Proposé par :

rubrik

Sécurité des données Zero Trust

pour les nuls

Comment prendre un bon départ avec la sécurité des données Zero Trust

Pourquoi votre organisation a besoin de la sécurité des données Zero Trust

Définition d'une architecture Zero Trust

Édition spéciale Rubrik

Lawrence Miller

À propos de Rubrik

Rubrik assure une sécurité sans faille des données, ce qui vous donne la possibilité de vous remettre de toute menace, attaque par ransomware ou interruption d'activité. Peu importe où se trouvent vos données, la plateforme de sécurité des données Zero Trust de Rubrik garantit que vos données ne seront jamais perdues et resteront prêtes en toutes circonstances. Avec Rubrik, l'activité de votre entreprise devient invincible.

Sécurité des données Zero Trust

Édition spéciale Rubrik

de Lawrence Miller

pour les nuls®

Sécurité des données Zero Trust pour Les Nuls®, une édition spéciale Rubrik

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

ISBN 978-1-119-98265-4 (pbk) ; ISBN 978-1-119-98266-1 (ebk)

Pour obtenir des renseignements généraux sur nos autres produits et services, ou sur la publication d'un livre sur mesure *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 : Camille Graves

Représentante du développement commercial : Jeremith Coward

Éditeur de la production : Tamilmani Varadharaj

Table des matières

Introduction

Les cybermenaces se multiplient rapidement et visent les organisations de tous les secteurs d'activité, tout au long de la chaîne d'approvisionnement. À elles seules, les attaques par ransomware ont bondi de 700 % en 2021, selon Bitdefender. Si les récentes attaques par ransomware les plus médiatisées ont visé des infrastructures stratégiques et la chaîne d'approvisionnement, il y en a eu beaucoup d'autres, mettant en péril les opérations commerciales essentielles de tous les types d'organisations.

Malgré des investissements massifs dans les défenses de sécurité du périmètre, des points d'accès et des applications, les cybercriminels continuent d'accéder aux données et l'on estime que deux attaques par ransomware sur trois visent désormais la dernière et meilleure défense d'une entreprise, à savoir ses systèmes de sauvegarde des données.

Le Zero Trust est généralement mis en œuvre en tant que modèle de sécurité des réseaux, mais ses principes s'appliquent également à la sécurité des données et à l'architecture de sécurité en général. Dans ce livre, vous découvrirez comment la sécurité des données Zero Trust peut renforcer l'efficacité des défenses de votre organisation contre les cybermenaces modernes.

À propos de cet ouvrage

Le livre *Sécurité des données Zero Trust pour Les Nuls*, Édition spéciale Rubrik, comporte quatre chapitres qui explorent les thèmes suivants :

- Pourquoi devez-vous implémenter la sécurité des données Zero Trust pour votre organisation (chapitre 1) ?
- Qu'est-ce qu'une architecture Zero Trust (chapitre 2) ?
- Comment prendre un bon départ avec la sécurité des données Zero Trust (chapitre 3) ?
- Dix clés pour une réponse efficace aux incidents (chapitre 4)

Chaque chapitre est rédigé comme un tout indépendant du reste de l'ouvrage. Si un sujet vous intéresse, vous pouvez donc passer directement au chapitre qui s'y rapporte. Vous pouvez lire cet ouvrage dans le sens qui vous convient, mais nous vous déconseillons de le lire à l'envers ou de droite à gauche.

Quelques suppositions simplistes

On dit que la plupart des hypothèses ont fait leur temps, mais nous en faisons tout de même quelques-unes !

Nous supposons principalement que vous êtes un directeur informatique (CIO), un directeur de la sécurité informatique (CISO), un vice-président, un architecte, un ingénieur, un administrateur ou un analyste responsable de la sauvegarde et de la récupération des données stratégiques de votre organisation. Ce livre s'adresse donc principalement aux techniciens qui comprennent au moins les rudiments des technologies et des défis en matière de sécurité et de sauvegarde.

Si l'une de ces hypothèses vous correspond, alors c'est le livre qu'il vous faut ! Si vous ne vous reconnaissez dans aucune de ces hypothèses, poursuivez quand même votre lecture. C'est un excellent livre et vous apprendrez énormément sur la sécurité des données Zero Trust.

Icônes employées dans ce livre

Tout au long de ce livre, nous utilisons occasionnellement certaines icônes pour attirer l'attention du lecteur sur des informations importantes. Voici à quoi vous pouvez vous attendre :

RAPPEL

Cette icône signale des informations importantes à inscrire obligatoirement dans votre mémoire non volatile, votre matière grise ou votre crâne.

JARGON TECHNIQUE

Cette icône explique le jargon qui se cache derrière le jargon ; il s'agit de l'étoffe dont les héros (les nerds) sont faits !

CONSEIL

Les conseils sont appréciés, jamais attendus. Nous espérons que vous apprécierez ces informations utiles.

ATTENTION

Ces avertissements soulignent des choses contre lesquelles votre mère vous a mis en garde. Ou peut-être pas. Mais ils offrent des conseils pratiques.

Au-delà de ce livre

Ce sujet est tellement vaste qu'il est impossible de tout aborder dans ce livre. Donc, si en arrivant à la fin du livre, vous vous demandez : « Où puis-je en savoir plus ? », il vous suffit de consulter `rubrik.com`.

DANS CE CHAPITRE

- Définir la sécurité des données Zero Trust
- Comprendre les défis liés aux architectures de sauvegarde existantes
- Explorer les problèmes de sécurité et de confidentialité des données
- Profiter des avantages de l'architecture Zero Trust

Chapitre 1
Reconnaître la nécessité d'une sécurité des données Zero Trust

Dans ce chapitre, vous apprendrez en quoi consiste la sécurité des données Zero Trust et pourquoi les anciennes architectures de sauvegarde sont vulnérables aux menaces modernes, notamment celles du ransomware. Vous découvrirez également les exigences en matière de sécurité des données et les avantages d'une architecture Zero Trust pour la protection des données.

Comprendre la sécurité des données Zero Trust

Les moyens de défense traditionnels qui protègent le réseau interne « fiable » d'une organisation contre les réseaux externes « non fiables » (comme Internet) sont en train d'échouer. Le périmètre du réseau a pratiquement disparu avec la prolifération des terminaux — notamment les PC de bureau et les ordinateurs portables, les smartphones et les tablettes, ainsi que les appareils de l'Internet des objets (IoT) — et l'adoption rapide du télétravail à domicile et du télétravail en tout lieu dans le sillage de la pandémie mondiale. En conséquence, les cybercriminels parviennent à faire une brèche dans les contrôles de

sécurité du réseau et contournent facilement les protections des terminaux.

Ces nouvelles menaces incitent de nombreuses organisations à adopter une approche de cybersécurité fondée sur le Zero Trust. Le modèle de sécurité « Zero Trust » s'appuie sur ce concept : « ne jamais faire confiance, toujours vérifier ». En d'autres termes, aucun utilisateur, aucun appareil ou aucune ressource (y compris les utilisateurs, les applications, les services, les bases de données, etc.) n'est intrinsèquement « fiable » du simple fait qu'il se trouve « sur le réseau ». Au contraire, l'identité de chaque utilisateur, appareil et ressource doit être vérifiée positivement à chaque connexion au réseau et le niveau minimum d'autorisations nécessaires est octroyé pour lui permettre d'exécuter une fonction autorisée sur un laps de temps limité.

Bien que le Zero Trust ne soit pas un nouveau concept, il a suscité beaucoup d'attention ces dernières années, car de plus en plus d'organisations reconnaissent son efficacité contre les nouvelles menaces et les fournisseurs de technologies cherchent à tirer parti de cette tendance. Malheureusement, cette situation peut souvent créer de la confusion car les fournisseurs tentent parfois de redéfinir une tendance pour l'adapter à leurs offres de produits. Pour éviter ce biais, de nombreux fournisseurs, dont Rubrik, suivent le modèle Zero Trust tel que défini par le National Institute of Standards and Technologies (NIST) des États-Unis dans la publication spéciale (SP) 800-207, *Zero Trust Architecture*.

