AU CŒUR
DU DÉBAT PUBLIC

COMMISSION
NUMERIQUE

LA SECURITE NUMERIQUE DES COLLECTIVITES TERRITORIALES

Comment se protéger des cyber-attaques ?

Note préparatoire du 01/02/2022

I INTERVENANTS

Julien Chambon, Maire de la Commune de Houilles (78)

Guillaume Crepin, Délégué régional de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

David Prache, Dirigeant et cofondateur de la startup de coaching en cybersécurité OPPENS – Groupe Société Générale

Laurent Verdier, Chargé de mission sensibilisation - risque cyber pour le Groupement d'Intérêt Public Action contre la Cyber-malveillance (GIP ACYMA)

Le mardi 1er février 2022 de 9h à 11h

En visioconférence

Élus référents :

- Eddie AÏT, maire de Carrières-sous-Poissy (78)
- Christophe IPPOLITO, adjoint au maire de Nogent-sur-Marne (94)
- Dominique TURPIN, maire de Nézel (78)

Pour rejoindre en visioconférence, veuillez cliquer ou copier/coller le lien suivant : https://zoom.us/j/93179323111?pwd=akVhVWo5bUpFQXVIM20wV0kyQ0gwUT09

ID de réunion : 931 7932 3111
Mot de passe : 058435

En cas de problème de connexion, veuillez contacter notre hotline : 0970 711 105 ou support@frv-sense.com

OBJECTIFS

- ✓ Echanger sur les enjeux de la cybersécurité pour les communes
- ✓ Echanger sur les bonnes pratiques pour se protéger des cyberattaques

CONTEXTE / ACTUALITÉ

L'année 2020 a été marquée par un grand nombre de cyber-attaques envers les collectivités locales. En effet, les signalements d'attaques par rançongiciels[1] ont été multipliés par 3 entre 2019 et 2020. Ces signalements émanaient autant de grandes collectivités que des plus petites. Au total, près de 30% des collectivités en France ont déjà été victimes de l'un de ces rançongiciels.

[1] Selon Cybermalveillance.gouv.fr : un rançongiciel est un logiciel malveillant qui bloque l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès

Selon une table-ronde sénatoriale sur la cybersécurité, quatre motifs expliqueraient la banalisation de ce type de cyberattaques :

- La numérisation de l'économie et des services publics, accélérée avec le confinement lié au développement du télétravail et le déploiement de la fibre
- La professionnalisation de la cybercriminalité, facilitée par sa « plateformisation », son industrialisation, et le développement des cryptomonnaies ;
- La difficulté de la prévention et de la répression, lesquelles nécessitent à la fois la prise de conscience de tous et une coopération internationale efficiente ;
- L'intégration du cyberespace comme nouveau vecteur de la conflictualité géopolitique dont les collectivités territoriales, leurs établissements publics et les établissements de santé, sont soit les cibles soit les victimes collatérales.

Une prise de conscience collective s'est faite que toutes les collectivités publiques pouvaient être des cibles potentielles, y compris les plus petites. Ces petites communes sont d'ailleurs bien souvent démunies et moins bien armées numériquement face aux attaques.

Une commune de 5 000 habitants, qui a témoigné anonymement pour Cyber-malveillance, a expliqué avoir subi un piratage du site internet de sa collectivité en raison des failles de sécurité liées à une non mise à jour du site. Plusieurs semaines furent nécessaires au rétablissement de l'ensemble des services de la collectivité.

Cette vigilance face aux vulnérabilités des systèmes d'information se trouve d'autant plus mise en avant par les acteurs de la cybersécurité dans le contexte de la tenue des scrutins présidentiel et législatifs de 2022.

Une note produite par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)[2] rappelle **plusieurs bonnes pratiques à adopter quotidiennement pour se prémunir face à ces attaques de rançongiciels, parmi lesquelles la sauvegarde régulière des données sur des supports hors ligne, la mise en place de mots de passe complexes et uniques et une vigilance accrue sur les pièces-jointes pouvant sembler douteuses.**

Les sujets liés à la sécurité numérique des systèmes d'information (SI) peuvent être difficiles à s'approprier par les élus locaux, du point de vue de la technicité de certains outils informatiques.

---

[2] Consultable à l'adresse suivante : https://www.cher.gouv.fr/content/download/31532/209786/file/20211217_np_anssi_plaquette_scrutins_2022_v1h.pdf

Néanmoins, l'élu a un rôle déterminant à jouer auprès de ses agents et de ses administrés pour :

- **Impulser un effort collectif** (former et sensibiliser ses collaborateurs, allouer des investissements à la sécurisation du numérique)
- **Forger une vision globale et définir des priorités d'action** (faire un état des lieux de sa collectivité, cartographier les systèmes d'information)
- **Préparer la collectivité à agir face à une situation de crise** (lister les contacts clefs, préparer une communication de crise, connaître les principales obligations juridiques)

Les acteurs de la cybersécurité en France :

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) :

Autorité nationale en matière de sécurité des systèmes d'information créée par décret en 2009, l'Agence est placée sous l'autorité du Premier ministre et est rattachée au secrétaire général de la défense et de la sécurité nationale.

A ce titre, l'ANSSI :

- Coordonne l'action gouvernementale en matière de défense des systèmes d'information à l'échelle nationale
- Elabore les mesures de protection des systèmes d'information et veille à leurs applications
- Se prononce sur la sécurité des dispositifs de protection des systèmes d'information et des prestataires de services de confiance

Le Groupement d'Intérêt Public Action contre la Cyber-malveillance (GIP ACYMA)

Le GIP ACYMA est la structure chargée de piloter la plateforme *Cybermalveillance.gouv.fr.* Elle est chargée de sensibiliser, de prévenir et d'aider les victimes de cyber-malveillance, que ce soit auprès des particuliers, des entreprises ou des collectivités. En tant que groupement d'intérêt public, le GIP ACYMA adopte une gouvernance partagée par un collège d'acteurs publics (Ministères, Agence d'Etat, collectivités, etc…) et privés (Orange, Google, Microsoft, Bouygues, etc…)

A ce titre, le GIP ACYMA :

- Assiste les victimes d'actes de cyber-malveillance
- Mène des actions de prévention des risques à la cybersécurité
- Observe et mène des études de prospection sur le risque numérique

PROPOSITION DE DEROULE

09H-09H05 : Introduction des élus référents (5 minutes)

09H05-09H15 Témoignage de Julien Chambon, Maire de Houilles (78) sur la cyberattaque subie par sa commune le 30 janvier 2021 (10 minutes)

09H15-10H00 Temps de présentation de Guillaume Crépin de l'Agence Nationale de Sécurité des Systèmes d'Information et de Laurent Verdier pour le GIP Action contre la Cyber-malveillance (45 minutes)

10H00-10H10 Temps de présentation de David Prache pour la start-up de coaching en cybersécurité OPPENS (10 minutes)

10H10-10H55 Temps d'échanges avec la salle (45 minutes)

10H55- 11H Conclusion par les élus référents (5 minutes)