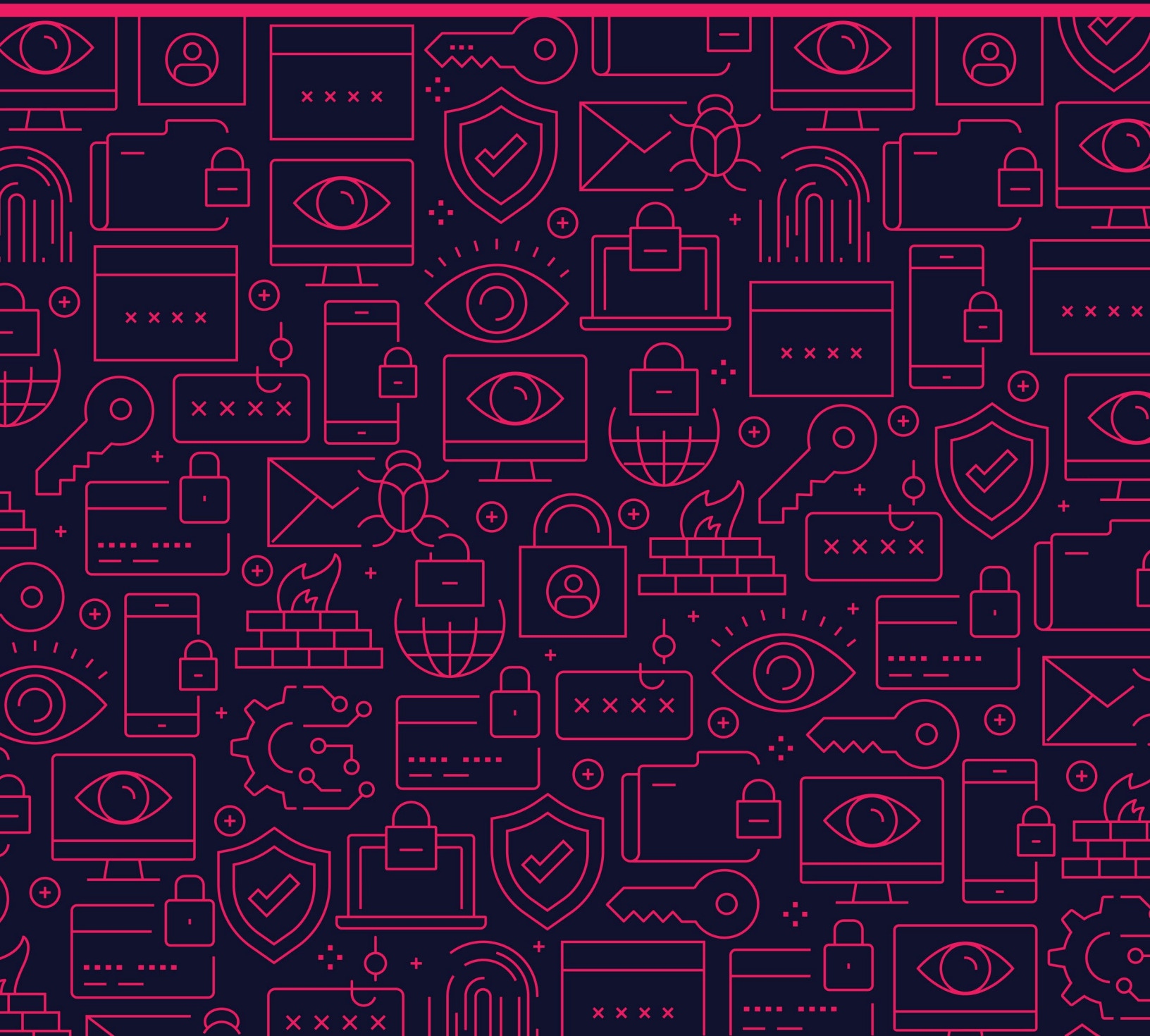
rubrik

E-BOOK

Comment élaborer un plan de remédiation efficace



Sommaire

Introduction

À l'heure où les entreprises cherchent de plus en plus à s'orienter vers des « business models » axés sur les données pour gagner en agilité, les données tendent à devenir une cible extrêmement lucrative pour les cyberattaques. Malgré le déploiement de mécanismes de défense, les attaques ransomware ne cessent de s'intensifier et parviennent à toucher de plus en plus de données d'entreprise.[1]