RAPPEL

Comme le définit le NIST, le Zero Trust comprend « un ensemble évolutif de paradigmes de cybersécurité qui déplacent les défenses des périmètres statiques basés sur le réseau, pour se concentrer sur les utilisateurs, les actifs et les ressources ». Selon le NIST, une architecture Zero Trust utilise les principes Zero Trust lors de la création d'infrastructures et de flux de production d'entreprise et l'accent est mis sur la protection des utilisateurs, des appareils et des ressources plutôt que sur un périmètre réseau arbitraire. Pour le NIST, une architecture Zero Trust adhère aux sept principes de base suivants :

- Tous les appareils et services qui se connectent au réseau et qui envoient, reçoivent ou traitent des données doivent être traités comme des ressources à vérifier et à protéger.
- Indépendamment de l'emplacement et de la propriété (c'est-à-dire une connexion dans et en dehors du réseau et de l'entreprise, personnelle ou tierce) d'une ressource, toutes les communications sont protégées par le moyen le plus sûr disponible.
- L'accès le moins privilégié aux différentes ressources de l'entreprise est accordé en fonction de la session après vérification de la fiabilité et n'est pas transférable à d'autres ressources de l'entreprise.

- Des stratégies dynamiques sont utilisées pour déterminer si l'accès à une ressource est accordé, en fonction d'attributs comportementaux et environnementaux comme la version du logiciel, l'emplacement réseau, la date et l'heure de la demande, etc.
- Toutes les ressources qui se connectent au réseau de l'entreprise sont surveillées et évaluées en permanence afin de garantir que la sécurité du réseau de l'entreprise n'est pas compromise.
- L'authentification et l'autorisation des ressources (y compris la réauthentification et la réautorisation) sont dynamiques et strictement appliquées (à l'aide de technologies comme l'authentification multifacteur (MFA) et la surveillance continue) avant que l'accès ne soit accordé.
- Un maximum de données est collecté sur l'état actuel des ressources, de l'infrastructure réseau et des communications afin d'améliorer la sécurité du réseau de l'entreprise.

Les composants logiques qui composent une architecture Zero Trust d'entreprise sont les suivants (voir la figure 1-1) :

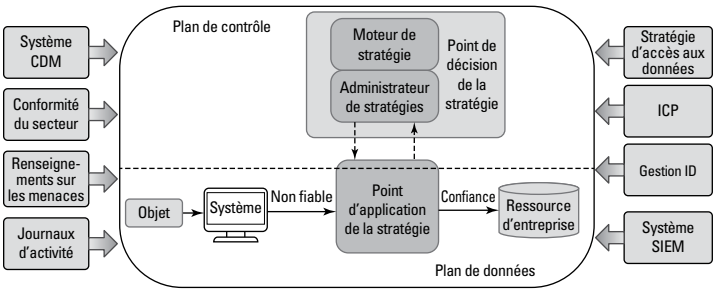

FIGURE 1-1 : Composants logiques d'une architecture Zero Trust. (Source : NIST SP 800-207, *Zero Trust Architecture*)

- **Plan de contrôle**

  Le *point de décision de stratégie* consistant en un *moteur de stratégies* responsable de l'octroi de l'accès à une ressource et un *administrateur de stratégies* responsable de la génération de tous les jetons (ou des identifiants) d'authentification et d'autorisation spécifiques à la session utilisés par le point d'application d'une stratégie pour permettre la communication entre les utilisateurs/appareils et les ressources d'entreprise.

- **Plan de données**

  Le *point d'application des stratégies*, chargé de l'activation, de la surveillance et de l'interruption des connexions entre les utilisateurs/appareils et les ressources de l'entreprise.

- **Composants supplémentaires**

  Système de diagnostic et d'atténuation en continu (CDM) chargé de collecter des informations sur l'état actuel d'une ressource d'entreprise et de mettre à jour la configuration et les composants logiciels.

  Moteur de *conformité du secteur* responsable des règles de stratégie d'entreprise personnalisées qui permettent d'assurer la conformité réglementaire applicable.

  Surveillance des menaces constituée de flux en direct provenant de sources internes et/ou externes.

  Journaux d'activité, y compris les journaux réseau et système, pour fournir un retour d'information en temps réel ou quasi réel sur l'état de la sécurité.

  Politique d'accès aux données comprenant les attributs, les règles et les politiques utilisés par le moteur de stratégies pour gérer l'accès.

  Infrastructure à clé publique (ICP) responsable de la gestion des certificats de ressources, de sujets, de services et d'applications émis par l'entreprise.

  Système de gestion des identités qui fournit des services de gestion des identités et des accès pour l'entreprise.

  Système de gestion des informations et des événements liés à la sécurité (SIEM) qui collecte et regroupe les événements liés à la sécurité provenant de nombreuses sources de données de l'entreprise et génère des alertes.

Identifier les problèmes liés à la sauvegarde des données existantes

Les architectures de sauvegarde traditionnelles sont vulnérables face au ransomware et autres cyberattaques. Les composants types d'une architecture de sauvegarde traditionnelle comprennent un serveur Windows ou Linux exécutant l'application de sauvegarde. Le serveur est déployé sur le même réseau que les clients de sauvegarde (c'est-à-dire les autres serveurs du datacenter) et a accès à Internet pour permettre les mises à jour logicielles et la gestion à distance. Les informations d'identification du serveur de sauvegarde sont stockées dans Active Directory, avec d'autres comptes privilégiés, et affectées à un rôle comme celui d'opérateur de sauvegarde. Les sauvegardes sont souvent stockées sur un volume NFS (Network File System) ou SMB (Server Message Block) utilisé comme référentiel de sauvegarde.

L'architecture de sauvegarde n'étant pas isolée du réseau de production, celle-ci reste également vulnérable face au ransomware. Par conséquent, le ransomware a de multiples occasions d'infecter ou de corrompre les tâches de sauvegarde, soit sur le serveur de sauvegarde, soit sur le référentiel de sauvegarde, soit les deux.

DES SAUVEGARDES RÉGULIÈRES PROTÈGENT-ELLES CONTRE LE RANSOMWARE ?

Souvent les entreprises ont une idée fausse du risque posé par le ransomware et elles se disent : « nous sommes protégés parce que nous sauvegardons toutes nos données ». Les sauvegardes régulières sont essentielles, mais elles peuvent donner aux organisations un faux sentiment de sécurité. Les stratégies de sauvegarde traditionnelles peuvent échouer à protéger contre les attaques de ransomware pour deux raisons importantes :

- **Les cybercriminels ont développé des moyens de chiffrer ou de corrompre les sauvegardes en ligne.** De plus en plus d'attaques par ransomware ciblent les sauvegardes. Souvent, lorsque les cybercriminels prennent pied sur un réseau, l'une de leurs premières actions est de commencer à chiffrer ou à corrompre les données de sauvegarde. En général, cela se produit deux semaines ou plus avant qu'ils ne commencent à chiffrer les données de production. Ainsi, lorsque les organisations réalisent qu'elles sont attaquées, elles constatent souvent que leurs sauvegardes sont inutilisables.
- **La récupération des données de sauvegarde peut prendre tellement de temps que les entreprises sont forcées de payer des rançons.** La sauvegarde des données sur des bandes et leur stockage hors site constituaient autrefois la référence en matière de protection des données, mais ce n'est plus le cas. Il faut parfois plusieurs jours pour trouver les dernières bandes, les transférer sur place, les monter et les exécuter. De plus, la restauration sélective à partir d'une bande est difficile ; il faut restaurer tous les fichiers, et pas seulement ceux qui ont été chiffrés. De nombreuses organisations ne peuvent pas se permettre d'attendre la fin de ces opérations avant de redémarrer les systèmes essentiels à leur activité et finissent donc par s'exécuter face à la demande de rançon.

