Cybersécurité comportementale
Enjeux et spécificités des collectivités territoriales : l'intérêt d'une cyber-culture individuelle et collective

Astrid FROIDURE
Présidente de Normandie Welcome
Référente Normand-ie Stratégie
Chargée de Relations Publiques d'Avant de Cliquer

Au cœur de l'évolution numérique, les collectivités territoriales se retrouvent dans un process de transformation accéléré depuis une dizaine d'années. Indispensable pour s'adapter à la vie quotidienne des citoyens comme pour mener les projets les plus ambitieux, le « chantier du numérique » est certainement le plus stratégique pour les organisations publiques.

Echanges dématérialisés avec les citoyens, les acteurs économiques et autres administrations publiques, e-administration, sites interactifs, communication réseaux… les interfaces numériques se sont multipliées. Dans le même temps, bien que les bénéfices de ces évolutions soient considérables, les collectivités sont aussi devenues des cibles d'attaques informatiques de plus en plus nombreuses (fragilité des systèmes d'information, faible acculturation numérique, mauvaise prise en compte des menaces). L'improvisation du recours au télétravail face à la crise du Covid 19, a ouvert un grand nombre de brèches sécuritaires, facilitant les attaques des hackers.

Hameçonnage, déni de service, piratage de compte, vol de données, défiguration de site, rançongiciels, la menace est quotidienne. Parmi les 70 victimes déclarées officiellement en 2020, on trouve des collectivités de toutes tailles, de la métropole d'Aix-Marseille-Provence à des petites villes de l'Oise. Qu'il s'agisse de défaçages, c'est-à-dire une intrusion sur le site web pour en modifier le contenu ; d'attaques par rançongiciels, aux conséquences souvent désastreuses ; de minages, c'est-à-dire l'utilisation des ordinateurs de la collectivité pour fabriquer des crypto-monnaies ou d'autres encore, comme le cheval de Troie Emotet qui ouvre une porte dans l'infrastructure pour faciliter les utilisations frauduleuses, l'ampleur des conséquences est fonction de la qualité de l'anticipation des cyberattaques.
Ces attaques constituent de véritable menace pour le fonctionnement global des collectivités locales. Le chiffrement des données peut bloquer l'accès aux systèmes d'informations des services pendant plusieurs jours, voire plusieurs semaines. Au-delà de l'empêchement des agents d'accéder à leur outil de travail, elle conduit à une restriction massive des services disponibles pour les utilisateurs. Elles impliquent également un coût

financier conséquent (redéploiement des terminaux, modification des serveurs, pertes des données) dans un contexte de diminution importante des budgets. La réputation est aussi impactée par une décrédibilisation de la collectivité auprès de sa population, mais également auprès des partenaires publics et privés. Enfin, ces attaques entrainent nécessairement des procédures juridiques longues et fastidieuses, notamment en l'absence de plan de continuité et de reprise d'activité.

Les collectivités publiques : nouvelles cibles privilégiées

Les cyberattaques se déplacent de plus en plus vers les organisations publiques, collectivités territoriales, structures hospitalières, détentrices de volumes importants de données confidentielles et porteuses des services essentiels pour les citoyens français. Elles sont devenues, en quelques années, les cibles privilégiés pour trois raisons majeures :

un service public empreint de bienveillance

Tout d'abord, fondamentalement, les collectivités territoriales, comme les établissements hospitaliers, répondent aux caractéristique de service public : entraide, solidarité, secours. Agents comme élus, mués par ces valeurs, rencontrent des difficultés à imaginer des attaques dommageables à leurs missions d'intérêt général. De surcroit, les cyberattaques ayant d'abord visé les entreprises, les organisations publiques concentrées sur leur transformation numérique accélérée ont principalement axé leur mutation sur les aspects techniques et matériels au service des publics sans toujours réaliser le danger.

des inégalités de territoire croissantes face au numérique

La disparité des collectivités locales complique la mise en place d'un process de sécurité unifié. Or les inégalités entre les territoires français s'accentuent.

Les territoires intégrés à la mondialisation concentrent les interactions économiques nécessitant un développement numérique fort. Les régions littorales, à l'ouest et au sud du pays, sont attractives et profitent de leur interface pour développer les échanges. Par exemple, les zones industrialo-portuaires (ZIP) de Dunkerque ou du Havre, ouvertes sur la *Northern Range,* s'imbriquent dans une nécessaire modernisation numérique des collectivités locales de ce territoire. Les régions frontalières du territoire sont également connectées à la mondialisation par l'intensité des échanges transfrontaliers.

Les inégalités entre les collectivités territoriales tendent à s'accélérer depuis les dernières réformes territoriales (Loi MAPTAM, et Loi NOTRe notamment) accompagnant le mouvement de métropolisation. L'avenir favorable aux métropoles concentrant emplois, économie et services accentue la fragilité des villes moyennes et des zones rurales (France Stratégie).