Les sauvegardes représentent l'un des principaux barrages, pour ne pas dire le plus important, contre le ransomware. Mais une fois corrompues, ces sauvegardes peuvent se retourner contre vous. **Les attaques de ransomware les plus évoluées ciblent désormais les sauvegardes. Leur but : les modifier voire les supprimer purement et simplement pour mettre à terre la dernière ligne de défense et augmenter les chances d'en tirer une rançon.** Malgré une forte communication sur le sujet afin de dissuader les victimes de payer des rançons, le FBI estime que les auteurs de ces attaques pourraient en dégager plus d'un milliard de dollars de bénéfices.[2]

Mais si le paiement de la rançon apparaît de toute évidence comme une mauvaise option, pourquoi les entreprises persistent-elles à suivre cette ligne stratégique ? Tout simplement parce qu'il peut être long et difficile de se sortir d'une attaque, si tant est qu'elles disposent encore de sauvegardes à partir desquelles restaurer leurs données. Qui plus est, les entreprises manquent de visibilité sur l'étendue des dommages, ce qui les amène à restaurer l'ensemble de leur environnement au lieu de se concentrer sur la récupération des données affectées. Une stratégie qui, à terme, ne peut qu'augmenter les pertes de données.

Les entreprises ne devraient pas avoir à payer de rançon et à subir une interruption d'activité coûteuse. Elles devraient pouvoir s'appuyer sur des sauvegardes fiables pour restaurer rapidement leurs données en limitant autant que possible les pertes de données et les impacts financiers. C'est pourquoi il est recommandé aux équipes IT de développer et tester en amont un plan de remédiation robuste.

Dans cet e-book, vous allez apprendre à repérer les fonctionnalités à privilégier dans une solution de sauvegarde et de restauration, et à élaborer un plan de remédiation efficace qui vous aidera à réagir rapidement face à une cyberattaque sans avoir à payer de rançon.

118% **Augmentation du nombre d'attaques de ransomware (1e trim. 2019)***

Les programmes de ransomware les plus sophistiqués ciblent désormais les fichiers de sauvegarde

Le FBI estime que les cybercriminels gagneront plus d'un milliard de dollars de rançons**

Le ransomware se propage par toutes sortes de mécanismes, notamment les e-mails de phishing et exploit kits

* McAfee Labs Threats Report, août 2019
** Fall 2019 OCR Cybersecurity Newsletter - The U.S. Department of Health and Human Services

Choisir la bonne solution de sauvegarde et de restauration pour la cyber-résilience

Après une attaque de ransomware, la solution la plus sûre et la plus fiable consiste à récupérer les fichiers à partir d'un système de sauvegarde. Mais parmi les innombrables éditeurs de protection des données, comment identifier celui qui saura le mieux vous préparer à ce type d'attaque ? Bien qu'il n'existe aucune approche universelle qui convienne à tous les scénarios, on note tout de même certaines fonctionnalités indispensables qu'il serait judicieux de privilégier dans l'élaboration d'un plan de remédiation :

Une restauration instantanée

La restauration est sans doute l'aspect le plus délicat que doivent gérer la plupart des victimes de ransomware. Bien souvent, les entreprises persistent à déployer des restaurations en plusieurs phases qui, en plus d'être complexes et inefficaces, ne font que générer des erreurs et allonger les temps d'interruption. Car plus vous mettez de temps à récupérer d'une attaque, plus elle aura d'incidences sur votre chiffre d'affaires, sur la productivité de vos employés et sur la fidélité de vos clients. Et que vous ayez affaire à un ransomware, à un délit d'initié ou à une attaque commise par un employé peu scrupuleux, ce principe se vérifie pour n'importe quel type d'incident de sécurité.

Pour être véritablement efficace, une solution de sauvegarde et de restauration devrait favoriser une reprise à la fois rapide et fiable. Même en cas de faille de sécurité, vous ne devriez avoir aucun mal à identifier et restaurer la dernière version de vos données, que ce soit dans le cadre d'une restauration totale ou partielle de votre système, pour éviter d'immobiliser vos activités ou de subir de lourdes défaillances système. Les données de sauvegarde devraient être disponibles instantanément et vous permettre de vous relever immédiatement d'une attaque sans avoir à réhydrater vos données. Par ailleurs, le recours à l'automatisation basée sur des API vous confère un maximum de flexibilité au moment de la restauration et peut accélérer vos efforts de recherche et de récupération à grande échelle.

