l'extérieur d'une organisation, elles peuvent également être lancées de l'intérieur. Imaginez un employé mécontent qui essaie de modifier ou de supprimer un grand ensemble de données. Se reposer exclusivement sur les taux de modification des données de sauvegarde ingérées ne suffit pas pour détecter ce genre de comportements. Votre organisation doit être en mesure de détecter une attaque en temps réel. Vous avez besoin d'une solution qui puisse surveiller et détecter de plus faibles taux de modification en continu en analysant les fichiers et les journaux d'audit, même lorsque vous n'y consacrez pas toute votre attention. La solution de sauvegarde adéquate protègera votre organisation des cyberattaques en permanence.

4. Le cloud public offre un point d'entrée pour les cybercriminels

Le cloud devient rapidement un point d'entrée pour les cyberattaques, ce qui menace vos données de sauvegarde. En fait, McAfee estime qu'un utilisateur de cloud public sur quatre a déjà expérimenté un vol de données. En d'autres termes, les données du cloud ne sont pas immunisées contre les ransomware. Le cloud public peut s'avérer économique pour les sauvegardes, mais il réduit dans le même temps la visibilité sur les données. Pour garder une longueur d'avance sur les ransomware, il faut se munir d'une solution de sauvegarde et de récupération qui offre un tableau de bord unique. Pouvoir consulter et gérer vos données de sauvegarde et prendre des mesures rapides les concernant (qu'il s'agisse de données locales ou dans le cloud public) vous aidera à protéger votre organisation des attaques de ransomware.

5. Des cycles de sauvegarde et de récupération lentes aggravent vos problèmes de ransomware

Si votre entreprise repose sur une sauvegarde d'ancienne génération qui requiert une sauvegarde complète synthétique et que cette dernière est victime d'une attaque de ransomware, votre équipe informatique peut passer plusieurs jours (voire semaines) en mode récupération. Un récent rapport du Ponemon Institute estime le coût moyen d'une seule attaque de 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 de récupération qui réponde rapidement aux attaques et vous permette de localiser et de supprimer les fichiers infectés dans l'ensemble de votre empreinte de données, y compris dans les clouds publics. Il faut également des capacités de restauration de masse instantanée qui permette la récupération de centaines de machines virtuelles en un instant, à l'échelle et à n'importe quel point dans le temps.

Prévenir, détecter et répondre rapidement aux menaces de ransomware

Les organisations telles que la vôtre ne souhaitent perdre aucune donnée en cas de cyberattaque et veulent pouvoir refuser le paiement d'une rançon en toute confiance. Protégez vos données avec une approche complète pour prévenir et détecter les attaques de ransomware et y répondre rapidement.

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

COHESITY