L'accès et l'utilisation des nouvelles technologies numériques, les inégalités entre territoires s'accroissent proportionnellement aux ressources tant techniques (infrastructures réseaux, équipement...) qu'humaines (services informatiques avec personnels dédiés : DSI, RSSI, DPO...).

des élus et des agents non sensibilisés et formés aux cyberisques

La nature même des collectivités territoriales, leur fonctionnement démocratique et le principe électif consubstantiel aux collectivités locales françaises impliquent plus de 520 000 élus locaux. Ces élus aux parcours divers et singuliers sont faiblement sensibilisés à la sécurité informatique.

La pression de la transformation numérique conduit à voir cette évolution comme un moyen performant d'amélioration des services, sans pour autant bien assimiler les risques qu'ils impliquent. Souvent mal accompagnés pendant le début de leur mandat, élus, comme fonctionnaires, subissent de plein fouet les fractures numériques du territoire. Au-delà des grandes collectivités dotées d'un service informatique et malgré l'évolution sociétale, les petites collectivités s'équipent et s'organisent souvent proportionnellement au niveau de l'utilisation personnelle des outils numériques par ses dirigeants. Infrastructure, équipement, sécurité informatique, formation, deviendront ou non prioritaires lors des débats budgétaires.

De la sécurité informatique à la cybersécurité comportementale

Proportionnellement au développement d'un arsenal technique en matière de sécurité numérique reposant sur des systèmes de sécurité supervisés par des équipes informatiques, la vulnérabilité humaine est devenue la faille la plus évidente des organisations. Du fait du facteur humain, il est nécessaire de renforcer la stratégie cyber autour de la sensibilisation et de l'apprentissage. L'apparition du concept de sécurité comportementale est récente en France. Il est né d'un constat simple : malgré toutes les sécurités techniques et organisationnelles, des cyberattaques parviennent tous les jours à paralyser, rançonner voire anéantir le fonctionnement des organisations françaises.

Le couple ransomware / phishing représente plus de 80% des cyberattaques françaises et tant l'ensemble des organisations publiques et privées que les citoyens, deviennent potentiellement une cible pour les hackers. Les courriels d'hameçonnage sont de plus en plus sophistiqués, les données les plus anodines convoitées pour les intégrer dans des mails crédibilisés par de « vraies » informations récupérées aisément sur les réseaux sociaux ou dans l'actualité. Il devient ainsi de plus en plus difficile de distinguer un mail malveillant d'un mail authentique.

La mise en place d'une culture organisationnelle et comportementale devient incontournable face à cette évolution afin que tous puissent acquérir les réflexes nécessaires à la protection de la collectivité. Une responsabilité collective s'installe reposant sur une nouvelle transversalité : nous ne sommes jamais trop petit pour être victime et la nouvelle campagne de l'Agence du Numérique en Santé « TOUS CYBERVIGILANTS ! » s'applique totalement aux collectivités territoriales.

Ainsi renforcer le pouvoir défensif des collectivités va impliquer plusieurs notions complémentaires :
- contribuer à une prise de conscience du rôle, à la fois individuel et collectif, de tous les agents et élus, quelles que soient leurs missions et compétences, en matière de cybervigilance ;
- intégrer élus et agents dans une mobilisation générale afin de protéger leur outil de travail et les données récoltées en associant sensibilisation, connaissances et responsabilités ;

- apprendre à communiquer tant vers la collectivité que ses partenaires, associations, prestataires, citoyens sur ces nouvelles menaces pour expliquer, rassurer et les accompagner dans une culture de cybersécurité partagée.

Installer une culture préventive forte peut s'appuyer sur différents outils mêlant habilement formation et communication. On pourrait penser qu'un grand séminaire de sensibilisation incluant tous les agents et élus pourrait déclencher une dynamique vers l'attitude de prophylaxie attendue.

Selon le rapport Building a Cyber Smart Culture réalisé par Fujitsu, il est important dans ce contexte particulier, d'intégrer une approche différente de la formation. L'objectif n'étant pas seulement de diffuser des connaissances mais d'acquérir des réflexes de cybersécurité.
Ainsi le rapport souligne qu'une bonne formation de sensibilisation se concentre sur deux aspects fondamentaux.
Le premier est le changement de comportement : motiver les gens à penser et à agir différemment. Ce type de formation doit reconnaître que les différentes sections des salariés, agents, élus sont motivées de différentes manières.
Le deuxième aspect d'une bonne formation de sensibilisation est l'intégration par la formation des gestes qui sauvent et des comportements à adopter selon les cas. Lorsque les employés sont confrontés à des tentatives d'hameçonnage, ils doivent immédiatement savoir ce qu'ils doivent faire, ce qu'ils ne doivent pas faire et qui ils doivent informer. En résumé « une formation innovante et interactive sur les problèmes que les employés rencontrent dans leur contexte personnel est susceptible d'obtenir un fort engagement ».

