Cyberattaque Ville de Lille

1. Identification de l'incident :

- Qui a détecté l'incident et comment ?
  - L'incident a était détecté par l'ANSSI
- Temps de détection de l'incident après qu'il s'est produit ?
  - Incident découvert dans la nuit
- L'incident aurait-il pu être identifié en amont ?
  - Oui, en interne
- Est-ce qu'une technologie ou un outil aurait pu aider à détecter l'incident plus rapidement ou de manière préventive ?
  - la sonde Jizo

2. Flux d'informations et communication

- Dans quel délai les parties prenantes ont-elles été informées de l'incident ?
  - Mercredi matin
- Quel canal a été utilisé pour relayer les notifications ?
  - Communication à l'aide de leur site internet
    La presse
    Les conférences
- Toutes les parties prenantes ont-elles été rapidement mises au courant des dernières informations ?
  - Oui, information relayée très rapidement à l'aide d'un point presse dans l'après midi
- À quel point a-t-il été facile de communiquer avec le ou les utilisateurs finaux pour réunir des informations et les tenir informer sur le statut du ticket ?
  - Communication multicanale rendant l'accès à l'information aisé : presse, site internet, TV et réseaux sociaux

3. Structure

- A l'origine, comment était structurée l'équipe de réponse à l'incident ?
  - L'ANSSI : organisme externe
    La mairie de Lille : organisme interne
    La PJ : organisme externe
    CNIL : organisme externe
- L'adhésion à cette structure s'est-elle faite au cours du cycle de vie de la gestion de l'incident ? Si non, pourquoi ? Quels changements ont dû être apportés à la structure ?
  - Oui elle s'est faite pendant l'incident avec la PJ et l'expert
- L'équipe de gestion de l'incident peut-elle être mieux organisée ? Si oui, comment ?
  - Oui, En recrutant des profils spécialisés
- Utilisation des ressources : Quelles ressources ont été employé pour gérer l'incident ?
  - Les alertes de l'ANSSI
    Les moyens de communication
    Les investigations interne
    La collaboration avec la PJ
    la collaboration avec la CNIL
    Un expert privée
    Agent municipaux
    expert recommandé
    Les différents services informatique
- Ces ressources ont-elle été utilisées de façon optimale ?
  - Oui, et cela a servit à la continuité et à la remise en place des services dans le délais
- À quelle vitesse les ressources ont-elle été mobilisées pour gérer l'incident ?
  - Aucun délais
    Plan de continuité en place
- L'utilisation des ressources peut-elle être améliorée à l'avenir ?
  - Oui, grâce aux auto-évaluations Ebios RM

4. Processus

- Jusqu'à quel point le processus de gestion d'incidents défini a-t-il été suivi avec précision ?
  - Communiqués réguliers jusqu'en date du 30 mars 2023
    8 communiqués
    Revendication du groupe Royal le 27 Mars
- Y a-t-il eu des écarts dans le processus et le flux de travail de gestion d'incidents ?
  - Message de rançon
- Les SLA de l'incident ont-ils été respectés ? Si ce n'est pas le cas, quels SLA ont été violés ? Pourquoi ?
  - Le SLA était fixée à Jeudi
- Une surveillance adéquate du processus a-t-elle été observée pour gérer l'incident ?
  - Module ITIL V4 respecté
- Le processus peut-il être amélioré pour le rendre plus efficace ? Si oui, comment ?
  - Système de sécurité de mail
    Filtre mail indésirable
    Hoshi
    Snort

5. Création de rapports

- Des rapports ont-ils été générés pour analyser la façon dont l'incident a été géré ?
  - Un diagnostic technique à était mis en place
- Quels paramètres étaient inclus dans le rapport ?
  - L'origine et la gravité de l'intrusion
- Quelles parties du cycle de vie de l'incident ont été analysé ?
  - Les étapes 1 à 7
- Y a-t-il une marge d'amélioration ? Si oui, comment peut-elle être réalisée ?
  - En exportant les tableaux d'analyse à l'aide des solutions Sesame IT