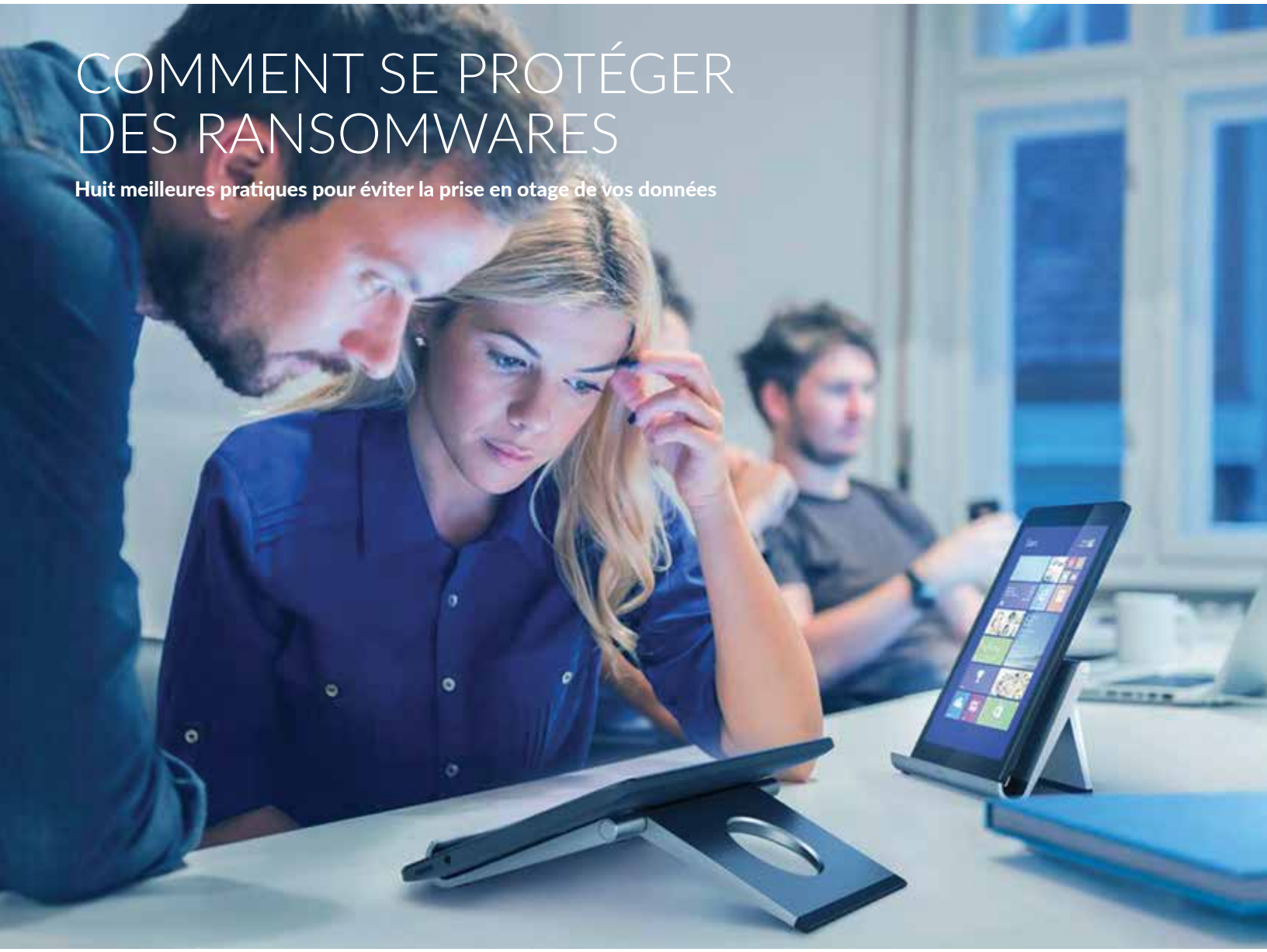
SONICWALL™

COMMENT SE PROTÉGER DES RANSOMWARES

Huit meilleures pratiques pour éviter la prise en otage de vos données



Ransomware : terme décrivant un programme malveillant qui refuse l'accès à des données ou des systèmes jusqu'au paiement d'une rançon. Toutes les entreprises peuvent être victimes d'une attaque par ransomware. Heureusement, de nombreuses mesures permettent de minimiser les risques auxquels elles s'exposent. Voici huit meilleures pratiques permettant de protéger votre entreprise des attaques par ransomwares.

