5 étapes pour se protéger contre les ransomwares

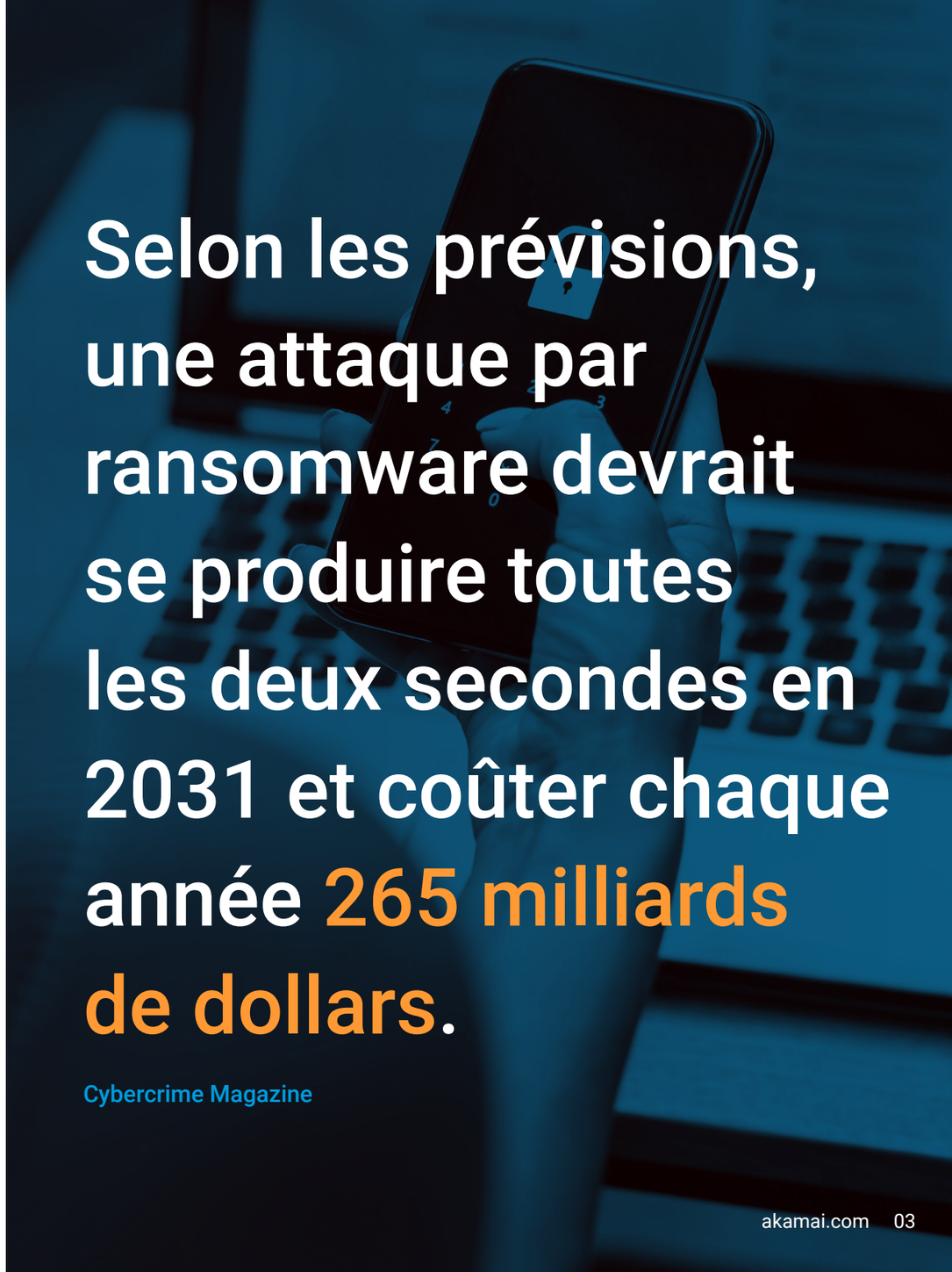
Comment renforcer vos défenses au-delà du périmètre

TABLE DES MATIÈRES

Introduction

L'émergence des ransomwares

Les ransomwares, qui étaient autrefois une simple variété de programmes malveillants utilisée par les malfaiteurs pour restreindre l'accès aux fichiers et données par le biais du cryptage, se sont transformés en une méthode d'attaque aux proportions démesurées. Alors que la menace de perte permanente de données est effrayante en soi, les cybercriminels et pirates informatiques ont désormais les moyens d'utiliser les ransomwares pour pénétrer et paralyser les grandes entreprises, les gouvernements fédéraux et locaux, les infrastructures mondiales et les organisations de santé, et bien d'autres encore. Beaucoup de ces groupes proposent même de louer leurs services sous forme de ransomware as a service (RaaS).



Selon les prévisions, une attaque par ransomware devrait se produire toutes les deux secondes en 2031 et coûter chaque année 265 milliards de dollars.

