AIDE-MÉMOIRE

SE PROTÉGER CONTRE LES RANÇONGICIELS

Objectif du document

Fournir des conseils et des outils pour se protéger contre les rançongiciels.

Les cybercriminels savent que les entreprises sont plus susceptibles de payer la rançon demandée, car les données sont vitales à leur survie.

Destinataire du document : Responsable des systèmes d'information

Date de la dernière modification : 2017-06

Les types de rançongiciels

- **Rançongiciel chiffrant** : Il chiffre les fichiers et les répertoires personnels.
- **Rançongiciel bloquant** : Il bloque l'écran de l'ordinateur et réclame une rançon.
- **Rançongiciel *Master Boot Record* (MBR)** : Il modifie une portion du disque dur du système d'exploitation pour interrompre le processus de démarrage.
- **Rançongiciel ciblant les serveurs Web** : Il chiffre des fichiers sur leur espace de stockage en exploitant une vulnérabilité dans le gestionnaire de contenu (CMS).
- **Rançongiciel mobile** : Il bloque le téléphone en se faisant passer pour une application connue.

Mesures préventives

1. **Sauvegarder.** Avoir un système de restauration en place afin d'empêcher qu'un rançongiciel détruise vos données personnelles pour toujours. Il est recommandé de faire deux copies de sauvegarde; l'une dans un service d'infonuagique et l'autre sur un support physique (ex. : disque dur, clé USB, ordinateur secondaire).
2. **Utiliser un antivirus.**
3. **Maintenir à jour les logiciels et le système d'exploitation de votre ordinateur.**
4. **Être vigilant.** Ne jamais ouvrir la pièce jointe incluse dans le courriel d'une personne que vous ne connaissez pas. En cas de doute, ne jamais cliquer sur un hyperlien inclus dans un courriel.
5. **Vérifier l'extension du fichier avant de l'ouvrir.** Demeurer vigilant face aux extensions de types .exe, .vbs, .js, .hta, .docx, .docm, .doc, .chm, .jar, .com, .ocx, .bat, .cmd, .pdf, .cpl, et .scr.
6. En cas de comportement inconnu sur l'ordinateur**, se déconnecter d'Internet ou de toute autre connexion réseau** afin d'empêcher l'infection de se propager.

En cas d'infection

Il est fortement recommandé de ne pas payer la rançon, même s'il est plus coûteux de restaurer les sauvegardes que de payer le montant demandé. En envoyant de l'argent aux criminels, non seulement vous confirmez que les rançongiciels fonctionnent, mais vous n'avez aucune garantie que la clé de déchiffrement vous sera communiquée.

1. Identifier le type de rançongiciel qui affecte votre système à l'aide de Crypto Sheriff (gratuit) : https://www.nomoreransom.org/fr/crypto-sheriff.php.

2. Restaurer votre poste avec une copie de sauvegarde qui ne contient pas le logiciel malveillant.

Pour les premières générations de rançongiciels, il est possible de déchiffrer vos fichiers avec les outils disponibles sur le site No More Ransom : https://www.nomoreransom.org/fr/decryption-tools.html.

Informations complémentaires

Consulter le site No More Ransom : https://www.nomoreransom.org/fr/prevention-advice.html