Proposé par

rubrik

La reprise après une attaque par ransomware

pour les nuls

Développer un plan de reprise

Apprendre comment récupérer après une attaque

Reprendre l'activité normale le plus vite possible

Une édition spéciale Rubrik

Michael G. Solomon

À propos de Rubrik

Rubrik aide les entreprises à contrôler leurs données de manière à améliorer la résilience de l'organisation, la mobilité dans le cloud et la conformité réglementaire. Rubrik comble l'écart entre une infrastructure propriétaire sur site et le cloud en découplant les données du datacenter au moyen d'un outil défini par les logiciels et en offrant une plateforme de gestion unique pour toutes les données, qu'elles se trouvent sur site ou dans le cloud. Sa solution complète de gestion des données repose sur l'accès instantané, une orchestration automatisée, la protection des données et une capacité de résilience de niveau professionnel.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

La reprise après une attaque par ransomware

Une édition spéciale Rubrik

par Michael G. Solomon

pour les nuls®

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

La reprise après une attaque par ransomware pour les Nuls®, une édition spéciale de Rubrik

Publié par **John Wiley & Sons, Inc.**
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2022 par John Wiley & Sons, Inc, Hoboken, New Jersey

Aucune partie de cet ouvrage ne peut être reproduite, conservée dans un système d'extraction, ou transmise sous quelque forme ou par quelque moyen que ce soit, par voie électronique ou mécanique, photocopie, enregistrement, numérisation ou autre, sans l'accord écrit préalable de l'éditeur, sauf si les articles 107 et 108 de la loi des États-Unis de 1976 relative au copyright (« United States Copyright Act ») l'autorisent. Les demandes d'autorisation adressées à l'éditeur doivent être adressées au service des autorisations, John Wiley & Sons, Inc. 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, ou en ligne à http://www.wiley.com/go/permissions.

Marques commerciales : Wiley, pour les Nuls, le logo Dummies Man, The Dummies Way, Dummies.com, Avec les Nuls, tout devient facile !, et les appellations commerciales afférentes sont des marques de commerce ou des marques déposées de John Wiley & Sons, Inc. et/ou de ses sociétés affiliées aux États-Unis et dans d'autres pays, et ne peuvent pas être utilisées sans autorisation écrite. Toutes les autres marques commerciales sont la propriété de leurs propriétaires respectifs. John Wiley & Sons, Inc. n'est associé à aucun produit ou distributeur mentionné dans cet ouvrage.

EXCLUSION DE GARANTIE ET LIMITATION DE RESPONSABILITÉ : L'ÉDITEUR ET L'AUTEUR NE FONT AUCUNE DÉCLARATION NI N'ACCORDENT AUCUNE GARANTIE QUANT À L'EXACTITUDE OU À L'EXHAUSTIVITÉ DU CONTENU DU PRÉSENT LIVRE ; EN PARTICULIER, ILS REJETTENT SPÉCIFIQUEMENT TOUTES LES GARANTIES, Y COMPRIS, SANS AUCUNE LIMITE, LES GARANTIES D'ADÉQUATION À UN USAGE PARTICULIER. AUCUNE GARANTIE NE PEUT ÊTRE CRÉÉE OU PROROGÉE PAR DES DOCUMENTS DE VENTE OU DE PROMOTION. LES CONSEILS ET STRATÉGIES CONTENUS DANS LE PRÉSENT LIVRE PEUVENT NE PAS CONVENIR À TOUTES LES SITUATIONS. LE PRÉSENT LIVRE EST VENDU ÉTANT ENTENDU QUE L'ÉDITEUR N'OFFRE PAS DE SERVICES JURIDIQUES, COMPTABLES OU AUTRES SERVICES PROFESSIONNELS. LES LECTEURS QUI VEULENT OBTENIR UNE ASSISTANCE PROFESSIONNELLE DOIVENT S'ADRESSER À UN PROFESSIONNEL COMPÉTENT. NI L'ÉDITEUR NI L'AUTEUR NE SERONT TENUS RESPONSABLES DES DOMMAGES DÉCOULANT DU CONTENU DU PRÉSENT LIVRE. LA MENTION D'UNE ORGANISATION OU D'UN SITE INTERNET DANS LE PRÉSENT LIVRE, EN CITATION ET/OU COMME SOURCE POTENTIELLE DE RENSEIGNEMENTS SUPPLÉMENTAIRES, NE SIGNIFIE PAS QUE L'AUTEUR OU L'ÉDITEUR ENTÉRINE LES INFORMATIONS OU LES RECOMMANDATIONS QUE PEUT FOURNIR L'ORGANISATION OU LE SITE INTERNET. EN OUTRE, LES LECTEURS DOIVENT SAVOIR QUE LES SITES INTERNET MENTIONNÉS DANS LE PRÉSENT LIVRE PEUVENT AVOIR CHANGÉ OU DISPARU DEPUIS LA DATE DE RÉDACTION DE CE LIVRE.

ISBN 978-1-119-84899-8 (pbk) ; ISBN 978-1-119-84900-1 (ebk)

Imprimé aux États-Unis d'Amérique

10 9 8 7 6 5 4 3 2 1

Pour obtenir des renseignements généraux sur nos autres produits et services, ou sur la publication d'un livre *pour les Nuls* destiné à votre entreprise ou organisation, veuillez contacter notre service de développement commercial aux États-Unis, par téléphone au 877-409-4177, par e-mail à info@dummies.biz, ou consulter notre site www.wiley.com/go/custompub. Pour obtenir des informations sur la licence de la marque *pour les Nuls* pour des produits ou services, veuillez contacter BrandedRights&Licenses@Wiley.com.

Remerciements de l'éditeur

Cet ouvrage a été réalisé avec la participation des personnes suivantes :

Éditeur de développement : Rebecca Senninger

Rédacteur chargé des acquisitions : Ashley Coffey

Responsable éditorial : Rev Mengle

Représentant du développement commercial : William Hull

Éditeur de production : Mohammed Zafar Ali

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Table des matières

INTRODUCTION 1
À propos de ce livre 1
Quelques suppositions idiotes 2
Icônes employées dans ce livre 2
Au-delà de cet ouvrage 2

CHAPITRE 1 : **Qu'est-ce qu'une attaque par ransomware ?** 3
Présentation du ransomware et de son impact informatique 3
Le problème du ransomware 4
Mode de fonctionnement du ransomware et son impact informatique 4
Quelques cas réels d'attaque par ransomware 5
Blocage des bureaux de change de Travelex 5
Crise évitée pour la ville de Durham en Caroline du Nord aux Etats-Unis 5
Examen des tendances en matière de ransomware 6
Résilience renforcée grâce aux multiples lignes de défense 7

CHAPITRE 2 : **Préparer sa défense contre le ransomware** 9
Développement d'un plan de reprise 9
Évaluation de vos besoins 9
Élaboration d›un plan 10
Mise à l'épreuve de votre plan 10
Protection de la dernière ligne de défense 11
L'immuabilité des sauvegardes et son importance 11
Définition de l'immuabilité 11
Application de l'immuabilité pour les sauvegardes 11
Récupération des données 12

CHAPITRE 3 : **Prévenir les attaques par ransomware** 13
Comprendre les points faibles du ransomware 13
Comment le ransomware attaque les ordinateurs 14
Comment un utilisateur est amené à infecter un ordinateur ... 14
Piège de l'objet attrayant qui infecte automatiquement les ordinateurs 14
Former les utilisateurs à se méfier des pièges 15
Reconnaître les attaques potentielles 15
Réagir à un contenu suspect 16

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Répéter le message 16
Mettre en œuvre les bonnes pratiques de sécurité 16
Adoption d'un comportement utilisateur sûr 17
Renforcer votre environnement informatique 17

CHAPITRE 4 : **Identifier une attaque par ransomware et évaluer le rayon d'explosion** 19

Détection d'une attaque au plus vite 19
Une réaction efficace dépend d'une alerte précoce 20
Réduction de la charge de travail (et du temps) de reprise 20
Aperçu des différentes méthodes de détection des attaques 20
Reconnaître les signatures de ransomware 20
L'apprentissage automatique mis à profit pour reconnaître les anomalies 21
Réaction face à une attaque 21
Mise en place de l'équipe d'intervention 21
Limiter les dommages et identifier les fichiers affectés 22
Limiter tout dommage supplémentaire 22
Évaluation du rayon d›explosion 22

CHAPITRE 5 : **Récupérer vos données avec une précision chirurgicale** 23

Création d'un plan de reprise rapide 23
La sauvegarde n'est qu'une première étape 24
Une reprise réussie repose sur l'évaluation du temps de reprise 24
Une reprise limitée aux fichiers nécessaires 25
Cibler seulement les données nécessaires 25
Suppression des pertes de temps 26
Automatisation de la reprise à grande échelle 26
Implémentation des API pour une reprise sans intervention 26
Scripts garants de haute performance 26

CHAPITRE 6 : **Dix conseils pour faire face aux attaques par ransomware** 27

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Introduction

Bienvenue dans *La reprise après une attaque par ransomware pour les Nuls*, le guide qui vous explique ce qu'est une attaque par ransomware et comment récupérer après celle-ci. Les attaques des logiciels malveillants, ou malware, ont gagné en gravité et ne sont plus simplement gênantes ; elles paralysent les processus des entreprises et provoquent même des pertes de données. Le ransomware est un type de logiciel malveillant de plus en plus répandu. Son nom décrit bien ce qu'il fait. Le ransomware chiffre les fichiers critiques sur l'ordinateur d'une victime et demande le paiement d'une rançon en échange d'une clé pour les déchiffrer. Le pirate ne détruit pas réellement les données mais les rend indisponibles pour la victime jusqu'au paiement de la rançon.