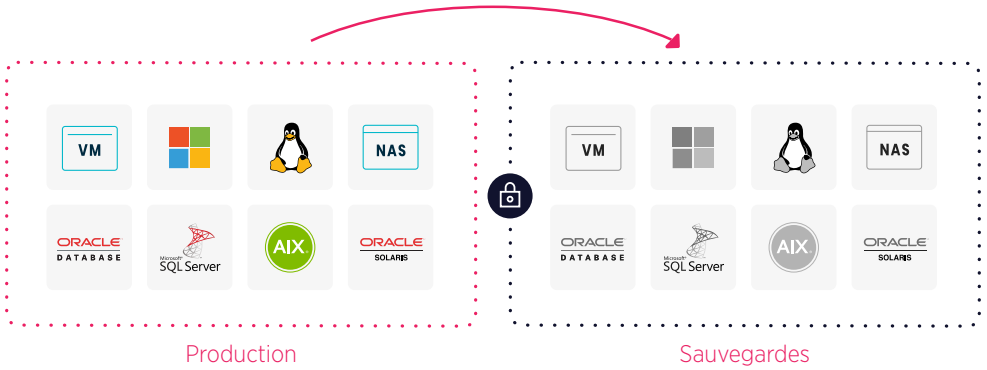
Les bonnes questions à poser aux éditeurs

Êtes-vous capable d'assurer des RTO proches de zéro pour les machines virtuelles, les partages de fichiers et les bases de données ?

Êtes-vous capable de restaurer instantanément les fichiers sans réhydratation des données ?

Un système de fichiers immuable en mode natif

L'une des raisons pour lesquelles les entreprises se révèlent incapables de se relever d'une attaque de ransomware est que leurs sauvegardes elles-mêmes se trouvent corrompues, ce qui oblige les équipes IT soit à payer tout simplement la rançon, soit à lancer une restauration à partir de sauvegardes distantes. Méfiez-vous des éditeurs qui vous conseillent de privilégier les sauvegardes distantes. Cette approche peut impliquer de longues semaines, voire plusieurs mois de restauration et soulever des problèmes d'intégrité des données, ce qui ne fait qu'allonger les RTO. Certains fournisseurs de solutions de sauvegarde recommandent de déployer une restauration isolée en réponse à une attaque de ransomware. Si cette option reste viable, elle n'en reste pas moins lourde sur le plan budgétaire et se révèle difficile à mettre en œuvre en termes de gestion. Voyez cela un peu comme la charge opérationnelle et financière d'une infrastructure de reprise après sinistre.



Les systèmes de fichiers immuables empêchent les hackers d'accéder à vos données ou de les chiffrer.

Mais comment avoir la certitude que vos sauvegardes en ligne ne sont pas corrompues par une attaque de ransomware ? En choisissant simplement un fournisseur de solutions de sauvegarde et de restauration capable de stocker toutes vos données et applications dans un format immuable, qui empêche tout client externe de lire, modifier ou supprimer vos données une fois ingérées. Les données de sauvegarde ne devraient jamais être accessibles en lecture/écriture à un client externe pour la simple raison qu'elles seraient alors exposées au risque d'être corrompues ou simplement supprimées par un hacker.

Les bonnes questions à poser aux éditeurs

Comment pouvez-vous garantir que vos sauvegardes sont capables de résister à une attaque de ransomware ?

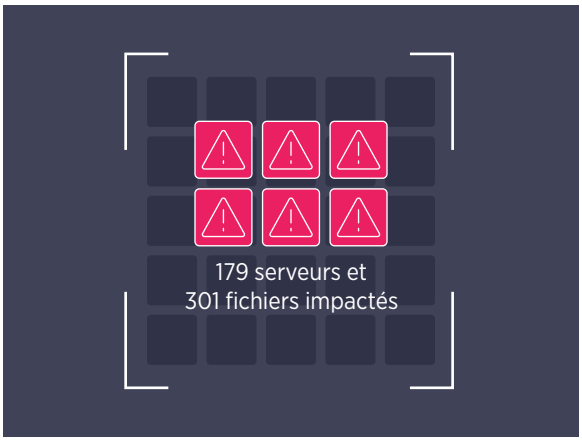
Vos sauvegardes sont-elles stockées dans des formats natifs exposés aux attaques ?

Vos archives de sauvegarde sont-elles adossées à un partage SMB ou NFS ouvert, accessible en lecture/écriture ?

