CYBER INCIDENT RESPONSE

RIJSEL

Historique des modifications

Version	Objet de la modification	Statut
05/09/2023	Incident response	En cours
06/09/2023	Ajout d'informations de la page 12 à la fin du document	En cours
06/09/2023	Edition du document	Réalisé

Public visé

Développeur	**Administrateur**	**RSSI**	**DSI**	Utilisateur

TABLE DES MATIERES

Identification de l'incident :

Qui a détecté l'incident et comment ?

L'incident a été détecté par l'ANSSI.

Nous ne sommes pas en mesure de donner de plus amples détails sur

Combien de temps a-t-il fallu pour détecter l'incident après qu'il s'est produit ?

L'incident a été découvert dans la nuit.

L'incident aurait-il pu être identifié plus tôt ?

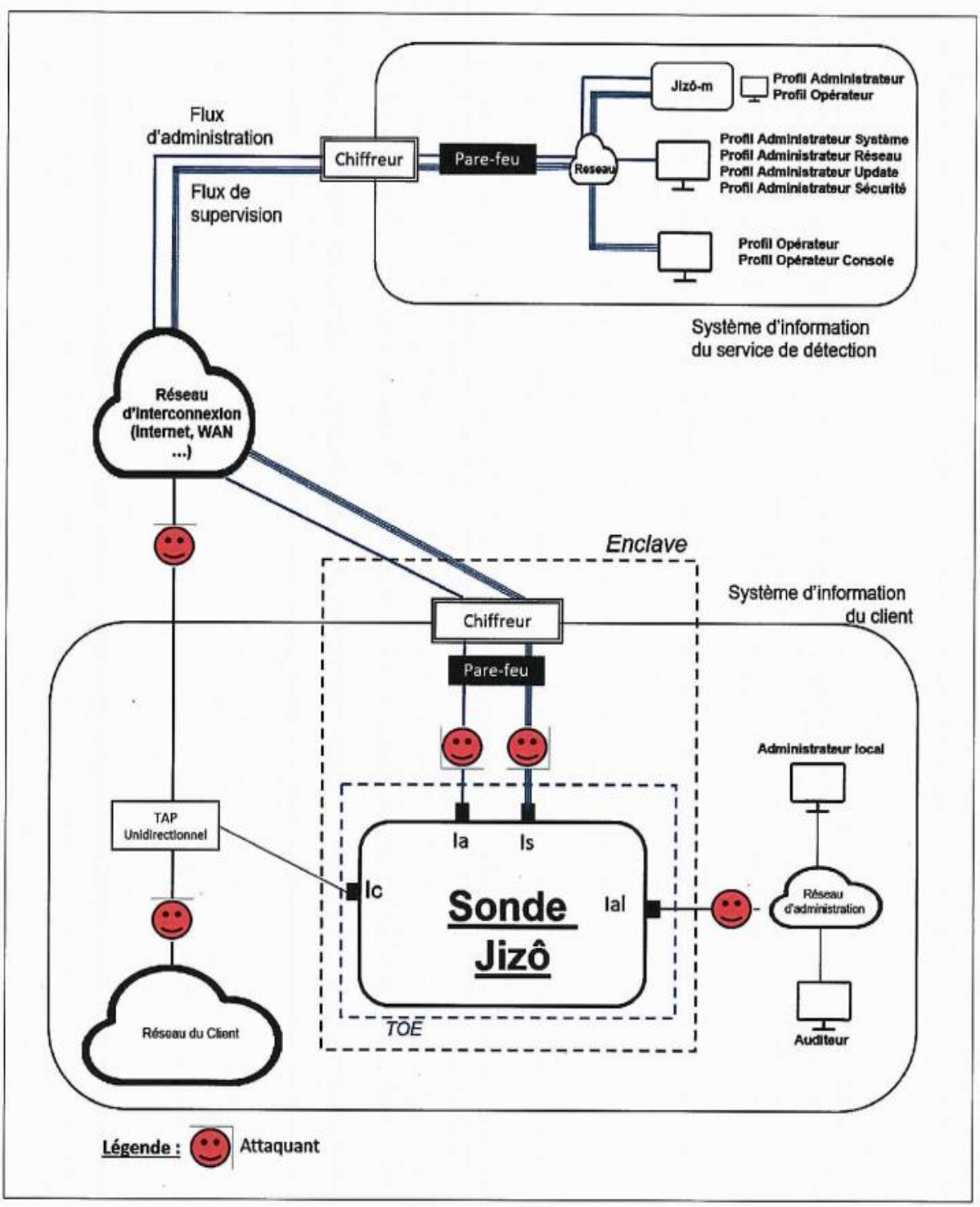
Oui, c'est possible car il existe de nouvelles solutions qui permettent d

Est-ce qu'une technologie ou un outil aurait-il pu aider à détecter l'incident plus rapidement ou de manière préventive ?