Pour récupérer au mieux après une attaque par ransomware, on conseille en général de restaurer entièrement un ordinateur affecté à partir de l'image de sauvegarde la plus récente. Bien qu'elle semble sensée, cette méthode présente des inconvénients. La plupart des ransomwares sophistiqués recherchent les images de sauvegarde et les chiffrent également. En outre, si vous ne disposez pas d'une bonne image de sauvegarde, la restauration d'un environnement complet prend du temps et risque d'effacer de nombreuses transactions. Il vous faut disposer d'une meilleure méthode.

Un plan de reprise efficace doit permettre à l'organisation affectée de reprendre rapidement ses opérations normales avec une perte de données minimale.

À propos de ce livre

La reprise après une attaque par ransomware pour les Nuls présente une approche intelligente pour récupérer facilement après une attaque par ransomware que vous ne pouvez éviter. Vous commencerez par examiner la menace que pose le ransomware, puis vous verrez comment créer un plan de reprise cohérent et maintenir la sécurité de votre organisation.

Vous explorerez ensuite le fonctionnement de base d'un ransomware et vous comprendrez l'importance des solutions de sauvegarde et quelles fonctions il vous faut pour contrer une attaque. Vous apprendrez comment assembler les différents éléments d'un plan de reprise comme dans un puzzle afin de développer un plan efficace. Enfin, vous passerez en revue dix astuces pour créer le plan de reprise le plus efficace.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Quelques suppositions idiotes

En rédigeant cet ouvrage, j'ai fait quelques suppositions concernant le lecteur, c'est-à-dire vous : Tout d'abord, je suppose que dans votre fonction, vous avez au moins entendu parler du ransomware. Toutefois, quel que soit votre rôle, je pars du principe que vous souhaitez en savoir plus sur la menace du ransomware et comment l'empêcher d'interrompre les opérations métier de votre organisation. Je suppose également que vous voulez connaître les étapes à suivre pour créer un plan de reprise solide.

Icônes employées dans ce livre

Chaque livre *pour les Nuls* renferme de petites images en forme d'icônes qui sont disposées dans la marge. Dans ce livre, j'utilise les icônes suivantes :

CONSEIL

Cette icône vous conseille des méthodes plus rapides et plus faciles pour effectuer une tâche ou la meilleure manière de mettre en œuvre la « blockchain » (chaîne de blocs) dans votre entreprise.

ATTENTION

Si vous voyez cette icône, agissez avec précaution. Vous trouverez ici des conseils pour éviter les écueils les plus courants.

Au-delà de cet ouvrage

Le sujet du ransomware est vaste et ce petit livre ne peut le décrire exhaustivement. Des entreprises innovantes ont étudié ce problème en profondeur et ont élaboré des solutions efficaces dont vous pouvez bénéficier. Rubrik est un leader dans la fourniture de services de récupération après une attaque par ransomware, destinés à des petites, moyennes ou grandes entreprises. Pour plus d'informations sur les offres de Rubrik, consultez la page `https://www.rubrik.com/en/products/polaris-overview/polaris-radar`.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

DANS CE CHAPITRE

- Présentation du ransomware et de son impact informatique
- Quelques cas réels d'attaque par ransomware
- Examen des tendances en matière de ransomware
- Plusieurs lignes de défense pour se protéger des attaques

Chapitre 1
Qu'est-ce qu'une attaque par ransomware ?

Un ransomware est un type de logiciel malveillant qui chiffre les données d'une victime et propose une clé de déchiffrement en échange du paiement d'une rançon. Le ransomware figure parmi les types de logiciels malveillants que l'on craint le plus et qui connaissent la plus forte croissance. Lorsqu'elle aboutit, une attaque par ransomware met ses victimes devant un dilemme : perdre des données précieuses et parfois irremplaçables, ou payer une rançon pour les récupérer. La menace posée par le ransomware est d'autant plus grande que les données prennent de plus en plus de valeur pour les particuliers comme les entreprises. Dans ce chapitre, vous découvrirez ce qu'est un ransomware, son impact informatique, et comment vous pouvez réduire votre risque d'être victime d'une attaque.

Présentation du ransomware et de son impact informatique

Le ransomware s'est d'abord fait connaître comme une menace contre les données personnelles. Pour la plupart, les premières attaques par ransomware ciblaient des particuliers en profitant de leur dépendance accrue à leurs données et leurs supports. La crainte de perdre des photos, des vidéos et des documents personnels était assez forte pour amener certaines victimes à payer la rançon. Forts de leur succès, les pirates ont gagné en assurance et s'en sont pris à des cibles de plus en plus importantes.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Le problème du ransomware

Aujourd'hui, le ransomware représente une menace réelle pour les personnes et les entreprises. En 2020, le ransomware a ciblé des groupes moins larges pour extorquer aux victimes des rançons plus élevées. Ainsi, selon un rapport récent d'Emisoft, « au moins 2354 administrations, établissements de soins et écoles aux États-Unis ont été impactés en 2020 » (https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/). Rien ne laisse à penser que le ransomware va bientôt disparaître. Au contraire, le ransomware a recours à des tactiques plus ciblées et plus sophistiquées.

Les pirates se sont aperçus que les entreprises et les prestataires de services critiques étaient souvent plus enclins que les particuliers à payer des rançons importantes pour mettre fin à des arrêts d'activité invalidants. Aujourd'hui, la plupart des organisations s'appuient sur les données et les systèmes d'information pour gérer les affaires courantes. Lorsque l'accès aux données critiques est impossible, c'est une catastrophe pour l'organisation. Bien que de nombreuses organisations disposent de plans de reprise d'activité, la plupart ne prévoient pas de réponse adaptée à une perte permanente des données opérationnelles critiques. Pour éviter d'être confronté à des interruptions dévastatrices des fonctions métiers critiques, il faut bien comprendre ce qui distingue le ransomware de la plupart des autres menaces.

Mode de fonctionnement du ransomware et son impact informatique

Pour les victimes de ransomware, la perspective d'une perte permanente des données critiques peut devenir réalité. La tendance dominante est de réduire sa surface d'attaque pour ne présenter aucune faille. Bien qu'il s'agisse d'une bonne approche en théorie, elle marche seulement quand elle est efficace à 100 %. La véritable question est de savoir « comment restaurer nos systèmes si l'un de nos contrôles préventifs ne parvient pas à arrêter une attaque par ransomware ». Il s'agit de mettre en œuvre les plans nécessaires à la prévention, l'évaluation et la reprise.

Un bon plan de résilience face au ransomware met en œuvre de multiples lignes ou niveaux de défense. Rester hors d'atteinte des menaces de ransomware n'est pas difficile si les contrôles et les plans appropriés sont mis en place. Cela vous demandera probablement d'apporter quelques changements à votre infrastructure informatique. Les pirates en général, et plus particulièrement ceux qui opèrent par ransomware, supposent qu'ils ont affaire à une infrastructure « normale ». Ils s'attendent à trouver un haut niveau d'automatisation et des connexions simples aux périphériques de stockage externe. Les surprendre avec une

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

infrastructure plus intelligente est la première condition pour réchapper d'une attaque par ransomware.

