RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

TÉMOIGNAGE D'UNE COLLECTIVITÉ ATTAQUÉE

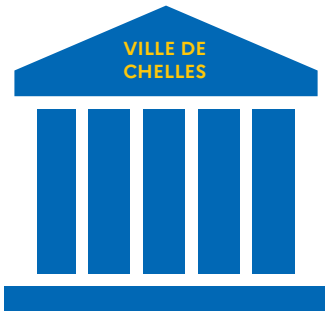
En janvier 2019, la ville de Chelles était cyberattaquée. **Retour sur cet incident avec Antoine Trillard, Directeur des Systèmes d'Information de la ville de Chelles.**

COMMENT AVEZ-VOUS DÉCOUVERT QUE VOUS VENIEZ DE SUBIR UNE ATTAQUE ?

L'attaque a eu lieu un vendredi midi. L'astreinte m'a appelé car il n'y avait plus accès aux logiciels sur 2 serveurs. Nous avons essayé de prendre la main sur le serveur en question mais tout était bloqué et inaccessible avec un écran figé demandant une rançon. Nous avons décidé d'éteindre le serveur et de vérifier si d'autres fichiers avaient été cryptés. Malheureusement, nous avons constaté que plus de 10000 fichiers sur 5 serveurs différents avaient été corrompus.

QUELS ONT ÉTÉ VOS PREMIERS RÉFLEXES ?

Nous avons vérifié que nos sauvegardes avaient fonctionné – ce qui était le cas – et nous avons décidé de restaurer le plus vite possible le système. Ainsi, dans les 3 heures qui ont suivi l'incident, nous avons pu repartir en mode dégradé. Après investigation, nous avons compris qu'un *phishing* avec un mauvais clic était à l'origine de l'attaque.



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

Cette attaque a dégradé les services de la ville une demi-journée et mis hors jeu une bonne partie du service de la police municipale ainsi que l'outil de délibération.

Cela a permis aux équipes IT de prendre conscience qu'ils n'étaient pas infaillibles et de réaliser qu'on a trop souvent tendance à oublier les fondamentaux comme les mises à jour et les sauvegardes. Ainsi, les priorités ont été recadrées et la sécurité est devenue un axe fort du schéma directeur de la collectivité.

Y A-T-IL EU UN AVANT ET UN APRÈS ?

Oui, et même si nous avons pu largement limiter les dégâts en restaurant la quasi-intégralité des services et documents grâce aux sauvegardes, les élus de la collectivité ont été sensibilisés par cette crise et ont compris que le système d'information est un outil de production qu'il est indispensable de sécuriser. Cela a permis de formaliser une feuille de route avec la sécurité comme axe fort du schéma directement intégré aux infrastructures et de dégager un budget dédié à la sécurité. Enfin, nous avons pu mettre en place une sensibilisation auprès des 1300 agents de la ville à l'issue de cette attaque.

QUELS CONSEILS PARTAGERIEZ-VOUS AVEC VOS PAIRS ?

Retour aux basiques avec deux priorités : faire les mises à jour de son/ses réseau(x), avoir des sauvegardes intouchables, sécuriser votre messagerie et votre Active Directory pour être serein car des attaques ont lieu tous les jours et de nouvelles failles sont découvertes régulièrement.

Et pour les plus petites collectivités qui n'ont pas de DSI en interne, se faire accompagner par un prestataire de confiance (labellisé ExpertCyber), opter pour des solutions clés en main managées sécurisant vos postes et votre messagerie et /ou mutualiser avec d'autres collectivités.

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