La prévention du risque cyber

Obligations et bonnes pratiques pour votre collectivité

L'Agence nationale de la sécurité des systèmes d'information (ANSSI), chargée de la protection de la France face aux cyberattaques, a recensé 218 incidents touchant les collectivités territoriales en 2024.
Cette fiche, destinée aux élu(e)s et responsables informatique/système d'information, présente les bonnes pratiques permettant de limiter les risques et les effets d'une cyberattaque.

Quelles sont vos obligations ?

LE CADRE RÉGLEMENTAIRE EUROPÉEN DE LA CYBER SÉCURITÉ

• Le règlement général sur la protection des données personnelles (RGPD)

Les collectivités doivent garantir la conformité de leurs fichiers et services numériques au RGPD, afin d'assurer la protection des données personnelles et la sécurité des systèmes d'information.

Le RGPD impose notamment de désigner un délégué à la protection des données (DPO), de recenser les traitements et de tenir à jour un registre.

L'ensemble des obligations est disponible sur le site cnil.fr

• La directive européenne NIS 2 relative à la cybersécurité

Les collectivités doivent également garantir un haut niveau de cybersécurité afin d'assurer la disponibilité, l'intégrité et la confidentialité de leurs systèmes d'information.

Pour vérifier si votre collectivité est concernée par la directive, réalisez le test « Mon entité est-elle concernée ? » sur monespacenis2.cyber.gouv.fr.

Dans le cadre de NIS 2, vous devez notamment procéder à un enregistrement auprès de l'ANSSI, désigner un responsable de la cybersécurité et définir une politique de cybersécurité claire, validée par votre organe de direction.

Pour en savoir plus et connaître le détail de toutes vos obligations, rendez-vous sur messervices.cyber.gouv.fr.

Les collectivités doivent démontrer leur conformité, notamment en cas de contrôle, à la fois au RGPD et, le cas échéant, à NIS 2.

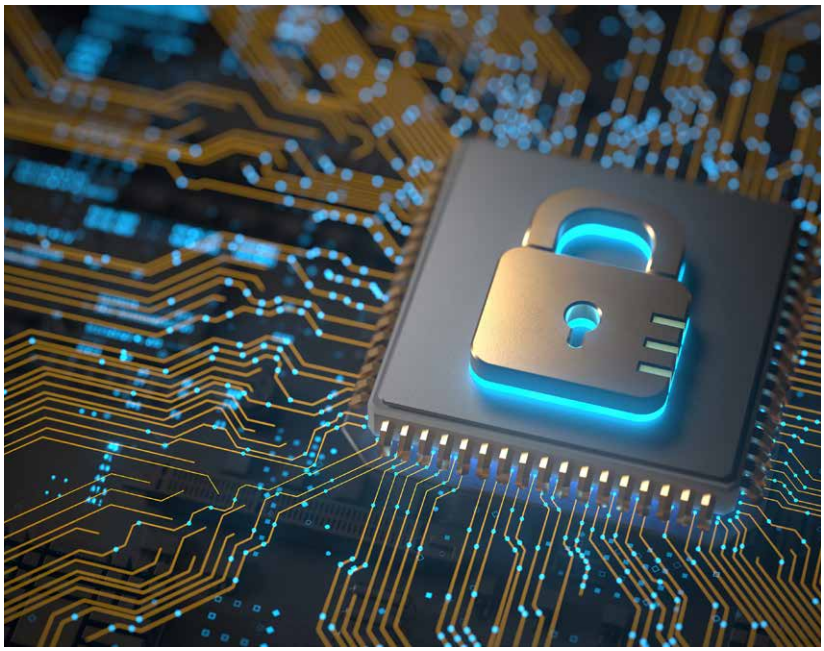
La mise en œuvre de la sécurité informatique

☑ Connaître le parc informatique de votre collectivité

- Identifier les équipements, services en ligne et logiciels critiques
- Déterminer les données essentielles à l'activité
- Contrôler les accès et supprimer les comptes obsolètes
- Sécuriser les connexions externes par des mesures de filtrage et de surveillance.

☑ Gérer les sauvegardes

- Sauvegarder régulièrement les données critiques
- Définir une périodicité adaptée
- Utiliser un espace de stockage sécurisé, isolé du réseau principal
- Tester régulièrement la restauration des sauvegardes pour en garantir la fiabilité.



☑ Protéger les accès

Mettre en œuvre une politique de protection des accès grâce à des pare-feu, c'est-à-dire des logiciels contrôlant les applications et les flux de données et restreignant le trafic entrant, sortant ou interne.

- Activer le pare-feu avec un paramétrage suffisamment restrictif
- Bloquer les flux inutiles
- Installer un pare-feu physique pour superviser l'accès à Internet et segmenter le réseau
- Recourir à un prestataire labélisé ExpertCyber *via* la plateforme cybermalveillance.gouv.fr.

