TOUS CONCERNÉS !

CYBERSÉCURITÉ des collectivités

Synthèse des recommandations de la matinée du 3 mars 2023

AGATE
AGENCE ALPINE DES TERRITOIRES

Comment prévenir et limiter les risques ?

1 Organisez des sessions de **sensibilisation** aux risques et des sessions de **formation** aux bonnes pratiques pour :

- ✓ vos agents
- ✓ vos élus

2 Mettez en œuvre les **bonnes pratiques** d'hygiène informatique recommandées par l'ANSSI

Notamment vérifiez que vous disposez (ou équipez-vous) de :

- ✓ **Un inventaire matériel, logiciel et réseau**
  Vérifiez que celui-ci est bien à jour !
- ✓ **Une sauvegarde sécurisée de vos données**
  - Vérifiez le temps de conservation de vos sauvegardes (minimum 30 jours)
  - Vérifiez qu'elles sont régulièrement testées
  - Vérifiez que l'ensemble des données nécessaires au fonctionnement de la collectivité sont bien sauvegardées
- ✓ **Un antivirus professionnel**
  - Vérifiez que tous vos serveurs et postes en sont équipés
- ✓ **Un gestionnaire de mots de passe et des pratiques d'authentification adaptées**
  - Vérifiez que vos mots de passe sont forts (minimum 12 caractères) et différents pour chaque service/site
  - Vérifiez que vos mots de passe ne sont pas stockés sur des supports non sécurisés tels que des fichiers excel, navigateurs, un cahier etc. et utilisez un gestionnaire de mots de passe sécurisé pour stocker et partager vos mots de passe
- ✓ **Un système de suivi des mises à jour de votre parc informatique**
  - Vérifiez la date de la dernière mise à jour de Windows sur vos postes, de vos serveurs, de vos logiciels

3 Faites **auditer** régulièrement la sécurité de votre système informatique par un tiers externe et suivez ses recommandations

4 Formalisez et testez un **plan de crise** afin d'anticiper une attaque, accélérer la reprise d'activité et être prêt à travailler en mode dégradé

Que faire en cas d'attaque (ou de suspicion d'attaque) ?

Alertez immédiatement vos différents contacts informatiques :

- ✓ votre service informatique interne (si existant)
- ✓ votre ou vos prestataires informatiques (maintenance, sauvegarde etc.)
- ✓ votre structure de mutualisation de proximité (Agate en Savoie)
- ✓ votre DPO

Saisissez dès que possible un dispositif d'aide et de réponse

- ✓ Commencez un parcours d'assistance victime sur Cybermalveillance.gouv.fr pour être mis en contact avec des prestataires spécialisés
- ✓ Appelez le 17 ou rapprochez-vous de votre gendarmerie (ou service de police)

TOUS CONCERNÉS !
CYBERSÉCURITÉ des collectivités

Ressources, liens clés

Ressource clé 1

Guide « Obligations et responsabilités des collectivités locales en matière de cybersécurité » (Cybermalveillance et CNIL / 2022)

Ressource clé 2

Guide « Cybersécurité : toutes les intercommunalités et communes sont concernées » (AMF et ANSSI/2020)

Ressource clé 3

IMMUNITÉ Cyber, une auto-évaluation du niveau de cybersécurité de la collectivité (AMF, Gendarmerie et Cybermalveillance / 2021)

Comment prévenir et limiter les risques ?

1 Organisez des sessions de sensibilisation aux risques et des sessions de formation aux bonnes pratiques

Ressource clé kit de sensibilisation aux risques numériques (Cybermalveillance/2022)

Ressource clé programme de sensibilisation des élus et agents (Cybermalveillance/2022)

Pour aller plus loin cours en ligne d'initiation à la cybersécurité (ANSSI/2022)

2 Mettez en œuvre les bonnes pratiques d'hygiène informatique recommandées par l'ANSSI

Ressource clé la cybersécurité en 13 questions document également adapté aux petites et moyennes collectivités (ANSS/2022)

Pour aller plus loin les guides méthodologiques de l'ANSSI

3 Faites auditer régulièrement la sécurité de votre système informatique par un tiers externe et suivez ses recommandations

Lien clé pour sélectionner un prestataire référencé et/ou labellisé sur **Cybermalveillance**

4 Formalisez et testez un plan de crise

Ressource clé gestion de crise cyber (ANSSI/2022)

Que faire en cas d'attaque (ou suspicion d'attaque) ?

Ressource clé Fiche pratique « Que faire en cas de cyberattaque » et « Affiche Premiers Gestes » (Cybermalveillance / 2022)

Lien clé dispositif de conseil et orientation des victimes de Cybermalveillance Parcours d'assistance victime

Les acteurs clés / vos contacts

Agate - Opérateur Public de Services Numériques (sensibilisation, fourniture d'outils cyber, audit, support en cas d'attaque) https://agate-territoires.fr/confiance-numerique
✉ **numerique@agate-territoires.fr** ✆ **04 79 68 53 00**

Gendarmerie (sensibilisation, pré-diagnostic, accompagnement en cas d'attaque) contactez votre brigade en cas d'attaque https://www.interieur.gouv.fr/Contact/Contacter-une-brigade-de-gendarmerie-ou-un-commissariat-de-police et pour une demande de pré-diagnostic ✉ **cptm.ggd73@gendarmerie.interieur.gouv.fr**

Cybermalveillance.gouv.fr (sensibilisation et parcours d'assistance victime)
www.cybermalveillance.gouv.fr/

ANSSI (sensibilisation, bonnes pratiques et support en cas d'attaque)
www.ssi.gouv.fr/ ✉ **auvergne-rhone-alpes@ssi.gouv.fr**