Analyse des problèmes de sécurité des données

Les données constituent l'actif le plus précieux d'une organisation et sont donc la cible des cybercriminels. Outre la protection de la confidentialité, de l'intégrité et de la disponibilité des données sensibles, les organisations doivent également garantir la confidentialité de leurs données.

Les réglementations relatives à la confidentialité des données, comme le règlement général sur la protection des données (RGPD), la loi californienne sur la protection de la vie privée des consommateurs (California Consumer Privacy Act, CCPA) et la loi californienne sur les droits à la vie privée (California Privacy Rights Act), imposent aux organisations des exigences strictes pour garantir la « confidentialité dès la conception » et la « confidentialité par défaut » dans leurs architectures de données. Ces exigences s'appliquent non seulement aux données des environnements de production, mais aussi à toutes les données stockées et utilisées dans un environnement, y compris les sauvegardes.

Profiter des avantages de la sécurité des données Zero Trust

RAPPEL

Les avantages d'une architecture de sécurité des données Zero Trust sont les suivants :

- Les **équipes informatiques** peuvent protéger les données stratégiques contre les attaques de ransomware, donnant à leur organisation la possibilité de récupérer rapidement les données et les applications sans payer de rançon.
- Les **équipes de sécurité** peuvent en toute confiance s'appuyer sur les données de sauvegarde sécurisées pour procéder à des investigations sur les attaques et lancer des opérations de récupération directement depuis leur centre d'opérations de sécurité (SOC).
- Les **propriétaires d'applications** peuvent dormir sur leurs deux oreilles en sachant que les données de l'entreprise sont protégées et qu'en cas d'attaque par ransomware, les applications peuvent être restaurées rapidement pour maintenir la continuité des activités.
- Les **directeurs des systèmes d'information (DSI) et les directeurs financiers** peuvent être assurés que les plans de récupération en cas de ransomware sont soutenus par une architecture Zero Trust qui permet à l'organisation de minimiser les coûts de cyberassurance et d'éviter les dommages à la réputation résultant d'attaques par ransomware.

DANS CE CHAPITRE

- Découvrir la protection des données Zero Trust
- Enquêter sur les ransomwares
- Découvrir des données sensibles
- Confiner les ransomwares pour accélérer la réponse aux incidents
- Orchestrer la reprise des applications

Chapitre 2
Comprendre l'architecture de sécurité des données Zero Trust

Dans ce chapitre, vous apprendrez comment les solutions de protection des données Zero Trust prennent en charge une architecture Zero Trust pour aider les clients à protéger leurs sauvegardes contre les attaques de ransomware et autres menaces.

Protection des données Zero Trust

La protection des données Zero Trust offre une gestion intelligente des données pour les environnements informatiques hybrides et multiclouds dans une plateforme logicielle unique qui assure en toute sécurité la sauvegarde, la restauration, l'analyse et la conformité dans les datacenters et les clouds.

Les principales fonctionnalités de la protection des données Zero Trust sont les suivantes :

- **Automatisation des contrats de niveau de service (contrats SLA) :** remplacez des centaines ou des milliers de tâches de sauvegarde par quelques stratégies qui peuvent être appliquées à toutes vos charges de travail.
- **Récupération rapide :** effectuez des recherches dans votre environnement global et trouvez exactement ce que vous cherchez. Cliquez sur « Récupérer et monter directement » pour atteindre des objectifs de délai de récupération (RTO) proches de zéro.
- **Priorité à l'utilisation des interfaces de programmation (API) :** tout comportement qui peut être déclenché à partir de l'interface utilisateur (IU) peut faire l'objet d'un script, être automatisé et intégré dans des outils que vous possédez probablement déjà.
- **Sécurité intégrée :** une fois les données de sauvegarde écrites, elles ne peuvent jamais être modifiées, ce qui signifie que vos sauvegardes sont protégées contre les ransomwares et autres menaces.

Enquête sur les ransomwares

La rapidité est primordiale en cas d'attaque par ransomware, mais il peut être difficile de déterminer l'ampleur de l'impact d'une attaque. Les récupérations rapides sont souvent une chimère et il faut, en moyenne, plus de sept jours pour se remettre d'une attaque par ransomware.

Les outils d'investigation des ransomwares analysent les changements dans les données de sauvegarde pour détecter les modifications malveillantes et évaluer le rayon de l'attaque. Ces informations permettent aux intervenants en cas d'incident d'accélérer la récupération. Les principales fonctionnalités d'investigation des ransomwares sont les suivantes :

- **Identifiez les anomalies :** analysez les données de sauvegarde à la recherche de comportements et de changements inhabituels et recevez des alertes en cas d'activité suspecte.
- **Évaluez l'impact :** comprenez l'étendue des fichiers et des applications qui ont été affectés par le ransomware et où ils se trouvent.
- **Facilitez la réponse rapide :** tirez parti de l'analyse d'impact pour restaurer de manière granulaire uniquement les fichiers et les applications les plus susceptibles d'avoir été affectés, afin d'accélérer la réponse aux incidents.

ASL AIRLINES FRANCE MET EN PLACE UNE STRATÉGIE DE DÉFENSE CONTRE LES RANSOMWARES

ASL Airlines France (ASL) est une compagnie de transport aérien de fret et de passagers basée à Tremblay-en-France au Bâtiment Le Séquoia. Sa principale base est l'aéroport Charles de Gaulle, la deuxième plateforme de trafic aérien la plus fréquentée d'Europe. Une majorité de la flotte d'ASL opère pour le compte de services de livraison pendant la nuit, notamment Amazon, FedEx, DHL, UPS et La Poste. Rien qu'en 2017, ASL a transporté 712 000 passagers et 38 600 tonnes de marchandises.

Fabrice De Biasio, directeur informatique d'ASL Airlines, supervise l'infrastructure opérationnelle de 3 000 employés et est chargé de garantir la disponibilité permanente des données et de respecter des normes de sécurité strictes. En 2018, alors que la menace des cyberattaques est en hausse, ASL s'est associé à Rubrik pour répondre de manière proactive à la menace des ransomwares avec Ransomware Investigation.

L'enjeu

Les attaques par ransomware s'intensifient en termes d'ampleur et de sophistication. Une récente enquête de NTT Security a révélé que ce type d'attaque a augmenté de 350 % en 2017 par rapport à l'année précédente. Près de 75 % des entreprises infectées par un ransomware sont privées d'accès à leurs fichiers pendant au moins deux jours, et 33 % pendant au moins cinq jours. Selon Cyber Security Ventures, les ransomwares devraient coûter aux victimes plus de 250 milliards de dollars par an d'ici 2031.

ASL est tenu de maintenir une disponibilité de 99,9 %, soit un maximum de 60 minutes de temps d'arrêt autorisé par an. Si le système informatique d'ASL est en panne pendant plus de 15 minutes, les avions ne peuvent pas décoller, les clients ne peuvent pas recevoir leurs marchandises et la compagnie aérienne risque de se voir infliger de très lourdes amendes. « Dans notre secteur, il ne peut y avoir de temps d'arrêt », a déclaré M. De Biasio. « Un ransomware peut rapidement paralyser une compagnie aérienne et l'empêcher de voler, point final ».

Solution

La solution précédente d'ASL n'était pas conçue pour une défense solide contre la menace croissante des ransomwares. « Le secteur des compagnies aériennes de fret est une cible courante des ransomwares, et

(suite)

(suite)

nous subissons au moins une attaque par mois », a déclaré M. De Biasio. « Par le passé, nous avons réussi à résoudre le problème en utilisant une multitude de scripts pour identifier et effacer manuellement les fichiers infectés. Cette expérience incroyablement pénible et chronophage a fait baisser la productivité de notre équipe pendant plusieurs jours ».

