Note de synthèse et de propositions option systèmes d'information et de communication :

Partie synthèse

Note à l'attention de Mme La Maire Présidente
de Mme/M. le/la directeur/trice de Cabinet

Le week-end dernier la collectivité a été victime d'une attaque informatique de type rançongiciel. Cette attaque impacte l'ensemble des services de la collectivité.
Dans cette note vous trouverez un point de situation et quelques éléments de langage pour la communication externe.

1) Points de situation

a) Opérationnel

D'un point de vue opérationnel, tous les outils informatiques sont à l'arrêt à l'exception des outils de la Smart City, info gérée dans une bulle étanche du périmètre impacté. Les arrêts impactent aussi tous les processus du service public délivrés pour les agents tant les procédures sont aujourd'hui fortement soutenues par l'informatique.

L'arrêt est une mesure de mise en sécurité des systèmes sur la base des constats préliminaires. L'ensemble des services à la population (Etat-Civil, Passeport-identité, Recensement, Sécurité Publique, Sports et Loisirs, bibliothèques, musées, éducation, jeunesse), les services techniques, les espaces verts, environnement-déchet, cycle de l'eau et transports) à l'exception de l'urbanisme sont concernés par l'attaque.
Les fonctions supports (finances, conseil de gestion, parcs, patrimoine, Rh-santé) sont affectés, la messagerie et autres outils collaboratifs (dont l'ensemble des fichiers partagés sont contaminés.
Le SI du CIAS doit encore faire l'objet de mesure d'audit.
Un diagnostic prioritaire sera également à conduire sur la zone de médiation et paiement.
Les autres briques ont été arrêtés à titre préventif et devraient pouvoir être relancés dès que possible en particulier le téléservice.

L'ensemble des personnels de la DNSI est mobilisé sur l'analyse de la situation et la définition du plan de restauration des services.
L'agence Nationale de la sécurité des systèmes d'information nous accompagne également en expertise et conseils.

Concernant les ordinateurs de bureau environ 80% ont été contaminés et devront faire l'objet d'interventions manuelles unitaires ou être remplacés à l'instar de ce que la ville de Bondy (1600 agents) a choisi de faire fin 2020/courant 2021.

b) Organisationnel

Comme évoqué supra, les équipes de la DNSI sont entièrement mobilisées. Ainsi les équipes projet seront recentrées sur la restauration des solutions informatiques de leurs portefeuilles.
Il ne s'agit pas d'une restauration minimaliste en retour à l'existant mais d'une réflexion à lancer et un juste équilibre à trouver entre le délai de retour du service et le niveau de cyber sécurité de l'infrastructure en cible y compris les options et hébergements Cloud en capitalisant sur l'expérience des 2 collègues en charge de la sécurité Smart City.
Le retour à la normale pourra s'avérer long malheureusement. L'exemple de Bondy s'étire de novembre 2020 jusque fin 2022 /début 2023 soit un peu plus de 2 années.

Se faisant, il convient d'aborder dans les services une organisation aux processus et procédure adaptées à l'absence des outils informatiques pour assurer une continuité minimale des services publics. Il faudra apprendre à travailler autrement comme le montre le retour d'expérience de Lille au printemps 2023.
Nous allons engager prioritairement la restauration du service de messagerie pour réduire au maximum la rupture de ce canal majeur de communication tant entre les usagers et la collectivité qu'au sein même de la collectivité, entre ses agents et élus.

c) Juridique

En concertation à l'ANSSI, il convient de mobiliser les services juridiques au regard de la médiane des rançons demandées.
De l'ordre de 6375 € en 2020, le montant exact n'est pas connu nous concernant et la garantie de déblocage n'est pas assurée. Mais sur cette ordre d'idée et pour peu que notre contrat d'assurance couvre ce risque de cyber attaque, cette option n'est pas à exclure.

Plus largement et dans le prolongement de ses investigations actuelles nous devrons

- Sur le volet rançongiciel constaté, nous conformer davantage au Référentiel général de sécurité (RGS) édicté en 2010 et révisé en 2014.
- Sur les autres risques non constatés à ce jour tel que le vol de données (constaté en effet retard à Lille) personnelles, le SI RH-santé en particulier, un autre processus d'alerte sera à mettre en œuvre.
- Enfin, sur la notion de services publics « essentiels », il nous faudra évaluer l'impact de la directive européenne de 2016 dans son périmètre et son application aux EPCI et autres collectivités.

d) Financeurs

Outre la rançon évoquée supra, les impacts financiers en retour d'expérience de Bondy (1600 agents), 1,5 M€ pourraient être de l'ordre de 3 à 4 M€.
La baisse de production de services publics varie de 4 mois (Caen 2022/09) à 2 ans (Bondy).

e) Politique

Les attendus des citoyens et usagers en matière de cyber-sécurité en plus généralement de télé services « public » sont de 3 ordres conformément aux objectifs de la réglementation.