Quelques cas réels d'attaque par ransomware

Avant de décrire en détail la préparation nécessaire pour contrer une attaque par ransomware, jetons un coup d'œil à deux cas réels d'organisations confrontées à ce type d'attaque. La première a été prise par surprise, tandis que la seconde avait soigneusement planifié des mesures de protection en cas d'attaque par ransomware. Non seulement la seconde organisation a résisté à l'attaque, mais elle a pu poursuivre ses opérations avec le minimum d'interruption. Et cette entreprise l'a fait sans faire exploser son budget informatique, ce qui veut dire que vous aussi, vous pouvez le faire.

Blocage des bureaux de change de Travelex

À la Saint-Sylvestre 2019, la société Travelex basée à Londres a été victime d>une attaque par le ransomware du groupe Sodinobiki. Travelex, une société de change qui opère dans 26 pays, a constaté que ses services de base étaient gravement impactés, que ses sauvegardes étaient supprimées et que 5 Go de données opérationnelles avaient été téléchargées et chiffrées. Les pirates réclamaient une rançon de 6 millions de dollars en échange d>une clé de déchiffrement et de la suppression des données téléchargées. Ayant négocié avec les pirates pendant plusieurs semaines, Travelex a finalement accepté de payer 2,3 millions de dollars en cryptomonnaie pour récupérer ses données et obtenir la garantie qu>elles ne soient pas rendues publiques. Après avoir payé la rançon, Travelex a pu reprendre ses opérations cœur de métier à la fin du mois de janvier 2020 et a retrouvé un fonctionnement normal en février 2020.

ATTENTION

Il est recommandé de mettre tout en œuvre pour éviter de payer une rançon. Chaque rançon versée augmente les profits des pirates et les maintient en activité. En outre, payer une rançon montre que vous êtes une « proie facile » pour de futures attaques.

Crise évitée pour la ville de Durham en Caroline du Nord aux Etats-Unis

Les attaques par ransomware finissent parfois sans trop de pertes d'argent ni de données. Il est tout à fait possible de bien planifier pour éviter de faire partie des statistiques. La ville de Durham en Caroline du Nord a été la cible d'une attaque par ransomware en mars 2020. Elle avait auparavant mis en œuvre un plan de surveillance et de sauvegarde au niveau de son infrastructure, basé sur un système de secours

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

non modifiable fourni par Rubrik qui garantissait la sécurité des sauvegardes.

Lorsque l'attaque a commencé, plusieurs services critiques ont été interrompus, notamment le serveur d'appels d'urgence 911. Le personnel a été capable d'identifier les fichiers affectés et de les récupérer pour rétablir rapidement les services les plus critiques. Une fois cette opération effectuée, ils ont pu rétablir toutes les autres données affectées par l'attaque et reconnecter l'ensemble des systèmes cœur de métier dès le lundi matin suivant.

Examen des tendances en matière de ransomware

Plusieurs tendances se dessinent en matière de ransomware, et elles ne sont pas de bon augure. En tant qu'intendant des données de votre organisation, votre objectif est de comprendre quelles sont les tendances en matière de menaces pour vous préparer aux attaques futures éventuelles. En dépit du niveau élevé de sophistication des ransomware, il est encore possible de devancer quelque peu les pirates, ce qui est une bonne nouvelle.

Voici quelques-unes des tendances actuelles en matière d'attaque :

- **Des montants de rançons en forte hausse.** Les pirates concentrent leurs attaques sur un nombre réduit de cibles mais exigent des rançons beaucoup plus élevées.
- **L'émergence des logiciels malveillants en tant que produits de consommation.** Il n'est pas nécessaire de développer des logiciels malveillants pour utiliser un ransomware. Les fournisseurs de RaaS (Ransomware as a Service) permettent à tout un chacun de mener facilement une attaque par ransomware.
- **Le ciblage des personnes en télétravail ou étudiants.** L'essor des activités de télétravail ou des études en distanciel, accéléré par les restrictions liées à la pandémie de COVID 19, a eu pour conséquence d'exposer de nouvelles cibles aux pirates : les prestataires de services de collaboration et d'enseignement.
- **L'exfiltration des données.** Non contents de chiffrer simplement les données, certains pirates transfèrent maintenant les données sur leurs propres sites. Ils peuvent alors les vendre pour en tirer des profits, les rendre publiques pour nuire à la réputation de l'entreprise ou entraîner des sanctions ou amendes pour infraction à la loi ou aux réglementations, telles que le RGPD.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

- **Le doublement de l'extorsion de fonds.** Les données exfiltrées sont utilisées pour exiger le paiement d'une seconde rançon afin d'éviter que les données sensibles soient divulguées. La seule menace de divulgation des données sensibles pourrait suffire à convaincre une victime de payer la rançon.
- **La recherche et la compromission des sauvegardes.** De nombreuses souches de ransomware ne se contentent plus aujourd'hui de chiffrer les données locales. Elles recherchent toutes les sources de données connectées et tentent de chiffrer également toutes les copies de sauvegarde.
- **Une croissance rapide qui se poursuit.** L'augmentation du montant des rançons, la facilité d'accès aux logiciels malveillants et un meilleur ciblage des victimes sont autant de facteurs qui démultiplient le nombre d'acteurs convoitant des profits dans la sphère des ransomware.

Résilience renforcée grâce aux multiples lignes de défense

Face à la menace croissante des attaques par ransomware et au succès florissant des pirates, envisager de se défendre peut sembler un défi de taille. Or, une défense bien calibrée peut empêcher de nombreux types d'attaques par ransomware et aider à la reprise rapide de vos systèmes lorsqu'un ransomware a franchi les défenses de votre périmètre. La clé d'une défense efficace consiste à créer de multiples lignes de défense. Dans le domaine de la cybersécurité, c'est ce qu'on appelle la méthode de *défense en profondeur*. Au fond, cela désigne le simple fait de placer autant de contrôles que possible entre vos données et un pirate.

Une idée répandue consiste à penser que les contrôles de prévention des attaques sont les meilleurs. Éviter une attaque est souhaitable, c'est vrai, mais on ne peut garantir de les éviter toutes. Si vous ne prévoyez pas l'éventualité d'une attaque qui aboutit, vous ne serez pas prêt à réagir si cela se produit vraiment.

Au rang des contrôles préventifs, on peut citer la formation du personnel et l'utilisation de pare-feux. La première ligne vise à repousser la plupart des attaques avant qu'elles ne prennent pied. Comme la plupart des attaques de logiciels malveillants, y compris celles de ransomware, commencent par un collaborateur qui clique sur un lien malveillant, il importe de former votre personnel à reconnaître les messages et les liens malveillants. Les pare-feux peuvent contribuer à bloquer le trafic visible, mais un utilisateur autorisé qui clique sur un lien malveillant ouvre une brèche.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

CONSEIL

Même si la prévention est importante, le véritable enjeu pour vaincre le ransomware est la résilience. Savoir comment réagir si vous êtes victime d'une attaque est aussi important que de savoir comment l'éviter.

Si une attaque arrive à déjouer les contrôles préventifs, il faut déjà savoir qu'elle est en train de se produire pour pouvoir y répondre. Une ligne de détection robuste est essentielle pour pouvoir prendre les mesures nécessaires avant qu'il ne soit trop tard. Il existe aujourd'hui une technologie de surveillance et d'analyse de comportement qui déclenche des alertes quasi-instantanées quand une attaque par ransomware est en cours.

CONSEIL

Il convient de mettre en place une surveillance en temps réel de toutes les copies de données primaires et critiques, ainsi que de recourir à l'intelligence artificielle pour gérer vos données de sauvegarde, afin de créer une dernière ligne défensive.

Le niveau suivant de votre stratégie de défense contre le ransomware met fin à l'attaque et détermine ce qu'elle a endommagé. Pour ce faire, vous déconnectez et mettez hors tension les ordinateurs impactés de votre réseau en suivant les procédures établies. En les réamorçant dans un environnement contrôlé, vous pouvez évaluer l'étendue des dommages. La conteneurisation peut faciliter cette étape. Il va de soi que les activités à ce niveau dépendent pour la plupart des politiques et procédures mises en place bien avant le début de l'attaque.

La ligne suivante de défense varie selon la solution de sauvegarde que vous avez choisie de mettre en œuvre. Une fois que vous avez identifié les fichiers que l'attaque a endommagés, il vous faut récupérer les images antérieures à l'attaque pour chaque fichier. Votre solution de sauvegarde devrait faciliter et accélérer la récupération des images de fichier prises à un moment donné.

Et pour finir : votre solution de sauvegarde sera une cible privilégiée des ransomware sophistiqués. Les seules sauvegardes auxquelles vous pouvez vous fier sont celles dont vous pouvez garantir l'intégrité. Votre solution de sauvegarde doit empêcher tout processus, y compris le ransomware, de modifier les images de sauvegarde une fois qu'elles sont écrites dans le système de fichiers.

