RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

TÉMOIGNAGE D'UNE COLLECTIVITÉ ATTAQUÉE

En juin 2021, la ville de Villepinte était touchée de plein fouet par une cyberattaque.
Retour sur cet incident avec Arnaud Hauwelle, Directeur de l'Innovation numérique et des systèmes d'information de la ville de Villepinte.

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

Nous avons été contactés en pleine nuit par notre Centre de Supervision Urbain (CSU). Il n'avait plus accès aux vidéos de la ville. Nous avons donc pris la main sur notre infrastructure pour effectuer les vérifications d'usure. Nous nous sommes alors rendu compte que le serveur dédié à la vidéo surveillance avait été cryptolocké.

QUELS ONT ÉTÉ VOS PREMIERS RÉFLEXES ?

Immédiatement nous avons pris la décision de couper les serveurs et d'isoler physiquement notre système d'information (SI). Puis nous nous sommes connectés sur Cybermalveillance.gouv.fr pour trouver de l'aide. La plateforme nous a proposé un diagnostic en ligne et d'entrer en relation avec un prestataire pour remédier au plus vite à la situation.

Et cela a été le cas : j'ai pu m'entretenir avec 2 prestataires qui m'ont répondu rapidement en m'apportant leurs conseils et j'ai pu les recevoir le lendemain matin.

Entre-temps, avec mes équipes, nous avons pu faire un état des lieux et établir que 40 serveurs qui géraient la quasi-totalité des services de la ville avaient été cryptolockés…

Ensuite, nous avons monté une cellule de crise avec le prestataire retenu afin de centraliser les informations, coordonner les actions, identifier les priorités. Lors de l'investigation nous avons découvert que l'attaque était en fait liée au facteur humain. En tapant 2 mots-clés, un agent a été aiguillé vers un site compromis, par lequel se sont introduits le ou les pirates.

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

Les services de la mairie étaient inaccessibles. La mairie a fait le choix de la transparence vis-à-vis de ses administrés et nous avons donc créé une boîte mail et des numéros de téléphone mobiles temporaires pour maintenir une continuité de service et rétablir un lien avec les concitoyens. Côté agents, cela a **largement modifié l'organisation du travail**, car nous n'y étions pas préparés et n'avions pas de procédure. L'attaque nous a tous contraints à réagir et à **nous adapter dans l'urgence pour gérer des services prioritaires** comme l'état civil, par exemple. Heureusement les salaires venaient d'être payés, et nous avons eu le temps de remonter le système d'information pour la paie de juillet. Mais **les agents sont revenus au papier et à la rédaction manuelle sur les registres**. Les populations les plus jeunes de nos agents n'avaient jamais été confrontées à ce type de process « papier ». Puis quand les logiciels ont refonctionné, **nous avons dû ressaisir toutes les informations pour les numériser**… Cela a considérablement **allongé le temps de traitement des demandes** même si nous n'avons finalement perdu « que » 2 jours de données, grâce aux sauvegardes protégées et fonctionnelles que nous avions.

Nous avons mis **plus de 2 mois à récupérer 70 % du système d'information** (messagerie, internet, logiciels d'inscription scolaire, etc.)

Y A-T-IL EU UN AVANT ET UN APRÈS ?

Oui indéniablement, nous avons eu la chance de bénéficier des Parcours de cybersécurité conçus par l'ANSSI* dans le cadre du plan France Relance et ainsi pu renforcer notre sécurité sur l'aspect technique en mettant en place un EDR (*Endpoint Detection & Response*) avec un SOC (*Security Operations Center*) et sur l'aspect humain développer des sensibilisations à nos 1 200 agents par de l'information régulière et l'organisation de campagnes de faux *phishing*.

UN DERNIER MOT À PARTAGER AVEC VOS PAIRS ?

Aucune collectivité ou même entité n'est à l'abri et le facteur humain est souvent responsable d'une intrusion, d'où la nécessité de sensibiliser tous les agents de façon régulière pour leur faire prendre conscience qu'ils sont acteurs de la sécurité.

Enfin, côté SI, ce sont les sauvegardes qui ont clairement permis de limiter les dégâts.

* Agence nationale de la sécurité des systèmes d'information

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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

TÉMOIGNAGE D'UNE COLLECTIVITÉ ATTAQUÉE

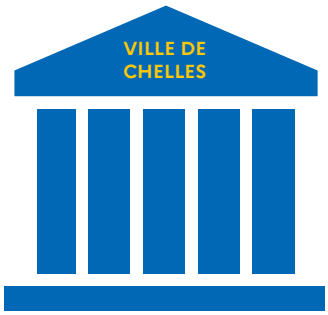
En janvier 2019, la ville de Chelles était cyberattaquée. **Retour sur cet incident avec Antoine Trillard, Directeur des Systèmes d'Information de la ville de Chelles.**

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

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