Avez-vous recours à un mécanisme de chiffrement ou d'empreinte digitale pour garantir l'intégrité de chaque sauvegarde ?

Un diagnostic granulaire des impacts

L'exécution d'une restauration ne représente qu'une partie du processus de reprise. Il est souvent plus difficile d'identifier *les applications et les fichiers qu'il vous faut restaurer et de les localiser*. Pour minimiser les pertes de données liées à une attaque de ransomware, les équipes IT se doivent d'en identifier rapidement l'impact. Mais pour évaluer manuellement la surface affectée, elles n'ont généralement d'autre choix que de passer au peigne fin des millions de fichiers pour tenter de mesurer l'étendue de l'attaque. Autant dire que ce processus peut prendre des jours, voire des semaines. Et pour éviter tout retard supplémentaire, la plupart des entreprises finissent par se résoudre à restaurer en masse l'intégralité de leur environnement, y compris les données qui n'ont pas été affectées.



Pour aider les équipes IT à restaurer rapidement leur environnement à un niveau plus granulaire, elles doivent s'orienter vers des technologies capables d'évaluer automatiquement l'impact d'une attaque et de leur procurer une bonne visibilité sur les applications et fichiers qui ont été chiffrés, tout en leur permettant de les localiser. Cette approche limite le risque de perte de données associé à des restaurations massives.

Les bonnes questions à poser aux éditeurs

Avez-vous prévu un système d'alerte pour signaler les cas suspects d'accès ou de chiffrement de fichiers ?

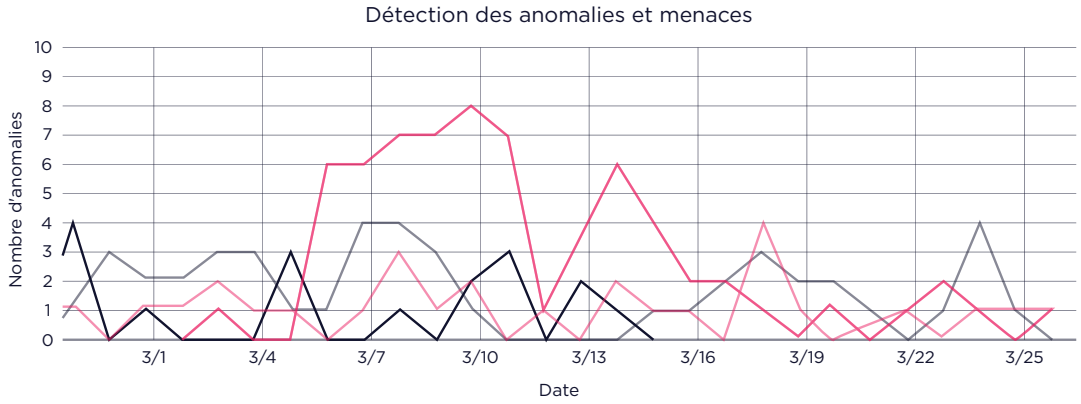
Êtes-vous capable d'identifier les fichiers impactés par une attaque de ransomware ?

Votre système prend-il en charge une restauration de niveau fichier qui cible uniquement les fichiers et données affectés ?

Une défense multicouche associée à des fonctions de détection avancées

Le ransomware devient de plus en plus sophistiqué et, dans ce contexte, même les efforts de prévention les plus démesurés peuvent se révéler insuffisants pour vous rendre totalement invulnérables. Dans son rapport d'enquête sur les violations de données de 2019, Verizon estime que dans 56 % des cas analysés, il a fallu au moins plusieurs mois pour détecter la violation.[3] Toute détection tardive peut impacter directement l'intégrité de vos données de sauvegarde et de restauration.

Les technologies modernes qui reposent sur des modèles de machine learning peuvent vous aider à détecter les menaces grâce à une analyse en profondeur du comportement des contenus et des systèmes de fichiers. Les sauvegardes recèlent une grande richesse de métadonnées qu'il est possible d'analyser en toute sécurité afin de détecter les activités anormales et de générer des alertes. Et pour compléter vos outils de détection et de prévention en temps réel, vous pouvez miser sur des technologies basées sur le machine learning que vous pourrez exploiter comme dernière ligne de défense. Car lorsque le système détecte un comportement suspect, notamment un cas de ransomware, il est préférable que les équipes IT en soient immédiatement informées afin de se pencher sur le problème et d'accélérer si besoin le retour à la normale.