Si vous mettez en œuvre toutes ces lignes de défense, vous disposerez des blocs fonctionnels nécessaires à la récupération complète et rapide suite à toute attaque ayant abouti.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

DANS CE CHAPITRE

- Création d'un plan de reprise
- L'intégrité, essentielle à votre dernière ligne de défense
- Présentation de l'immuabilité
- Récupération de vos données après une attaque

Chapitre 2
Préparer sa défense contre le ransomware

Surmonter une attaque par ransomware n'est pas le fruit du hasard. La seule manière de ne pas être victime d'un ransomware, c'est de planifier et d'entreprendre des actions de récupération avant que l'attaque n'ait lieu. Dans ce chapitre, vous verrez comment créer un plan que vous pouvez utiliser si votre société est victime de ransomware.

Développement d'un plan de reprise

En cas d'attaque par ransomware, le manque de préparation est le plus problématique car il rend difficile la reprise. Même en étant préparé, la reprise peut être impossible sans un plan solide. Mais ne perdez pas espoir ; vous apprendrez ici à développer ce plan qui peut faciliter et accélérer la reprise après une attaque par ransomware.

Évaluation de vos besoins

Pour se préparer à surmonter une attaque par ransomware, la première étape consiste à identifier ce qui a de la valeur pour votre organisation et ce qui intéresse les pirates. Une analyse d'impact sur les activités (Business Impact Assessment – BIA) est un processus important dans lequel vous identifiez les processus critiques pour votre organisation et les ressources sur lesquelles ils reposent. En résumé, il s'agit de se demander ce qu'il faut à votre organisation pour poursuivre ses activités.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Une fois que vous connaîtrez les conditions requises par votre organisation pour exécuter ses processus métier critiques (critical business function - CBF), vous saurez quelles données comptent à vos yeux. Ainsi, un commerçant en ligne accorde probablement une grande valeur à ses bases de données client et produit. En revanche, une bibliothèque de tutoriels vidéo sera sans doute moins importante pour ses opérations courantes.

Une fois que vous avez identifié ce qui a de l'importance pour vos activités, réfléchissez à ce qui intéresse les pirates. Ils veulent généralement capturer les données qui sont pour vous les plus précieuses. En d'autres termes, ils ciblent les données sur lesquelles reposent vos CBF. Vous paierez plus volontiers une rançon si les données à restaurer sont indispensables à la poursuite de vos activités.

Élaboration d›un plan

Une fois que vous avez cerné les données qui sont les plus critiques pour votre organisation (et pour les pirates), vous pouvez maintenant développer un plan permettant de récupérer ces données si une attaque par ransomware vous atteint. Vous en saurez plus sur ce qu'il vous faut intégrer dans vos plans dans les chapitres 4 et 5, mais pour l'instant, commencez à réfléchir à la composition de votre équipe de planification et à la manière dont vous allez documenter ce plan. Votre équipe devrait comprendre un représentant de chaque groupe ayant une influence sur le plan ou étant potentiellement affecté par le plan.

Mise à l'épreuve de votre plan

Une fois que vous avez élaboré votre plan de reprise après une attaque par ransomware, vos efforts ne s'arrêtent pas là. Un plan n'est entièrement fiable que si vous l'avez testé de manière exhaustive. Investir du temps et des efforts à développer un plan ne sert à rien si vous découvrez, après une attaque, que vous avez omis une petite partie du système qui revêt malgré tout une importance critique. Un plan qui échoue n'apporte aucune valeur ajoutée (ni de capacité de reprise).

Différents types de test sont possibles, s'approchant chacun un peu plus d'un cas d'attaque réel. La plupart des organisations partent de tests de liste de contrôle qui demandent aux parties prenantes d'examiner ensemble le plan et de s'assurer que l'ensemble des tâches sont couvertes. Un test plus complet prendrait la forme d'une simulation dans laquelle chaque acteur met en œuvre les actions qu'il ferait s'il était confronté à une attaque réelle. Le dernier type d'attaque simulé est une attaque dans laquelle les fichiers sont réellement endommagés, pour voir si l'équipe de récupération peut les restaurer dans un état utilisable. Ce dernier type de test comporte bien sûr des risques, mais c'est également le meilleur test pour évaluer un plan de reprise.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Protection de la dernière ligne de défense

Tout ransomware qui parvient à chiffrer des fichiers suppose que la victime ne peut accéder à une copie du fichier affecté. Cela signifie que les pirates s'efforcent par tous les moyens de trouver les copies de sauvegarde des fichiers et de les chiffrer également. De nos jours, avec l'essor de l'automatisation et de la connectivité, la plupart des référentiels de sauvegarde sont faciles à trouver et à infecter.

Récupérer des fichiers chiffrés par un ransomware est un processus en trois étapes : 1) Arrêter l'attaque. 2) Identifier les fichiers affectés. 3) Récupérer une version non chiffrée, et intègre, du fichier à partir d'une sauvegarde.

Cette troisième étape qui est la plus importante dépend du fait de disposer de sauvegardes intègres non affectées par le ransomware, et auxquelles vous pouvez vous fier. Le choix de vos services de sauvegarde est donc crucial pour la récupération après une attaque par ransomware.

L'immuabilité des sauvegardes et son importance

Un plan de reprise efficace repose sur l'intégrité de sauvegardes auxquelles vous pouvez vous fier. Si vous pouvez avoir la certitude que le ransomware n'a pas endommagé vos fichiers sauvegardés, il est alors possible de récupérer vos données après une attaque.

Définition de l'immuabilité

Pour être résilient face à une attaque par ransomware, il est essentiel d'assurer l'immuabilité des sauvegardes. Celle-ci implique qu'une fois les données écrites, elles ne peuvent jamais être endommagées. Rien ni personne, pas même un processus de ransomware, ne peut modifier les données une fois qu'elles ont été écrites. Si vous disposez de sauvegardes non modifiables, vous avez alors un référentiel parfait de données préalables à l'attaque que vous pouvez utiliser pour la reprise.

Application de l'immuabilité pour les sauvegardes

L'immuabilité à des fins de sécurité n'est pas une idée nouvelle. Depuis des années, les systèmes de consignation sont basés sur l'immuabilité. Il y a longtemps que les pirates ont compris que la suppression ou l'altération des fichiers journaux était un moyen facile de cacher leurs agissements et de supprimer les traces de leurs délits. Les professionnels de la sécurité ont vite réalisé qu'ils avaient besoin de stratégies de

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

consignation permettant à un service d'écrire une entrée de fichier journal, mais sans jamais pouvoir l'endommager.

Rubrik a développé entièrement un système de fichiers unique pour sa solution de sauvegarde, qui met en œuvre l'immuabilité pour tous les fichiers. Sauvegarder un fichier est facile ; il vous suffit de l'écrire à l'aide d'un appel à l'API Rubrik. Une fois qu'un fichier est écrit, il ne peut jamais être modifié. Le système de fichiers de Rubrik stocke tous les fichiers en mode immuable et natif, qui sont ainsi accessibles en lecture seule, et empêche tout client externe sur le réseau de chiffrer ou de supprimer un fichier stocké. Vous pouvez lire les fichiers via une API, mais aucune modification n'est possible. L'immuabilité du système de fichiers de Rubrik vous garantit de disposer de fichiers intègres que vous pouvez utiliser pour une reprise rapide après une attaque par ransomware.

Récupération des données

Avant de récupérer vos fichiers, il est indispensable d'identifier les fichiers affectés. Bien que récupérer l'ensemble des fichiers soit possible, cela rallongerait considérablement le temps de reprise. Pour assurer la continuité des opérations, il vous faut réduire le temps d'indisponibilité en ne récupérant que ce qui est nécessaire à la poursuite de l'activité.

Vous avez d'abord pris le temps d'identifier les données critiques aux CBF de votre organisation. Déterminez maintenant quels fichiers critiques ont été chiffrés. Selon le type de ransomware, il peut être assez facile d'identifier les fichiers chiffrés. Comme tous les logiciels, un ransomware a besoin d'un registre, d'un manifeste ou d'une autre technique pour identifier les fichiers chiffrés. Après tout, une fois la rançon payée, les pirates veulent tout de même être en mesure de déchiffrer ces fichiers (c'est du moins ce qu'ils veulent vous faire croire).

ATTENTION

La plupart des pirates par ransomware fournissent des clés de déchiffrement après avoir touché la rançon, mais faire confiance à un cybercriminel est toujours risqué.

