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