Oui, des solutions de détection préventive permettent de réduire le délai de réponse à intrusions.

La sonde de détection JIZÔ de la société SESAME IT est recommandée par l'ANSSI et possède un visa de sécurité délivré par le service de qualification des produits et services de l'ANSSI.

Schéma de la sonde de détection JIZÔ :



Flux d'informations et communication :

Dans quel délai les parties prenantes ont-elles été informées de l'incident ?

L'incident ayant été détecté dans la nuit entre le Mardi 28 Février 2023 et le Mercredi 01 Mars 2023. « La ville de Lille assure n'avoir reçu aucun message en lien avec l'intrusion et n'avoir aucune idée de son origine » (cf. La Voix du Nord / Lien : https://www.lavoixdunord.fr/1297134/article/2023-03-01/la-mairie-de-lille-victime-d-une-cyberattaque-des-services-perturbes).

Le délai n'est pas connu, cependant, l'ANSSI a prévenu aussi vite que possible le service informatique de la ville de Lille.

L'incident a été vérifié par les équipes de la ville de Lille et la mise au jour d'un risque potentiel a été confirmé le Mercredi 01 Mars 2023.

Quel canal a été utilisé pour relayer les notifications ?

Plusieurs canaux de communication ont été utilisés pour informer les citoyens, les utilisateurs des services municipaux, mais aussi les journalistes afin d'informer de manière claire et concise les relais d'informations.

Toutes les parties prenantes concernées ont-elles été rapidement mises au courant des dernières informations ?

Un point presse a été organisé dès le Mercredi matin et a eu lieu dans l'après-midi. La première adjointe Audrey Linkendheld.

Les utilisateurs ont été informés dès que possible via plusieurs canaux de communication.

La Police Judiciaire a été alertée pour enquêter sur la cyberattaque.

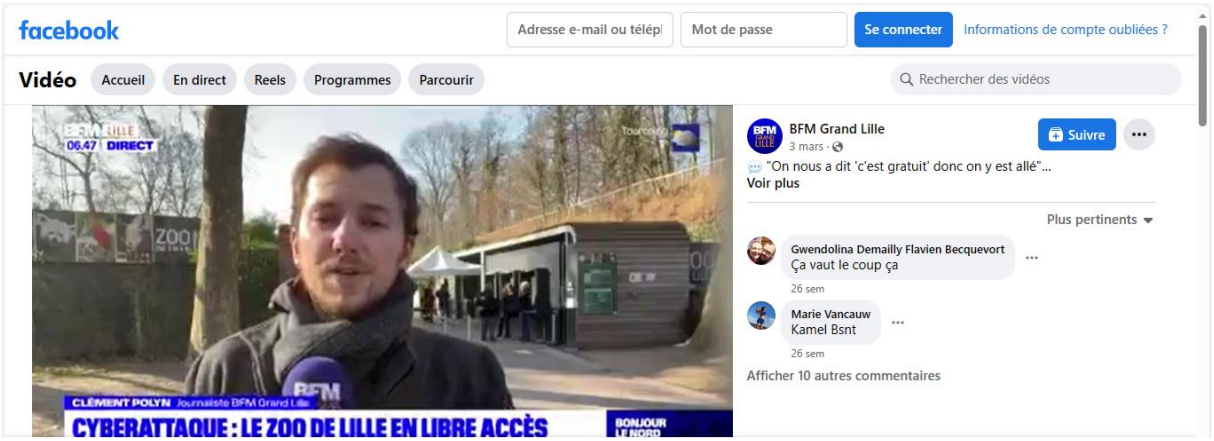
À quel point a-t-il été facile de communiquer avec le ou les utilisateurs finaux pour réunir des informations et les tenir informer sur le statut du ticket ?