Une fois que vous avez identifié le fichier que vous souhaitez récupérer, la récupération est l'étape suivante. Pour ce faire, la méthode optimale consiste à implémenter une solution de sauvegarde qui vous permet d'accéder rapidement aux fichiers sauvegardés via des interfaces de programmation (application programming interface - API). En procédant ainsi, vous pouvez écrire des scripts qui récupèrent rapidement les fichiers chiffrés pour permettre à votre organisation de reprendre son activité.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

DANS CE CHAPITRE

- Identification des points faibles du ransomware
- Blocage des ouvertures possibles pour les attaques
- Formation des utilisateurs pour éviter les pièges du ransomware
- Adoption de bonnes pratiques pour éviter les attaques par ransomware

Chapitre 3
Prévenir les attaques par ransomware

À notre époque où les attaques de logiciels malveillants sont fréquentes, les surmonter n>est possible qu>en combinant d'une part une stratégie de prévention pour parer à la plupart des attaques et, d'autre part, la récupération des données. Bien qu>il soit nécessaire de mettre en place un plan robuste pour pallier les attaques une fois qu>elles ont réussi à faire une brèche, le meilleur scénario est d'arriver à éviter l'attaque en premier lieu. Pour réagir à toute attaque par ransomware, il est essentiel de comprendre d>abord la nature de l>attaque puis de prendre des mesures pour l'empêcher et enfin de réagir si celle-ci vous atteint. Dans ce chapitre, vous verrez comment mettre en œuvre les mesures qui permettent d>éviter les attaques par ransomware.

Comprendre les points faibles du ransomware

Bien qu'il ait des conséquences graves, le ransomware est un type de logiciel malveillant qui n'a rien d'invincible. Comprendre le mode opératoire du ransomware peut permettre d'élaborer des pratiques et des contrôles qui déjouent la plupart des attaques. Dans cette section, vous découvrirez certains des points faibles inhérents à un plan d'attaque par ransomware.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Comment le ransomware attaque les ordinateurs

Le succès d'un ransomware dépend de sa capacité à exécuter un programme malveillant sur l'ordinateur d'une victime. Ce fichier exécutable arrive à sa destination de plusieurs manières. Les méthodes les plus répandues consistent à tromper l'utilisateur pour qu'il ouvre un lien malveillant, qu'il navigue jusqu'à un site Web malveillant, ou qu'il se connecte à un dispositif infecté.

Comment un utilisateur est amené à infecter un ordinateur

De loin, le piège le plus répandu par lequel un ransomware infecte un ordinateur est celui qui amène l'utilisateur à effectuer une opération exécutant le code malveillant. La plupart des utilisateurs n'ont aucune intention délibérée d'exécuter un code malveillant sur leur ordinateur, mais ils peuvent être facilement trompés et faire inconsciemment le jeu des pirates. Convaincre un utilisateur autorisé d'effectuer une opération pour le compte d'un utilisateur non autorisé est une pratique dénommée ingénierie sociale.

La plupart des personnes sont vulnérables face à l'ingénierie sociale parce qu'elles veulent se rendre utiles, bénéficier d'un service gratuit ou éviter les ennuis. Les pirates savent qu'ils peuvent exploiter une ou plusieurs de ces motivations. C'est pourquoi un si grand nombre d'infections par ransomware commencent par l'utilisateur qui clique par inadvertance sur un lien dans un site Web ou dans un e-mail par générosité (« Cliquez sur ce lien pour faire un don à une œuvre de charité »), pour satisfaire sa curiosité (« Cliquez ici pour demander votre argent »), ou éviter d'avoir des ennuis (« Cliquez ici pour modifier votre mot de passe »).

Piège de l'objet attrayant qui infecte automatiquement les ordinateurs

Le ransomware ne commence pas toujours par le clic d'un utilisateur. Dans une attaque menée par téléchargement, un code malveillant est téléchargé quand l'utilisateur visite un site Web infecté. Un autre type d'attaque consiste à abandonner des clés USB infectées sur des lieux fréquentés par des personnes susceptibles de les remarquer. La première chose que font la plupart des personnes qui reçoivent une clé USB gratuite, c'est l'insérer dans un ordinateur pour voir ce qu'elle contient. Dans le cas d'une clé USB infectée, le simple fait de l'insérer dans un ordinateur permet de copier et de lancer le ransomware.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

ATTENTION

De nombreux types de pirates utilisent le piège des clés USB pour implanter un logiciel malveillant. Ne faites jamais confiance aveuglément aux clés USB de source inconnue, y compris celles qui vous sont données gratuitement à l'occasion de colloques ou congrès.

Former les utilisateurs à se méfier des pièges

Former l'utilisateur final est l'un des meilleurs investissements que puisse faire une organisation pour éviter le ransomware. Les utilisateurs fournissent quasiment tous les points d'entrée nécessaires au succès d'une attaque et leur rôle est crucial pour stopper les attaques avant qu'elles ne commencent. Former les utilisateurs à reconnaître les attaques potentielles et à résister à la tentation de cliquer sur des liens douteux peut considérablement réduire la probabilité qu'une attaque réussisse.

Dans la formation de sensibilisation à la sécurité que vous dispensez, ne vous bornez pas à couvrir les choses à faire ou à ne pas faire. Outre la formation aux différentes utilisations permises, profitez de cette occasion pour inciter les utilisateurs à devenir eux-mêmes des acteurs en matière de sécurité. La sécurité est la responsabilité de chacun, et ne se limite pas à un petit groupe de spécialistes. Faites savoir à l'ensemble du personnel qu'une bonne sécurité est l'affaire de tous, et que chacun doit faire preuve de diligence. Un simple acte de négligence peut exposer l'ensemble de l'organisation à une attaque, chacun doit donc faire des efforts pour dérouter les pirates.

CONSEIL

Rendre chaque utilisateur propriétaire de la sécurité de l'organisation peut avoir un grand impact sur l'élimination des opérations négligentes susceptibles de faire une brèche dans la protection des données.

Reconnaître les attaques potentielles

Étant donné que les utilisateurs offrent si souvent un point d>entrée au ransomware, leur apprendre à être vigilants et à reconnaître un contenu suspect est une manière sûre de réduire l'éventualité d'une attaque. Montrez aux utilisateurs des exemples d'e-mails de hameçonnage et donnez-leur des consignes sur la manière d'identifier une attaque potentielle.

Les e-mails de hameçonnage sont de plus en plus sophistiqués, mais ils sont pour la plupart faciles à repérer. Donnez des astuces aux utilisateurs afin qu'ils identifient d'éventuels e-mails malveillants. Apprenez-leur à faire attention à la grammaire (le message a-t-il un sens ?), au mode de salutation (s'adresse-t-on à vous de façon nominative ?) et

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

à la spécificité du contenu (le message contient-il des détails ou est-il générique ?) qui peuvent tous révéler un message malveillant. Une fois que les utilisateurs savent ce qu'il faut rechercher, ils peuvent jouer un rôle dans la prévention des attaques.

Réagir à un contenu suspect

Reconnaître un contenu suspect est un bon début, mais les utilisateurs ont également besoin de savoir ce qu'il faut faire ensuite. Votre organisation doit mettre en place un système de signalement des messages e-mails suspects, ou d'autres supports et comportements douteux. Pour les e-mails, il est recommandé que les utilisateurs transfèrent tout ce qu'ils trouvent bizarre vers une adresse e-mail spécifique. Il s'agit pour votre personnel de sécurité de surveiller cette adresse e-mail et d'examiner tous les messages signalés. Au début, vous constaterez peut-être que les utilisateurs transfèrent des messages en surnombre vers l'adresse e-mail surveillée. Toutefois, si votre personnel de sécurité répond en expliquant si oui ou non le message était malveillant et pourquoi, les utilisateurs affineront leurs connaissances et le nombre de fausses alertes liées à des messages suspects devrait diminuer.

Répéter le message

Il serait formidable que la formation de sensibilisation à la sécurité soit « mémorisée » pour toujours, mais malheureusement les choses ne se passent pas ainsi. Les utilisateurs oublient combien la sécurité est importante, ils se préoccupent de leurs délais et se lassent d'être toujours vigilants. Une caractéristique qui se retrouve dans tous les programmes de sensibilisation à la sécurité est leur permanence.

Au lieu d'offrir une seule formation ponctuelle de sensibilisation à la sécurité, une formation périodique récurrente doit être exigée. Variez également les modes de diffusion. Une série mensuelle ou trimestrielle de courtes sessions de formations est souvent plus efficace qu'une session annuelle d'une demi-journée. L'objectif de ce type de formation devrait être de rappeler périodiquement au personnel son rôle en matière de sécurité et comment s'en acquitter de manière optimale.

