Intervenir sur le territoire pour faire face

Cybersécurité : un partenariat renforcé entre le Centre de Gestion de la Fonction Publique Territoriale du Finistère (CDG29) et le Groupement de Gendarmerie Départementale du Finistère (GGD29)

Signature de la convention de partenariat entre le CDG et le GGD29 pour proposer aux collectivités une réponse coordonnée et adaptée pour faire face aux menaces cyber.

Dans un contexte d'exposition croissante des collectivités aux cyberattaques, le CDG29 et le GGD29 unissent leurs forces pour proposer une réponse coordonnée et adaptée.

Une convention, signée le 16 janvier 2024 à Quimper par M. Yohann Nédélec, président du CDG29, et le colonel Pierre-Yves Caniotti, commandant du GGD29, formalise cette coopération. Elle vise à offrir aux collectivités une offre globale, coordonnée et facilement accessible, tout en mutualisant les moyens pour garantir un service optimisé.

Prévention, sensibilisation, accompagnement : des actions concrètes au service des collectivités

Le CDG29 propose un accompagnement forfaitaire sur le long terme incluant sensibilisations, diagnostics de sécurité, et conseils pour sécuriser les outils numériques. Des ateliers pratiques comme l'accompagnement à la mise en place d'une charte informatique au sein de la collectivité, des ateliers de gestion de crise et d'aide à l'élaboration d'un plan de continuité d'activité (contexte, objectifs, risques) seront également proposés.

En 2024, plus de 500 agents ont été sensibilisés à la cybersécurité, sur des sujets comme la gestion des mots de passe et les risques de l'hameçonnage.

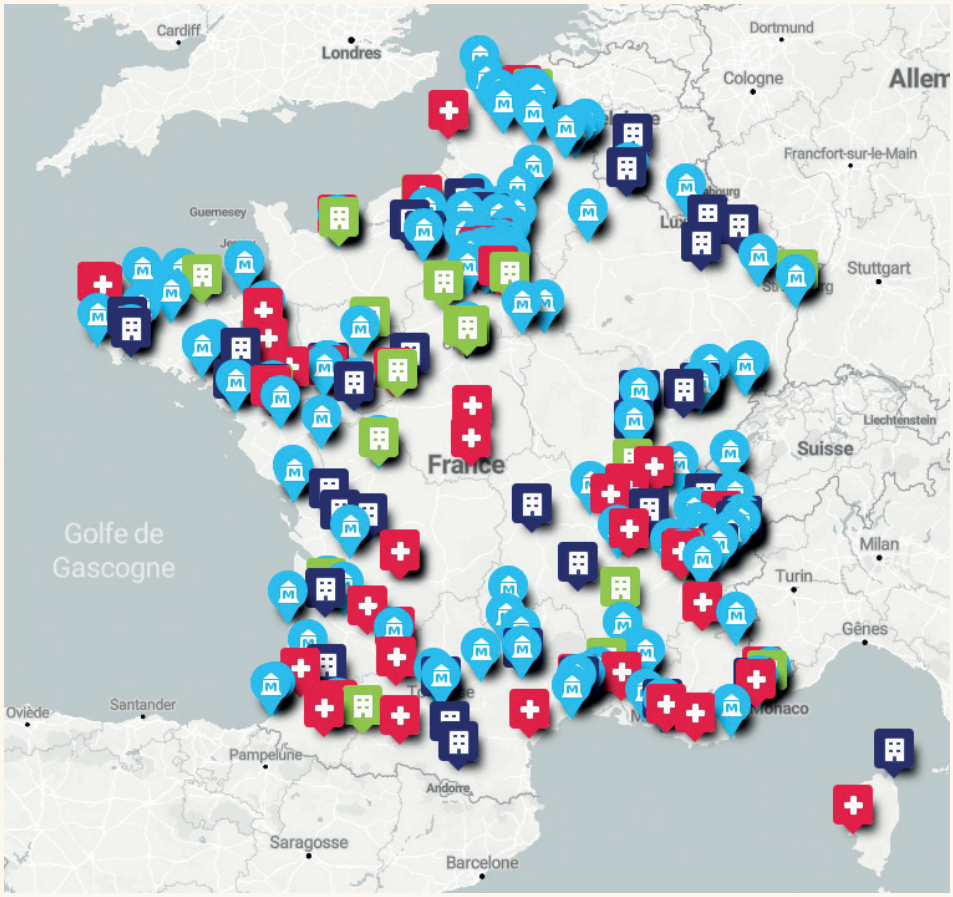
Dans le Finistère, la Gendarmerie Nationale a quant à elle mis en place plusieurs dispositifs gratuits :

