MN&P-VP/Note n° 18 (#8950)
Dossier suivi par Véronique PICARD

Paris, le 11 juillet 2024

Cybersécurité

Jeux Olympiques et Paralympiques Paris 2024

A quelques jours de l'ouverture des Jeux Olympiques et Paralympiques, l'AMF invite les communes et les intercommunalités à être attentives à leur sécurité numérique. Vous trouverez ci-dessous des premières recommandations faciles à mettre en œuvre avant de s'engager dans une démarche de protection plus importante.

Les bonnes pratiques à adopter

Les mairies sont aujourd'hui régulièrement la cible d'attaques par rançongiciels, la période des Jeux Olympiques et Paralympiques nécessite que l'on redouble de vigilance.

Dans ce contexte, l'AMF rappelle les recommandations minimums de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en matière de sécurité numérique :

⟶ Sauvegarder régulièrement les données indispensables ;
⟶ Être attentif avant d'ouvrir les pièces jointes contenues dans les courriels et ne pas cliquer sur les liens internet qui semblent douteux ;
⟶ Protéger les accès aux ordinateurs, aux sites internet et aux applications par des mots de passe complexes, uniques et secrets ;
⟶ Mettre régulièrement à jour les principaux logiciels (notamment antivirus) et les équipements informatiques.

Réagir en cas de cyberattaque

Pour limiter les impacts d'une cyberattaque :

⟶ Déconnectez immédiatement du réseau (câble ou Wi-Fi) les équipements piratés afin d'éviter la propagation de l'attaque et de préserver les preuves nécessaires à l'enquête ;
⟶ Ne connectez plus aucun appareil sur le réseau.

Contactez immédiatement votre service ou votre prestataire informatique et :

⟶ Notifiez les autorités et portez plainte auprès des services compétents (police ou gendarmerie) ;
⟶ Constituez une équipe pour gérer les conséquences de la cyberattaque et préparer une stratégie de communication ;
⟶ Déclarez rapidement l'incident à la CNIL et au plus tard dans les 72 heures.

Pour aller plus loin

→ **« Mon Aide Cyber »,** un service d'accompagnement de l'ANSSI : MonAideCyber (ssi.gouv.fr)

→ **Guide de l'AMF, avec le soutien de l'ANSSI, du mois de novembre 2020** : *Cybersécurité : toutes les communes et intercommunalités concernées :* Cybersécurité : toutes les communes et intercommunalités sont concernées (amf.asso.fr)

→ **Guide du GIP Cybermalveillance, en partenariat avec l'AMF** : *Cybersécurité : méthode clé en main pour sensibiliser les agents des collectivités :* AMF Association des Maires de France et des présidents d'intercommunalité

→ **Programme d'e-sensibilisation du GIP Cybermalveillance :** *comprendre les menaces et adopter les bonnes pratiques* **:** e-sensibilisation

→ **Fiches réflexe du GIP Cybermalveillance.gouv.fr** : *Les rançongiciels, Que faire en cas de cyberattaque* - www.cybermalveillance.gouv.fr

→ **Guide de l'ANSSI** : *Attaques par rançongiciels : tous concernés* –
Attaques par rançongiciels, tous concernés. | ANSSI (cyber.gouv.fr)

→ **En cas d'incident de sécurité informatique** : *accompagnement dans les démarches* - www.ssi.gouv.fr/en-cas-dincident