En permettant des récupérations rapides et en fournissant des évaluations d'impact détaillées, Ransomware Investigation permet aux entreprises de minimiser considérablement les temps d'arrêt, les coûts de récupération et les atteintes à la réputation après une attaque.

Résultats

Avant Rubrik, la menace des ransomwares empêchait M. De Biasio de dormir la nuit. Désormais, grâce à la défense à plusieurs niveaux de Ransomware Investigation, M. De Biasio a l'esprit tranquille et bénéficie des avantages suivants :

Économies opérationnelles

- **Entre 15 et 100 heures ou plus d'administration informatique économisées en cas d'attaque :** « Nous subissons au minimum une attaque par ransomware par mois. Avant Ransomware Investigation, l'équipe passait 15 heures à se remettre d'une attaque mineure de ransomware. Si nous avions été frappés par une attaque majeure, j'ai bien peur que la récupération aurait pris des semaines ».
- **25 % de gain de temps pour l'administration informatique (plus de 40 heures économisées par mois) :** « Notre équipe avait l'habitude de passer jusqu'à deux heures par jour à surveiller nos applications pour détecter les ransomwares. Désormais, nous passons seulement quelques minutes par jour à la vérification sur Ransomware Investigation, de sorte que notre équipe peut consacrer plus de temps aux initiatives qui apportent de la valeur à l'entreprise ».
- **Récupération automatique et aucun temps d'arrêt :** « Avant Ransomware Investigation, nous parvenions à nous remettre des attaques à l'aide de plusieurs scripts et en identifiant et en effaçant manuellement les fichiers infectés. Ces opérations étaient malheureusement très pénibles. Notre administrateur informatique adore Ransomware Investigation, car tout ce travail est réalisé automatiquement. Quand Ransomware Investigation découvre un fichier infecté, il lui envoie une alerte et il lui suffit de cocher quelques cases pour restaurer les données ».

Impact sur l'entreprise

- **Visibilité globale et réponse instantanée aux menaces :** « Avec Ransomware Investigation, nous pouvons suivre l'activité des serveurs en temps réel et réagir rapidement. Si quelque chose n'est pas normal, nous le savons immédiatement ».
- **Capacité à protéger notre entreprise contre les risques catastrophiques grâce à une cyberassurance :** « Le secteur des compagnies aériennes de fret étant une cible fréquente pour les attaques de ransomware, il est incroyablement difficile pour ces compagnies de souscrire une cyberassurance. Si nous n'avions pas eu Ransomware Investigation, nous n'aurions pas été approuvés pour un contrat de cyberassurance ».
- **Des millions d'euros d'économies potentielles en cas d'attaque :** « Ransomware Investigation nous aidera à protéger notre chiffre d'affaires et nous permettra potentiellement d'économiser des millions d'euros en cas d'attaque ».

Grâce à la détection des anomalies et à la récupération accélérée de Ransomware Investigation, alimentée par le Machine Learning, l'équipe d'ASL est désormais confiante dans sa capacité à rétablir rapidement l'état antérieur à l'infection en cas de menace. « L'immuabilité native de Rubrik, associée à l'alerte et à la détection de Ransomware Investigation pilotées par l'IA, sont les outils de protection des données et de continuité des activités les plus essentiels de mon arsenal contre l'intensification des cybermenaces actuelles », a déclaré M. De Biasio.

Découverte de données sensibles

De solides stratégies de préparation et de réaction sont essentielles pour atténuer les effets des ransomwares et autres catastrophes. Mais un manque de visibilité sur les données sensibles peut entraîner des vulnérabilités et des coûts inutiles de réponse aux incidents.

La localisation des données sensibles dans les fichiers et les applications est essentielle pour vous aider à maintenir la conformité et à garder le contrôle. Voici quelques fonctionnalités clés de découverte de données sensibles que votre plateforme doit avoir :

- **Automatisation de l'application des stratégies :** votre plateforme de sécurité des données doit vous permettre de sélectionner les types d'informations personnelles identifiables (IPI) et autres données sensibles que vous souhaitez surveiller pour l'application

automatique des stratégies. Elle doit également disposer de modèles prédéfinis ou créer des stratégies personnalisées pour identifier et classer rapidement les données sensibles sans nuire aux performances de production.

- **Évaluation de l'exposition des données :** identifiez les données sensibles qui risquent d'être exposées lors d'une exfiltration de données ou d'un autre accès non autorisé. Effectuez une recherche dans l'index à l'aide de mots clés ou de champs personnalisés comme le nom, le numéro de sécurité sociale ou le numéro de carte bancaire, afin d'identifier les risques.
- **Simplification de la conformité :** documentez l'emplacement des données sensibles et les personnes qui y ont accès, afin de respecter les exigences réglementaires et de recevoir des alertes lorsque des données risquent de violer les stratégies. Vous pouvez également programmer des rapports périodiques pour garantir une conformité permanente avec le Règlement général sur la protection des données (RGPD), les normes de sécurité des données de l'industrie des cartes de paiement (PCI-DSS), la loi sur la portabilité et la responsabilité de l'assurance maladie (Health Insurance Portability and Accountability Act, HIPAA) et la loi Gramm-Leach-Bliley (Gramm-Leach-Bliley Act, GLBA).

LA VILLE DE SIOUX FALLS MINIMISE LE RISQUE DE VIOLATION DES DONNÉES GRÂCE À LA DÉCOUVERTE DE DONNÉES SENSIBLES

Sioux Falls est la plus grande ville du Dakota du Sud, avec plus de 182 000 habitants. Avec un taux de croissance annuel de 4 %, la ville est rapidement en train de devenir une grande région métropolitaine du Midwest. Du fait de la croissance démographique, la ville est confrontée à une augmentation exponentielle de l'empreinte des données et à un étalement massif des données, ce qui rend plus difficiles la découverte et la protection des données sensibles des employés et des citoyens.

Brandon Morris, administrateur système, fait partie d'une équipe informatique de 28 personnes chargée de soutenir les services centraux de la ville pour ses 1 200 employés et ses citoyens, y compris la gestion du centre de contrôle pour les pompiers, la police et les secours. « Nous avons accès à toutes sortes de données sur les citoyens, comme les dossiers médi-

caux, les permis et les IPI. Nous devons en assurer la confidentialité. Par conséquent, il est essentiel que nous mettions en œuvre des processus de gouvernance des données solides et continus », a déclaré M. Morris. « [Sensitive Data Discovery] de Rubrik renforce notre stratégie de gouvernance des données en offrant une visibilité sur l'emplacement où se trouve le contenu sensible et sur des référentiels auparavant obscurs, ce qui nous permet de minimiser le risque d'exposition et de violations des données et de favoriser une conformité continue ».

L'enjeu

Par le passé, les tâches de découverte et de classification des données sensibles étaient extrêmement manuelles et laborieuses. Elles nécessitaient des équipes dédiées de plusieurs ingénieurs à plein temps. « Avant Rubrik, nous n'avions aucun outil pour rechercher et catégoriser les données sensibles. Pour trouver des documents contenant certains types de contenu, plusieurs employés devaient exécuter manuellement un script de requêtes pour chaque mot clé, un par un, pour chaque emplacement possible. Je n'ai jamais pu exécuter ce script sur l'ensemble de notre environnement, car il ne fonctionnait que sur un petit ensemble de données et nécessitait que nous sachions où se trouvait le contenu sensible. En plus de cela, l'interface était très difficile à utiliser », a déclaré M. Morris.