Cybercrime Magazine

Les ransomwares peuvent vous coûter cher

En 2022, une attaque par ransomware a contraint 7-Eleven à fermer 175 magasins, car ils n'étaient plus en mesure d'utiliser leurs caisses enregistreuses ou d'accepter des paiements. Plus tôt dans l'année, une attaque par ransomware BlackCat contre une compagnie pétrolière allemande a touché 233 stations-service, Royal Dutch Shell ayant dû réacheminer ses expéditions vers différents dépôts d'approvisionnement en raison de ce problème. L'attaque de Colonial Pipeline s'est produite en mai 2021, perturbant les livraisons de pétrole et de gaz sur toute la côte est des États-Unis. En 2020, l'attaque par ransomware Snake a paralysé les opérations mondiales de Honda.

Aujourd'hui, des organisations de toutes tailles sont menacées, que ce soit dû à des technologies dépassées, à des stratégies de défense « suffisantes » qui ne couvrent que le périmètre et les points de terminaison, au manque de formation (et de bonnes pratiques de sécurité) ou à l'absence de « solution miracle » connue. Les cybercriminels s'efforcent de chiffrer les réseaux d'entreprise le plus possible afin d'extorquer des rançons allant de plusieurs milliers à plusieurs millions de dollars.

Mais il y a plus en jeu que votre seul résultat financier. Les conséquences d'une attaque par ransomware peuvent être préjudiciables : les temps d'arrêt peuvent interrompre les opérations de l'entreprise, perturber la productivité et compromettre vos données.

Une fois les données propriétaires de l'entreprise divulguées ou compromises, votre marque peut subir des dégâts et vous risquez de perdre la fidélité de vos clients. Selon une étude de 2020, 80 % des violations de données comprenaient les informations à caractère personnel de clients ; la propriété intellectuelle était compromise dans 32 % des violations ; et les données clients anonymisées étaient compromises dans 24 % des violations. Sans parler des acteurs malveillants pouvant utiliser ces données sensibles contre votre entreprise ou pour mener à bien d'autres actes insidieux, y compris la vente de données confidentielles.

La menace des ransomwares se propageant rapidement à travers les réseaux, la protection du périmètre seul ne suffit tout simplement pas.

Akamai

Bloquez les mouvements latéraux. Bloquez la propagation des ransomwares.

Les attaques par ransomware sont lancées à partir d'une violation initiale, généralement obtenue via un e-mail d'hameçonnage, une vulnérabilité dans le périmètre du réseau ou des attaques de force brute créant des ouvertures en concentrant les défenses à distance du véritable point d'attaque de l'attaquant.

Une fois que l'attaque a atteint un terminal ou une application, elle se poursuit par un mouvement latéral sur le réseau et plusieurs terminaux afin d'optimiser les points d'infection et de chiffrement. Les attaquants mettent généralement la main sur un contrôleur de domaine, compromettent les informations d'identification, puis trouvent et chiffrent la sauvegarde pour empêcher l'opérateur de restaurer les services gelés.

Le mouvement latéral est essentiel à la réussite d'une attaque. Si le programme malveillant ne peut pas se propager au-delà de son point d'entrée, il est inutile. La prévention des mouvements latéraux est donc cruciale.

Votre stratégie d'atténuation des menaces par ransomware est-elle complète ?

Atténuation des risques

Élaboration d'une stratégie de défense invulnérable

La détection et la prévention des mouvements latéraux au sein de votre réseau se résument à deux domaines d'intervention principaux : tout d'abord, **réduisez le vecteur d'attaque initial** puis **limitez les chemins de propagation**.

Vous pouvez par exemple limiter le nombre de serveurs exposés à Internet, suivre la gestion des correctifs afin de réduire la surface d'attaque, pratiquer le cloisonnement pour réduire les chemins de propagation entre les applications, et sauvegarder vos données pour pouvoir vous connecter rapidement et éviter une perte de données généralisée en cas d'attaque.

Quatre façons de faire de la planification de la sécurité une priorité

La sécurité devrait faire partie de la stratégie, de la planification et du budget de préparation générale de votre organisation. Cela implique de sensibiliser les cadres supérieurs et les membres du conseil d'administration et de rester vigilants quant aux risques et à ce que vous devez faire pour les atténuer.

1. Assurez-vous d'inclure la cybersécurité dans la fonction gérant l'atténuation globale des risques pour votre entreprise. Assurez-vous également que votre équipe de direction dispose d'une expertise en matière de sécurité.
2. N'oubliez pas de consacrer du budget et des ressources à la génération de sauvegardes et à la segmentation du réseau.
3. Créez des plans de réponse avant un sinistre ou un événement indésirable (comme une attaque par ransomware). Être organisé et préparé vous permet de réagir plus rapidement et plus efficacement.
4. Chaque fois que vous intégrez, concevez ou développez de nouveaux produits et services, analysez leur impact sur la sécurité. Posez-vous la question suivante : suis-je en train d'ouvrir une nouvelle porte aux attaquants ?

