RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

TÉMOIGNAGE D'UNE COLLECTIVITÉ ATTAQUÉE

En 2018, la commune de Kergrist-Moëlou subissait une cyberattaque. Comment cela s'est-il passé ? Comment les élus ont-ils fait face ? Quelles mesures ont été prises à l'issue de cet incident ?
Alain Cupcic, Maire de Kergrist-Moëlou partage son expérience avec nous.

POUVEZ-VOUS NOUS DIRE CE QU'IL S'EST PASSÉ ?

À l'époque je n'étais pas encore maire, mais j'étais très impliqué dans la vie communale comme conseiller technique, notamment sur l'aspect informatique. Travaillant chez un opérateur télécom, j'étais en effet amené à gérer les questions de sécurité.

La secrétaire de mairie m'a contacté le matin en arrivant, car son PC ne répondait plus comme avant. En fait, il était verrouillé et chaque tentative pour ouvrir un dossier était bloquée par un message de rançon qui demandait 500 euros pour récupérer les données de la commune.

Ces données verrouillées correspondaient en fait aux données personnelles des administrés, les délibérations de conseils et les comptes rendus, la vie du cimetière, de l'école, les notes de la secrétaire de mairie, bref sur une majorité de sujets et d'informations quelquefois confidentielles ayant trait à la vie de la commune et de ses habitants.

QUELS ONT ÉTÉ VOS PREMIERS RÉFLEXES ?

J'ai commencé par isoler le PC du réseau et plus particulièrement l'imprimante. Dans la mesure où je disposais de ces compétences réseau et sécurité, j'ai réussi à faire moi-même ce qu'il fallait pour remédier à l'incident sans faire appel à un prestataire spécialisé dans le domaine. Et enfin, j'ai appelé la gendarmerie pour savoir ce que je devais faire face à ce type d'attaque. Ils ont lancé une procédure et saisi le disque dur pour pouvoir investiguer.

POUVEZ-VOUS NOUS EXPLIQUER QUELS ONT ÉTÉ LES IMPACTS CONCRETS POUR LES AGENTS ET LES ADMINISTRÉS ?

- **La mairie est restée coupée du reste du monde** sans aucun lien avec l'extérieur, qu'il s'agisse des administrés, de la préfecture, des instances départementales, régionales, ou de toute administration qui ont l'habitude de communiquer avec nous par e-mail.
- Il n'y avait pas de sauvegardes, ce qui signifie **plus de mémoire ou plus d'accès possible aux dossiers archivés** (plus de plan de cimetière, plus de photos des événements de la commune…) ou même en cours !
- Sur un plan purement financier, **il a fallu racheter un PC neuf, un antivirus, des disques durs de sauvegarde, réactiver les licences professionnelles** et s'appuyer sur les services d'un prestataire.
- D'un point de vue humain, **ce genre d'incident n'est pas anodin et marque la vie d'un agent**. Même si elle était aux aguets et sensibilisée, notre secrétaire de mairie a éprouvé un sentiment de culpabilité et s'en est beaucoup voulu ; un mauvais clic a eu des conséquences désastreuses.
- **L'effet positif,** c'est que Valérie y pense encore de temps en temps !

Y A-T-IL EU UN AVANT ET UN APRÈS ?

Oui, cette attaque a fortement marqué les esprits. Depuis cette expérience, nous avons mis en place des règles de sécurité avec des consignes sur la nécessité de renforcer les mots de passe, de faire régulièrement des sauvegardes et les mises à jour, par exemple. Maintenant on est encore plus vigilant, et on regarde ensemble, si besoin, les e-mails qui semblent suspicieux.

UN DERNIER MOT À PARTAGER AVEC VOS PAIRS ?

Être prêt en amont, anticiper, cela peut arriver à n'importe quelle collectivité !

Rappeler les règles de sécurité régulièrement (RGPD*, dangers et obligations informatiques).

Si jamais cela arrive, ne bricolez pas tout seul, faites-vous accompagner par un prestataire de confiance ou allez sur Cybermalveillance.gouv.fr. Et surtout, n'hésitez pas à aller déposer plainte à la gendarmerie, ils sont là pour nous aider.

*RGPD : Règlement Général sur la Protection des Données

AMF
ASSOCIATION DES MAIRES DE FRANCE ET DES PRÉSIDENTS D'INTERCOMMUNALITÉ