Certains éditeurs utilisent des mécanismes de détection basés sur des signatures, qui comparent les schémas et les séquences à des variantes connues de logiciels malveillants. Mais cette approche n'est pas toujours efficace face à une espèce qui mute aussi facilement que le ransomware. Qui plus est, la détection par signature ne marche que si vous n'êtes pas la première victime de l'attaque, car la plupart des attaques de ransomware utilisent des techniques de morphing et d'obscurcissement du code avec une signature zero-day. L'idéal est donc de se tourner vers un éditeur qui privilégie une détection fondée sur des schémas comportementaux afin de repérer les attaques de ransomware de type zero-day.

Les bonnes questions à poser aux éditeurs

Quelle méthode utilisez-vous pour détecter les attaques de ransomware ?

Votre plateforme exploite-t-elle les technologies de machine learning ?

Autres aspects techniques indispensables pour sécuriser votre architecture

Pour vous protéger comme il se doit contre les ransomwares, les meilleurs éditeurs de solutions de sauvegarde et de restauration optent pour des systèmes qui intègrent des contrôles de sécurité renforcés dans leur conception même. Vous trouverez ici quelques considérations techniques à prendre en compte pour évaluer votre architecture sous-jacente :

- L'accès en lecture/écriture au système de fichiers doit être exclusivement réservé à l'éditeur lui-même, et jamais disponible pour un client externe.
- L'éditeur ne doit jamais exposer de protocoles de stockage standard (de type NFS ou SMB) pour interagir avec le système de fichiers.
- L'éditeur ne doit jamais permettre à des clients externes d'accéder en lecture à des données dans leur format natif.
- L'éditeur doit procéder à des contrôles de validation pour vérifier que les données de sauvegarde ne sont jamais altérées et vous garantir que les données restaurées correspondent exactement au contenu de la copie d'origine.
- Le système de fichiers doit être nativement immuable sans que vous ayez à déployer des efforts de configuration ou d'administration.

Mise en situation réelle et principaux constats

Les études de cas ci-dessous retracent la manière dont des entreprises de tous horizons ont réagi face à des attaques de ransomware. Ces exemples tirés de la vie réelle se révèlent riches d'enseignements et peuvent vous aider à mettre au point une stratégie efficace.

ASL Airlines France élabore une stratégie de défense multiniveau contre le ransomware

ASL Airlines France est une compagnie aérienne spécialisée dans le transport de marchandises et de passagers. Implantée à Tremblay-en-France, elle évolue dans un secteur d'activité fortement ciblé par les ransomwares. Dans un contexte aussi risqué, il est incroyablement difficile pour ASL comme pour les autres compagnies aériennes d'obtenir une véritable cyberassurance. La compagnie aérienne a choisi de déployer Rubrik qui, avec son système de défense multiniveau, lui permet d'accélérer la détection des cyberattaques, d'évaluer les impacts dans le détail et de récupérer plus facilement en cas d'attaque de ransomware. En optant pour cette solution, ASL Airlines est parfaitement positionnée pour protéger ses activités de manière proactive face aux cyberattaques.

L'établissement Kern Medical Center parvient à restaurer rapidement l'intégralité de ses systèmes protégés

Le Kern Medical Center, un grand établissement de santé implanté en Californie, a subi une attaque de ransomware en juin 2019. Les auteurs de l'attaque sont parvenus à infiltrer son environnement avant d'entreprendre de chiffrer ses données de production au point de les rendre inexploitables. L'attaque a été détectée au bout d'une heure, après que les utilisateurs aient commencé à se plaindre de ne plus pouvoir accéder à leurs systèmes. Grâce à la solution Rubrik, l'équipe IT a réussi à restaurer la totalité de ses systèmes affectés en seulement quelques minutes, et en particulier rétablir son très précieux système des dossiers médicaux électroniques. À la suite de l'attaque, le Kern Medical Center a choisi d'intensifier la migration de ses anciens systèmes vers la plateforme Rubrik afin de mieux se préserver des futures attaques potentielles. Dans cette décision, les sauvegardes immuables ont très largement pesé dans la balance.

