A+ A-

Cinq conseils pour se prémunir contre les « rançongiciels » (ransomware)

Par **Bercy Infos < https://economie.gouv.fr/entreprises/bercy-infos-qui-sommes-nous>** , le 11/10/2021 - **Sécurité numérique**

Vous avez reçu un message douteux contenant des pièces jointes ? Vous avez retrouvé par hasard une clé USB ? Gare aux « rançongiciels » (ou « ransomware ») ! Vos données peuvent-être chiffrées et prises en otage contre rançon. Voici 5 conseils pour minimiser les risques.

Qu'est qu'un ransomware ou rançongiciel ?

Vous êtes de plus en plus nombreux à recevoir des **messages douteux** contenant des **pièces jointes** ou des **liens** vous invitant à les ouvrir.

Prenez garde ! Des **logiciels malveillants** appelés « rançongiciels » ou « ransomware » peuvent s'y cacher.

Leur but ? **Chiffrer (coder) vos données** pour vous les rendre moyennant une **rançon**. Bien entendu, la payer ne garantit pas la récupération de vos données. Mieux vaut donc vous prémunir contre ce type d'attaque.

Comment se prémunir d'un ransomware ?

Conseil n°1 : effectuez des sauvegardes régulières de vos données

C'est le meilleur moyen de couper l'herbe sous le pied aux pirates souhaitant prendre vos données en otage ! Déplacez physiquement la sauvegarde de votre réseau (hors réseau), placez-la en lieu sûr et veillez à ce qu'elle fonctionne !

Conseil n°2 : n'ouvrez pas les messages dont la provenance ou la forme est douteuse

Ne vous laissez pas tromper par un simple logo ! Pire, le hacker peut avoir récupéré certaines de vos données préalablement (les noms de vos clients par exemple) et créer des adresses de messagerie ressemblant à un détail près à celle de vos interlocuteurs habituels.

Restez donc très vigilants ! Certains messages paraissent tout à fait authentiques.

Apprenez à identifier les courriels piégés (ou autres formes de récupération de vos données) sur le site de l'**Agence nationale de la sécurité des systèmes d'information (ANSSI) < https://www.ssi.gouv.fr/entreprise/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel/> . < https://www.hack-academy.fr/techniques>**

Vous avez un doute ? Contactez le messager par un autre biais.

Conseil n°3 : apprenez à identifier les extensions douteuses des fichiers

Vous recevez habituellement des fichiers en .doc ou .mp4 (par exemple) et le fichier du message dont vous avez un doute se finit par un autre type d'extension ?

Ne les ouvrez surtout pas ! Voici quelques exemples d'extensions douteuses : .pif, .com, .bat ; .exe, .vbs, .lnk, ...

Attention à l'ouverture de pièces jointes de type .scr ou .cab. Comme le rappelle l'**Agence nationale de la sécurité des systèmes d'information (ANSSI) < https://www.ssi.gouv.fr/actualite/alerte-campagne-de-rancongiciel/>** , il s'agit des extensions de compression des campagnes CTB-Locker sévissant chez les particuliers, les PME ou les mairies.

Conseil n° 4 : mettez à jour vos principaux outils

On ne vous le dira jamais assez : traitement de texte, lecteur PDF, navigateur mais aussi antivirus... Veillez à mettre à jour vos logiciels !

Si possible, désactivez les macros des solutions de bureautique qui permettent d'effectuer des tâches de manière automatisée. Cette règle évitera en effet la propagation des rançongiciels via les vulnérabilités des applications.

Considérez que, d'une manière générale, les systèmes d'exploitation en fin de vie, qui ne sont plus mis à jour, donnent aux attaquants un moyen d'accès plus facile à vos systèmes.

Conseil n° 5 : utilisez un compte « utilisateur » plutôt qu'un compte « administrateur »

Évitez de naviguer depuis un compte administrateur. L'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés de votre ordinateur.

Préférez l'utilisation d'un compte utilisateur. Cela ralentira, voire dissuadera le voleur dans ses actions malveillantes.

Tout savoir sur les attaques par rançonlogiciel

Attaque par rançongiciel : le guide de l'ANSSI pour les anticiper < https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/>

État de la menace rançongiciels à l'encontre des entreprises et institutions en 2021 < https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-001/>

Ces contenus peuvent aussi vous intéresser

Sécurité de vos données : les 7 méthodes de piratage les plus courantes

Dix règles pour vous prémunir contre le piratage de vos données personnelles

Lutter contre les spams

Thématiques : **Sécurité numérique**

Ce sujet vous intéresse ? Chaque jeudi avec la lettre Bercy infos Entreprises, recevez les toutes les dernières actus fiscales, comptables RH et financières… utiles à la gestion de votre activité.