Fiche n°6 : Sécurité informatique

Les attaques informatiques à l'encontre des collectivités territoriales ne cessent de se multiplier.

Via des messages frauduleux, les pirates paralysent les systèmes informatiques et les comptes rendant impossible l'accès aux logiciels, boites mail et autres ressources numériques.

Quels sont les conséquences pour les collectivités victimes d'un piratage ?

- Interruption des services administratifs ;
- Inaccessibilité des documents financiers ou administratifs ;
- Fuites de données à caractère personnel ;
- Atteinte à la réputation ;
- Risques juridiques, etc.

Comment identifier une attaque ?

Le procédé est souvent le même :

- Réutilisation d'une ancienne conversation ;
- Envoi d'un mail avec un nom d'émetteur connu mais une adresse mail inconnue ;
- Un lien pour télécharger un document qui contient des codes malicieux et dangereux ;
- Etc.

Qu'est-ce qu'un rançongiciel ?

Un **rançongiciel est un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon.**

Lors d'une attaque, l'ordinateur ou le système d'information de la victime est mis hors d'état de fonctionner de manière réversible.

La plupart des rançongiciels chiffrent, par des mécanismes cryptographiques, les données de l'ordinateur ou du système rendant leur consultation, ou leur utilisation, impossibles.

L'attaquant adresse alors un message à la victime où il propose, contre le paiement d'une rançon, de lui fournir le moyen de déchiffrer ses données.

Fiche n°6 : Sécurité informatique

Comment réduire les risques d'attaque ?

- **Sauvegarder régulièrement** ses **données**, par exemple sur un support externe tel qu'un disque dur (à débrancher après utilisation et heures de travail) ;
- **Maintenir à jour les logiciels et les systèmes ;**
- Utiliser et **maintenir à jour les logiciels antivirus**, faire des scans réguliers de son ordinateur afin de détecter la présence éventuelle de logiciels malveillants ;
- **Sécuriser les messageries** en utilisant des solutions anti-spam ;
- **Créer des mots de passe complexes** et les renouveler régulièrement ; ne pas utiliser le même mot de passe pour sa session et sa messagerie ; ne pas l'enregistrer dans les navigateurs web ;
- **Limiter les droits des utilisateurs**, donner des habilitations en fonction des missions de chacun ;
- **Sensibiliser** les **agents** sur les **bonnes pratiques** à mettre en œuvre, comme ne pas ouvrir la pièce jointe d'un mail dont on ne connait pas l'expéditeur, vérifier systématiquement l'adresse mail de l'émetteur.

Voir les préconisations dispensées par :

- L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) https://www.ssi.gouv.fr/
- La plateforme mis en place par le Gouvernement : https://www.cybermalveillance.gouv.fr/

Que faire en cas d'attaque ?

Premiers gestes :

- **Prévenir son service informatique** ou prestataire informatique ;
- **Informer son délégué à la protection des données ;**
- **Déconnecter** du réseau au plus vite les équipements infectés (câble, wifi) ;
- **Bloquer toutes les communications** vers et depuis Internet ;
- **Laisser éteints tous les équipements** informatiques non démarrés.

Piloter la gestion de la crise cyber

- **Trouver de l'assistance technique** → site cybermalveillance qui permet d'entrer en contact avec des prestataires de proximité ;
- **Ne pas payer la rançon**, rien ne prouve que vous récupériez vos données si vous le faites ;
- **Déposer plainte ;**
- **Restaurer les systèmes** depuis des **sources saines** → concernant les équipements infectés, il est préférable de réinstaller le système sur un support connu et de restaurer les données depuis les sauvegardes effectuées.