CYBER CERCLE
collection

SÉCURITÉ NUMÉRIQUE & COLLECTIVITÉS

Regards croisés

Jérôme BUZIN
François CHARBONNIER
Mireille CLAPOT
François COUPEZ
Josiane CORNELOUP
Michel DUBOIS
Fabien FERRAZZA
Rémy FÉVRIER
Astrid FROIDURE
Loïc GUÉZO
Christophe GUILLOTEAU
Juliette JARRY
William LECAT
Philippe LOUDENOT
Jérôme NOTIN
Vincent TRELY

Préface de Bénédicte PILLIET

2021

SÉCURITÉ NUMÉRIQUE & COLLECTIVITÉS

Regards croisés

Ce livre est édité sous la direction de
Bénédicte PILLIET, Présidente du CyberCercle

Préface

BÉNÉDICTE PILLIET
Présidente
CyberCercle

Les collectivités et, au-delà, les territoires, sont au cœur de l'action et de la réflexion du CyberCercle depuis 2015.

A l'initiative du sénateur-maire de Fleurance, Raymond VALL, et avec le soutien de l'amiral Arnaud COUSTILLIERE, alors officier général cyberdéfense et autorité de référence de la Réserve Citoyenne Cyberdéfense, nous avons en 2015 créé nos premiers rendez-vous en région avec Cyber & Territoires. Une journée d'informations et d'échanges sur la cybersécurité à destination des acteurs locaux, publics et privés, à Fleurance, au cœur du Gers, qui a réuni plus de 200 participants.
Cet événement atypique dans le panorama des événements cyber, a été le point de départ de notre implication sur les territoires pour porter cette culture de confiance et de sécurité numériques au-delà du cercle très restreint de ses experts, en région, avec le soutien des collectivités et des élus, et avec une approche didactique adaptée au contexte économique dans lequel nous nous trouvions.

Cette implication sur les territoires a donné naissance en 2018 au Tour de France de la Cybersécurité qui, chaque année, fait étape dans plusieurs régions avec cet esprit de partage de connaissances, cette philosophie de fédérer les acteurs locaux, non seulement pour leur permettre de mieux appréhender la sécurité numérique dans toutes ses dimensions, mais également pour créer des synergies, des dynamiques sur le terrain pour construire des territoires de confiance numérique.

Au-delà de l'organisation de ces journées, des matinales bimestrielles qui se déroulent désormais sur plusieurs régions, convaincus de la nécessité

de faire de la sécurité numérique un pilier majeur de la transformation numérique des collectivités mais aussi des territoires dont ils ont la responsabilité, c'est un travail de confiance que nous menons en étroite collaboration avec les élus.

Cette prise en compte des territoires et du rôle majeur que jouent les collectivités dans la sécurité numérique de la Nation, est désormais une des préoccupations de l'Etat, comme le montre notamment la feuille de route « Cybersécuriser les Territoires » du Plan de Relance Cyber présenté le 18 février dernier par le Président de la République.

Nous ne pouvons que nous réjouir au CyberCercle de la montée en puissance de la prise en compte de cette dimension, d'autant plus que le nombre de collectivités victimes d'incidents de sécurité numérique n'a cessé d'augmenté ces derniers mois.

Mais la route est encore longue, nous le savons tous.

C'est ainsi pour faire le point sur les enjeux, les actions déjà conduites mais également celles qui devront être menées demain, que nous avons consacré le deuxième opus de notre Collection CyberCercle - Regards croisés à cette thématique majeure.

Non pas comme un aboutissement de notre travail depuis 2015, mais comme un instantané de la situation aujourd'hui et des actions que tous nous aurons à conduire collectivement.

Pour notre part, nous continuerons au CyberCercle à promouvoir en région cette culture de sécurité numérique partagée et à accompagner certaines collectivités dans leurs démarches vertueuses autour de cette dimension.
Par ailleurs, nous avons lancé un Observatoire des Territoires de Confiance Numérique qui suivra la définition et la mise en œuvre des politiques publiques de sécurité numérique portées par les collectivités, que ce soit en matière d'innovation, de formation, de recherche, de dispositifs et d'infrastructures dédiées… afin, là encore, de valoriser les actions conduites et dans un esprit de partage des expertises.

