E6. Se protéger contre les « rançongiciels »

Le terme « rançongiciel » (ou *ransomware* en anglais) est une contraction des mots « rançon » et « logiciel ». Il s'agit donc par définition d'un programme malveillant visant à obtenir le paiement d'une rançon. Pour y parvenir, le rançongiciel va empêcher l'utilisateur d'accéder à ses données (fichiers clients, comptabilité, factures, devis, plans, photographies, messages, etc.), en les chiffrant, puis lui donner les instructions utiles au paiement de la rançon. Lorsqu'un rançongiciel infecte un poste de travail, le plus souvent (mais pas nécessairement) par l'envoi d'un courrier électronique piégé, l'infection est dès lors susceptible de s'étendre au reste du système d'information (serveurs, ordinateurs, téléphonie, systèmes industriels, etc.).

ORGANISATIONNEL

➤ **Effectuer des sauvegardes de données régulières**

Les sauvegardes constituent la meilleure parade contre les rançongiciels. Effectuées régulièrement, elles permettent de retrouver ses données si une telle attaque survient. Ces sauvegardes sont à appliquer en priorité aux données sensibles, aux serveurs et aux applications métiers dont la paralysie serait très néfaste pour l'activité de l'entité.

Enfin, le moyen le plus sûr, mais aussi le plus simple, de protéger ses données consiste à stocker une copie de ses sauvegardes sur un support déconnecté comme par exemple un disque dur amovible. Pour les entités plus larges où une telle solution n'est pas envisageable de manière générale, elle pourra être réservée aux données les plus sensibles. De la même manière, si le stockage des données est externalisé (i.e. sur le cloud), il est essentiel de se déconnecter à l'issue de chaque sauvegarde.

➤ **Ne pas payer les rançons !**

Accepter le paiement de la rançon entretient d'une part le système frauduleux et, d'autre part, ne garantit en rien la récupération de ses données. Il est en revanche conseillé de porter plainte auprès des services de police ou gendarmerie spécialisés.

TECHNIQUE

➤ **Assurer la mise à jour automatique de tous ses logiciels et applications**

Les rançongiciels utilisent les vulnérabilités des programmes pour se propager. Mettre à jour l'intégralité de ses logiciels et applications limite leur risque de propagation au sein du système d'information.

➤ **Créer et se servir d'un compte « utilisateur »**

Par défaut, la plupart des personnes bénéficient sur leur ordinateur de « droits **administrateur** ». Une telle élévation de droits fait courir le risque, en cas d'attaque, de faciliter la propagation du rançongiciel de l'ordinateur au reste du système. Créer et utiliser un compte « utilisateur » permet au contraire de ralentir ces attaques ou d'en limiter les effets.

➤ **Renforcer la configuration des logiciels bureautiques ou manipulant des données issues d'internet**

Restreindre l'autorisation des macros dans les suites bureautiques permet d'éviter la réalisation de tâches automatisées. Si un logiciel lambda demande de les activer à l'issue de l'exécution d'un document inconnu, il convient de toujours répondre « non ».

COMPORTEMENTAL

➤ **Ne pas ouvrir les messages dont l'origine ou la forme semblent douteuses**

Les courriers électroniques suspects (fautes d'orthographe ou de frappe, langage inapproprié, mauvaise résolution graphique ou déformation des images, etc.), peuvent contenir des liens ou des pièces jointes qui, par un simple clic, sont susceptibles de permettre l'exécution d'un programme malveillant sur le système. Au moindre doute, mieux vaut privilégier l'accès au site internet dont il est fait mention dans le message en tapant directement l'adresse dans la barre de recherche.

Pour tromper la vigilance de l'utilisateur, certains de ces courriers électroniques vont parfois plus loin en adressant à ce dernier un contenu personnalisé qui fera écho à son environnement familier. On parle alors de « hameçonnage ciblé » (*spear phishing* en anglais).

Mots clés

Chiffrement : procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'information impossible à toute personne qui ne possède pas la clé de (dé)chiffrement.

Droits « administrateur » : faculté d'effectuer des modifications affectant la configuration du poste de travail (modifier des paramètres de sécurité, installer des logiciels, etc.).

Pour aller plus loin

➤ Agence nationale de la sécurité des systèmes d'information (Anssi)

- Guide des bonnes pratiques de l'informatique
- Note d'information du CERT-FR relative à la protection contre les rançongiciels
- Initiative pour aider les victimes de rançongiciels à récupérer leurs données chiffrées sans avoir à payer de rançons aux délinquants
- Fédération EBEN, Alerte aux rançongiciels – Vos données en otage contre de l'argent, flyer

Plateforme cybermalveillance.gouv.fr

- Fiche réflexe - Les rançongiciels (ransomware)