Pour les employés de la ville de Lille : des affiches

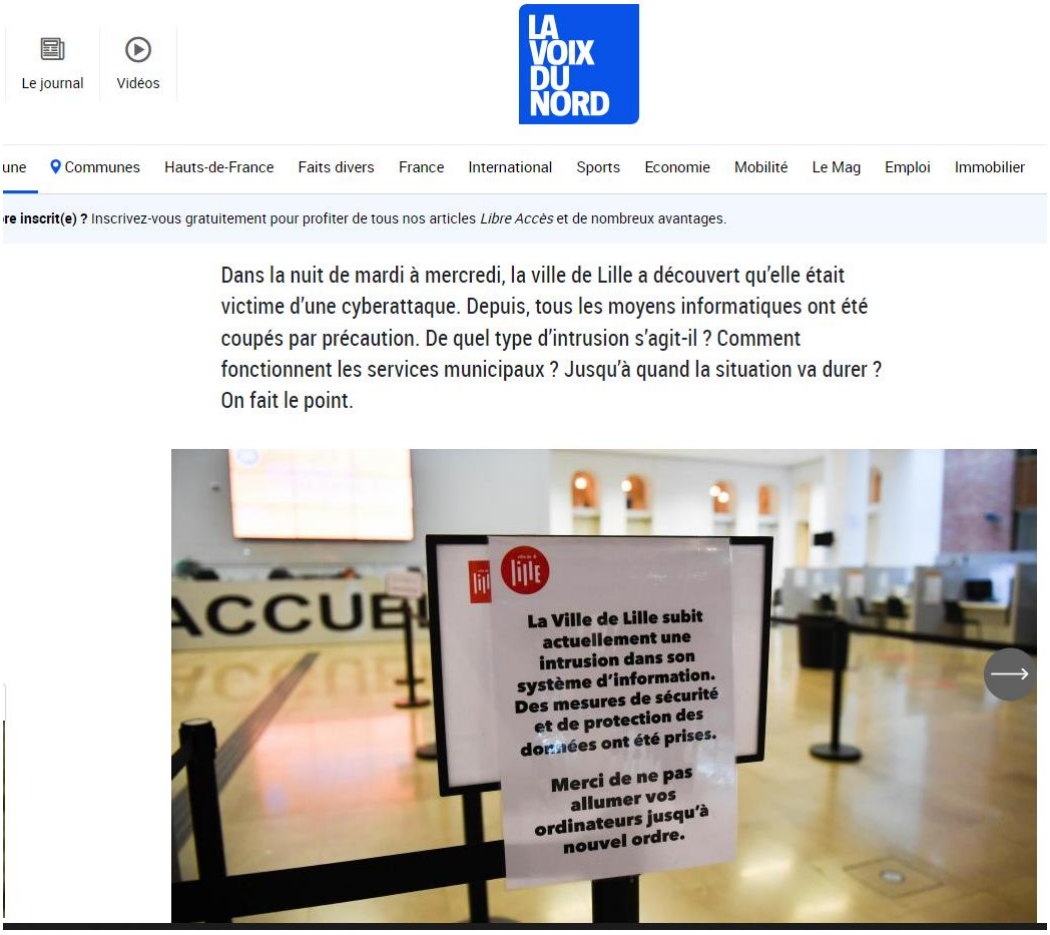
Pour les utilisateurs citoyens des services municipaux : BFM, post sur réseaux sociaux, affiches, site web. Les lignes téléphoniques ont été coupées dans un premier temps, le maximum de relais d'information possible a été utilisé.

➢ Communiqué « Réseaux sociaux » :

➢ Communiqué «TV» :



