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

I - Note de synthèse manuscrite à Madame La Maire – Présidente sur la situation numérique de notre collectivité

Copie au cabinet

Hautement Confidentiel (lettre scellée)

Lundi 4 septembre 2023

Madame la Maire – Présidente,

Cette note est manuscrite et retrouve les voies de nos anciens parapheurs papiers car samedi matin (2 septembre), nous avons subi une attaque informatique.

A l'heure actuelle, tous nos systèmes numériques sont coupés. Certains sont inaccessibles, d'autres sont éteints en préventif.

Notre système d'Information (S.I.) commun à la ville et à la Communauté d'Agglomération est arrêté et tous les services correspondants sont stoppés.

Cette note vise à :

1. Vous donner une vision claire sur notre situation
2. Vous proposer des explications sur ce que nous savons déjà
3. Vous indiquer les grandes lignes de ce que nous avons prévu pour revenir disponible le plus vite possible
4. Vous soumettre des éléments clefs issus d'autres expériences pour vous aider à communiquer vers nos 400 000 administrés, l'Etat, et les tiers de nos collectivités.

1) La situation ce lundi matin

Notre astreinte a été informée samedi matin de l'indisponibilité informatique par les services communaux ouverts : bibliothèques, musées, transports, …

Les premières investigations ont permis de comprendre qu'il ne s'agissait pas d'une panne, mais d'une attaque ayant pris les contrôles de nos systèmes.

Nous avons donc informé la hiérarchie et les services de l'Etat au travers de l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information). Cette obligation a été respectée dans les temps réglementaires.

En ce moment, nous investiguons ce qui peut éventuellement être une bonne nouvelle : le cœur de notre S.I, le CCAS et le système des assemblées ne sont peut-être pas atteints. La réactivité de l'astreinte samedi matin a peut-être permis de les protéger à temps.
La téléphonie fixe est également en attente d'investigation.

Nos 2 ingénieurs et 3 techniciens sécurité seront assistés par un expert de l'ANSSI et un expert d'un cabinet spécialisé qui doivent arriver dans la journée – Tous sont mobilisés sur les recherches qui peuvent éviter que le problème n'empire ; et sur le redémarrage rapide, de nos systèmes centraux dans de bonnes conditions de sécurité.

2) Ce que nous savons

Actuellement, presque 3 000 ordinateurs en plus de nos serveurs sont infectés et il faudra tous les reconfigurer via un plan d'urgence qui sera soumis au Directeur Général des Services.

Comme indiqué en introduction, ce plan évoquera la nécessité pour l'administration de revenir à un processus papier et téléphonique le temps que la DNSI fasse son travail pour tout rétablir.

Les bonnes nouvelles sont que notre réseau « Smart City » et surtout nos sauvegardes ne sont pas touchées par l'attaque. Les premiers diagnostics ont permis de vérifier cela.

Les systèmes qui sont chiffrés par les attaquants sont les ordinateurs des utilisateurs, ainsi que les systèmes de l'Etat Civil, l'identité, le recensement, la sécurité publique, les sports, les bibliothèques, les musées, la jeunesse et le service des écoles, les espaces verts, l'environnement et les déchets, le transport, les ressources (finances, moyens généraux, RH) et surtout notre messagerie et nos espaces de fichiers.

Cette longue liste montre que les pirates nous ont durement touchés.

Bien évidemment, ils demandent une rançon en crypto monnaie que l'ANSSI avise de ne pas payer.

3) Grandes lignes du Plan

Nous avons déjà établi une cellule de crise technique et informé la direction générale que nous communiquerons avec la cellule de crise stratégique via le Responsable de la Sécurité des Systèmes d'Information (RSSI).

Nos sauvegardes étant utilisables, nous avons déjà lancé l'achat de nouveau matériel pour les restaurer au plus vite et relancer le système.
En effet, les serveurs actuels sont considérés comme une scène de crime et doivent être investigués par l'ANSSI.

Nos 20 agents non affectés à la restauration du système sont mobilisés pour reconditionner proprement des ordinateurs (autorisés par les investigateurs) et les affecter aux services les plus urgents.

Nous devrions ainsi pouvoir remettre le numérique en service étape par étape en fonction des priorités guidées par la cellule de crise de direction générale.

4) Eléments de communication et d'expériences externes

Les cyberattaques sont devenues un décor commun du paysage médiatique actuel. En juin 2020, déjà 30 % des collectivités avaient été victimes d'un rançongiciel au moins partiellement.

En 2019, l'Etat et les assureurs déclaraient au Forum International de la Cyber sécurité que la seule question à poser était : « Quand cela va-t-il arriver ? ».

Nous vivons ici une situation qui peut arriver à n'importe quelle organisation et qui est subie chaque jour par des dizaines d'institutions.