Liste de contrôle de détection des ransomwares

Que se passe-t-il dans votre réseau ?

Si votre organisation est comme beaucoup d'autres, la détection des ransomwares peut être un défi. Malheureusement, cela signifie que votre réseau est vulnérable aux attaques. Sans de fortes capacités de détection, au moment où vous recevez une demande de rançon, il est déjà trop tard : la plus grande partie de votre réseau sera cryptée en même temps.

En matière de détection, vous devez arrêter les ransomwares pendant qu'ils se propagent. Voici ce dont vous aurez besoin :

Visibilité élevée

Si vous ne savez pas ce qui se passe dans votre réseau, vous ne pouvez pas détecter les ransomwares ou autres cybermenaces indésirables.

Règle de segmentation

Une fois que chaque communication est définie et prise en compte, tout ce qui n'est pas dans la norme émergera et vous serez alerté.

Système IDS et outils de détection des programmes malveillants

Ces derniers détecteront les tentatives de propagation des opérateurs de ransomware, à l'aide de règles et signatures prédéfinies pour les vulnérabilités ou les exploits connus, ou à l'aide d'une détection d'anomalie plus générale ou automatisée.

Outils de tromperie

La mise en place de leurres, de pots de miel ou d'une plateforme de tromperie distribuée, capable d'identifier un mouvement latéral non autorisé peut être un moyen efficace de découvrir une violation active en cours avec des incidents haute-fidélité.

Élaboration d'une stratégie de défense contre les ransomwares

Même avec les meilleures défenses de périmètre, les violations sont inévitables. C'est pourquoi vous devez mettre en place une stratégie de défense qui minimise l'efficacité d'une attaque et interrompt la propagation au sein de votre réseau. Trouvez un fournisseur qui offre une solution de sécurité complète qui détecte les menaces dans le trafic est-ouest du centre de données et bloque les mouvements latéraux.

Préparer

Trouvez une solution vous permettant d'identifier chaque application et chaque ressource en cours d'exécution dans votre environnement informatique. Ce niveau de visibilité granulaire vous permet de cartographier rapidement les ressources, données et sauvegardes critiques, et d'identifier les vulnérabilités et les risques. En ayant une vue complète sur votre environnement réseau, vous pourrez réagir et activer rapidement des règles en cas de violation.

Prévenir

Votre solution devrait vous permettre de créer des règles pour bloquer les techniques de propagation de ransomware courantes. En utilisant la segmentation logicielle, vous pouvez créer des micro-périmètres Zero Trust autour des applications critiques, des sauvegardes, des serveurs de fichiers et des bases de données. Vous pouvez également créer des règles de segmentation limitant le trafic entre les utilisateurs, les applications et les terminaux, bloquant ainsi les tentatives de déplacement latéral.

Détecter

Mettez en œuvre une solution qui vous avertit de toute tentative d'accès aux applications segmentées et aux sauvegardes. Ces tentatives d'accès bloquées sont des indicateurs de mouvement latéral. Vous devez également intégrer une détection reposant sur la réputation qui alerte de la présence de domaines et de processus malveillants connus. En permettant la détection rapide des attaques ayant réussi à dépasser le périmètre, vous pouvez réduire le temps d'arrêt et détecter les attaquants avant qu'ils ne puissent dépasser leur point d'entrée.

Corriger

Le lancement automatique de mesures de confinement des menaces et de quarantaine lorsqu'une attaque est détectée est crucial. Appliquez des règles d'isolation permettant la déconnexion rapide des zones affectées du réseau, tandis que les politiques de segmentation bloquent l'accès aux applications critiques et aux sauvegardes système.

Récupérer

Enfin, vous avez besoin de fonctionnalités de visualisation prenant en charge les stratégies de reprise par phases dans lesquelles la connectivité est progressivement restaurée à mesure que l'alerte est levée sur les différentes zones du réseau.

Conclusion

Bilan

Avez-vous confiance en votre stratégie de défense actuelle ?

Les ransomwares restent une réalité. En fait, les ransomwares ont touché 66 % des organisations en 2021, soit une augmentation de 78 % par rapport à 2020, et ce chiffre ne semble pas baisser. Cela signifie que le monde continuera à subir des attaques à une fréquence plus élevée, avec des cibles plus vastes et plus importantes ainsi que des demandes de rançon plus coûteuses, le tout avec des conséquences désastreuses pour votre entreprise. Aujourd'hui, plus que jamais, vous avez besoin de stratégies de planification et d'atténuation des risques avancées allant au-delà d'une approche limitée au périmètre.

Interrompez le mouvement latéral des ransomwares dans votre réseau. Laissez Akamai vous montrer comment faire.

Pour plus d'informations, consultez le site **akamai.com/guardicore**.