Je tiens à remercier l'ensemble des contributeurs d'avoir accepté de partager leur expertise et leur vision, ainsi que nos partenaires, Cybermalveillance.gouv.fr, Proofpoint, le Groupe la Poste, la Banque des Territoires, Avant de Cliquer et Certitude Numérique qui ont contribué avec nous au financement de cet ouvrage.

Donner des clefs aux élus, aux agents des collectivités sur les enjeux que représentent aujourd'hui la confiance et la sécurité numériques, et, au-delà, la protection des informations, pour leurs territoires, apporter de la visibilité sur les dispositifs publics qui accompagnent cette indispensable montée en puissance des territoires dans ces domaines, permettre un partage de connaissances au bénéfice de tous, sont les objectifs de cet ouvrage et, au-delà, de notre action.

« *Il ne peut y avoir aujourd'hui de développement responsable et d'attractivité des territoires sans numérique, pas de numérique pérenne sans confiance numérique, et pas de confiance numérique sans sécurité numérique* » : ce mantra du CyberCercle en ouverture des étapes du Tour de France de la Cybersécurité illustre le défi majeur qui est aujourd'hui lancé aux collectivités et à leurs élus.

Je vous souhaite une bonne lecture.

La cybersécurité, une composante de la sécurité globale

JÉRÔME BUZIN
Directeur de projets stratégiques numériques
Administrateur général des données
Métropole européenne de Lille

Le continuum de sécurité : une notion de l'espace physique qui pourrait s'étendre à l'espace numérique

En 2018, dans un rapport au Premier ministre, les députés Alice Thourot et Jean-Michel Fauvergue proposent de passer d'un continuum de sécurité vers une sécurité globale qui englobe « l'ensemble des 430 000 membres des forces de sécurité intérieure, des polices municipales et des entreprises privées de sécurité, qui concourent, à des degrés et par des chemins différents, à garantir la protection des personnes et des biens dans notre pays ». Cette définition pourrait s'appliquer telle quelle aux questions de cybersécurité et Mme Thourot et M. Fauvergue appelaient d'ailleurs, dans leur proposition n° 17, à anticiper en « intégrant la dimension cybersécurité dans la démarche de coproduction de sécurité de demain ».

Par la suite, en 2020, lors des débats à l'Assemblée Nationale sur la proposition de loi relative à la sécurité globale, M. Fauvergue mettait en avant que « si, en application de l'article L. 111–1 du code de la sécurité intérieure, l'État a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, (...) au maintien de la paix et de l'ordre publics, à la protection des personnes et des biens, il est également prévu qu'il associe d'autres acteurs à la politique de sécurité parmi lesquels les collectivités territoriales et les représentants des professions de sécurité. »

L'action des collectivités territoriales en matière de cybersécurité

Maillon essentiel en matière de cybersécurité, les collectivités territoriales

font pourtant office de chainon manquant. Ce n'est pourtant pas faute d'initiatives pour les impliquer.

Dès 2012, l'ANSSI a créé des postes de coordinateurs territoriaux devenus depuis les délégués à la sécurité du numérique en région ; le Campus Cyber qui s'installera en 2021 à La Défense, près de Paris, s'appuiera sur un réseau de Campus Cyber régionaux ; le plan de relance post-covid intègre un volet Cyber dont l'une des composantes vise le renforcement de la sécurité des collectivités territoriales notamment au travers de la création de CSIRT[1] régionaux ; l'association des maires de France et des présidents d'intercommunalité (AMF) et la Banque des Territoires ont chacune publié en 2020 un guide à destination des élus des collectivités… Les exemples ne manquent pas.

Du côté du secteur privé, il existe également plusieurs initiatives visant à sensibiliser et mobiliser les responsables publics locaux et nationaux, dont le CyberCercle qui a développé depuis plusieurs années des actions en direction des élus et des collectivités locales notamment via le Tour de France de la Cybersécurité mis en place depuis 2018.