Les agences des états anglais et américains publient chaque semaine des attaques identiques à la nôtre.

Les CHU, les grandes villes comme Lille ou Aix-Marseille ont mis des mois avant de retrouver une situation acceptable. Le coût de la réparation n'est pas négligeable en plus de cette mobilisation forte des équipes.

Il existe aujourd'hui des conseillers en communication de crise Cyber qui ont su accompagner des situations internationales complexes comme France TV et faire sortir leur client par le haut.

En général, ils conseillent une communication claire et lisible vers le public ; et une communication plus précise vers nos tiers réguliers.

En effet, le public pourra entendre que nous faisons tout pour remettre le service public en état et que nous allons garantir une qualité d'accueil et une continuité d'activité (cantines, musées, parcs, sports, culture, recensement,…).

Mais les tiers qui ont un lien numérique avec nous vont attendre des garanties pour s'assurer que nous ne les infecterons pas (comme un virus humain).

Cette communication spécifique est plus la responsabilité de l'administration vis-à-vis des tiers mais pourra nécessiter votre soutien d'édile.

En espérant, Madame la Maire-Présidente, vous avoir suffisamment éclairée et informée, les équipes de la DNSI et moi-même nous tenons à votre disposition autant que nécessaire.

Le Directeur DNSI

II - Dossier du plan de route DNSI suite à la Cyberattaque du 2 septembre 2023

A l'attention du Directeur Général des Services

Sous couvert du Directeur Général Adjoint au Numérique

Monsieur le Directeur Général des Services,

Comme vous en avez été informé par téléphone, nos 2 collectivités, Communauté d'agglomération mais aussi ville, ont subi une cyberattaque.

Suite à votre demande d'avoir une route précise pour les prochains mois et de saisir l'opportunité de transformer notre système d'information (S.I) en Numérique Responsable, nous vous proposons un dossier découpé en 2 grands axes.

Le 1er axe visera à faire un point détaillé sur notre situation, nos ressources disponibles, les moyens à engager et les risques à gérer. Cela permettra de vous proposer un scénario immédiat et plusieurs scénarios à moyen terme. L'idée étant de rétablir rapidement et efficacement ce que vous jugerez comme service essentiel.
Puis de remonter l'escalier d'une collectivité totalement opérationnelle en adaptant les coûts à la vitesse que vous estimerez nécessaire.

Le 2nd axe visera à vous proposer des pistes en adéquation avec votre souhait de transformer notre numérique pour le rendre durable et responsable. Cela sera possible via les ajustements de stratégie, de vitesse et de moyens que vous validerez pour remonter l'escalier évoqué.

1) Situation et Plan

Comme vous le savez, presque 3 000 ordinateurs sur 3 500 sont inutilisables.
Les systèmes centraux et serveurs de la plupart de nos métiers sont également inutilisables. Les autres sont éteints pour les protéger.
Nos sauvegardes sont disponibles et le plan qui vous sera proposé s'appuie sur cet élément fondamental.

Notre DNSI n'a pas encore établi de Plan de secours informatique qui aurait permis de redémarrer immédiatement certains services essentiels déjà validés à l'avance par la direction générale. Cela aurait été en coordination avec un plan de continuité d'activité établi pour chaque direction sur son périmètre.
Cette question immédiate de la Continuité d'Activité va donc devoir s'organiser sans le numérique dans un temps court. Chaque métier devra s'organiser pour ouvrir les services essentiels aux habitants pour une période la plus courte possible. Nous ferons tout pour que cette période ne dure pas 3 ans comme pour la ville de Bondy attaquée en 2020.

Depuis ce matin, nous avons organisé la DNSI en gestion de crise afin de rétablir l'essentiel au plus vite.

Cette gestion de crise a redéfini l'organisation de la direction :

- Une cellule de crise Cybersécurité est composée des 2 ingénieurs sécurité, du RSSI et des 3 techniciens de sécurité.
  Cette cellule sera conseillée par l'expert de l'ANSSI et assistée par l'expert du cabinet spécialisé que nous avons déjà appelé grâce au marché que nous avions passé pour cela.

- Une cellule de reprise et réinstallation des systèmes centraux composée de 5 ingénieurs systèmes, 10 chefs de projet, 1 acheteur, 1 logisticien et 2 assistants administratifs.

- Une cellule de préparation des postes utilisateurs et de formation et support auprès des agents réinstallés composée de tout le reste de la direction.
  Cette cellule est chargée de communiquer avec les utilisateurs sur les procédures spécifiques en mode dégradé.

- La coordination de ces équipes est assurée par le Directeur.

- Le lien avec la cellule de crise à votre niveau est assuré par le RSSI.