« La dernière fois que nous avons dû passer par ce processus, cela a été très pénible et nécessité beaucoup de temps, entre 40 et 80 heures de travail. Chaque requête de recherche prenait environ une à deux semaines, avec plusieurs jours pour effectuer l'analyse de nos applications pour chaque mot clé. Nous devions ensuite classer manuellement toutes ces données dans des feuilles de calcul. Cela représente un nombre d'heures de travail trop important », a déclaré M. Morris. « Grâce à [Sensitive Data Discovery], nous pouvons complètement automatiser le processus et effectuer des recherches à la demande pour des centaines de requêtes sur tous nos serveurs de fichiers. Aujourd'hui, il ne faut qu'une heure pour effectuer une recherche. Nous pouvons donc exécuter la classification des données de manière transparente en arrière-plan, sans équipes dédiées ni recours à plusieurs ingénieurs à plein temps, ce qui nous permet de réaliser des gains de productivité massifs et de libérer des employés pour des tâches à plus forte valeur ajoutée ».

Solution

Obtenir plus de visibilité et de contrôle sur l'emplacement du contenu sensible était l'un des objectifs clés recherché par la ville de Sioux Falls avec Sensitive Data Discovery de Rubrik. Ce dernier lui a permis d'identifier les endroits où les données étaient surexposées, comme les numéros de carte bancaire et les numéros de sécurité sociale des employés et des citoyens, et où les niveaux d'accès étaient plus élevés que prévu.

(suite)

(suite)

« [Sensitive Data Discovery] nous a donné une visibilité sur des référentiels de données que nous n'aurions jamais pu consulter auparavant. En conséquence, nous avons pu éviter d'exposer certaines données et créer de manière proactive des plans de remédiation pour traiter les incidents à haut risque. L'avantage pour l'entreprise est énorme. L'exposition des données risque d'entacher notre réputation et d'avoir un impact sur le bien-être de nos citoyens en cas de violation. [Sensitive Data Discovery] nous aide à minimiser le risque d'exposition des données tout en permettant un gain de temps substantiel pour la gestion ».

Résultats

La ville de Sioux Falls a tiré de nombreux avantages de la solution Sensitive Data Discovery, notamment :

- Mise en service en moins de 30 minutes sans infrastructure supplémentaire : « Nous avons constaté la valeur immédiate de [Sensitive Data Discovery]. Puisque cette solution exploite nos déploiements existants de Rubrik Cloud Data Management..., nous n'avons pas eu besoin d'acheter des serveurs ou du stockage supplémentaire et il nous a suffi de basculer sur l'application à partir de l'interface utilisateur ... pour commencer ».
- **Gouvernance continue des données sans impact sur la production :** « [Sensitive Data Discovery] surveille en permanence toutes nos données de sauvegarde existantes en arrière-plan pour nous alerter en cas de violation ou de donnée sensible stockée dans de mauvais emplacements, sans utiliser d'agents ni toucher à nos données de production ».
- **Accès à la demande aux données pour les audits :** « Nous devons nous conformer aux audits et aux réglementations. Avec [Sensitive Data Discovery], nous sommes en mesure de fournir à un auditeur ou à notre équipe juridique interne un accès aux données dont ils ont besoin ».

Confinement des incidents

Avant qu'une organisation puisse se remettre d'une attaque par ransomware, elle doit d'abord contenir la menace. Sinon, elle risque de réinfecter les données pendant la récupération. Or, identifier les systèmes qui ont été touchés par une attaque par ransomware peut s'avérer difficile.

Votre plateforme de sécurité des données doit analyser les instantanés de sauvegarde et fournir des informations permettant d'éviter la réinfection par des logiciels malveillants lors de la restauration. Les principales fonctionnalités de confinement des incidents sont les suivantes :

- **Recherche des menaces :** analysez les sauvegardes à l'aide de modèles de fichiers, de hachages de fichiers et de règles YARA (Yet Another Recursive Acronym), pour rechercher tout indicateur de compromission (IoC) sur tous les objets de la sauvegarde.
- **Identification des points de récupération :** analysez une série chronologique d'instantanés de sauvegarde pour trouver un instantané propre et non infecté à restaurer.
- **Réduction de la probabilité de réinfection par les logiciels malveillants :** tirez parti de vos connaissances pour effectuer une récupération rapide avec moins de risques de réintroduction de logiciels malveillants et pour fournir des preuves légales lors d'enquêtes internes et externes.

Récupération orchestrée des applications

Assurer la sécurité et la résilience des données et services métiers face aux cyberattaques et autres catastrophes est une responsabilité essentielle des entreprises numériques modernes. Cependant, l'installation et la maintenance d'une nouvelle infrastructure et de nouveaux logiciels pour la reprise après sinistre (DR) peuvent être coûteuses et prendre du temps. L'exécution de plans manuels pour des applications comportant plusieurs niveaux et interdépendances ralentit le processus de récupération et introduit des possibilités d'erreur.

Les entreprises peuvent éviter ces contraintes en utilisant la reprise d'application orchestrée pour un service de reprise après sinistre étroitement intégré et automatisé.

JARGON TECHNIQUE

La récupération orchestrée est fournie sous la forme d'une application de type SaaS (Software-as-a-Service). Elle permet d'orchestrer le basculement/la restauration automatique après un sinistre ou les tests et, grâce à l'enquête sur les ransomwares axée sur les applications, elle simplifiera radicalement la récupération des services métiers dans les environnements VMware vSphere. Ainsi, les organisations informatiques peuvent éliminer les multiples solutions ponctuelles, la complexité de la gestion et éviter les coûts inutiles.

Les principales fonctionnalités de récupération d'applications orchestrées sont les suivantes :

- **Simplification de l'orchestration :** récupérez les données sur votre site de secours sur place, dans VMware Cloud sur AWS ou dans la solution Azure VMware.
- **Prêt pour la reprise après sinistre :** confirmez la disponibilité de l'application, démontrez la conformité et prouvez la préparation à la reprise après sinistre.
- **Récupération après une attaque :** identifiez les données chiffrées et récupérez l'état propre le plus récent à partir de vos sauvegardes non compromises.

DANS CE CHAPITRE

- Comprendre les composants essentiels d'une architecture Zero Trust pour la protection des données
- Tirer parti du Machine Learning
- Classifier les données sensibles
- Assurer la chasse proactive aux menaces
- Automatiser et orchestrer des flux de récupération

Chapitre 3
Prendre un bon départ avec la sécurité des données Zero Trust

Dans ce chapitre, vous découvrirez les composants fondamentaux d'une architecture Zero Trust pour la sécurité des données Zero Trust. Vous découvrirez également comment le Machine Learning, la classification des données, la chasse aux menaces, ainsi que l'automatisation et l'orchestration des flux de récupération contribuent tous à une stratégie moderne et complète de protection des données.

Sauvegarde immuable des données et disponibilité des données

Le fait que les sauvegardes soient compromises est l'une des raisons pour lesquelles les entreprises ne peuvent pas se remettre d'une attaque par ransomware : cela les oblige à payer la rançon ou à restaurer à partir de sauvegardes hors site. Méfiez-vous des fournisseurs de solutions de protection des données qui recommandent les sauvegardes hors site comme principale option de récupération, car la restauration peut prendre des semaines, voire des mois, et est souvent sujette à des problèmes d'intégrité des données, ce qui entraîne des objectifs de délai de

récupération (RTO) plus longs. En outre, certains fournisseurs de solutions de sauvegarde conseillent de mettre en œuvre une restauration isolée pour faire face aux ransomwares. Bien qu'il s'agisse d'une option viable, sa mise en œuvre s'accompagne d'une charge financière importante et d'une gestion complexe. En somme, elle équivaut à des frais généraux opérationnels et financiers d'une infrastructure de reprise après sinistre.