La municipalité de Durham mise sur des sauvegardes nativement immuables pour accélérer ses capacités de restauration

La ville de Durham a détecté une attaque de ransomware et est parvenue à réagir en un temps record, une capacité de réponse que les dirigeants municipaux attribuent à la solution de sauvegarde de Rubrik. Grâce à ses fonctions d'immuabilité intégrées, ils ont été en mesure de restaurer très rapidement les services essentiels de la ville, notamment l'accessibilité des lignes téléphoniques réservées aux services de police. D'après Kerry Goode, le DSI de Durham, les systèmes stratégiques de la ville et notamment le système de gestion de la paie étaient de nouveau opérationnels dès le début de la semaine.

> **« La ville peut être rassurée sur l'extrême efficacité de nos systèmes de sauvegarde, que l'on doit à leur caractéristique immuable. [Autrement dit] ils sont invulnérables face au ransomware. »**
>
> **Kerry Goode**
> DSI pour la ville de Durham

Conseils à suivre pour survivre à une attaque de ransomware

Tout plan de restauration efficace face aux attaques de ransomware doit chercher à développer la capacité d'identifier rapidement les impacts d'une cyberattaque et de s'en relever. Pour garantir une reprise efficace et faire en sorte que l'entreprise continue d'atteindre ses objectifs après une attaque, les équipes IT doivent planifier et tester rigoureusement leur stratégie de réponse.

Voici quelques mesures que nous vous invitons à suivre si vous êtes frappé de plein fouet par une attaque de ransomware :

- ☐ **Isolez le terminal affecté du réseau.**
  La réussite d'une attaque de ransomware dépend de la rapidité à laquelle elle peut se propager à travers votre réseau. Une réponse rapide peut considérablement réduire l'impact pour votre entreprise et empêcher l'infection de se propager. Pour isoler l'infection, arrêtez immédiatement tous les appareils affectés et isolez-les du réseau et de tout système de stockage partagé. Éteignez tous les appareils qui n'ont pas été infectés afin de limiter les dommages.

- ☐ **Assurez-vous que les sauvegardes n'ont pas été compromises.**
  Le ransomware tend à évoluer, ce qui menace lourdement l'intégrité des sauvegardes. Pour protéger vos sauvegardes, vous devez rendre immuables les données qu'elles contiennent. Une fois que des données sont écrites, elles ne sont plus jamais accessibles en lecture/écriture pour les clients externes. Aucun hacker qui parvient à faire intrusion dans votre réseau ne pourra donc les lire, les modifier ou les supprimer. C'est là le seul moyen de récupérer les données de vos systèmes de production infectés.

  Nous vous recommandons également de suspendre toutes les sauvegardes tant que vous n'avez pas compris d'où provenait l'infection, que vous n'avez pas étudié entièrement le problème et que vous n'avez pas identifié les derniers snapshots à jour.

- ☐ **Identifiez la nature de l'infection.**
  Pour pouvoir enrayer l'infection, il est essentiel d'en comprendre l'étendue. Le mieux est de commencer par repérer le premier ordinateur infecté et de tâcher d'identifier les données auxquelles il a accédé. Une autre solution consiste à vérifier le registre de ransomware, qui répertorie les fichiers chiffrés afin que le logiciel sache quels fichiers déchiffrer une fois que la rançon a été payée. Rapprochez-vous de votre équipe ou de vos experts en sécurité pour faciliter le travail d'enquête.

- ☐ **Vérifiez le délai de rétention.**
  Il peut être avantageux d'allonger les délais de rétention de vos sauvegardes le temps d'analyser les impacts et de trouver une solution. Avec des délais de rétention courts, vos sauvegardes risquent d'expirer avant que vous n'ayez terminé votre processus de restauration. Un allongement de ces délais permet de restaurer votre environnement à l'état tel qu'il se trouvait avant l'infection.

☐ **Activez votre plan lié aux incidents.**

Dernière étape : faire intervenir votre équipe de gestion des incidents, informer les principales parties prenantes et évaluer vos options pour vous aider à récupérer vos données et remettre sur pied votre environnement. Vous disposez de différents plans d'action :

Option 1 : restaurer vos fichiers à partir d'une sauvegarde. Le moyen le plus fiable de se relever d'une attaque de ransomware sans payer la rançon consiste à restaurer les systèmes affectés à l'état tel qu'ils se trouvaient avant l'attaque. Pour réagir efficacement face au ransomware, il est donc essentiel d'élaborer un plan de sauvegarde complet et de le tester régulièrement.