1. Formation et sensibilisation :

La formation et la sensibilisation des utilisateurs sont des éléments essentiels et constituent la première mesure à mettre en place pour se protéger des ransomwares. Les utilisateurs doivent savoir :

- considérer avec précaution tous les messages suspects ;
- inspecter le nom de domaine qui a envoyé le message ;
- repérer les fautes d'orthographe, inspecter la signature et la légitimité de la demande ;
- passer la souris sur les liens pour en vérifier la destination ; si une URL paraît suspecte, saisir directement l'adresse du site Web ou le rechercher via un moteur de recherche au lieu de cliquer sur le lien du message.

2. Sécurisation de messagerie

Il est conseillé de déployer une solution de sécurisation de messagerie qui analyse toutes les pièces jointes en plus de filtrer les logiciels espions et les spams. Parallèlement à la formation régulière des utilisateurs et à l'évaluation des risques, il est également conseillé d'effectuer des tests de vulnérabilité au phishing.

3. Anti-malware

Qu'il s'agisse d'appareils personnels ou professionnels, les terminaux sont particulièrement vulnérables s'ils ne sont pas gérés par le service informatique ou s'ils ne sont pas dotés de la protection anti-malware appropriée. La plupart des solutions anti-virus sont basées sur les signatures et s'avèrent inefficaces si elles ne font pas l'objet de mises à jour régulières. Les nouvelles variantes de ransomwares sont codées de manière unique et sont donc indétectables à l'aide des techniques ayant recours aux signatures.

Aussi, beaucoup d'utilisateurs désactivent l'analyse anti-virus de leur système afin de ne pas ralentir ses performances. En réponse à ces limites, il existe des solutions de sécurité des terminaux qui utilisent l'apprentissage machine avancé et l'intelligence artificielle pour détecter les programmes malveillants. Ces solutions ont également une faible empreinte, ce qui entraîne un impact réduit sur les performances.

4. Terminaux mobiles

La gestion des terminaux constitue également un défi croissant car de nouveaux appareils aux multiples facteurs de forme et systèmes d'exploitation sont introduits sur le réseau. Les appareils mobiles sont particulièrement vulnérables, comme l'indique le rapport annuel 2016 de Dell sur les menaces, en raison des menaces émergentes par ransomwares sur la plate-forme Android™. Le choix d'une solution capable d'automatiser les correctifs et les mises à niveau de versions dans un environnement hétérogène composés de divers appareils, systèmes d'exploitation et applications, est important pour apporter une réponse adéquate à la palette de cyber menaces dont font partie les ransomwares.

Pour les utilisateurs distants situés à l'extérieur du périmètre du pare-feu d'entreprise, l'accès VPN doit non seulement établir une connexion sécurisée mais aussi réaliser un niveau d'interrogation des appareils suffisant pour vérifier le respect des règles applicables au terminal. Si un terminal ne possède pas les mises à jour de sécurité requises, il ne sera pas autorisé sur le réseau ou n'obtiendra l'accès qu'à un ensemble limité de ressources.

Pour les utilisateurs d'appareils mobiles Android en particulier, les étapes suivantes sont recommandées :

- Ne pas rooter l'appareil, car cela expose les fichiers système aux modifications.
- Toujours installer les applications depuis Google Play, car celles provenant de boutiques ou de sites inconnus peuvent être fausses et potentiellement malveillantes.
- Désactiver l'installation des applications provenant de sources inconnues.
- Autoriser Google à rechercher les menaces sur l'appareil.
- Prendre garde lors de l'ouverture de liens inconnus reçus dans des SMS ou des e-mails.
- Installer des applications de sécurité tierces qui analysent l'appareil régulièrement afin de détecter des contenus malveillants.
- Surveiller quelles applications sont enregistrées au titre d'administrateur de l'appareil.
- Pour les appareils gérés par l'entreprise, créer une liste noire d'applications non autorisées.

