TOUS CONCERNÉS !

CYBERSÉCURITÉ des collectivités

Comment exposer votre collectivité aux cyberattaques ?

10 pratiques à proscrire dans une collectivité en matière de sécurité informatique

AGATE
AGENCE ALPINE DES TERRITOIRES

*« Sur la base des audits de cybersécurité réalisés au sein des collectivités savoyardes, voici **le « top 10 » des erreurs** que nos spécialistes du numérique ont pu observer (et donc à vérifier dans vos collectivités) ! »*

1 Disposer de sauvegardes sur un disque dur externe, un NAS ou un serveur local, non isolé du reste du réseau

« Non isolé » signifie localisé sur le même réseau que vos imprimantes ou vos ordinateurs. Si vous êtes dans cette situation, en cas d'attaque, vous perdrez toutes vos données (y compris vos sauvegardes) !

À faire

Vérifier auprès de votre prestataire que vos sauvegardes locales sont isolées et protégées et/ou passer par une sauvegarde cloud de qualité.
Dans tous les cas, se conformer au principe essentiel du 3-2-1-1-0 (3 copies de vos données – 2 supports différents – 1 copie hors site – 1 test de restauration par an – 0 erreur au test).

2 Disposer d'un antivirus grand public

Les antivirus gratuits ou grand public ne permettent plus aujourd'hui d'assurer un niveau de sécurité suffisant face à la menace pesant sur les collectivités (ils ne détectent en effet que les menaces les plus connues).

À faire

Utiliser un antivirus de type EDR. Basés sur de l'analyse comportementale, ces antivirus contrôlent le parc informatique et détectent les incidents beaucoup plus efficacement.

3 Utiliser des imprimantes ou scanners non sécurisés

Encore bien souvent, vos copieurs ont des comptes d'administration avec des mots de passe très faibles (comme par exemple « admin » ou « macommune73 ») et des droits trop élevés sur le réseau.

Les attaquants le savent et s'engouffrent dans la brèche !

À faire

Vérifier auprès de votre prestataire que les comptes réservés aux copieurs sont protégés par un mot de passe suffisamment fort et sont bien des comptes dits « de services ». Garder également à l'esprit que les copieurs permettent de détourner facilement de nombreuses données sensibles (par exemple, numérisation des données de santé d'enfants accueillis au périscolaire).

4 Avoir des postes informatiques sans mot de passe ou compte administrateur

Si vos ordinateurs ne sont pas protégés par un mot de passe et/ou ont directement les droits « administrateur » (par exemple pour faciliter l'installation d'un logiciel), il sera enfantin pour un attaquant de déployer son virus. De même, en cas de « mauvais clic », les conséquences seront fatales car aucune protection ne préviendra l'exécution sur le poste d'un logiciel infecté.

À faire

Séparer les comptes utilisateur et administrateur, utiliser des mots de passe forts sur les ordinateurs, et respecter le principe du moindre privilège.

5 Stocker ses mots de passe dans un fichier Excel sur son ordinateur, un serveur ou une base de données non protégée

En cas d'attaque, l'attaquant aura accès à tous vos fichiers sensibles, y compris vos listes de mots de passe !

À faire

Utiliser un gestionnaire de mots de passe sécurisé et si possible, activer la double authentification.

6 Utiliser des versions obsolètes pour vos systèmes d'exploitation

Vos ordinateurs sont encore sous Windows 7 ?
Vos serveurs sont encore sous Windows server 2012 ? Alors sachez que ces systèmes d'exploitation ne sont plus maintenus par leur fabriquant. Cette obsolescence est une porte ouverte à beaucoup de failles et d'attaques potentielles.

À faire

Mettre à jour vos systèmes d'exploitation et acheter (si besoin) des licences récentes.

7 Regrouper tous vos équipements sur un seul réseau

Si tous vos usages (copieur, ordinateur, serveur, accès grand public etc.) sont sur le même réseau, une vulnérabilité sur un composant du système affectera les autres parties de ce dernier.

À faire

Demander à votre prestataire de dissocier les réseaux des ordinateurs, des copieurs, de la téléphonie, du wifi public et évidemment du réseau pour les éventuelles sauvegardes locales ! Il s'agit d'une condition primordiale lorsque l'on réalise des sauvegardes sur un NAS, un disque dur ou un serveur local.

8 Ne pas avoir d'équipements de sécurité appropriés (pare-feu, système de contrôle...)

Une simple box internet n'est pas dimensionnée pour répondre aux besoins d'une collectivité. Ce matériel grand public ne permet pas de sécuriser l'infrastructure et ses composants.

À faire

Prévoir l'achat d'une connexion Internet professionnelle avec un pare-feu - ainsi que sa configuration - afin de mettre en place un réel filtrage à l'entrée et à la sortie du système d'information et mettre en place un service de journalisation des éléments critiques (flux internet, historique de navigation, téléchargements etc.).

9 Ne pas faire vérifier régulièrement son système d'information par un tiers

Les prestataires informatiques sont humains et ne sont pas infaillibles. L'informatique évoluant constamment, il peut être difficile de suivre toutes les composantes. Chacune d'entre elles fait désormais l'objet de compétences et formations spécifiques (réseau, accès internet, bureautique, cybersécurité, etc.). De même, les contrats (de maintenance, support etc.) dont vous disposez sont peut-être anciens et inadaptés aux besoins actuels.

À faire

Penser à vérifier vos contrats (pour être sûr d'être bien assisté). Demander également des **rapports d'intervention** certifiant certaines opérations ainsi que les **documentations techniques** (utiles en cas d'attaque). Ne pas hésiter à demander à vos prestataires des labels type « ExpertCyber ». Et surtout faire régulièrement **auditer vos infrastructures et processus** par un tiers spécialisé en cybersécurité !

10 Ne pas avoir de système de journalisation et d'historique

En cas d'attaque, vous devrez être en capacité d'identifier le problème ou de retracer le parcours de l'attaquant. Une absence de système de journalisation rendra ce travail très difficile ou demandera l'intervention d'expertise à très hauts coûts.

À faire

Demander à vos prestataires d'activer les politiques d'audits, les flux de journalisations, l'horodatage des actions, ce qui permet la surveillance des comportements suspects

AGATE AGENCE ALPINE DES TERRITOIRES

Agate - Opérateur Public de Services Numériques est à disposition des collectivités sur les questions cyber (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 20**