1. Renforcer la confiance des usagers dans les services numériques
2. Garantir la protection des données personnelles
3. Renforcer la sécurité des activités d'importances vitales et services essentiels au titre de la continuité du service public

Il apparaît clairement que, politiquement parlant, la collectivité est en défaut au moins sur les points 1 et 3, le 2 restant à infirmer.
Ainsi, la réputation de la collectivité est fortement altérée et il convient de travailler en transparence notre situation dans un contexte et une démarche, une dynamique de résilience face à cette attaque.

II) Les éléments de langage

a) Transparence

La collectivité (ville centre et EPCI) a été victime d'une cyber-attaque le week-end passé de type rançongiciel.
Les services ont réagi rapidement pour endiguer l'attaque. Malgré cela 80% des services sont infectés et le reste est arrêté par mesure de prévention.
L'ANSSI accompagne la collectivité sur l'évaluation des impacts, les méthodes de rétablissement des services.
Les services restent ouverts à l'accueil du public mais les procédures seront fortement impactées et ralenties.

b) Contexte

Cette attaque s'inscrit dans une longue liste d'attaques ayant visées des services publics : Lille en 2023-02, Caen en 2022-09, Bondy 2020-11, CHU Rouen 2019.
En XXX les attaques de ce type ont été multipliées par 3,5 en 2019-2021, 30% des collectivités ont été victimes d'un rançongiciel selon une étude de Clusif en date de 2020-06.
Mais ce contexte, nous oblige non à la fatalité mais à l'opportunité de restaurer les services en augmentant la résilience de la structure technique sous-jacente.

c) Dynamique résiliente et durable

La démarche de restauration s'inscrit en un équilibre entre la disponibilité rapide du service rétabli et la robustesse renouvelée au regard des normes et référentiels actuels, des règles de l'art en matière de gestion, de solutions informatiques en particulier l'informatique en image (« Cloud »).
Un chantier déjà lancé en amont se voit en opportunité partir en axe majeur de la dynamique : la sobriété numérique (green IT). Objectif : en profiter pour réduire la consommation énergétique liée au numérique en ramenant la croissance annuelle de 9% à 1,5% comme le suggère le « Shift Project ».

Sur ces éléments complets en point de situation du jour et en perspectives, vous serez informée en temps continu et en tant que de besoin sur la suite de la résolution de cet incident majeur.

Partie Note de Proposition

Note à l'attention du Directeur Général

Depuis samedi, les équipes de la DNSI sont présentées pour contenir les conséquences de la cyber-attaque par rançongiciel dont a été victime la collectivité. Vous trouverez dans cette note les modalités d'organisation mises en œuvre en gestion de la crise (courts termes) et au-delà (moyens termes), le plan d'actions pour la reprise d'activité (1), pour la gestion des acteurs et agents (2), pour la gestion du risque cyber sécurité (3).
Enfin, profitant de cette opportunité, s'il est possible de la considérer comme telle, l'ambition d'un rétablissement vertueux, inscrit dans une démarche durable, sera présentée.

I) Organisation

a) Les acteurs

Les agents de la DNSI sont les principaux acteurs du rétablissement technique des SI. Ce dernier point est la priorité absolue tous projets cessant.
Un binômage sera mis en place entre les chefs de projet selon leur porte-feuille applicatif et les ingénieurs et techniciens système/sécurité de réseaux pour évaluer les impacts sur les dossiers et les systèmes, évaluer la qualité et périmètres de sauvegarde disponibles ainsi que le niveau cyber de restauration et rénovation des services applicatifs.
Cette dernière étape ne se fera que sous la validation du RSSI.

La cellule achats et logistique en relation avec les collègues de la direction des finances étudie les modalités et le financement des :

- PC portables neufs (sains) en avance de renouvellement et en retour d'expérience des collectivités ayant subi ce type d'attaque
- L'ouverture d'un marché à commande à destination des entreprises de services numériques (ESNI) pour dédoubler nos capacités d'intervention sur deux domaines cibles Messagerie et PC

Une task force a été mise en place. Elle est composée du RSSI des chefs des services Achats et Logistique, Systèmes, Projets, Sécurité et Réseaux et Support aux utilisateurs. Je préside cette instance et un compte-rendu vous informera ainsi que tous les directeurs et le Cabinet en temps continu.

Les agents hors DSSI se doivent d'être accompagnés dans les changements des procédures faute d'outils informatiques. Un groupe de travail est en cours de création en concertation avec la DS, la DRH et la DNSI.

Les relais informatiques sont également impliqués dans la vigilance à maintenir durant la période de crise.

La gestion singulière du CIAS appelle à un traitement différencié qui sera pris en charge par une ESN dédiée tant ils ne semblent pas a priori impactés et compte-tenu de leur autonomie organisationnelle.

Les autres directeurs métiers seraient appelés et sollicités en priorisation des restaurations dans leurs périmètres respectifs.