- La proposition d'auto-évaluation destinée à tester la maturité de la collectivité en matière de cyber protection suivie d'un diagnostic plus précis réalisé in situ avec des cybergendarmes visant à dispenser des conseils aux élus et agents ;
- La participation des élus à des modules de sensibilisation animés par les militaires des sections opérationnelles de lutte contre les cybermenaces ou des référents sûreté. L'objectif est de leur proposer une mallette pédagogique, avec des outils simples pour se prémunir des risques de cyberattaque, mais aussi de partager entre élus les expériences et les bonnes pratiques.

e à la menace cyber

CENTRE DE GESTION FINISTÈRE

La cybersécurité, un enjeu pour les collectivités



© Openstreetmap et Association DECLIC.

Cyberattaques sur les organismes publics, depuis 2020.

NIS2, la directive européenne qui va impacter le paysage de la cybersécurité

Publiée en décembre 2022, la directive NIS2 vise à renforcer le niveau de cybersécurité des tissus économique et administratif des pays membres de l'Union Européenne. Elle s'appliquera désormais à des milliers d'entités importantes pour le quotidien des citoyens.

Chaque entité régulée devra ainsi fournir certaines informations à l'ANSSI, mettre en place des mesures adaptées de gestion des risques, et déclarer ses incidents de sécurité. En cas de manquement, des sanctions financières pourront être imposées. Les collectivités concernées doivent se mettre en conformité d'ici le 31 décembre 2027.

Ces mesures de protection ne sont pas forcément techniques. Elles peuvent être organisationnelles comme la mise en place d'une charte de bon usage des outils numériques (charte informatique) ou la mise en place de règles de sécurité à destination des prestataires.

Protéger les citoyens et les services publics

Protéger ses systèmes numériques est essentiel pour garantir d'une part la continuité des services publics et d'autres part la sécurité des données personnelles des citoyens. Après avoir désigné un référent cybersécurité au sein de la collectivité, l'AMF recommande d'évaluer d'abord les exigences en matière de sécurité numérique pour pouvoir ensuite dimensionner le budget à allouer (diagnostic).

De son côté, l'ANSSI recommande plusieurs mesures prioritaires :

- renforcer l'authentification sur les systèmes d'information (savoir gérer ses mots de passe) ;
- sauvegarder hors-ligne les données et les applications critiques (et réaliser des tests de restauration) ;
- établir une liste priorisée des services numériques critiques de l'entité (faire l'inventaire complet des outils numériques) ;
- s'assurer de l'existence d'un dispositif de gestion de crise adapté à une cyberattaque.

Or en 2024, peu de communes déclarent avoir renforcé leur politique cyber et 3 élus sur 10 estiment ne pas se sentir suffisamment protégés. Seulement 14 % estiment être suffisamment préparées en cas d'attaque et 1 collectivité sur 10 déclare avoir été confrontée à un incident de sécurité informatique. Si une prise de conscience collective commence à s'opérer, il reste encore beaucoup à faire pour atteindre un bon niveau de sécurité. La sécurité informatique est la responsabilité de tous, il est urgent que les collectivités se saisissent du sujet.

Pour en savoir plus, consultez le guide de l'AMF et de l'ANSSI : « Cybersécurité : toutes les communes et intercommunalités sont concernées » (novembre 2020).

Contactez-nous :
Les demandes d'intervention peuvent être adressées simultanément aux Centre de Gestion du Finistère et GGD29 par courriel :
- **protection.donnees@cdg29.bzh**
- **presansce-29@gendarmerie.interieur.gouv.fr**