Mettre en œuvre les bonnes pratiques de sécurité

Au lieu d'essayer de réinventer la roue, établissez des bonnes pratiques qui soient bien respectées : c'est un bon point de départ pour élaborer un plan de sécurité. Heureusement, de nombreuses organisations ont reconnu l'utilité de bonnes pratiques éprouvées et efficaces pour la prévention des attaques par ransomware. Ces bonnes pratiques ne figurent

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

dans aucun référentiel, mais cette section répertorie certaines des actions les plus utiles qu'une organisation puisse entreprendre pour prévenir les attaques par ransomware.

Adoption d'un comportement utilisateur sûr

Une fois que votre personnel comprend le mode de fonctionnement du ransomware, il accepte plus facilement de suivre les consignes applicables au comportement en ligne. Les utilisateurs peuvent faire (ou éviter) un grand nombre de tâches pour rendre leur environnement informatique plus sûr et moins sujet aux attaques par ransomware. Voici certaines opérations qu'ils peuvent effectuer pour rester en sécurité :

- Vérifier l'expéditeur de l'e-mail avant d'ouvrir un message.
- N'ouvrir les pièces jointes que si vous faites confiance à l'expéditeur.
- Ne pas ouvrir des pièces jointes que vous n'attendez pas.
- Ne pas suivre les liens contenus dans les e-mails.
- Ne pas répondre aux messages qui semblent suspects.
- Transférer tout message suspect à votre groupe de sécurité.
- Consulter uniquement les sites Web dignes de confiance.
- Ne pas fournir des informations personnelles, à moins de faire confiance au site Web, à la raison pour laquelle les données sont nécessaires, et uniquement pour des interactions dont vous avez eu l'initiative.
- Ne connecter/insérer/installer un dispositif externe (tel qu'une clé USB) que si son origine est digne de confiance.
- Toujours utiliser un réseau privé virtuel lorsque vous vous connectez depuis un site distant.
- Appliquer tous les correctifs à vos logiciels et système d'exploitation et les tenir à jour.

Si vous suivez ces bonnes pratiques, il sera difficile pour un pirate de réussir son attaque par ransomware.

Renforcer votre environnement informatique

La mise en œuvre des bonnes pratiques concerne aussi les personnels informatique et de sécurité. Les bonnes pratiques suivantes permettent

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

de fournir et de maintenir un environnement plus sécurisé pour vos utilisateurs.

- Identifier toutes les données critiques.
- Créer des copies de sauvegarde périodiques de toutes les données critiques.
- Développer et tester un plan de récupération complet.
- Installer les derniers correctifs de sécurité sur tous les ordinateurs et périphériques.
- Exiger un réseau privé virtuel pour tout accès distant.
- Exiger un logiciel antivirus/antimalware sur tous les ordinateurs et périphériques.
- Mettre en œuvre l'analyse et le filtrage des logiciels malveillants sur les serveurs de messagerie.
- Implémenter des pare-feux comprenant des jeux de règles restrictifs sur chaque frontière de confiance.
- Fournir en continu une formation de sensibilisation à la sécurité pour l'ensemble du personnel.
- Instaurer, faire connaître et doter en personnel une fonction de support qui enquête sur tous les messages ou les sites Web suspects signalés.

Aucun niveau de prévention n'étant efficace à 100 %, c'est chaque petit effort qui compte. Chaque attaque de ransomware que vous empêchez est une attaque dont vous n'aurez pas à récupérer. La meilleure stratégie est d'empêcher le plus grand nombre d'attaques possible et de vous préparer pour la reprise si une attaque réussit à vous atteindre.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

DANS CE CHAPITRE

- Identification d'une attaque au moment où elle se produit
- Signalement aux personnes concernées pour qu'elles répondent à l'attaque
- Évaluation de l'étendue des dommages résultant d'une attaque

Chapitre 4
Identifier une attaque par ransomware et évaluer le rayon d'explosion

Même si vous mettez tout en jeu pour éviter une attaque par ransomware, il est possible qu'une attaque vous atteigne. Dans ce chapitre, vous verrez comment identifier dès le départ une attaque par ransomware et comment évaluer l'étendue des dommages.

Détection d'une attaque au plus vite

Lorsqu'elle réussit, une attaque par ransomware infecte un ou plusieurs systèmes, puis elle trouve et chiffre les fichiers critiques. Comme le chiffrement des fichiers prend du temps, plus vous détectez et arrêtez l'attaque à un stade précoce, plus vous limiterez le nombre de fichiers à récupérer.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Une réaction efficace dépend d'une alerte précoce

Comme pour tout type d'attaque (cyberattaque ou autre), une détection précoce permet de limiter les dommages et de récupérer plus vite les données. Si, grâce à une prise en charge rapide, vous empêchez le pirate d'endommager vos données comme il le souhaite, vous aurez moins de nettoyage à faire.

S'atteler précocement au travail de reprise n'est possible que si vous disposez d'un système d'alerte précoce. Hélas, selon une enquête récente, plus de la moitié des ransomware signalés et analysés n'ont été découverts qu'après plus d'un mois. Cela signifie que, dans la plupart des cas, l'attaque sévissait depuis plusieurs semaines. Vous ne voulez évidemment pas faire partie de ces statistiques.

Réduction de la charge de travail (et du temps) de reprise

Même si vous détectez une attaque dans un délai bien inférieur à un mois, le travail nécessaire pour la reprise peut être conséquent. Plus le temps s'écoule, plus le nombre de fichiers chiffrés par l'attaque augmente. Une alerte précoce et une réaction rapide peuvent considérablement réduire le volume du travail de récupération. D'autre part, si le nombre de fichiers à récupérer est plus faible, l'activité de votre entreprise peut reprendre plus rapidement que si vous êtes moins réactif.

Aperçu des différentes méthodes de détection des attaques

Les opérations effectuées par les logiciels de ransomware ne sont pas de même nature que les opérations normales. Contrairement aux applications classiques de chiffrement des fichiers, le ransomware chiffre des fichiers en plus grand nombre et en un laps de temps très court. Déceler une attaque par ransomware repose sur la détection d'un comportement ou de changements inhabituels. Dans cette section, nous vous présenterons deux approches de détection des attaques par ransomware.

Reconnaître les signatures de ransomware

La première approche de détection du ransomware consiste à étendre le champ de détection des logiciels malveillants quels qu'ils soient. Il est facile de détecter des logiciels malveillants connus en comparant une partie du code d'un programme exécutable avec les signatures de code stockées dans une base de données. Si ces données correspondent, vous

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

avez probablement trouvé un programme malveillant. Cette méthode peut également s'appliquer aux signatures de ransomware. Cette approche a pour principal inconvénient que vous devez tenir à jour vos bases de données avec les signatures les plus récentes, et que tout ransomware totalement nouveau ou légèrement modifié sera impossible à détecter. Une nouvelle attaque ne sera détectée que si quelqu'un la signale et si la signature du ransomware est ajoutée dans la version suivante de la base de données de signatures.

ATTENTION

La comparaison des signatures présente l'inconvénient que le ransomware est toujours plus sophistiqué et évolue rapidement, de sorte que de nouvelles signatures apparaissent sans cesse.

L'apprentissage automatique mis à profit pour reconnaître les anomalies

Une autre approche pour détecter les comportements malveillants consiste à utiliser des algorithmes d'apprentissage automatique (machine learning - ML) pour comparer le comportement en cours avec un comportement et un état du système de fichiers normaux. Les algorithmes ML sont très performants pour assimiler les caractéristiques d'un comportement « normal » et signaler tout comportement qui semble anormal. Ils peuvent analyser les processus en cours d'exécution et les ressources utilisées par ces derniers, ainsi que les changements inhabituels apparaissant dans le système de fichiers.

Par exemple, l'application Radar de Rubrik exploite l'intelligence artificielle pour analyser les changements du système de fichiers. Radar examine le type et la fréquence des changements, ainsi que les signes de chiffrement et les changements dans l'entropie des fichiers. Radar fournit une couche d'intelligence supplémentaire qui alerte en cas de comportement inhabituel.

CONSEIL

Votre première ligne de défense doit être constituée d'outils de détection et de surveillance en temps réel qui décèlent assez tôt les changements suspects.

Réaction face à une attaque

Face à tout incident de sécurité, y compris la détection d'une attaque par ransomware, votre réaction devrait être de suivre tout simplement votre plan d'intervention. Pour ce faire, vous devez évidemment disposer d'un plan et d'une équipe bien entraînée.