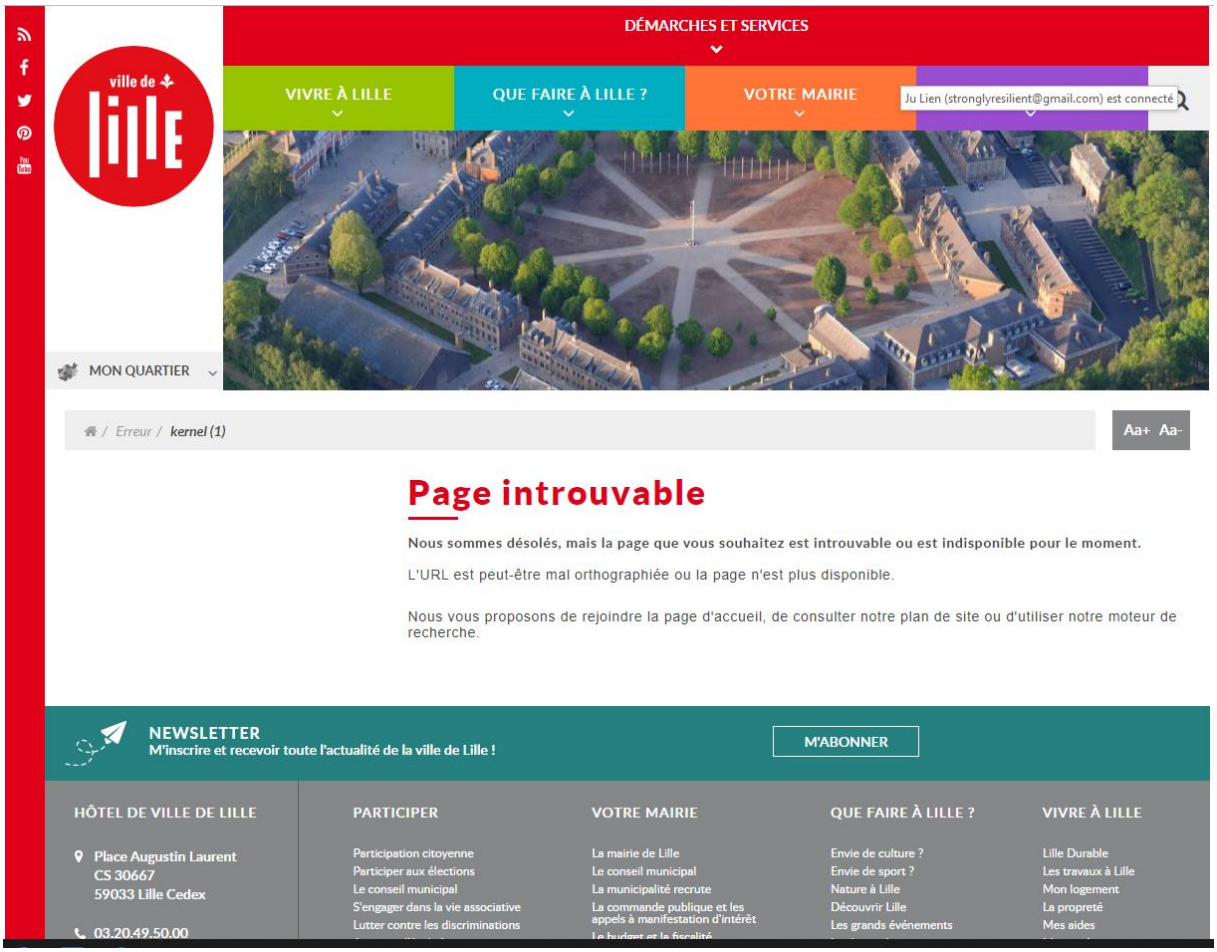
➢ <u>Communiqué Presse Journaux :</u>



➢ Communiqué Point Presse :

Lors d'un point presse, la ville de Lille a précisé que le diagnostic technique lié à la cyberattaque découverte dans la nuit de mardi à mercredi était toujours en cours. - PHOTO HELENE DECAESTECKER - LA VOIX DU NORD - VDNPQR

➢ Communiqué Site web :

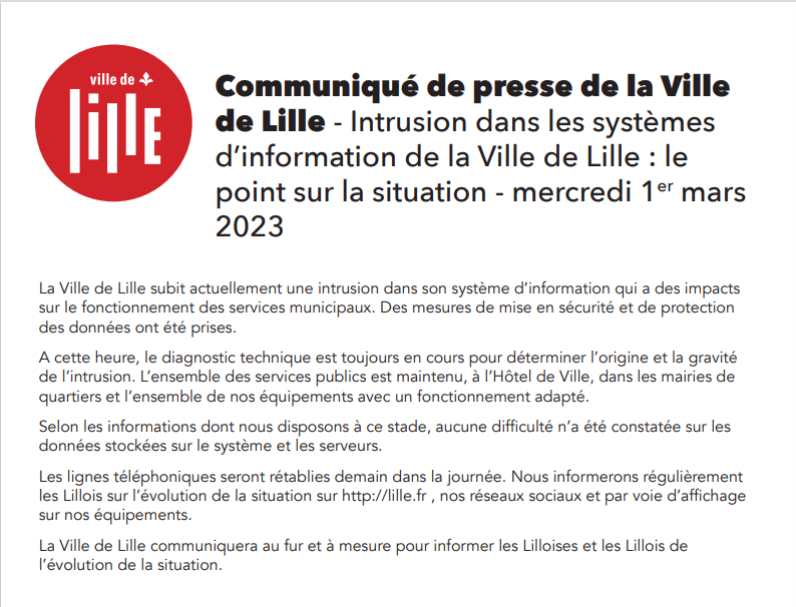


- Communiqués par affiches en Mairie :