Enfin le DPO délégué à la protection des données sera par nature particulièrement concerné par l'investigation en cours sur les éventuels vols de données.

b) La comitologie

La task force se réunit tous les jours jusqu'au rétablissement de la messagerie et outil collaboratif. Ensuite à minima 2 fois par semaine.

Un comité cyber sera créé à l'issue avec une rencontre trimestrielle sous le même format que la task force auquel s'ajoutera le responsable de service des données ouverture.

La démarche Green IT ou sobriété numérique fera l'objet d'une note ultérieure une fois la démarche validée.

II) Le plan d'action

1) Volets techniques

Faute de Plan de Reprise d'Activité (PRA) prédéfini, il nous appartient de le définir à chaud. C'est-à-dire qu'il faut arbitrer l'ordre de rétablissement des services pour prioriser les effets des agents de la DNSI.

a) A court termes, il faut lister les applications anticipées de rang 1

- A minima et sous validation, la messagerie, les SIRH et finances seront dans le 1er train
- Les PC neufs fraichement acquis serviront à doter les agents de ses mêmes services
- Pour les autres SI, les Directeurs seront sollicités avec un arbitrage en soutenabilité par la DG
- L'ESN sera mobilisé pour le nettoyage de 80% de PC infectés avec un risque fort de perte total des données
- Le DPO, le RSSI appuyés par l'ANSSI devront rapidement évaluer le risque de vol de données, risque qui expose fortement la collectivité.

b) A moyens termes, au regard de la robustesse de la partie du SI en cloud, les outils de « Smart City », il convient d'étudier à minima le transfert de la messagerie et des fichiers partagés en service Saas de type M365.
En retour d'expérience, il nous appartient de comprendre les défauts de notre architecture qui ont causés cet effet domino sur l'ensemble du SI. Une architecture, au plus, en isolement des briques est à reconstruire en Saas XX en On Premises

- Failles majeures et non corrigées
- Faibles diversités de nos plateformes
- Défaut de gestion ou d'administration
- Malveillance

Autant de causes qu'il faudra analyser et corriger

2) Volets services publics

S'il est possible de justifier à fermeture des SP sur quelques jours, la situation doit conduire à adapter les processus et procédure en mode très dégradé

a. A CT faute de PRA ou de Plan de Continuité d'activité (PCA) il appartient à chaque directeur métier d'y travailler en fonction du planning prévisionnel de restauration applicative.

Le partage de ce PCA ad hoc et sa cohérence globale doit faire l'objet de travaux en partage DG.

b. A moyens termes, nous devrons poser la méthode de construction concertée de PRA/PCA avec les mises en œuvres, sectorielle, d'exercice à l'image des exercices demandées.

3) Volet cyber sécurité

Cette partie du plan adresse le CT/MT : pour évaluer les compétences en matière de cyber sécurité tant pour augmenter en volume celles-ci (recrutement) qu'en qualité (formation) en concertation avec la DRH.
Un choix en GPEEC sera à opérer entre la formation parfois contenue des ingénieurs sécurités sur un marché de l'emploi très concurrentiel sur le secteur et la délégation de gestion en cloud.

Outre les compétences des agents de la DNSSI c'est bien tous les agents de la collectivité qu'il convient de former à la cyber sécurité dans un grand plan de format triennal renouvelable.

Nous devrons inscrire la collectivité dans une démarche d'audit régulier pour s'assurer que le maillon faible ne puisse emporter toute la collectivité.

III) Sobriété numérique

3 axes de travail sont proposés :

1) La consommation énergétique

a) Les postes de travail

Pour les nouveaux matériels, l'énergie de fonctionnement est moins élevée. Un renouvellement des plus vieux PC est envisagé.
Reste que 80% de l'énergie nécessaire au PC relève de sa fabrication.

Ainsi, une réflexion sur les produits en date peut être lamée avec un smartphone plutôt qu'un PC.

b) Les serveurs et e-free

Pour la gestion des serveurs, clairement la bascule en cloud augmente le ratio efficacité / usage tant il tend vers 1 pour les meilleurs data center et qui même s'il reste à quantifier pour nous, oscille sans doute entre 5 et 6.
Cette logique cloud opère un transfert budgétaire des RH + fluide vers les prestations de service cloud.

c) Les achats

La clause des RSE seront à mesurer dans les DCE/CCTP

d) Les usages des numériques

Ici le gros des efforts est à porter

Les mails :

- en volume envoyés et la taille des PJ ➔ bascule en GED
- en historique de conservation

Les documents :

- poids (vidées, photos)
- en doublons
- en historique faute d'archivage

Les contenus web :

Consultation vidéo par les agents
Communication de la collectivité par les usagers

S'il est possible d'optimiser l'impact environnemental sur les couches techniques et nous le ferons, le gros de la complexité de la sobriété numérique restera sur les usagers. Sauf à subir une attaque cyber qui fait effondrer notre impact en consommation énergétique en nous renvoyant à l'âge de pierre.