Pour protéger efficacement vos données contre les attaques par ransomware, votre système de sauvegarde et de récupération doit être capable de créer des copies immuables de vos données, c'est-à-dire des sauvegardes qui ne peuvent pas être chiffrées par un ransomware. Zero Trust Data Security fournit les bases d'un système moderne de sauvegarde et de récupération avec les fonctionnalités et les éléments fondamentaux suivants :

- **Réduction du risque d'intrusion.** Toutes les interfaces du système sont sécurisées, basées sur les rôles, les moins privilégiées et protégées par une authentification multifacteur (MFA).
- **Sécurisation des données.** Les données sont toujours chiffrées en vol et au repos, et les données de sauvegarde sont stockées dans un système de fichiers de type « ajout uniquement » spécialement conçu à cet effet. Les données sauvegardées sont toujours isolées logiquement via un Air Gap. Elles sont donc hors ligne et ne sont pas accessibles via des protocoles réseau standard.
- **Détection des comportements anormaux et lancement d'alertes.** Les attaques sont détectées et l'équipe SecOps est alertée afin qu'un point de récupération propre puisse être identifié rapidement et en toute confiance.
- **Conformité garantie.** Les nouvelles charges de travail sont automatiquement protégées par la conservation des verrous et la possibilité de retrouver certaines données sensibles exposées qui ont pu être exfiltrées.

JARGON TECHNIQUE

CONSEIL

Les données dans un format immuable ne peuvent être ni lues, ni modifiées, ni supprimées par un client externe une fois qu'elles ont été ingérées.

L'architecture « Zero Trust » repose sur un ensemble de technologies de base dans les solutions de sauvegarde et de récupération, qui prennent en charge un système de fichiers spécialement conçu pour ne jamais exposer les données de sauvegarde via des protocoles réseau ouverts. L'architecture Zero Trust crée un vide logique, qui empêche les données d'être découvertes ou accessibles sur le réseau et comprend les éléments suivants (voir la figure 3-1) :

- **Une plateforme de données immuable :** une fois les données ingérées, aucune opération externe ou interne ne doit pouvoir modifier les données. Les données gérées par la plateforme ne doivent jamais être disponibles dans un état de lecture/écriture pour le client. Puisqu'il est impossible d'écraser les données, même les données infectées ingérées ultérieurement par la plateforme ne peuvent pas infecter d'autres fichiers ou dossiers existants.
- **Un moteur de stratégie déclarative :** cet outil permet aux administrateurs de se débarrasser d'une grande partie des tâches de base nécessaires à la mise en place et à la maintenance de la protection des données, afin qu'ils puissent se concentrer sur la création de valeur à un niveau plus stratégique dans l'ensemble de l'entreprise.
- **Un moteur de menaces :** au fur et à mesure que les métadonnées de chaque instantané de sauvegarde sont collectées, le Machine Learning permet d'obtenir une vision complète de ce qui se passe dans la charge de travail. Le réseau est formé pour identifier les tendances qui existent dans tous les échantillons et classer les nouvelles données en fonction de leurs similitudes, sans nécessiter d'intervention humaine. Vous serez en mesure de détecter les anomalies, d'analyser les menaces et d'accélérer la récupération en quelques clics.
- **Une architecture sécurisée donnant la priorité aux interfaces de programmation (API) :** une architecture orientée API signifie que chaque action de l'interface utilisateur (IU) de votre plateforme a une API correspondante, documentée et disponible. En d'autres termes, si vous pouvez effectuer une opération via l'interface utilisateur, celle-ci peut également être exécutée par programmation via l'API, qui est sécurisée par un accès basé sur les rôles et des jetons d'API.

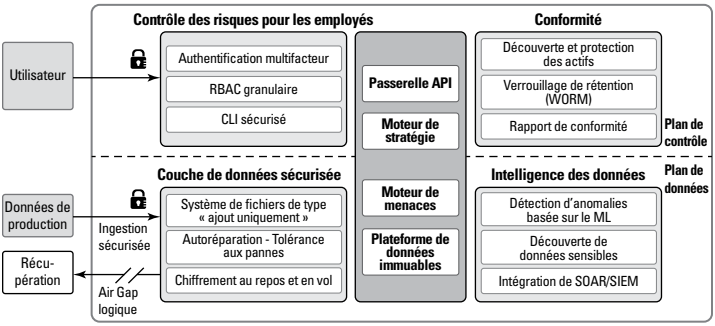

FIGURE 3-1 : Composants de base de l'architecture Zero Trust.

RAPPEL

Avec une plateforme immuable, une fois que les données sont écrites dans le système, elles ne peuvent pas être modifiées, supprimées ou chiffrées par une attaque, ce qui garantit qu'une copie propre des données est toujours disponible pour la récupération.

Découverte d'anomalies dans les données grâce au Machine Learning

Les outils de Machine Learning intégrés au système de sauvegarde et de récupération constituent un autre élément important d'une stratégie de protection de la sécurité des données fondée sur les principes du Zero Trust. Ces outils surveillent les métadonnées des applications afin de détecter et de vous alerter sur les signes d'activité anormale pouvant indiquer une attaque par ransomware.

Idéalement, ces outils doivent fournir des informations à un niveau très granulaire afin que vous puissiez rapidement identifier les fichiers spécifiques qui ont été compromis, puis restaurer rapidement ces fichiers plutôt que des machines virtuelles entières, en un seul clic.

RAPPEL

Cette combinaison d'outils de Machine Learning fonctionnant en temps réel, associée à la capacité de récupérer rapidement les données infectées à partir de sauvegardes immuables, doit faire partie de votre stratégie de protection de la sécurité des données Zero Trust.

Classification des données et évaluation du risque d'exfiltration

Les attaques par ransomware ont évolué, et de nombreux cybercriminels ciblent désormais les victimes avec des « ransomwares à double extorsion ». Dans une attaque par ransomware à double extorsion, une copie des données des victimes est exfiltrée avant que les fichiers originaux ne soient chiffrés. Les victimes sont alors menacées de deux conséquences négatives : la perte de leurs données de production et la fuite sur le Web d'informations sensibles comme des informations personnelles identifiables (IPI) des clients et des employés, les comptes financiers et les numéros de sécurité sociale, les conceptions de produits et autres propriétés intellectuelles, les logiciels propriétaires et les e-mails et documents internes potentiellement embarrassants.

ATTENTION

Le paiement d'une rançon ne garantit pas qu'un cybercriminel vous fournira les clés nécessaires au déchiffrement de vos données, bien qu'il le fasse généralement. (Le modèle économique des ransomwares ne serait pas viable s'il n'y avait pas une attente raisonnable que le

paiement de la rançon vous permette de déverrouiller vos données). Toutefois, payer la rançon ne garantit en rien qu'un cybercriminel ne conservera pas une copie de vos données et ne l'utilisera pas pour vous extorquer une nouvelle rançon à une date ultérieure. Un cybercriminel peut également choisir de vendre la copie volée de vos données (comme les numéros de sécurité sociale et les numéros de carte bancaire des clients) sur le Dark Web.

Pour limiter l'impact potentiel des ransomwares à double extorsion, les organisations doivent identifier leurs données pour faciliter les opérations suivantes :

- **Déterminer rapidement si des données sensibles ont été compromises** en cas d'attaque par ransomware (ou toute autre cyberattaque, d'ailleurs). Cette opération aidera également l'organisation à respecter toute exigence de divulgation ou de notification. Par exemple, le Règlement général sur la protection des données (RGPD) exige une notification rapide de l'autorité de protection des données du pays ou de la région impactée par une violation de données, ainsi que la notification des personnes concernées.
- **Mettre en œuvre de façon appropriée des contrôles de sécurité** pour différents niveaux de classification des données en fonction de leur niveau de sensibilité et de leur valeur. Ces protections peuvent inclure des mesures comme la limitation de l'accès, le chiffrement des fichiers, l'augmentation de la journalisation et de l'audit, et la sauvegarde plus fréquente des ensembles de données.