À l'entrée de la mairie, des affiches préviennent les agents et les usagers. PHOTO HELENE DECAESTECKER - LA VOIX DU NORD - VDNPQR

À l'entrée de la mairie, des affiches préviennent les agents et les usagers. PHOTO HELENE DECAESTECKER - LA VOIX DU NORD - VDNPQR

➢ Communiqués de Presse officiels de la Ville de Lille :



Communiqué de presse de la Ville de Lille - Intrusion dans les systèmes d'information de la Ville de Lille : le point sur la situation - mercredi 1er mars 2023

La Ville de Lille subit actuellement une intrusion dans son système d'information qui a des impacts sur le fonctionnement des services municipaux. Des mesures de mise en sécurité et de protection des données ont été prises.

A cette heure, le diagnostic technique est toujours en cours pour déterminer l'origine et la gravité de l'intrusion. L'ensemble des services publics est maintenu, à l'Hôtel de Ville, dans les mairies de quartiers et l'ensemble de nos équipements avec un fonctionnement adapté.

Selon les informations dont nous disposons à ce stade, aucune difficulté n'a été constatée sur les données stockées sur le système et les serveurs.

Les lignes téléphoniques seront rétablies demain dans la journée. Nous informerons régulièrement les Lillois sur l'évolution de la situation sur http://lille.fr , nos réseaux sociaux et par voie d'affichage sur nos équipements.

La Ville de Lille communiquera au fur et à mesure pour informer les Lilloises et les Lillois de l'évolution de la situation.

Structure

Comment était structurée l'équipe de réponse à l'incident à l'origine ?

- ANSSI
- Equipes SI de la Ville de Lille
- Service Communication de la Ville de Lille
- Elus municipaux de la Ville de Lille
- Elus municipaux des communes voisines (Hellemmes, Lomme)
- Police Judiciaire
- Experts recommandés par l'Etat
- Experts de la Ville de Lille
- CNIL
- Expert privé 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 ?

Cette structure s'est composée au cours du cycle de vie de la gestion de l'incident.

Le caractère exceptionnel de l'incident a nécessité le recours à différents experts internes et externes à la Ville de Lille.

L'intervention d'experts pourrait avoir impliquer des métiers comme ceux précisés ci-dessous :

- Expert sécurité logiciels
- Expert en sécurisation des technologies Microsoft
- Expert en cryptographie
- Expert en protocoles de communications sécurisées
- Chargé de mission en management des risques cyber
- Expert réseaux et télécoms
- Expert en sécurité matérielle
- Ingénieur détection d'intrusions

L'équipe de gestion de l'incident peut-elle être mieux organisée ? Si oui, comment ?

La Ville de Lille pourrait soit recruter soit faire appel de manière ponctuelle et/ou récurrente à des profils spécialisés dans différents domaines, comme par exemple :

- Ingénieur en traitement des données de détection
- Analyste sécurité expert – Veille en vulnérabilités
- Ingénieur systèmes et réseaux d'exploitation – administrateur
- Pilote technique spécialise en traitement d'incidents informatiques
- Expert en résilience et management des crises cyber
- Auditeur de sécurité technique
- Auditeur de sécurité organisationnelle

Utilisation des ressources

Quelles ressources ont été employées pour gérer l'incident ?

- Les alertes de l'ANSSI
- Les différents canaux de communication
- Les élus municipaux
- Les agents municipaux
- Les investigations internes
- La collaboration avec la Police Judiciaire
- La collaboration avec la CNIL
- Les experts recommandés par l'Etat
- Le service informatique de Lille
- L'ensemble de l'infrastructure informatique de la Ville de Lille
- La plateforme d'accueil téléphonique de l'Hôtel de Ville

- Centre opérationnel de la Police municipale
-

Ces ressources ont-elles été utilisées de façon optimale ?

Oui, cela a servi à la continuité des services utiles aux Lilloises et Lillois. Un Plan de Continuité d'Activité a donc été activé dès le premier jour. Tous les équipements sont restés ouverts : Hôtel de Ville, Mairies de quartier, parcs et jardins, crèches et établissements scolaires, sportifs, culturels, cimetières, etc.

Un plan de sécurisation a été déclenché : les serveurs et les postes clients ont été éteints. Par précaution, les messagerie des agents municipaux ont été désactivées.

La remise en fonction opérationnelle s'est effectuée par palier afin d'assurer la non-propagation de tout risque informatique.

À quelle vitesse les ressources ont-elles été mobilisées pour gérer l'incident ?

