PRÉFÈTE
DES VOSGES
Liberté
Égalité
Fraternité

CABINET

0Cabinet
Affaire suivie par :
Conseiller Sécurité Numérique
Courriel : conseiller-secnum@vosges.gouv.fr

Épinal, le 13 janvier 2025

Madame la Directrice de Cabinet

à

l'ensemble des Collectivités Territoriales du département des Vosges

Objet : alerte aux collectivités territoriales sur l'état de la menace en matière de cyberattaques

La préfecture des Vosges a été récemment informée de cyberattaques à l'encontre des collectivités territoriales. En effet, avec le recours important aux services numériques pour les administrés, les collectivités territoriales sont particulièrement exposées aux risques de cyberattaques.

En 2024, les administrations ont fait l'objet de 1690 infractions numériques, soit une hausse de 42 % par rapport à l'année 2023 (1172 infractions). 312 plaintes ont été déposées par les seules collectivités territoriales.

Les collectivités territoriales sont des cibles de choix pour les groupes cybercriminels hacktivistes, les groupes de rançongiciels, ou les groupes liés à la criminalité organisée spécialisée dans les escroqueries massives.

Les escroqueries représentent 59 % des plaintes déposées par les collectivités territoriales en 2024.

Les conséquences des cyberattaques sur une collectivité territoriale sont grandes, elles engendrent l'arrêt ou la dégradation des missions de services publics en raison de sites internet ou de services en ligne rendus indisponibles, l'exposition de données personnelles ou sensibles, des effets de rebonds sur d'autres collectivités ou administrations, des pertes financières, et une atteinte à la sécurité des données des administrés.

Pour se prémunir des cyberattaques il convient de :
- former et sensibiliser les agents aux risques cyber et à l'hygiène informatique,
- effectuer des mises à jour régulières sur les logiciels et systèmes d'exploitations,
- détecter les vulnérabilités et mettre en place une politique de sécurité des systèmes d'information,
- effectuer des audits de cybersécurité,
- mettre en place des systèmes de sauvegardes robustes,
- préparer des scénarios de gestion de crise et des reprises d'activité pour optimiser la célérité de remise en état des serveurs en cas de cyberattaque, et la possibilité de continuer les activités du service en cas de panne informatique

Je vous invite à la plus grande vigilance face à cette menace. Il est important de prendre conscience du risque et de l'anticiper. En cas d'attaque, il est également primordial d'avoir les bons réflexes. Vous trouverez en pièce-jointe la fiche de bons réflexe en cas de cyberattaque réalisée par le groupement d'intérêt public action contre la cybermalveillance (https://www.cybermalveillance.gouv.fr).

Je souhaite également porter à votre connaissance l'existence du nouveau dispositif 17Cyber destiné à toutes les victimes d'infractions numériques (particuliers, entreprises et collectivités) pour une assistance en ligne. Disponible 24 heures sur 24 et 7 jours sur 7 et assuré conjointement par la police nationale, la gendarmerie nationale, et cybermalveillance.gouv, les victimes de cybermalveillance pourront recevoir des conseils. Vous trouverez toutes les informations sur le site (https://17cyber.gouv.fr/).

Je sais pouvoir compter sur votre vigilance et votre mobilisation.

Pour la préfète,
la Directrice de Cabinet

Lynda BOUDJEMA