Protéger Contre les Ransomwares

Un guide de ressources du PCI Security Standards Council

LE RANSOMWARE EST LA MENACE DE LOGICIEL MALVEILLANT QUI CONNAÎT LA CROISSANCE LA PLUS RAPIDE.

Les ransomwares sont un type de logiciels malveillants qui volent ou empêchent l'accès à des fichiers, systèmes ou réseaux informatiques d'entreprise et exigent une rançon pour leur restitution. Les attaques de ransomware peuvent provoquer des perturbations coûteuses des opérations et la perte ou l'exposition d'informations et de données critiques.[1]

1 Source : FBI

COMPRENDRE LE RISQUE

Les pertes mondiaux dues aux ransomwares devraient atteindre **20 milliards de dollars** en 2021, selon le dernier rapport de Cybersecurity Ventures[2].

Le coût total moyen de récupération d'une attaque par ransomware a plus que doublé, passant de 761 106 $ en 2020 à **1,85 million de dollars** en 2021.[3]

Il faut en moyenne **287 jours** pour qu'une entreprise se remette complètement d'une attaque par ransomware, selon plus de 60 experts du secteur, du gouvernement, des organisations à but non lucratif et du monde universitaire connus sous le nom de Ransomware Task Force.[4]

2 : Source : Cybersecurity Ventures Report (Rapport de Cybersecurity Ventures) 3 : Source : Sophos State of Ransomware Report 2021 (Rapport Sophos sur l'état des ransomwares 2021) 4: Source : Ransomware Task Force (Groupe de travail sur les Ransomware)

L'ATTAQUE

L'hameçonnage est la principale « variété d'action » observée dans les attaques de l'année dernière et **43 %** desdites attaques impliquaient un hameçonnage et/ou un faux-semblant.[5]

COURRIELS D'HAMEÇONNAGE

Les courriels d'hameçonnage sont un véhicule de livraison courant des ransomwares. Ces courriels ont l'air légitimes, tels qu'une facture ou un fax électronique, mais ils contiennent des liens et/ou des pièces jointes malveillants qui peuvent infecter votre ordinateur et votre système.[5]

50% des vulnérabilités des applications internes sont considérées comme un risque élevé ou critique.[6]

VULNÉRABILITÉS DES SITES WEB ET DES LOGICIELS

Les cybercriminels implantent des ransomwares sur les sites Web et profitent des vulnérabilités logicielles pour lancer des attaques sur les visiteurs utilisant un logiciel obsolète (navigateur, plugin de navigateur).

5 : Source : Report by the Deloitte Cyber Inteligence Centre (Rapport par le Deloitte Cyber Intelligence Centre) 6: Source : Vulnerability Statistics Report 2021 (Rapport statistique sur les vulnérabilités en 2021)

PCI Security Standards Council

PROTÉGEZ VOTRE ENTREPRISE

SOYEZ PRUDENT

Formez vos employés. PCI DSS 12.6

- Développez un plan qui forme vos employés sur les meilleurs moyens d'éviter ces types d'attaques et sur la façon de les reconnaître et d'y répondre si elles se produisent.
- Assurez-vous qu'ils sont conscients des risques et qu'ils comprennent qu'il n'y a pas de mal à supprimer un courriel s'il semble suspect.
- Réfléchissez avant de cliquer. Les courriels peuvent sembler provenir de d'un collègue dans l'entreprise. En cas de doute, contactez toujours ce collègue pour confirmer avant de cliquer sur un lien ou d'ouvrir un fichier.

RESTEZ VIGILANT

Testez vos systèmes. PCI DSS 11.3

- Avez-vous testé vos systèmes dernièrement pour voir s'il est facile pour quelqu'un de s'y introduire ? Les cybercriminels sont tenaces, vous devriez l'être aussi.
- Une vulnérabilité constitue une porte « cassée » que les cybercriminels peuvent simplement franchir. Il est important que les vulnérabilités découvertes lors des tests soient corrigées et que vous ayez d'autres contrôles en place pour empêcher un individu malveillant de s'introduire dans vos systèmes.

Appliquez les correctifs aux mises à jour actuelles. PCI DSS 6.2

- Vos fournisseurs vous envoient des « patchs » pour corriger les problèmes de vos systèmes de paiement ou d'autres systèmes.
- Quand avez-vous vérifié pour la dernière fois les nouveaux correctifs de sécurité de vos fournisseurs de systèmes de paiement et de logiciels ?
- Les correctifs ferment les portes que les cybercriminels utilisent pour pénétrer dans vos systèmes. Suivez les instructions de vos fournisseurs et installez les correctifs dès que possible.