Face à ce constat, des outils se développent, portés par les entreprises spécialisées du monde numérique qui essaient d'intégrer de plus en plus des solutions de sensibilisation à la cybersécurité à leurs prestations.

Les outils de la cybersécurité comportementale

La première étape consiste à réaliser un audit de vulnérabilité afin d'évaluer la résistance collective et individuelle. Quelles que soient les structures, publiques ou privées, le service concerné ou la sociologie des utilisateurs, le taux de vulnérabilité face à des attaques dites « de masse » (non personnalisées pour l'établissement) est en moyenne de 24% sur les structures n'ayant pas mis en place de programme spécifique de cybersécurité comportementale.
Réalisé de manière impromptu, avec des caractéristiques prédéterminées conjointement avec les responsables des services informatiques, un audit consiste à envoyer de « faux mails de phishing » à tous les utilisateurs : élus et agents, sur une durée déterminée avec un degré de difficulté croissant. Les clics malencontreux les rassureront en les informant qu'il s'agit d'une évaluation globale de la vulnérabilité de la structure.
Au-delà de l'établissement d'un référentiel de base sur la vulnérabilité de la structure, les résultats de cet audit font généralement l'effet d'un électrochoc pour les dirigeants lorsqu'ils réalisent que près d'un quart des utilisateurs cliquent sur un mail imitant un mail malveillant lors d'un audit d'une semaine.

Les méthodes de sensibilisation à la cybersécurité

Elles sont nombreuses et en pleine évolution.

Ainsi on distinguera :

les actions de formation en présentiel

Que ce soit sous forme de journée(s) de formation ou de séminaire d'équipes, voire de séminaires annuels permettent une interaction directe avec les formateurs et intervenants avec des réponses immédiates aux questions et un partage d'expérience. Accompagnées d'une gestion logistique et administrative importante, elles mobilisent les collaborateurs en impliquant une organisation de continuité d'activité. Les coûts directs et indirects s'additionnent. La complexité pour les collectivités est particulière car leurs engagements en matière de formation sont principalement noués avec le CNFPT (Centre National de la Fonction Publique Territoriale) avec des modules de formations indépendants dispensés sur des temps limités. Importants sur la dimension technique et de sensibilisation, leur impact est cependant limité par l'approche forcément généraliste de la problématique cyber face à une menace de plus en plus ciblée et personnalisée des attaques par phishing.

le e-learning ou formation en ligne

De nombreux modules de formation permettent d'accroitre les connaissances sur la cybersécurité. Solution flexible, asynchrone, le e-learning permet d'assister à la séance à l'endroit et au moment de son choix. Il n'est malheureusement pas adapté à tous les publics car il nécessite, au-delà d'une certaine pratique du numérique, rigueur, autonomie, et de savoir s'auto-évaluer. Aussi, il est parfois difficile d'obtenir l'adhésion de tous dans la pérennité. Leur prix est variable et va dépendre de l'outil utilisé et de la personnalisation possible pour la collectivité. Certains MOOC de sécurité numérique ont été réalisés par les structures de l'Etat comme le MOOC de l'ANSSI ou celui de la CNIL et sont mis à disposition gratuitement sur leur site. Des plateformes spécifiques de e-learning se développent de plus en plus. Proposées en complément des outils techniques par de nombreux opérateurs, certaines entreprises ont choisi de développer des plateformes de e-learning modulables en fonction des spécificités des utilisateurs.

les outils de communication visuelle

Affiches, écrans de veille permettent à la fois de rappeler les bonnes pratiques et de donner les consignes en cas d'alerte : premiers gestes, coordonnées du service informatique… Le kit de sensibilisation de Cybermalveillance étant particulièrement adapté aux collectivités.

des guides et livrets utilisateurs

La mise à disposition de guides ou de livrets spécifiques pour les utilisateurs et notamment remis aux nouveaux arrivants, accompagne de plus en plus les prises de poste. Certains sont spécifiques pour les collectivités territoriales comme celui élaboré par l'ANSSI avec l'AMF et nombreux destinés initialement aux entreprises sont aussi adaptables aux collectivités (Cybermalveillance, Medef, Gendarmerie nationale...).

la formation par le jeu

La formation par le jeu, comme les *serious-games* ou les *escape-games*, se développe souvent en parallèle des formations professionnelles ou des plateformes d'e-learning. Plus ludiques, elles permettent de mettre l'utilisateur dans différents

contextes et abordent aussi les notions de sécurité physique et économique.