Malgré cela, les collectivités territoriales ne se sont pas emparé du sujet et ne l'ont pas intégré dans leurs politiques publiques. Quelques exceptions existent tout de même, telles que le Pôle d'Excellence Cyber et le CSIRT maritime en région Bretagne ou, plus récemment, le Centre Ressources Régional Cyber (C2RC) en région PACA. Mais au-delà de ces singularités, les projets régionaux sont rares et aucun ne s'inscrit dans le cadre d'une stratégie de cybersécurité du territoire.

Intégrer la cybersécurité dans les politiques publiques

Quelques élus commencent cependant à évoquer ces aspects. Ainsi la présidente de la région Ile-de-France a évoqué en 2021 lors d'un point d'étape du Campus Cyber de La Défense l'idée de déployer des « casernes cyber » pour être en mesure d'intervenir au plus près des victimes. Ce dispositif viendrait compléter l'action du CSIRT régional en cours de création à Saint-Quentin-en-Yvelines. Il pourrait s'agir des prémisses d'une stratégie régionale de cybersécurité consistant à vouloir protéger nos

concitoyens des attaques cyber comme ils le sont contre les incendies ou les agressions physiques. Mais, au moment de l'écriture de ces lignes, ce concept n'a pas été détaillé, du moins pas publiquement et il n'est pas repris dans le programme de la candidate en vue de sa réélection à la tête de la région.

Au regard de l'importance de la menace cyber, il y a pourtant une réelle urgence pour les pouvoirs publics territoriaux à développer une vision ambitieuse, voire audacieuse, permettant de prendre en compte la sécurité dans l'espace public numérique au même titre qu'ils le font dans l'espace physique, dans une approche de sécurité globale telle qu'évoquée en introduction.

L'élaboration d'une stratégie territoriale de cybersécurité est un bon moyen pour les élus concernés de préciser leurs ambitions tout en impliquant les acteurs du territoire, que ce soit lors de la phase de réflexion et de conception ou lors de la mise en œuvre.

Composantes d'une stratégie territoriale de cybersécurité

Les composantes d'une stratégie territoriale en matière de sécurité numérique sont plurielles. Elle concerne en effet aussi bien les acteurs : collectivités, entreprises, artisans, commerçants, associations, particuliers, … que les infrastructures : transports, énergie, eau, capteurs de la ville connectée, etc.

Gouvernance

La gouvernance devra par conséquent être solide et pensée très sérieusement pour permettre d'adresser l'ensemble des enjeux en incluant toutes les parties prenantes. Au regard de leurs compétences respectives, l'ensemble des collectivités territoriales (Région, départements, communes) et des établissements publics de coopération intercommunale (EPCI) français à fiscalité propre (Métropoles, communautés de communes, etc.) devraient être prises en compte dans l'élaboration de la stratégie ainsi que dans sa gouvernance. Les EPCI sans fiscalité propre

pourraient également être mobilisés, ainsi que les représentants de la société civile, organisations patronales, représentants d'associations, syndicats de commerçants, etc.

L'association des maires de France et des présidents d'intercommunalité (AMF) proposait dans un guide publié en novembre 2020 de s'appuyer sur le service commun tel que permis à l'article L. 5211-4-2 du Code général des collectivités territoriales (CGCT). D'autres solutions, y compris la régie ou la délégation de service public, sont bien évidemment possibles et doivent être choisies en fonction des caractéristiques propres à chaque territoire.

Néanmoins une instance de niveau politique devra assurer la prise de décision des grandes orientations stratégiques. Elle réunirait les élus et les responsables locaux concernés pour permettre la prise en compte au plus haut niveau des enjeux opérationnels, communicationnels, organisationnels et budgétaires. Les décideurs disposeraient ainsi d'une information précise sur la situation Cyber du territoire leur permettant d'orienter leurs priorités.

Le pilotage opérationnel devra être confié à une autre instance placée sous l'autorité d'un élu référent et d'un directeur général spécialement désigné dont les principales missions seraient :
• d'informer le comité stratégique sur le niveau de risque ;
• de conduire la politique de cybersécurité ;
• de viser les dossiers d'homologation des systèmes les plus sensibles ;
• de gérer les crises.

Budget

Le coût de la cybersécurité est lourd mais celui de l'insécurité sera toujours plus élevé. En effet, après une attaque, au montant de la remédiation, qui peut inclure le changement complet du parc informatique, s'ajouteront les frais de sécurisation en urgence.