CONSEIL

Si une organisation peut rapidement déterminer que les données sensibles n'ont pas été compromises, elle peut limiter les sanctions réglementaires et les coûts liés à la notification de la violation. Et bien sûr, le fait de savoir quelles données ont été chiffrées par un ransomware permet aux équipes de récupération de hiérarchiser leurs efforts en fonction des besoins de l'entreprise et de réduire le temps, les efforts et les dépenses associés aux opérations de récupération.

Les organisations doivent également envisager des mesures qui protègent l'ensemble de l'environnement, comme l'extension de l'utilisation de l'authentification multifacteur (AMF). De nombreuses campagnes de ransomware tirent parti d'informations d'identification faibles ou volées, ou utilisent des techniques de craquage de mots de passe par force brute pour accéder aux réseaux et systèmes cibles. L'AMF peut empêcher ou limiter la propagation des ransomwares en atténuant les vulnérabilités inhérentes aux mots de passe statiques.

Chasse aux menaces pour empêcher la réinfection

Pour éviter la réinfection, les entreprises doivent pouvoir effectuer des recherches dans leurs sauvegardes sans avoir à les restaurer, afin d'identifier les sauvegardes potentiellement compromises. En examinant vos machines virtuelles et vos ensembles de fichiers, vous pouvez déterminer avec précision à quel moment l'infection a commencé, afin d'éviter la réinfection par des logiciels malveillants pendant la restauration.

Récupération des applications et des données avec des flux de travail guidés

Les organisations faisant de plus en plus appel à des généralistes informatiques pour répondre à leurs besoins technologiques, les stratégies traditionnelles de gestion des sauvegardes, qui reposaient sur des compétences de création de scripts pour programmer et gérer les tâches de sauvegarde, sont devenues trop compliquées à maintenir.

Les systèmes modernes de sauvegarde et de récupération qui prennent en charge un modèle de gestion déclaratif répondent au besoin des organisations d'aujourd'hui qui souhaitent disposer d'un système suffisamment simple et intuitif pour que pratiquement tout le monde puisse le gérer. Dans ce type de modèle, un administrateur entre l'état qu'il souhaite pour une charge de travail dans un moteur de règles. Une fois qu'une règle est définie, un système intelligent et automatisé exécute les travaux nécessaires pour parvenir à cet état (voir la figure 3-2).

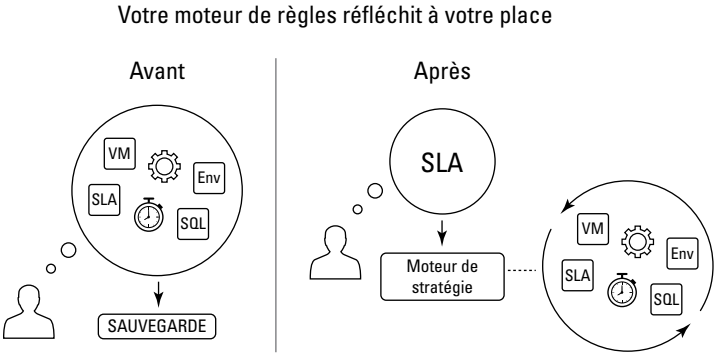

FIGURE 3-2 : Synthèse de multiples paramètres mis en œuvre manuellement en une politique déclarative unique, facile à configurer et sans maintenance.

Un moteur de stratégie solide peut également faciliter d'autres aspects de l'automatisation des services, en réduisant le nombre d'étapes manuelles qu'un administrateur informatique peut avoir à effectuer pour accomplir une tâche. Si la solution de sauvegarde et de récupération est dotée d'une architecture orientée API, l'organisation bénéficie d'avantages encore plus importants. Un administrateur peut utiliser ces fonctionnalités pour :

- Intégrer la sauvegarde et la restauration dans un catalogue de services informatiques (par exemple, ServiceNow et VMware vRealize Automation ou vCloud Director)
- Simplifier la gestion des environnements distribués de grande taille grâce à des outils de gestion de la configuration ou d'infrastructure en tant que code (IaC) (par exemple, Puppet, Chef, SaltStack ou Ansible)
- Automatiser les flux de gestion des données tout au long de leur cycle de vie, et centraliser la surveillance et le reporting (par exemple, Splunk ou un tableau de bord de surveillance personnalisé)

En outre, l'automatisation permet de valider les sauvegardes régulières, ce qui est nécessaire pour atténuer le risque « d'insuffisance des tests », présenté à la figure 3-3. Si les sauvegardes ne sont pas testées régulièrement, le service informatique ne peut pas garantir leur validité pour l'entreprise.

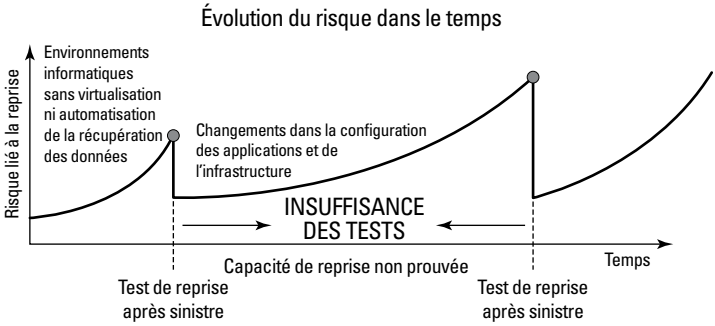

FIGURE 3-3 : Sans des tests réguliers, il est impossible de garantir une restauration fiable.

DANS CE CHAPITRE

- **Planifier et se préparer au pire**
- **Prendre en compte l'authentification multifacteur et l'accès via le moindre privilège**
- **Segmenter votre réseau et isoler votre système de sauvegarde**
- **Tester vos capacités de sauvegarde et de récupération**
- **Surveiller vos journaux**
- **Protéger vos terminaux et former vos utilisateurs finaux**
- **Souscrire une cyberassurance**

Chapitre 4
Dix clés pour une réponse efficace aux incidents

La mise en œuvre de la sécurité des données Zero Trust permet à votre entreprise d'atténuer les menaces qui pèsent sur vos données stratégiques et de vous assurer que vous pouvez vous remettre d'une attaque par ransomware (ainsi que d'autres cybermenaces et incidents). Voici dix conseils supplémentaires sur les meilleures pratiques en matière de réponse aux incidents :

- **Tenez à jour vos plans de réponse aux incidents, de continuité des activités et de reprise après sinistre et testez-les souvent.** L'improvisation de ces plans essentiels pendant une attaque par ransomware est une recette qui aboutira, eh bien ... à un désastre. Chacun de ces plans doit être un document évolutif, revu, mis à jour et testé régulièrement, ainsi qu'à chaque fois qu'un événement

important se produit, par exemple : une mise à niveau majeure du matériel ou des logiciels, une fusion ou une acquisition, une croissance de l'entreprise sur de nouveaux marchés ou un changement radical au niveau des effectifs, comme le passage à un modèle de travail à domicile ou de travail à distance. Ces plans doivent porter sur tous les domaines d'activité de l'entreprise, et pas seulement sur l'informatique, et les tests doivent comprendre des exercices de simulation, des visites structurées et des simulations complètes.

- **Déployez l'authentification multifacteur (AMF).** En termes simples, les mots de passe ne sont pas efficaces pour sécuriser les comptes des utilisateurs. L'AMF exige que les utilisateurs se connectent à leurs comptes en associant un nom d'utilisateur, un mot de passe/une phrase secrète et un troisième « facteur », comme un code d'accès à usage unique envoyé à un smartphone enregistré ou un jeton de sécurité.

  
  ATTENTION

  Bien que l'AMF offre une sécurité des comptes bien plus solide que les seuls noms d'utilisateur et mots de passe, elle ne constitue pas un remède miracle. Les cybercriminels utilisent des techniques sophistiquées pour déjouer l'AMF, notamment des codes d'accès à usage unique qui sont envoyés par SMS sur les smartphones.