Restez vigilent pour toute activité suspecte. PCI DSS 11.5

- Surveillez-vous les changements dans vos systèmes ? Les modifications suspectes ou non autorisées/ non approuvées ont-elles été examinées ?
- La surveillance des changements dans vos systèmes vous aide à voir quand quelqu'un fait un changement que vous n'avez pas autorisé ou approuvé. En enquêtant sur les changements dès qu'ils se produisent, vous pouvez trouver les problèmes plus rapidement et améliorer vos chances de mettre fin à une attaque.
- Un processus de gestion des changements vous aidera à déterminer si les changements sont approuvés. Si le changement n'a pas été approuvé ou est inconnu, vous devez immédiatement enquêter pour déterminer si votre système a été compromis.

Sauvegardez vos systèmes. PCI DSS 9.5.1, 12.10.1

- Veillez à ce que votre sauvegarde n'écrase pas les bonnes sauvegardes précédentes. Cela peut permettre d'éviter de sauvegarder les données cryptées par un ransomware et d'écraser une bonne sauvegarde. La bonne pratique, quelle que soit la méthode de sauvegarde, consiste à effectuer régulièrement des sauvegardes complètes du disque et des sauvegardes incrémentielles (qui ne sauvegardent que les récentes données depuis la dernière sauvegarde).
- Pour réduire vos risques, évitez de conserver les données de sauvegarde en ligne (connectées aux systèmes qui sont sauvegardés). Stockez plutôt vos données de sauvegarde hors site et hors ligne (le stockage de vos sauvegardes « dans le cloud » est une méthode courante de stockage hors ligne ; voir toutefois la dernière puce de la liste). Il est ainsi plus facile de récupérer votre sauvegarde la plus récente si vos fichiers de données font l'objet d'une demande de rançon.
- Conservez plusieurs générations de sauvegardes et prévoyez une période de conservation compatible avec la capacité de votre entreprise à détecter les ransomwares et sa capacité à effectuer une reconstruction à l'aide d'enregistrements plus anciens.
- Avez-vous récemment testé l'intégrité de vos sauvegardes ? Avez-vous récemment testé le processus de sauvegarde et de récupération ? Il est crucial de s'assurer que vous pouvez récupérer les données de vos sauvegardes au cas où vos systèmes seraient verrouillés par un ransomware.
- Lorsque vous utilisez des sauvegardes en cloud, assurez-vous que votre fournisseur de services cloud est diligent et qu'il vous protège contre les logiciels malveillants de toutes sortes. Le stockage en cloud peut également être verrouillé par l'attaquant s'il est connecté aux systèmes de sauvegarde effectuant une synchronisation persistante.

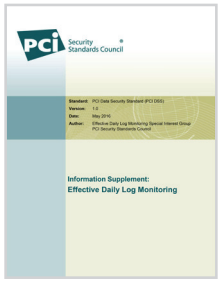
FAITES UN PLAN

Soyez prêt. PCI DSS 12.10

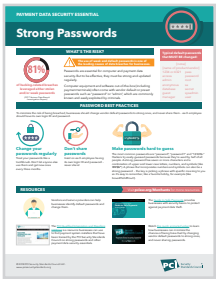
- Vous et vos employés devez savoir comment répondre à une attaque et ce qu'il faut faire quand elle se produit, y compris la personne à contacter.
- Assurez-vous d'avoir mis en place un plan et de le communiquer à vos employés.
- Révisez ce plan régulièrement et engagez-vous à fournir une formation continue à votre personnel.

DOCUMENTS DE RÉFÉRENCE APPROFONDIS SUR LE PCI

pdf PCI Norme de sécurité des données version 3.2.1

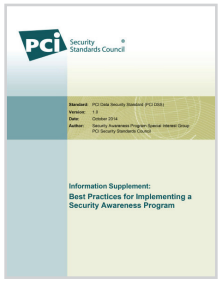


pdf Complément d'informations : Surveillance efficace des journaux quotidiens



pdf Essentiel de la sécurité des données de paiement: Mots de passe robustes

pdf Essentiel de la sécurité des données de paiement: L'installation de correctifs



pdf Meilleures pratiques pour la mise en œuvre d'un programme de sensibilisation à la sécurité

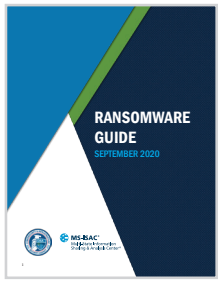
pdf Ressources de protection des paiements pour les petits commerçants: Guide pour des paiements sécurisés

RESSOURCES CONNEXES DU SECTEUR

pdf Évitez d'être la prochaine victime d'un ransomware. Aidez à protéger votre entreprise avec ces meilleures pratiques

pdf Ransomware : De quoi s'agit-il et que faire ?

www Projet « Finies les rançons »



pdf Guide CISA MS-ISAC sur les ransomwares

Pour tout commentaire d'expert ou toute question, veuillez contacter: press@pcisecuritystandards.org
Pour plus d'informations sur les normes PCI et les ressources, consultez: www.pcisecuritystandards.org.