☑ Contrôler les accès

Appliquer le principe du moindre privilège : chaque utilisateur ne doit accéder qu'aux ressources nécessaires à l'exercice de son activité.
Pour cela, utiliser des outils de gestion des identités et des accès (IAM) afin d'attribuer les droits à chaque utilisateur en fonction de son rôle et surveiller les accès.

☑ Appliquer les mises à jour de sécurité

Maintenir à jour systèmes et logiciels afin de limiter les vulnérabilités.
Pour cela, activer les mises à jour automatiques et s'assurer que les sous-traitants en font de même.

☑ Utiliser un antivirus

Installer un antivirus sur chaque poste, activer les mises à jour et analyses automatiques et privilégier les solutions intégrant pare-feu, filtrage web et anti-hameçonnage.

☑ Définir des mots de passe robustes

- Opter pour des mots de passe longs (12 caractères minimum, 16 pour les services critiques), complexes et uniques pour chaque service
- Utiliser un coffre-fort numérique pour les gérer.

☑ S'assurer de la conformité des fournisseurs

- Évaluer la conformité des prestataires
- Sélectionner des partenaires respectant les normes
- Réaliser des audits réguliers et assurer un suivi des incidents.

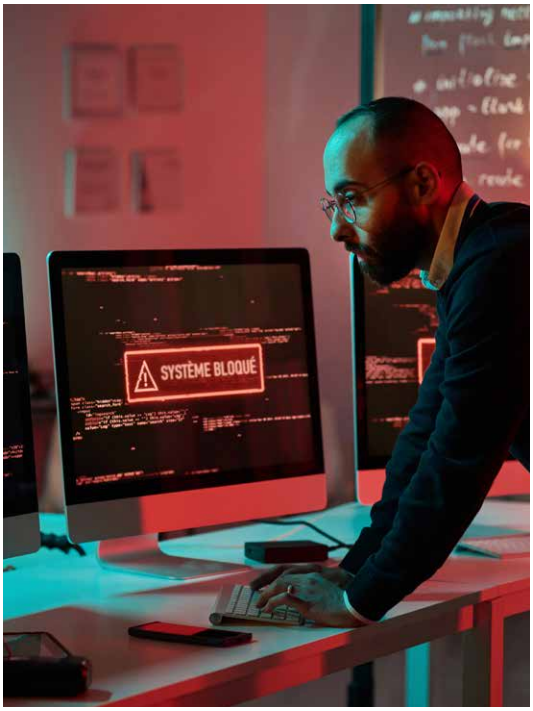
La veille et la sensibilisation des agents

- ☑ Suivre les recommandations et alertes de cybermalveillance.gouv.fr pour rester informé des menaces.
- ☑ Consulter les analyses techniques du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR).
- ☑ Promouvoir une culture de cyber prévention par la sensibilisation des agents, la diffusion de conseils pratiques et l'encouragement à la déclaration des incidents.
- ☑ Organiser des simulations (fausses tentatives de *phishing*) pour tester la réactivité des agents, renforcer la résilience et assurer une gestion efficace des crises.

🔎 Repères : comment réagir en cas de cyberattaque ?

Élaborer un plan de réponse aux incidents incluant des procédures pour identifier, contenir, éradiquer et récupérer.

- **Déconnecter** immédiatement les équipements infectés du réseau.
- **Notifier la CNIL** dans les 72 h en cas de violations de données personnelles.
- **Informer l'ANSSI,** si votre collectivité est concernée par NIS 2, dans les délais prévus : alerte initiale sous 24 h, mise à jour des informations 72 h après la notification et rapport final au plus tard un mois après la notification.
- **Contacter des interlocuteurs spécialisés** (GIP cybermalveillance, ANSSI, prestataires certifiés, assureur).
- **Porter plainte** auprès des autorités compétentes (gendarmerie, commissariat).
- **Signaler** éventuellement l'incident sur la plateforme 17Cyber.gouv.fr.
- Élaborer, si nécessaire, un **plan de communication** pour rassurer les usagers/citoyens.
- **Consulter le site cybermalveillance.gouv.fr** pour obtenir de l'aide, des contacts de proximité et effectuer une demande de sécurisation de votre collectivité.



Photos : iStock

À RETENIR

Renforcer la cybersécurité de votre collectivité passe par l'adoption de bonnes pratiques techniques et organisationnelles. S'appuyer sur des outils adaptés, des prestataires fiables et une veille active permet de mieux anticiper les menaces et de garantir la continuité des activités. Des contrats d'assurance dédiés au risque cyber peuvent vous accompagner pour la prévention des risques et en cas de cyberattaque, en vous apportant une assistance d'urgence pour endiguer sa propagation, initier des remédiations et vous aider à gérer la crise.