Angers : les enseignements de la cyberattaque, 4 ans après

Victime d'une cyberattaque par rançongiciel en janvier 2021, la ville d'Angers, dans le Maine-et-Loire, a mis deux ans pour se remettre progressivement de l'incident.
La municipalité a tiré les enseignements de cette crise.

Entretien avec :

Jérôme GUIHO
Directeur Général adjoint
en charge de la Transition Numérique
Angers Loire Métropole

Luc DUFRESNE
RSSI
Angers Loire Métropole

Que s'est-il passé dans la soirée du 16 janvier 2021 ?

Jérôme Guiho : La Ville et l'agglomération d'Angers ont été la cible d'une cyberattaque, par rançongiciel. C'était un vendredi soir, tout le système d'information a été totalement paralysé. Les conséquences ont été très lourdes et très impactantes pour l'organisation puisque l'ensemble des agents de la collectivité, qui sont connectés au système d'information, ne pouvaient plus travailler avec les outils bureautiques : plus de boîte mail, plus d'accès à la messagerie… Cela a duré plusieurs jours. Nous sommes revenus à la mode du papier et du crayon.

Connaissez-vous l'origine de l'attaque ?

Luc Dufresne : C'est une intrusion avec une demande de rançon pour rétablir le système d'information.

Quel était le montant ?

Jérôme Guiho : Nous ne savons pas, nous avons eu le réflexe de ne pas cliquer. Et de toute façon, et l'ANSSI et les policiers nous ont demandé de ne pas aller plus loin.

Luc Dufresne : Nous avons tout transmis au service juridique.

Combien de temps avez-vous été impactés ensuite ?

Jérôme Guiho : Nous avons passé trois à quatre jours avec l'absence totale d'outils. Petit à petit, les outils bureautiques basiques ont été rétablis puis les logiciels métiers. Nous en avions identifié près de 200 dans la collectivité. Les services se sont d'abord occupés des plus urgents, notamment tout ce qui concernait la paye, les finances, les RH. Nous étions alors en pleine période de paye pour 4000 agents, vous pouvez imaginer un peu les conséquences, donc ça c'était vraiment des sujets prioritaires.
Cela a pris plusieurs mois pour remédier et remettre en place l'ensemble des logiciels métiers. L'ANSSI nous avait dit qu'il nous fallait deux ans pour nous remettre de cet incident et reconstruire un système qui soit véritablement robuste et à l'identique en termes de Fonctionnalités, et effectivement, cela a pris deux ans.

Luc Dufresne : Le message qu'on a eu, c'était « deux semaines très difficiles ». Il nous a fallu un peu plus d'une semaine pour remonter la messagerie par exemple, deux à trois mois après pour obtenir un

système d'information minimal avec vraiment les grosses fonctions régaliennes, RH, finance, etc. et puis après bien deux ans de sécurisation, de travaux de sécurisation complémentaires.

Jérôme Guiho : Ça a été très impactant pour la Direction du Système d'Information et du Numérique (DSIN). L'épisode a été assez long et assez lourd à gérer pour ses agents.

Quel a été l'impact sur les administrés d'Angers ?

Jérôme Guiho : Très limité, même si nous sommes revenus à des modes de fonctionnement un peu rudimentaires. La première décision a été d'ouvrir l'hôtel de ville aux usagers dès le lundi matin. Nous avons fonctionné en mode dégradé mais les rendez-vous se sont tenus, les actes de naissance ont été rédigés à la main, les mariages aussi.

Quelles ont été les décisions au lendemain de la cyberattaque ?

Jérôme Guiho : Du jour au lendemain, la cybersécurité, jusque là sujet technique, est devenue un sujet stratégique, un enjeu majeur impliquant toute la direction générale de la ville dans la gestion quotidienne.
En termes de gouvernance, tous les trois mois, nous avons un comité stratégique autour des questions numériques et il y a toujours un volet cybersécurité. Ensuite, C'est un point de sensibilisation permanent, que ce soit auprès des directeurs ou auprès de nos agents.
Les 3 000 collaborateurs municipaux et de l'agglomération connectés sont régulièrement formés et entrainés lors de simulations d'attaque, à l'aide de (faux) messages trompeurs par exemple, les télétravailleurs suivent une formation obligatoire avant d'être autorisés à travailler à distance. Les SI d'Angers sont surveillés 24h/24 par un SOC nantais. Ce qui permet à la collectivité de traiter plus d'une vingtaine d'incidents de cybersécurité par mois, illustrant la réalité permanente de la menace cyber.

A combien sont évalués les impacts financiers ?

Jérôme Guiho : Je ne pourrais pas vous dire mais ce sont des grosses sommes, vraiment de très grosses sommes. Je vais vous donner un exemple : sur le volet territoire intelligent, nous avons installé ce qu'on appelle un WAF, qui est un gros firewall pour ce projet de territoire intelligent. On est sur des outils à 600 000 euros.
Ensuite, tous les ans, la maquette budgétaire maintenant intègre ce volet cybersécurité. C'est coûteux mais indispensable.