Cette organisation de crise pourra s'assouplir lorsque nous aurons atteint un niveau de reprise d'activité suffisant selon votre appréciation.

Afin que vous ayez une visibilité précise, voici les étapes que nous allons traverser à la DNSI.

Les investigations de la « scène de crime » sont nécessaires pour éviter ce qu'on appelle une répétition. Ce serait dramatique de subir une nouvelle attaque juste après le rétablissement.
Cette méthode était la spécialité d'un groupe appelé « The Hive » et démantelé fin 2022.

Elles vont se découper en 3 groupes.

Le 1er groupe va évaluer la possibilité de redémarrer nos systèmes non chiffrés par les attaquants. S'ils ne sont pas atteints, cela peut nous faire gagner un temps précieux.

Le 2nd groupe va essayer de trouver les virus et outils malveillants installés sur les ordinateurs via des techniques appelées Forensique (comme le médico-légal). Les outils recherchés sont appelés C2 ou RAT et les trouver nous permettra de remonter la chaîne d'attaque afin de bloquer la brèche par laquelle les pirates sont entrés.

Le 3ème groupe va faire le même travail de forensic, mais sur le système central afin de savoir ce qu'on peut redémarrer via les sauvegardes et ce qui est trop dangereux pour l'instant.

En parallèle de ces investigations, notre Délégué à la protection des Données a l'obligation d'informer la CNIL et nous le tiendrons au courant des fuites de données personnelles que nous trouverons. Cela se fera par le lien du RSSI comme indiqué plus haut.

Dans le même temps les 2 autres cellules prépareront les démarrages possibles en achetant et en installant du matériel neuf. Vous l'avez compris les disques durs existants doivent être scellés pour les investigations.

Elles suivront les directives de la direction générale pour déployer au fur et à mesure selon les priorités que vous donnerez en termes de métiers et fonctions essentiels.

Les achats s'appuieront sur nos marchés actifs, sur les centrales d'achat dont nous sommes membres et en dernier recours sur des dérogations DG telles que prévue au code des marchés publics et largement utilisé pendant les confinements COVID.

Ce plan immédiat de remise en service urgent et dégradé devrait permettre de redémarrer les fonctions que vous jugerez essentielles dans un délai qui se compte en jours et inférieur au mois. Vous serez informé des détails de chaque possibilité technique au moins 2 fois par jour par téléphone et via un récapitulatif par note tous les 2 jours.

Le plan de remise en service devra également intégrer des mesures de sécurité techniques immédiates pour améliorer fortement le niveau initial de sécurité.

La réouverture de notre accès à Internet et aux emails est un moment critique qui doit pouvoir être contrôlé et surveillé via des outils que nous installerons avant toute ouverture. Vous verrez ainsi monter à votre signature la commande d'outils comme des sondes réseaux, des IDS, des XDR… Ces termes peuvent vous être détaillés dans une note à part si vous le souhaitez.

La mise en place d'un changement fort comme l'authentification à multifacteurs peut également intervenir avant tout redémarrage.

On passera ainsi du login / mot de passe à un outil sur smartphone ou sur SMS pour accéder à son ordinateur ou à un logiciel. Ces méthodes ne sont pas infaillibles mais elles augmentent grandement notre niveau de sécurité en nous faisant passer sur une dynamique appelée « zéro Trust ». Le fait d'avoir à prouver qu'on est autorisé à se connecter à chaque utilisation est un changement culturel que la cellule support devra sûrement accompagner avec votre soutien.

Passées ces étapes de remédiation d'urgence, on pourra s'atteler à une remise en service totale qui peut inclure plusieurs scénarios et adopter une démarche de numérique responsable.

2) <u>Plan de Reprise d'Activité totale et opportunités de changement</u>

Les pistes de ce plan peuvent déjà être évoquées et discutées à partir de la fin du plan d'urgence.

Les questions de choix de vitesse de reprise totale ne nécessitent pas forcément d'ingénierie complexe.

Il s'agit surtout de choisir la quantité d'experts appelés pour installer et paramétrer les nouveaux systèmes de sécurité ; de choisir de mettre en place rapidement ou non un SOC (Security Operationnal Center) qui surveille en temps réel toutes les alertes paramétrées ; de choisir la vitesse à laquelle on rachète du matériel ou non (une fois les investigations validées, on peut réutiliser le matériel scellé) ; de choisir d'arrêter un logiciel obsolète qu'on n'avait jamais osé suspendre ; etc…

Les questions d'ingénierie complexes se posent surtout dans des choix stratégiques de changement d'orientation numérique.

Cela peut nécessiter la création de groupes projets et d'instances de pilotage qu'on verra un peu après.

Les grandes orientations de changement tournent autour de la question de la souveraineté et du Cloud, de la question de la sobriété logicielle et de la question de la place du numérique dans notre relation au citoyen.