5. Segmentation du réseau

La plupart des ransomwares vont essayer de se propager depuis le terminal vers le serveur/stockage sur lequel résident toutes les données et applications stratégiques. La segmentation du réseau et l'isolement des applications et appareils sensibles sur un réseau distinct ou un LAN virtuel permet de limiter la propagation.

6. Sauvegarde et récupération

L'autre façon de se prémunir contre le paiement d'une rançon consiste à établir une solide stratégie de sauvegarde et de récupération. Autrement dit, à sauvegarder régulièrement les données. En effet, l'existence d'une sauvegarde distante permet de réduire les risques de pertes de données en cas d'infection. Selon la rapidité avec laquelle l'attaque est détectée, selon l'étendue de la propagation et le niveau acceptable de perte de données, la récupération depuis une sauvegarde peut être une bonne option. Cela demande toutefois une stratégie de sauvegarde mieux réfléchie, alignée sur le degré de confidentialité de vos données et les besoins de votre entreprise par rapport aux objectifs RPO (perte de données maximale admissible) et RTO (durée maximale d'interruption admissible). La majorité des données stratégiques doit être récupérable le plus rapidement possible. Et enfin, notons que l'existence d'une stratégie n'est pas suffisante. Il est tout aussi important d'effectuer des tests réguliers de récupération après sinistre et de continuité des activités.

7. Attaques chiffrées

Il est également essentiel de disposer d'un pare-feu approprié, capable d'analyser l'ensemble du trafic quelle que soit la taille des fichiers. Avec la rapide augmentation du trafic SSL chiffré, comme l'indique le rapport SonicWall sur les menaces, il existe toujours un risque lors du téléchargement de programmes malveillants chiffrés, invisibles pour les pare-feux classiques. Il est donc important de garantir que le pare-feu/IPS est en mesure de déchiffrer et d'inspecter le trafic chiffré sans trop ralentir le réseau.

> Pour un blocage efficace des ransomwares, il faut bien coordonner formation à la sécurité, technologie et gestion.

Une autre recommandation utile est d'afficher les extensions de fichiers. Par exemple, les programmes malveillants peuvent parfois pénétrer le système alors qu'ils portent une icône .pdf ou .mp3, alors qu'il s'agit en réalité d'un fichier .exe.

8. Surveillance et gestion

Le pare-feu de l'entreprise doit être capable de surveiller le trafic entrant et le trafic sortant ainsi que de bloquer la communication avec les adresses IP figurant en liste noire tandis que le ransomware tente d'établir le contact avec ses serveurs de commande et de contrôle.

Si une infection par ransomware est détectée, il convient de déconnecter immédiatement le système du réseau de l'entreprise. Dès qu'une nouvelle variante de programme malveillant sera détectée, le pare-feu doit avoir un processus de mise à jour automatisée et de gestion centralisée afin d'appliquer les mises à jour et les règles de manière rapide et cohérente pour tous les nœuds. Il est par ailleurs primordial de mettre à jour régulièrement vos logiciels et systèmes d'exploitation.

Conclusion

Les solutions SonicWall peuvent améliorer la protection à l'échelle de votre entreprise en filtrant chaque paquet et en contrôlant chaque identité. Par conséquent, vos données seront protégées, où qu'elles se trouvent, et les mesures de sauvegarde seront partagées pour de nombreuses menaces, y compris les ransomwares.

En savoir plus sur nos pare-feux nouvelle génération.

À propos de nous

En 25 ans d'histoire, SonicWall a toujours été un partenaire industriel de confiance dans le domaine de la sécurité. De la sécurité réseau à celle des accès, en passant par la sécurisation de messagerie, SonicWall n'a cessé de développer son portefeuille de produits, permettant aux entreprises d'innover, d'aller plus vite et de croître. Avec plus d'un million d'appareils de sécurité en place dans près de 200 pays et territoires de par le monde, SonicWall permet à ses clients de dire en toute confiance oui à l'avenir.

Pour toute question concernant l'usage potentiel de ce document, contactez :

SonicWall Inc.
5455 Great America Parkway,
Santa Clara, CA 95054

Consultez notre site Internet pour plus d'informations sur les bureaux nationaux et internationaux.
www.sonicwall.com

SolutionBrief-HowToProtect-EU-IMAG-29233