Luc Dufresne : Ce qui est intéressant, c'est de parler en pourcentage du budget informatique. L'ANSSI préconise qu'il faudrait être entre 5 à 10 % du budget informatique consacré à la sécurité. Nous en étions loin en 2021. Aujourd'hui, on s'en rapproche.

Comment avez-vous échelonné la mise en œuvre d'outils de cyber protection ?

Luc Dufresne : On avait commencé à travailler avant la cyberattaque. J'ai pris mes fonctions de RSSI en 2020, un an avant la crise. L'idée était de travailler de manière cohérente, faire un état des lieux de la cartographie des risques, mettre en place une politique accompagnée d'un plan d'action. On a commencé à dérouler, malheureusement on s'est fait attaquer trop tôt.
Suite à la cyberattaque, la première chose était de comprendre comment on avait été attaqué, quel avait été le chemin utilisé pour rompre notre système. Nous avons ensuite réorganisé le plan d'action pour venir corriger les grosses failles utilisées tout de suite.
Le plan d'action peut être découpé en quatre types d'actions.
Il y a les actions de gouvernance, qu'évoquait Jérôme Guiho ; des actions de protection : mettre en place des « parpaings », des barbelés, tout ce qu'on imagine derrière la sécurité informatique, les aspects vraiment techniques.
Après la défense, il y a la surveillance de ce qui se

passe chez nous, on va traiter les incidents et puis après aussi préparer la crise avec la résilience, avec de la sensibilisation et de la formation.
De la même manière, nous commençons à être moins dans les conséquences de l'attaque, nous allons aussi devoir travailler à la préparation de la prochaine crise éventuelle. On va commencer à faire des exercices de gestion de crise, de procéder, formaliser notre gestion de crise.

On imagine que vos 3 000 agents connectés sont ultra-vigilants…

Jerôme Guiho : En tout cas, on fait en sorte qu'ils le soient ! Pour vous donner un exemple, les télétravailleurs sont assujettis à une formation obligatoire sur le volet cybersécurité avant de pouvoir faire du télétravail. On est très rigoureux là-dessus. Mais vous savez, on est très humbles.

Luc Dufresne : Nous avons 3000 personnes qui travaillent, peut-être qu'il y en aura 2 999 qui seront parfaits. Il suffit d'une seule personne…
On considère qu'il peut y avoir quelqu'un qui fait une erreur et c'est pour ça que nous on va parler de défense en profondeur. On sensibilise l'utilisateur mais on met aussi d'autres protections derrière. Un peu comme un mode d'aéroport.

C'est-à-dire ?

Luc Dufresne : Avant de rentrer dans un avion, on a été scanné deux ou trois fois. D'un point de vue sécurité. On a plusieurs barrières pour retarder l'attaquant, pour le détecter et pour se défendre et le mettre dehors si jamais il rentre.

Quel SOC utilisez-vous aujourd'hui ?

Luc Dufresne : Nous faisons appel à un prestataire, n'étant pas assez nombreux pour surveiller 24h sur 24. Il s'agit d'une société privée de Nantes. Ils nous alertent quand ils détectent des signaux inquiétants. Nous poursuivons l'investigation nous-mêmes.
Nous traitons plus de 20 incidents de sécurité chaque mois, qui sont des faux positifs, des fausses alertes ou qui relèvent de mauvais usages...

Cette cyberattaque a-t 'elle eut un impact sur le territoire intelligent ?

Jérôme Guiho : Non, aucun, si ce n'est qu'on a là aussi renforcé le volet sécurité au sein du projet, à l'image de ce qui s'est fait et de ce qui s'est déployé au sein de la collectivité.
Le territoire intelligent est un projet parmi d'autres, on déploie un certain nombre de projets avec des outils numériques donc celui-ci en est un, mais c'est loin d'être le seul.

Luc Dufresne : C'était quand même une motivation pour créer, à l'époque, le poste de RSSI que j'occupe. La collectivité a anticipé ce besoin de sécurité, notamment pour ce type de projet qui concerne le territoire.

Dernière question : le budget dédié à la cybersécurité est stable depuis la cyberattaque. Va-t-il être augmenté ?

Jerôme Guiho : La somme varie chaque année, en fonction des projets, de la capacité, de la dimension du projet et de la capacité des agents de la DSIN notamment à porter ce projet. Nous sommes à leur écoute.

Luc Dufresne : Si j'avais un budget illimité, je serais incapable de le dépenser. Ce n'est pas moi qui sécurise le système d'information mais ce sont mes collègues qui font du réseau, du système.
L'idée c'est surtout de convaincre tout le monde de prendre son rôle dans la sécurité via la gouvernance, de l'élu, du maire président jusqu'à l'agent de l'autre côté de la pyramide, chacun a un rôle à jouer.

Jerôme Guiho : C'est une question d'acculturation, de maturité, de formation aussi pour certains.

Luc Dufresne : C'est comme de la sécurité au travail, c'est comme de la sécurité routière, c'est comme tout.

Jerôme Guiho : Ce n'est pas quelque chose qu'on a envie de faire de manière native. C'est un peu à l'image de la protection des données. On a mis en place une culture interne autour de la protection des données qui aujourd'hui porte totalement ses fruits.