Mise en place de l'équipe d'intervention

Votre équipe d'intervention doit être constituée et formée bien avant qu'elle soit prête à récupérer vos données après une attaque par

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

ransomware. L'équipe d'intervention en cas d'attaque par ransomware peut être celle qui répond aux autres incidents de sécurité, mais elle doit être formée spécifiquement à ce type d'attaque. L'essentiel est de constituer une équipe, de la former, et qu'elle exécute des tests de plan d'intervention pour être prête en cas d'attaque.

Limiter les dommages et identifier les fichiers affectés

Une fois que vous avez lancé votre processus de reprise après une attaque par ransomware, les choses sérieuses commencent. Votre principal objectif est d'arrêter l'attaque et tout dommage supplémentaire, puis de restaurer les ordinateurs et les fichiers affectés dans un état utilisable. La première phase de récupération consiste à limiter les dommages de l'attaque et à évaluer leur envergure.

Limiter tout dommage supplémentaire

L'équipe d'intervention devrait déjà avoir cerné quels ordinateurs participent à l'attaque. Sa première action doit être de stopper les processus de ransomware, généralement en mettant hors tension tous les ordinateurs affectés. L'étape suivante consiste à vérifier si d'autres ordinateurs participent activement à l'attaque et à les mettre également hors tension.

Les ordinateurs affectés peuvent être remis en service en les déconnectant de l'ensemble des réseaux. Ceci vous permet d'accéder aux ordinateurs et périphériques de stockage pour en retirer le ransomware.

Évaluation du rayon d›explosion

Une fois que vous avez arrêté l'attaque, il est temps d'évaluer les dommages. L'envergure des dommages est souvent désignée par le terme de rayon d'explosion. Pour une attaque par ransomware, le rayon d'explosion représente la série de fichiers ayant été modifiés au cours de l'attaque. Lorsqu'il chiffre les fichiers, dans la plupart des cas, le ransomware ajoute ou modifie leur extension ce qui facilite grandement l'identification des fichiers endommagés. Le ransomware crée parfois un manifeste au fur et à mesure du chiffrement des fichiers. Dans les deux cas, vous devriez être en mesure de déterminer l'étendue du rayon d'explosion. Le rayon d'explosion est lié à la durée de l'attaque — plus vous attendez, plus vous avez de dommages à réparer.

L'évaluation du rayon d'explosion vous prépare pour l'étape suivante — la reprise. Si vous avez élaboré un bon plan d'intervention en cas d'attaque par ransomware et avez protégé vos fichiers de sauvegarde, la reprise devrait être assez simple.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

DANS CE CHAPITRE

- Élaboration d'un plan pour atteindre vos objectifs de reprise
- Processus de récupération limité aux seules données impactées
- Récupération automatisée pour plus de rapidité et fiabilité
- Plusieurs couches de défense pour une réponse homogène face au ransomware

Chapitre 5
Récupérer vos données avec une précision chirurgicale

Une fois que vous avez détecté une attaque, mis fin à sa propagation et identifié les fichiers qui ont été affectés, c'est alors qu'il vous faut déclencher votre plan de reprise. Un bon plan de reprise rend le retour à la normale aussi rapide et facile que possible. La précision et la vitesse sont les clés d'une récupération rapide et fiable. Dans ce chapitre, vous découvrirez comment créer, tester et appliquer un plan de reprise après une attaque de ransomware, qui vous protégera de toute menace.

Création d'un plan de reprise rapide

Pour la reprise après une attaque par ransomware, il est essentiel qu'un plan offre la souplesse nécessaire pour récupérer les fichiers de façon granulaire. Une reprise granulaire signifie que vous pouvez extraire une copie des fichiers affectés qui soit antérieure au chiffrement par le ransomware. Cela vous évite de restaurer l'ensemble des fichiers sauvegardés. Une fois que vous savez quels fichiers récupérer, le reste du plan consiste simplement à exécuter les étapes nécessaires à leur récupération.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

La sauvegarde n'est qu'une première étape

La reprise après une attaque par ransomware repose sur une bonne stratégie de sauvegarde, mais le plan ne s'arrête pas là. Les sauvegardes auxquelles vous pouvez vous fier et que vous pouvez utiliser pour la reprise après une attaque par ransomware doivent garantir l'immuabilité et fournir l'accès facile aux personnes autorisées. Vous devez créer un plan avec des procédures simples mais détaillées vous permettant de récupérer une liste de fichiers. Ce plan devrait vous guider dans le développement des actions de récupération et l'estimation du temps nécessaire à la reprise.

Les spécifications d'évaluation sont l'un des rouages essentiels dans un plan de reprise. Chaque plan de reprise devrait contenir des directives sur les méthodes à suivre et la fréquence des tests.

CONSEIL

Ne faites jamais confiance à un plan qui n'a pas été testé. Il est recommandé de procéder à des tests récurrents et de différents niveaux d'intensité, allant d'une simple analyse à une reprise après incident complète. Plus vous avancez vers les tests de reprise complète, plus le risque augmente ; vous devez donc planifier minutieusement comment tester votre plan de reprise sans vous exposer à un risque excessif. Une méthode simple consiste à récupérer d'abord les fichiers hors de l'environnement de production pour évaluer la validité des procédures de reprise. Vous pourriez ensuite récupérer les fichiers non critiques dans un environnement de production avant de passer à un test de reprise après une interruption totale.

Une reprise réussie repose sur l'évaluation du temps de reprise

Dans tout plan de reprise, une exigence métier importante est d'atteindre l'objectif de temps de reprise (recovery time objective - RTO) de l'organisation. Votre plan de reprise doit restaurer votre organisation à un objectif de point de reprise (recovery point objective - RPO) au sein du RTO. Le RPO définit les conditions que vous devez remplir pour restaurer vos CBF et reprendre vos opérations normales.

Autrement dit, votre plan de reprise doit restaurer les opérations définies par le RPO et le faire avant l'expiration du délai défini par le RTO. Si le processus de reprise dépasse le délai du RTO, vos processus métier en souffriront. Considérez le RPO et le RTO comme des contraintes qui limitent l'envergure de votre intervention et le temps qui est nécessaire à la reprise. Si vous ne vous limitez pas au RPO, vous risquez presque toujours de dépasser le RTO.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Une reprise limitée aux fichiers nécessaires

De nombreux plans de reprise après une attaque par ransomware reposent sur la restauration complète des ordinateurs. Que vous utilisiez la virtualisation et des points de contrôle, ou une image de sauvegarde complète pour restaurer un ordinateur, ces méthodes manquent de finesse. Une attaque par ransomware ne chiffre pas tous les fichiers, vous ne devriez donc pas tous les restaurer. Dans cette section, vous découvrirez une meilleure méthode qui évite des tâches et un temps de reprise trop importants.

Cibler seulement les données nécessaires

Une approche trop lourde de la reprise après une attaque par ransomware pourrait augmenter l'étendue des dommages. Vous n'avez besoin de restaurer que les fichiers chiffrés par le ransomware ; pourquoi donc restaurer autre chose ?

Les fonctions de l'entreprise chargées des opérations courantes normales modifient les données chaque jour. Ces changements sont coordonnés en grand nombre entre plusieurs fichiers, bases de données ou même ordinateurs. Toute opération qui écrase les changements apportés aux données en restaurant une version antérieure « annule » en fait les changements. Si vous restaurez des fichiers qui n'ont pas été affectés par une attaque de ransomware, vous risquez de perdre des transactions ou même de vous désynchroniser des autres systèmes.

Par exemple, supposons que votre entreprise vende des articles pour animaux en ligne. Une attaque par ransomware a commencé par chiffrer vos documents Microsoft Word et Adobe Acrobat sur votre serveur de traitement des commandes. Vous avez détecté l'attaque après plusieurs heures et suivi l'ancienne procédure de reprise après une attaque par ransomware. Cette procédure obsolète a conduit l'équipe d'intervention à mettre hors tension l'ordinateur et à restaurer toutes les données depuis un point temporel antérieur à l'attaque. Au lieu de récupérer seulement les fichiers affectés, vous avez supprimé toutes les commandes reçues après le début de l'attaque et perdu le lien de toutes les commandes déjà envoyées à votre service d'expédition. Votre service de facturation se plaint du désordre engendré par votre « reprise ».