- **Mettez en œuvre le principe du moindre privilège et créez des comptes d'administrateur distincts.** Effectuez régulièrement des examens d'accès pour tous vos utilisateurs afin de vous assurer qu'ils ne disposent que des privilèges dont ils ont besoin pour remplir leurs fonctions. Supprimez tous les droits inutiles et vérifiez soigneusement les appartenances aux groupes. Créez des comptes d'administrateur distincts (ou, mieux encore, mettez en œuvre une gestion des accès privilégiés, ou PAM) pour les utilisateurs ayant besoin d'un accès privilégié afin qu'ils puissent utiliser un compte d'utilisateur standard pour les activités quotidiennes ne nécessitant pas de privilèges Administrateur.

- **Segmentez et verrouillez votre réseau.** Une fois qu'une organisation ciblée a été violée, les cybercriminels profitent d'un mouvement latéral plus ou moins illimité dans les réseaux relativement plats qui sont courants dans les modèles de sécurité traditionnels basés sur le périmètre. Segmentez votre réseau à l'aide de pare-feux nouvelle génération et d'autres outils de sécurité pour inspecter et contrôler le trafic est-ouest au sein de votre réseau et le trafic nord-sud entre différents réseaux. Supprimez également tous les services réseau inutiles, comme l'accès externe au protocole de bureau à distance (RDP).

- **Isolez votre système de sauvegarde et de récupération du reste de votre réseau.** Pour garantir la viabilité de vos sauvegardes de données en cas de cyberattaque, isolez votre système de sauvegarde et de récupération du reste de votre réseau.
- **Mettez en place une stratégie de sauvegarde 3-2-1 et testez vos capacités de récupération.** Au minimum, conservez trois copies de vos données stratégiques (une de production et deux de sauvegarde) sur deux dispositifs de stockage (ou supports) différents et gardez une copie hors site (par exemple, dans le cloud ou dans un datacenter distinct). N'oubliez pas non plus que toutes les sauvegardes du monde ne servent à rien si vous ne pouvez pas récupérer vos données. Veillez à tester régulièrement vos capacités de récupération pour vous assurer que votre équipe connaît la marche à suivre et que vos sauvegardes sont fiables et suffisantes pour atteindre les objectifs de délai de récupération (RTO) et de point de récupération (RPO) de votre organisation.
- **Vérifiez vos journaux pour détecter toute activité inhabituelle.** Bien trop souvent, les organisations découvrent que leurs journaux système et réseau sont incomplets, inadéquats ou inaccessibles pendant ou après une attaque. Ces journaux fournissent des données essentielles qui permettent aux plateformes de gestion des informations et des événements de sécurité (SIEM) de générer des événements et des alertes précis et aident à former des modèles de Machine Learning pour mieux détecter les comportements anormaux.

  
  CONSEIL

  Vos journaux fournissent également des informations importantes pour vous aider à répondre aux questions « qui, quoi et quand » dans le cadre d'une enquête légale, notamment pour savoir si des données sensibles (et réglementées) – y compris des informations de santé protégées (ISP), des informations personnellement identifiables (IPI) ou des informations sur les titulaires de cartes – ont été compromises ou exfiltrées.
- **Sécurisez vos terminaux.** Les terminaux – y compris les ordinateurs de bureau et les ordinateurs portables, les smartphones et les tablettes, ainsi que les dispositifs de l'Internet des objets (IoT) – représentent la surface d'attaque la plus importante et généralement la plus vulnérable d'une organisation. Aujourd'hui, les employés, de plus en plus éloignés, doivent prendre d'importantes décisions en matière de sécurité des terminaux – comme autoriser une application téléchargée à accéder aux données d'un appareil mobile – sans comprendre pleinement le risque que ces décisions

peuvent représenter pour l'organisation dans son ensemble. Déployez (et mettez régulièrement à jour) des solutions de protection des terminaux – notamment des logiciels anti-programme malveillant, des solutions de protection de la messagerie, des solutions de prévention des pertes de données (DLP) et des solutions de détection et de réponse pour les terminaux (EDR) – afin de sécuriser vos appareils.

- **Formez vos utilisateurs finaux.** Le personnel est traditionnellement le maillon le plus faible de toute stratégie de sécurité, mais lorsqu'il est formé régulièrement et efficacement, il peut devenir un outil formidable de protection pour votre équipe de sécurité. Les simulations d'hameçonnage sont un excellent exemple de formation interactive et engageante de sensibilisation à la sécurité des utilisateurs finaux ; elles ont aidé bien des organisations à réduire les risques associés aux campagnes d'hameçonnage par e-mail. L'extension de cette méthode de formation à d'autres menaces de sécurité modernes, notamment les ransomwares, contribue à instaurer une culture plus sûre au sein de votre organisation.
- **Assurez-vous d'avoir mis en place un contrat d'assurance adéquat.** Même avec un plan de réponse aux incidents efficace qui inclut une solution de sauvegarde et de récupération robuste, une cyberattaque reste coûteuse. En outre, ses conséquences sont multiples : interruptions d'activité (et perte de revenus), reconstruction ou remplacement des systèmes, services d'expertise judiciaire de tiers, frais juridiques, sanctions civiles et réglementaires, notifications aux clients, atteinte à la réputation de la marque, etc. Selon l'*enquête* ITIC *2021 sur le coût horaire des temps d'arrêt* (`www.itic-corp.com/tag/hourly-cost-of-downtime/`), le coût des temps d'arrêt est estimé à 300 000 dollars en moyenne pour une seule heure d'arrêt. La cyberassurance (également appelée assurance contre les cyberrisques) peut aider les organisations à récupérer une grande partie de ces coûts afin de réduire l'impact financier d'une attaque.

CONSEIL

Pour de nombreuses entreprises, leur fournisseur de cyberassurance joue un rôle majeur dans la définition des stratégies de réponse aux attaques par ransomware et sur les circonstances dans lesquelles il faut payer les rançons. Il est essentiel d'obtenir la contribution de la compagnie d'assurance, soit directement, soit par l'intermédiaire d'un membre du service juridique ou du groupe de gouvernance, risques et conformité (GRC) qui a une connaissance détaillée de ses pratiques et de ses exigences.

Adoptez une approche Zero Trust pour la sécurité de vos données

Une économie florissante de ransomware a émergé. Les hackers s'attaquent désormais directement à vos données de sauvegarde. Et si les solutions de sauvegarde traditionnelles permettent de se remettre d'une catastrophe naturelle ou d'une panne informatique, la reprise après un ransomware vous oblige à repenser votre stratégie en matière de sécurité. Si les données sont la cible, la défense doit commencer à ce niveau-là. Grâce à ce livre, vous comprendrez clairement comment une architecture Zero Trust permet de sécuriser les données afin que les cybercriminels ne puissent pas les prendre en otage. Vous apprendrez également à évaluer les capacités de sécurité Zero Trust d'un fournisseur.

Dans ce livre ...

- Explorez les problèmes liés à la sécurité et à la protection des données
- Comprenez les avantages du Zero Trust
- Sécurisez vos applications et données stratégiques
- Localisez, classez et signalez les données sensibles
- Évaluez l'impact des cyberattaques
- Détectez les logiciels malveillants et évitez la réinfection
- Accélérez la récupération après un ransomware

Lawrence Miller a exercé en tant que Chief Petty Officer dans la marine américaine et travaille depuis plus de 25 ans dans les départements informatiques de divers secteurs. Il a co-écrit *CISSP pour les Nuls* et plus de 200 autres livres *pour les Nuls* portant sur diverses questions de sécurité et de technologie.

Allez sur Dummies.com®
pour voir des vidéos, des tutoriels en photos, des articles pratiques ou pour faire des achats !

ISBN 978-1-119-98265-4

pour les nuls®

WILEY END USER LICENSE AGREEMENT

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