ManageEngine

PG Software Europe

Comment protéger votre entreprise contre les

RANSOMWARES

Les ransomwares sont une catégorie sophistiquée de logiciels malveillants qui retiennent vos données en otage jusqu'au paiement d'une rançon.

Prévention

- Sauvegardez vos fichiers
- Corrigez les vulnérabilités
- Utilisez le filtrage des e-mails
- Limitez les privilèges
- Sensibilisez les utilisateurs finaux
- Placez les applications sur une liste blanche

Détection

- Utilisez un outil robuste d'alerte aux ransomwares en temps réel pour signaler les invasions de malwares
- Apprenez à reconnaître les signes révélateurs d'une attaque de malwares tels que l'accès à des fichiers, leur renommage, leur suppression ou leur chiffrement en masse.

Mise en quarantaine

- Utilisez un outil de détection des ransomwares préconfiguré et automatisé pour détecter et éliminer instantanément les menaces.
- Arrêtez les systèmes infectés et isolez-les du réseau pour protéger vos autres serveurs de fichiers.

Restauration

- Avant de récupérer vos fichiers à partir d'une sauvegarde, assurez-vous que le malware a été complètement éliminé de votre entreprise.
- Affichez les détails forensiques de l'attaque par ransomware - par exemple qui a fait quoi et à partir d'où - afin d'identifier la source de la menace et d'éviter de nouvelles violations.

Payer ou ne pas payer ?

- Si votre entreprise est victime d'une attaque par ransomware, ne payez jamais la rançon, l'honneur n'existe pas chez les voleurs.
- Selon le **Kapersky Security Bulletin 2016**, une entreprise sur cinq qui paie la rançon ne récupère jamais ses données.
- Visitez nomoreransom.org pour signaler les cybercrimes et vérifiez les outils de déchiffrement des ransomwares disponibles.