Fiche pratique pour la mise en oeuvre de votre plan d'actions cyber dans votre collectivité.

Description rapide de l'objectif visé :

S'assurer avec le prestataire qu'une vérification des alertes est réalisée au moins une fois par an.
La collectivité possède son propre nom de domaine.

Coût estimé :

400€/an

Niveau de difficulté de l'action :

Modérée

Ressources nécessaires :

Ordinateur, licence Antivirus professionnel

Niveau d'accompagnement :

Standard

Temps estimé :

2-5 jours

Public visé pour l'action :

Responsable informatique
Personne en charge de l'informatique

Organisation conseillée pour la mise en œuvre dans votre collectivité :

1. Qui fait quoi ? Définir les rôles et responsabilités.
Qui réalise l'administration de la console centralisée de la solution antivirus ?
Qui réalise l'installation et le paramétrage du nom de domaine de la collectivité ?

2. Pourquoi ?
S'assurer du niveau de sécurité et l'absence de logiciels malveillants sur les équipements informatiques sans avoir à se déplacer et interrompre le travail des utilisateurs. Vérifier que les alertes sont prises en compte et amène à une résolution ou un plan de traitement le cas échéant.

Pour le nom de domaine, il s'agit de faire face au cyber squatting et de faire en sorte que la mairie dispose d'adresses mail composées de son nom (exemple : secretariat@nomdelamairie.fr).

3. Comment ?
Vérifier une fois par an la console des évènements remontés afin d'en détecter la cause racine.
Se rapprocher de son OPSN pour disposer d'un nom de domaine.

4. Combien ?
Chaque poste, chaque serveur doit posséder une solution antivirale connectée à la console.
Un nom de domaine par collectivité.

5. Quand ?
Dès que possible et une fois par an.

Livrable de l'action terminée :

Le prestataire fournit un registre des évènements sécurité qui se sont réalisés sur l'ensemble des équipements avec les résolutions associées.
La collectivité possède son propre nom de domaine.

Description étape par étape pour la mise en œuvre :

1. Lors de la création du contrat avec le prestataire, prévoir la création d'un registre des événements de sécurité et de leurs résolutions par ce dernier et y inscrire qu'il pourra être audité durant l'année.

2. Questionner le prestataire une fois par an pour qu'il vous fournisse le registre des évènements.

3. Louer un nom de domaine en lien avec votre collectivité. Rapprochez-vous de votre OPSN pour être accompagnés dans cette démarche.

Pour aller plus loin :

ANSSI :
- Guide des bonnes pratiques de l'ANSSI
- Guide d'hygiène informatique

Cybermalveillance :
- Fiche virus informatique