des campagnes de phishing régulières

Les campagnes de phishing régulières sont parfois instaurées dans l'objectif de garder en alerte les utilisateurs. Souvent accompagnées d'une plateforme d'e-learning, ces campagnes sont alors répétées annuellement ou semestriellement. Elles permettent de réaliser une photographie de la vulnérabilité cyber à un instant T et de suivre son évolution au fil du temps. Malheureusement, leur effet est temporaire sans accompagnement par une formation associée pour permettre de développer des réflexes de cybersécurité.

la sensibilisation sur poste de travail

Elle consiste à envoyer régulièrement des mails d'apprentissages imitant une cyberattaque par phishing. Lorsqu'un utilisateur clique malencontreusement sur un mail, une page d'information (ou une mini vidéo) va s'ouvrir afin de lui expliquer comment il aurait pu déjouer l'attaque et ce qu'il aurait dû vérifier avant de cliquer. Certaines sociétés ont développé plusieurs degrés d'attaques spécifiques : de l'attaque de masse aux attaques personnalisées en s'inspirant de mails réels internes à la structure ou à son environnement de travail. Au-delà de la pédagogie par l'action, l'intérêt de cette méthode d'apprentissage est une mise en place pour tous les agents, même en télétravail.

le bouton d'alerte phishing

Ce bouton est installé sur la barre d'outils des messageries des utilisateurs. Il permet lorsque ceux-ci détectent une attaque de transférer directement le mail suspect au service informatique qui sera alors en capacité d'analyser les attaques et de prendre les mesures appropriées. Son utilisation entraine un écran de félicitations qui va entretenir la culture de veille cyber et développer le sentiment d'appartenance pour protéger la collectivité.

Certaines sociétés comme « Avant de Cliquer » se sont spécialisées pour développer une culture de cybersécurité pérenne. Elles mettent en place un programme complet avec tous les outils existants : audit, rapport de vulnérabilité, plateforme de e-learning, outils de communication visuelle et bouton d'alerte cyber en les interfaçant entre eux afin d'optimiser l'acquisition de réflexes pérennes. De plus, les décideurs et services informatiques ont un tableau de bord permettant de suivre l'évolution de la vulnérabilité de leur collectivité tout en évaluant les risques d'attaques.

Parce que les attaques par phishing constituent plus de 80% des cyberattaques et que dans une collectivité, comme dans une entreprise, chaque élu, chaque agent, a une boite mail, la cybersécurité est devenue l'affaire de tous. Quelle que soit la personne qui aura cliqué sur un courriel malveillant, l'impact sera le même. Sans oublier que la responsabilité de chacun pour protéger la collectivité s'étend bien au-delà par l'interconnexion avec l'ensemble du territoire, associations, entreprises, citoyens.

Devant l'inégalité structurelle des territoires tant en compétences qu'organisationnelle, il semble évident que la mutualisation des services informatiques doit devenir une priorité pour les petites collectivités. Est-ce au cœur des EPCI qui rencontrent les mêmes difficultés que des collectivités de taille moyenne ou les PME à

recruter des RSI et à former leurs équipes, ou plus largement au sein des Centres de Gestion Départementaux qui gèrent déjà les services de ressources humaines, archives, remplacements, des « petites » collectivités territoriales ? La dynamique de l'Etat, notamment avec le Plan France Relance, joue le rôle d'accélérateur à la fois de soutien vers des projets concrets et de prise de conscience par les élus de la réalité des menaces. L'implication des dirigeants, élus, DGS, responsables juridiques et de service informatique, doit se matérialiser par une anticipation de leur sécurité. Développer une culture de cybersécurité n'est pas une dépense, c'est un investissement. La cybersécurité devient un enjeu majeur de management et de direction pour réussir à transformer le maillon faible en un maillon fort. Comme le relève Cybermalveillance dans son rapport d'activité 2020, la sensibilisation est la première arme contre les cyberattaques. La cybersécurité doit ainsi dépasser la formation individuelle pour intégrer le socle de la culture territoriale pour tous, agents comme élus, avec des outils spécifiques, innovants, inscrits sur la durée, permettant de mettre en place une cyberculture territoriale pérenne.

Quelques références

Les collectivités face aux enjeux de cybersécurité / ANSSI

Rapport d'activité 2020 – Kit de sensibilisation aux risques numériques / Cybermalveillance

L'essentiel de la sécurité numérique pour les dirigeants et les dirigeantes / Challenge

Quels sont les axes majeurs pour lutter contre les cyberattaques ? / L'usine digitale

Cybersécurité : comment former les télétravailleurs pour réduire les vulnérabilités comportementales / IT Social

Vigilance face aux cyberattaques : les collectivités sont toutes concernées ! / Cybermalveillance

"Au moins 4% des communes françaises ont été piratées en 2020" Jérôme Notin – Cybermalveillance / Journal Du Net

Le rapport Fujitsu sur la cyberculture