Notez que toutes les solutions de protection des données ne protègent pas vos sauvegardes elles-mêmes pendant une attaque, ce qui signifie que les sauvegardes peuvent elles aussi être affectées. C'est pourquoi nous vous recommandons de privilégier une solution qui empêche les programmes de ransomware de modifier vos données de sauvegarde, tout en assurant des restaurations rapides et en procurant un maximum de visibilité.

Option 2 : tenter de trouver un décrypteur. Dès lors que vous avez identifié la souche exacte de l'attaque, vous pouvez trouver facilement un décrypteur sur des sites Web tiers. Sachez toutefois que les dernières versions de ransomware sont de plus en plus sophistiquées et qu'elles mutent rapidement, ce qui rend difficile de trouver un décrypteur qui convient.[4] Qui plus est, lorsque vous utilisez un décrypteur tiers, vous risquez de télécharger d'autres logiciels malveillants. Cette approche n'est donc ni très fiable, ni recommandée.

Option 3 : ne rien faire et accepter la perte de données. Les entreprises qui n'avaient pas défini en amont une stratégie de sauvegarde robuste ou qui ne parviennent pas à trouver un décrypteur peuvent choisir tout simplement de ne pas récupérer leurs fichiers. Bien évidemment, il leur faudrait après cela développer, tester et déployer un plan de restauration efficace pour s'assurer une reprise rapide dans l'éventualité où elles seraient de nouveau victimes d'une attaque.

Option 4 : négocier et payer la rançon. Pour ceux qui ont essayé toutes les autres options et qui ne parviennent toujours pas à remettre la main sur leurs fichiers, la seule solution viable, en apparence, pourrait être simplement de payer la rançon. Mais le FBI et la plupart des experts en sécurité déconseillent fortement de se résigner à une telle extrémité, car cela ne garantit en rien que vous puissiez récupérer vos données. Selon un rapport rédigé en 2019 par le CyberEdge Group, 17 % des entreprises qui ont choisi de payer la rançon n'ont jamais réussi à récupérer l'accès à leurs données chiffrées ou à leurs systèmes infectés.[5] Payer la rançon peut aussi inciter les hackers à commettre de nouvelles attaques (en rehaussant éventuellement le montant de la rançon), exposer votre entreprise à des risques plus grands encore, et perpétuer le cycle en récompensant les acteurs mal intentionnés.

☐ **Évaluez l'étendue de l'infection.**

Pour minimiser les pertes de données liées à une attaque de ransomware, les équipes IT doivent être en mesure d'identifier rapidement les fichiers et applications affectés… un processus qui peut prendre des jours, voire des semaines, avec une technologie d'ancienne génération. Et pourtant, il est impératif de commencer par identifier les applications et les fichiers qui ont été impactés, et de déterminer à quel niveau lancer la restauration. Cela permet de limiter les risques de pertes de données associés à des restaurations en masse qui englobent des données intègres.

☐ **Alertez les autorités.**

Signalez l'incident aux forces de l'ordre, à vos clients et à toute autre autorité compétente. Certaines entreprises peuvent être juridiquement tenues d'informer à la fois les autorités et les utilisateurs. Cette contrainte varie selon votre activité, votre secteur et votre localisation géographique.

Limitations de garantie

Le présent document a été rédigé dans l'intention de compléter les plans de réponse, de remédiation et de reprise après sinistre actuellement en place en cas d'attaques de ransomware. Il n'est destiné en aucun cas à s'y substituer.

Ce modèle est disponible « en l'état », sans garantie d'aucune sorte. Il n'a été approuvé par aucune autorité ou instance officielle et son auteur ne saurait engager sa responsabilité au titre des dommages découlant de l'utilisation des informations qu'il contient.

Pour réussir, il est impératif d'adapter ce modèle et de tester le plan élaboré.

Sources

1 *McAfee Labs Threats Report, août 2019.* McAfee, www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf.

2 *Fall 2019 OCR Cybersecurity Newsletter: What Happened to My Data?: Update on Preventing, Mitigating and Responding to Ransomware.* The U.S. Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2019/index.html

3 *2019 Data Breach Investigations Report.* Verizon, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

4 Alessandrini, Adam. *RANSOMWARE: Hostage Rescue Manual.* KnowBe4, 2016, www.wired.com/wp-content/uploads/2016/03/RansomwareManual-1.pdf.

5 *2019 Cyberthreat Defense Report,* CyberEdge Group, LLC. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

rubrik

Siège global
1001 Page Mill Rd., Building 2
Palo Alto, CA 94304
États-Unis

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