CONSEIL

Une bien meilleure approche serait d'intégrer au plan de reprise un service multicouches, tel que les services de reprise de Rubrik, qui peut faciliter une reprise ciblée.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Suppression des pertes de temps

En plus d'éviter une opération de reprise qui écrase trop de données, une reprise ciblée vous fait gagner du temps. Et si votre fournisseur de solution de sauvegarde expose les API pour qu'elles facilitent une reprise granulaire, vous pouvez récupérer facilement et vite les seuls éléments dont vous avez besoin. Rubrik vous donne la capacité d'identifier les fichiers affectés et de ne restaurer que ceux-ci à l'état dans lequel ils étaient avant l'attaque, à partir d'un référentiel de sauvegarde digne de confiance et non modifiable.

Automatisation de la reprise à grande échelle

Enfin, l'élément déterminant pour un processus de reprise aisé après une attaque est l'automatisation des actions répétitives et redondantes. Si 10 000 de vos fichiers ont été chiffrés par une attaque, l'automatisation de la restauration de tous ces fichiers rend le processus plus rapide et plus fiable. Dans cette section, vous verrez comment Rubrik permet une restauration des fichiers rapide et efficace grâce à l'automatisation.

Implémentation des API pour une reprise sans intervention

Rubrik fournit des API permettant d'accéder à des fichiers et de les extraire de son système de fichiers de sauvegarde non modifiables. Les API de Rubrik fournissent un accès sécurisé à vos fichiers à la demande et dans n'importe quel langage hôte. Vous pouvez créer un logiciel dans le langage de votre choix pour accéder à vos fichiers. Rubrik n'impose aucune interface utilisateur rigide comme seul moyen d'accès à vos données. Ce sont vos données. Vous êtes en droit d'y accéder ; en revanche, il vous faut utiliser des interfaces de programmation souples et sécurisées.

Scripts garants de haute performance

Les interfaces de programmation d'accès aux données de Rubrik sont le nec plus ultra en matière de reprise après une attaque par ransomware. Une fois que vous avez identifié la liste des fichiers chiffrés par le ransomware, vous pouvez écrire un script dans le langage de votre choix pour procéder à la restauration. Pour chaque fichier dans la liste, il suffit de lancer une requête sur vos données de sauvegarde à l'aide de l'API Rubrik pour trouver la dernière version de sauvegarde antérieure à l'attaque, puis d'appeler une autre API pour la restaurer. Vos scripts, pris en charge par les systèmes de Rubrik, restaureront les données de votre organisation à un état opérationnel de façon rapide et efficace.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Chapitre 6
Dix conseils pour faire face aux attaques par ransomware

Après avoir appris ce qu'est un ransomware, survivre à une attaque peut sembler une tâche ardue. Toutefois, une fois que vous avez compris le mode opératoire d'une attaque, que vous savez comment éviter une attaque et comment récupérer une fois qu'elle se produit, la planification de votre stratégie de défense peut être un projet assez simple. Cette liste répertorie dix conseils pour constituer un plan qui vous permettra non seulement de surmonter une attaque mais également de poursuivre vos activités.

- **Former les utilisateurs à éviter les attaques par ransomware.** Formez tous les utilisateurs à reconnaître les attaques par ransomware courantes, pour éviter d'en être victime. Fournissez-leur un moyen simple de signaler les messages ou sites Web suspects et formez les utilisateurs sur les procédures à suivre pour signaler toute activité anormale.
- **Activer le filtrage des serveurs de messagerie.** Les serveurs de messagerie actuels comprennent des options ou prennent en charge des modules complémentaires permettant de filtrer les e-mails et les pièces jointes afin d'en déceler les contenus suspects. Recherchez comment activer et utiliser cette fonction sur votre serveur de messagerie.
- **Identifier les fichiers critiques.** Faites l'inventaire des fonctions métier critiques de votre organisation et des données nécessaires à chacune pour opérer. Créez un manifeste des fichiers critiques à la poursuite des activités de votre organisation. Vos efforts de protection et de récupération devraient être axés sur cette liste de fichiers.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

- **Choisir le bon fournisseur de services de sauvegarde.** Choisissez un fournisseur de services de sauvegarde capable de garantir l'immuabilité des sauvegardes et un accès facile aux fichiers déchiffrés via des API flexibles mais sécurisées. Ces deux fonctions font partie intégrante de la conception de l'offre de services de Rubrik.
- **Sauvegarder vos données critiques en un lieu non modifiable.** Sauvegardez fréquemment tous les fichiers figurant sur votre manifeste de fichiers critiques chez un fournisseur de services de sauvegarde qui garantit l'immuabilité, tel que Rubrik, afin d'assurer qu'un ransomware ne peut chiffrer vos sauvegardes.
- **Développer un plan de récupération des fichiers.** Bien que sauvegarder les fichiers critiques soit déjà un premier pas majeur, il s'agit de développer un plan en bonne et due forme pour récupérer les fichiers si un processus de récupération devient nécessaire. Documentez les conditions dans lesquelles il convient d'effectuer une reprise, qui en sera chargé, comment identifier les fichiers à récupérer et procéder aux restaurations.
- **Créer des modèles d'automatisation pour une reprise rapide.** Lorsque vous avez besoin d'activer votre plan, la fourniture d'une simple liste des fichiers à récupérer devrait suffire. Cela signifie que votre plan doit intégrer des modèles de script permettant de procéder à la récupération de n'importe quelle liste de fichiers. Les modèles de script vous donnent la capacité de tester le processus de récupération à de nombreuses reprises et d'en affiner l'exécution.
- **Tester fréquemment votre plan.** En plus de tester les différents scripts, il importe de tester fréquemment l'ensemble du plan de reprise. Le seul plan valide est un plan qui répond à vos exigences en matière de RPO et de RTO. Vérifiez que chaque collaborateur concerné est bien familiarisé avec son rôle et les étapes du plan. Des tests fréquents valident l'efficacité du plan dans des environnements changeants et maintiennent le personnel apte et prêt à réagir.
- **Surveiller les fichiers critiques pour déceler des changements anormaux.** Mettez en œuvre la surveillance d'intégrité sur les systèmes de fichiers de production afin de détecter des changements anormaux comme ceux qui sont significatifs d'un ransomware. Pour ajouter une couche de protection, mettez en œuvre une surveillance similaire pour les lieux de sauvegarde. Toutes les modifications de sauvegarde non autorisées ou les changements inhabituels apportés aux fichiers précédemment sauvegardés doivent être relevés. Vérifiez que votre fournisseur de services de sauvegarde émet des alertes en cas de modifications suspectes des sauvegardes.
- **Former et déployer une équipe d'intervention en cas d'incident.** Constituez une équipe de collaborateurs ayant expressément pour mission de réagir à toute suspicion d'attaque par ransomware. Cette équipe doit parfaitement maîtriser le plan de reprise, avec des rôles bien définis et rodés pour chacun de ses membres. Assurez-vous que chaque membre de l'équipe prend part à des tests fréquents pour que tous soient prêts à réagir en cas de demande d'intervention.

Ces documents sont protégés par le copyright © 2022 John Wiley & Sons, Inc. Toute divulgation, toute distribution et tout usage non autorisés sont strictement interdits.

Accélérer la reprise après une attaque par ransomware

Aujourd'hui, les entreprises dépendent de leurs données et à mesure que celles-ci ont gagné en valeur, le ransomware est devenu une vraie menace. Une menace que l'on ne peut se permettre d'ignorer. L'exploitation des connaissances est la clé pour déjouer les attaques. Ces connaissances ont trait au fonctionnement du ransomware et aux méthodes à suivre pour reprendre votre activité après une attaque. *La reprise après une attaque par ransomware pour les Nuls* vous montre comment, quand et où le ransomware peut attaquer, ainsi que la procédure à suivre par votre organisation pour se préparer à une attaque, en évaluer l'impact et récupérer rapidement si elle se produit.

À l'intérieur...

- Sachez-en plus sur les modes d'attaque par ransomware
- Appliquez une stratégie de défense en profondeur
- Garantissez la sécurité en formant les utilisateurs
- Accédez aux fichiers endommagés après une attaque
- Reprenez rapidement vos opérations avec une perte de données minimale

rubrik

Michael G. Solomon, PhD, est un consultant en cybersécurité qui propose aux dirigeants une méthode pour aligner leurs exigences de conformité sur leurs objectifs stratégiques. Le Dr Solomon est professeur à l'Université des Cumberlands et titulaire d'un PhD en Sciences informatiques décerné par l'Université Emory.

Allez sur Dummies.com®
pour voir des vidéos, des exemples pas à pas, des articles pratiques, ou pour faire des achats !

ISBN: 978-1-119-84899-8
Revente interdite

9 781119 848998

pour les nuls®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.