Suite à une crise comme la nôtre, on peut être tenté de se tourner vers le « Cloud » en pensant qu'on y délègue la question de la sécurité et celle de la maintenance. On peut même penser que c'est énergétiquement plus écologique et économique.

Les études récentes ont tendance à montrer que les promesses du « Cloud » peuvent être vite chimériques et qu'elles demandent la même quantité d'effort au quotidien. C'est juste un autre mode de gestion et d'accès. On a du mal à imaginer le numérique sans Internet, mais le Cloud ne fonctionne plus lorsqu'Internet se met à tousser. Ainsi une application Cloud peut paralyser la collectivité à cause de quelques incidents techniques mineurs sur l'Internet.

A l'inverse, les serveurs Cloud sont sensés garantir l'un des piliers du numérique moderne : la Disponibilité.

Ce choix n'est pas absolu pour la collectivité et peut se poser pour chaque besoin et chaque application.

Ainsi, la gestion du transport intercommunal peut être repensée dans une application Cloud interconnectée avec les capteurs de notre Smart City afin d'offrir un meilleur service à la population.

Alors que notre gestion des finances ou des associations peut rester souveraine sur nos serveurs internes.

Ce sont des exemples qui permettent d'illustrer les choix qui permettront de trouver le meilleur équilibre entre usage, service et économie de communication et d'énergie.

La question de la sobriété logicielle devient ainsi centrale. On peut faire le constat que le numérique des collectivités comme des entreprises s'est construit via l'achat de logiciel pour répondre à un besoin de manière successive.

Dans les systèmes les mieux urbanisés la question de la réutilisation d'un logiciel pour plusieurs métiers a déjà été appliquée. Mais ce n'est pas le cas partout.

Nous sommes dans une phase d'opportunité où nous pouvons faire le choix de reposer nos besoins numériques de manière globale en éclatant les silos existants. Sur les traces de la mode des PGI (Progiciel de Gestion Intégrée = ERP) dans les entreprises des années 2000, on peut repenser tous les besoins en travail collaboratif, télétravail, communication et gestion documentaire. Le terme actuel est « Digital Workplace » ou « Espace de Travail Numérique ». Il peut inclure une gestion d'identité et une traçabilité des échanges de manière native qui réduit de 50 % la quantité d'emails. En sachant qu'un email émet 4g de CO^2 à chaque envoi et le même volume au stockage hebdomadaire.

On peut également inclure nativement la question du cycle de la donnée en travaillant avec des archivistes pour résoudre le problème de coût écologique du stockage. Si un document possède sa durée de vie au moment de sa création, il peut être archivé et détruit automatiquement en total respect des contraintes légales. Cela permet d'envisager un assainissement de toutes nos données stockées et non gérées.

Afin d'évaluer sereinement toutes ces questions et surtout de garantir l'adhésion aux changements, il sera opportun de créer une organisation qui inclut toutes les parties prenantes.

Ainsi, là où la direction générale choisit de remettre l'ancien système en place, la DNSI effectuera l'opération technique.

On pourra néanmoins inclure de nouvelles pratiques comme l'allongement de la durée de vie du matériel, le conventionnement avec les ressourceries ou la réduction des appareils avec batterie.

Dans les usages où la direction générale choisit de repenser le numérique pour le rendre plus durable et responsable, on pourra créer des groupes projets qui incluent des représentants de chaque acteur impacté. Si cela touche les citoyens, les outils de concertation et de démocratie participative sont simples à mettre en œuvre et peuvent être éphémères.

Ces groupes projets pourront proposer de revenir aux racines d'un usage collégial. On pourra en profiter pour simplifier certaines règles administratives historiques qui complexifient les applications. On pourra aussi repenser la relation au citoyen avec plus de services en ligne (en les faisant homologuer RGS), mais aussi plus d'inclusion face à l'illectronisme.

Ces groupes projets reporteront à un comité de pilotage qui choisira de s'orienter vers de la réutilisation de logiciel existant ou de valider une nouvelle acquisition à chaque nouveau besoin.

La quantité de logiciels de notre administration peut envisager une réduction significative avec un impact direct sur les coûts de maintenance.

Afin d'inclure ça dans un plan politique, des indicateurs liés à l'écologie et aux économies d'usage ou au taux d'utilisation citoyen seront remontés de manière régulière à l'exécutif.

Conclusion

La liste des idées et propositions faites dans ce dossier n'est pas exhaustive car le temps est compté et les urgences de la crise en cours mobilisent la DNSI dans son ensemble.

J'espère néanmoins que cette première réponse à votre question est un éclairage suffisant pour l'instant et reste à votre disposition si vous l'estimez nécessaire.