Aucun détail à ce sujet n'a été communiqué par la Ville de Lille.

Le Plan de Continuité d'Activité a été déclenché dans un délai très court sans nul doute après l'alerte de l'ANSSI.

Le Plan de Reprise d'Activité a été déclenché aussi en parallèle.

L'utilisation des ressources peut-elle être améliorée à l'avenir ?

L'utilisation de l'outil d'autoévaluation de gestion de crise cyber pourrait s'avérer très utile pour mieux se préparer.

Publication d'un outil d'autoévaluation de gestion de crise cyber | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

La méthode d'audit EBIOS RISK MANAGER est aussi une possibilité.

Processus

Jusqu'à quel point le processus de gestion d'incidents défini a-t-il été suivi avec précision ?

Huit communiqués de presse ont été publiés entre le 01 Mars et le 30 Mars 2023.

Ne connaissant pas le détail du processus de gestion d'incidents, il nous est difficile de répondre précisément à cette question.

Le résultat des investigations ne sont pas connues.

La revendication de la cyber attaque a été faite par le Groupe « Royal » et publiée par la Ville de Lille et La Voix Du Nord le 27 Mars 2023.

Y a-t-il eu des écarts dans le processus et le flux de travail de gestion d'incidents ?

Un élément perturbateur est venu modifier la gestion et la réponse à cette crise cyber. Des emails de demande de rançons ont été reçus par quatre agents de la Ville de Lille.

Cette situation a été immédiatement signalée à l'ANSSI, la CNIL et la Police judiciaire.

Un rappel des bonnes pratiques a été communiqué à tous les agents possédant une messagerie internet personnelle.

Les SLA de l'incident ont-ils été respectés ? Si ce n'est pas le cas, quels SLA ont été violés ? Pourquoi ?

La résilience de la Ville de Lille a permis d'assurer les services utiles et publics critiques et essentiels aux Lilloises et Lillois.

L'objectif était fixé au Jeudi 02 Mars après-midi. Ce qui a été respecté.

Un SLA de moins de 48 heures était prévu, voire de 36 heures.

Une surveillance adéquate du processus a-t-elle été observée pour gérer l'incident ?

Au vu du nombre de communiqués, et des informations que nous avons trouvées, nous constatons que le processus pour gérer l'incident prends soin d'étudier le modèle à quatre dimensions mentionnées dans le référentiel ITIL V4.

Les organisations et individus, l'information et la technologie, les partenaires et fournisseurs, le flux de valeur et les processus, sont à chaque communiqué présents, donc ont été étudiés et respectés à la lettre par les équipes de réponse à incident et de gestion de crise cyber.

Le processus peut-il être amélioré pour le rendre plus efficace ? Si oui, comment ?

Les courriels de demande de rançons sont venus perturber le processus de gestion de l'incident.

Notre avis serait d'étudier une solution de filtrage renforcé des courriels comme « SNORT ». C'est une solution open source Linux.

La sonde détection JIZÔ préconisée précédemment peut être combinée à la solution HOSHI.

Il s'agit d'un logiciel permettant de bénéficier des dernières innovations en matière de scénarios d'attaques cyber issus de la recherche en vulnérabilités informatiques et de l'Industrie. Ces scenarios combinés à la sonde de détection JIZÔ apportent un atout majeur dans la réponse à incident et la gestion de crise cyber.

Création de rapports

Des rapports ont-ils été générés pour analyser la façon dont l'incident a été géré ?

Un diagnostique de sécurité technique a été mis en place et communiqué le 1er Mars 2023.

Quels paramètres étaient inclus dans le rapport ?

L'origine et la gravité de l'intrusion (cf. Communiqué du 1er Mars 2023).

Quelles parties du cycle de vie de l'incident ont été analysées ?

Les étapes de 1 à 7 ont été analysées à savoir :

- Etape 1 : Enregistrement de l'incident
- Etape 2 : Catégorisation de l'incident
- Etape 3 : Hiérarchisation de l'incident
- Etape 4 : Affectation de l'incident
- Etape 5 : Création et gestion d'une tâche
- Etape 6 : Gestion du SLA et réaffectation
- Etape 7 : Résolution de l'incident

Y a-t-il une marge d'amélioration ? Si oui, comment peut-elle être réalisée ?

Outre un durcissement de la détection d'intrusions, les solutions de SESAME IT permettent l'édition de tableaux de bord et de rapports pouvant aider à s'améliorer dans la création, la planification, l'organisation, la réalisation et la gestion d'exercices de crise cyber.