COMMENT PROTÉGER VOTRE ENTREPRISE DES

RANSOMWARES

Prenez les devants et empêchez les fichiers de votre entreprise d'être pris en otage

Trois niveaux de danger

Ransomware : logiciel malveillant conçu pour bloquer l'accès à un système jusqu'au paiement d'une rançon.

Danger faible

☆

Scareware

De faux utilitaires antivirus prétendent détecter des programmes malveillants et réclament un paiement en échange de leur suppression.

Danger moyen

☆☆☆

Ransomware bloqueur de navigateur ou d'écran

Messages prétendant émaner du FBI ou du Département américain de la justice et réclamant le paiement d'une amende du fait d'une activité illégale détectée sur votre ordinateur.

Danger maximal

☆☆☆☆

Ransomwares chiffreurs

Des messages intempestifs annoncent que vos fichiers sont chiffrés et exigent le paiement d'une rançon avant une date limite pour les récupérer.

Ransomwares chiffreurs : quels dangers pour votre entreprise ?

Fréquence

Des millions d'attaques de ransomwares sont perpétrées sur des entreprises de toutes tailles chaque année.*

*KPN, All Things Considered, 22/02/16

Données

Les ransomwares peuvent chiffrer les fichiers les plus importants de votre entreprise : fichiers comptables, médicaux, données clients confidentielles, etc. Une fois chiffrés, vous ne pouvez plus récupérer ces fichiers à moins de payer la rançon.

Argent

En février 2016, l'hôpital presbytérien d'Hollywood a payé 17 000 $ pour récupérer les données de ses patients. Dans son rapport « Data Breach Investigations », Verizon estime que la perte de 1 000 fichiers peut se traduire pour une entreprise par une perte financière dépassant 67 000 $. Ce coût pour l'entreprise augmente exponentiellement en fonction de l'ampleur de l'intrusion.

Réputation

En plus du chiffrement, de nouvelles générations de ransomwares menacent les entreprises de diffuser le contenu des fichiers en ligne.

Faut-il payer la rançon ?

Le FBI et les forces publiques peuvent parfois vous recommander le paiement de la rançon pour récupérer vos fichiers plus rapidement. Mais les professionnels de la cybersécurité vous le déconseillent. En effet, le paiement de la rançon ne garantit en rien l'accès à vos fichiers. Par contre, vous deviendrez sûrement la cible de nouvelles attaques de programmes malveillants.

Vous êtes vulnérable si…

- Vous utilisez des logiciels obsolètes.
- Votre navigateur et votre système d'exploitation ne bénéficient pas des derniers correctifs.
- Votre équipement est obsolète.
- Vous n'avez pas de stratégie de sauvegarde adaptée.
- Vous n'avez pas de stratégie de cybersécurité complète.

Prévention proactive

La meilleure protection reste la prévention. Suivez les étapes suivantes afin de protéger votre entreprise contre les ransomwares.

1

Installez les correctifs

Installez les dernières mises à jour de vos navigateurs, systèmes d'exploitation et autres applications.

2

Formez les utilisateurs

L'ingénierie sociale est l'une des méthodes les plus répandues d'infection par des ransomwares. Formez les utilisateurs à détecter les campagnes d'hameçonnage, les sites Web suspects et autres arnaques.

3

Sauvegardez les fichiers

Effectuez des copies sécurisées de vos données à intervalles réguliers et stockez-les hors de vos bureaux.

Assurez-vous de ne pas stocker vos sauvegardes sur un lecteur mappé. Certains ransomwares parviennent à chiffrer des fichiers sur des partages réseau non mappés.

Si vos sauvegardes sont stockées sur un périphérique USB ou un disque dur externe, vérifiez que ces appareils sont bien physiquement déconnectés des ordinateurs.

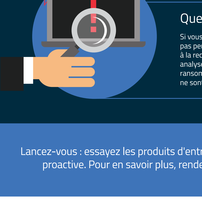
Nous vous recommandons de stocker vos sauvegardes sur un serveur sécurisé du cloud bénéficiant d'un haut niveau de chiffrement et d'un système d'authentification multifacteur.

4

Investissez dans une sécurité multicouche

Une solution de cybersécurité multicouche peut détecter et bloquer les attaques de ransomwares avant qu'elles se produisent. Pour une protection optimale, nous recommandons les couches suivantes :

- Pare-feu
- Protection anti-exploit
- Antivirus avec surveillance active
- Protection anti-malware
- Protection anti-ransomware



Que faire en cas d'infection ?

Si vous avez correctement sauvegardé vos fichiers, tout espoir n'est pas perdu. Sur un ordinateur non infecté, analysez vos sauvegardes à la recherche de programmes malveillants. Ensuite, lancez une analyse sur l'ordinateur infecté pour supprimer toute trace de ransomwares et autres programmes malveillants. Si vos sauvegardes ne sont pas infectées, vous pouvez les restaurer sur votre ordinateur.

Lancez-vous : essayez les produits d'entreprise Malwarebytes et adoptez la prévention proactive. Pour en savoir plus, rendez-vous sur **malwarebytes.com/business**

Malwarebytes