La stratégie devra s'accompagner d'un budget pluriannuel couvrant *a minima* les éléments suivants :

- les investissements en moyens de détection, de protection et de gestion de crise ;
- le fonctionnement pour rémunérer les expertises et maintenir le niveau de sécurité, mais également pour porter et animer la stratégie sur l'ensemble du territoire ;
- l'assurance et la remédiation.

Connaissance et anticipation

L'une des difficultés majeures pour appréhender la menace cyber est de parvenir à la comprendre, en suivre les évolutions et déterminer comment elle peut affecter les systèmes opérés sur le territoire.

Il est ainsi essentiel de disposer d'une veille généraliste pour informer les décideurs mais également d'une veille technique permettant de rester à l'état de l'art. Des services de veille personnalisés, adossés à un travail de cartographie des systèmes et de diagnostic de sécurité, permettront aux différents acteurs de mieux connaitre leurs besoins et de fixer leurs priorités.

Pour permettre de réagir au mieux aux attaques, il est indispensable de les détecter au plus vite. Les collectivités devraient en particulier se doter des moyens de superviser leurs systèmes mais également l'ensemble de leurs connexions avec leurs prestataires et délégataires. Les contrats, notamment les délégations de services publics, devraient systématiquement intégrer des obligations de prise en compte de la cybersécurité dans une démarche structurée découlant de la stratégie territoriale.

Un dispositif composé d'un centre de supervision territorial de type SOC (security operational center) mutualisé associé à un centre de réponse à incident (CSIRT – Cyber Security Incident Response Team) constitue la tour de contrôle permettant d'informer en permanence les équipes opérationnelles de l'état de santé numérique du territoire et de piloter la gestion des crises.

Dans le cadre du volet pour la protection des territoires du plan de relance, l'ANSSI a choisi de soutenir le développement de CSIRT au niveau

régional. Il s'agit d'un échelon raisonnable pour assurer les investissements et les coûts de fonctionnement nécessaires de ces dispositifs inaccessibles à la plupart des collectivités locales. Des fournisseurs de services privés proposent des solutions qu'ils adaptent à la taille de leurs clients mais ces services ne couvrent pas l'ensemble des besoins et ne présentent d'intérêt dans le cadre d'une stratégie territoriale que si les éléments de détection dont disposent ces entreprises sont partagés avec la structure commune de supervision.

Dans une logique de sécurité globale, la supervision mutualisée devrait inclure les communes mais pourrait être étendue aux délégataires de services publics, aux acteurs sociaux-économiques, aux infrastructures critiques, etc. Les capteurs du territoire connecté, dont la sécurisation individuelle est illusoire, pourraient également être couverts par ce dispositif ainsi que les box internet des opérateurs partenaires qui accepteraient de partager des informations anonymisées de compromission ou de tentatives d'attaques.

Réaction aux attaques sur le territoire

La menace Cyber est telle que les actions de protection permettront de la réduire mais pas de l'éliminer. Des attaques continueront à aboutir et faire des victimes qu'il conviendra d'accompagner dans leur gestion de crise et leur remédiation.

La stratégie territoriale pourra ainsi prévoir, en lien avec la préfecture et l'ANSSI, l'ensemble des moyens nécessaires à la conduite d'une crise majeure touchant le territoire, mais également un dispositif d'accompagnement à la gestion de crise pour les victimes, incluant la mise à disposition de locaux, de moyens de communication, d'outils, d'experts, etc. Ce dispositif de réaction devra s'appuyer sur un déploiement de proximité, sur le modèle des casernes Cyber envisagées en Ile-de-France. L'assistance du secteur privé sera nécessaire pour démultiplier l'effort et disposer de toutes les compétences, le secteur public ayant la responsabilité d'engager la démarche, d'organiser la coordination et d'amener ce service dans les zones les plus isolées.

Une fois l'urgence passée, les victimes sont confrontés à la reprise d'activité et à la remédiation. Or, bien souvent, elles n'ont pas miraculeusement acquis une compétence en cybersécurité pendant la période de crise. Afin de s'assurer qu'une victime qui se remet d'une attaque ne sera pas de nouveau touchée lors de sa reconnexion et pour lui permettre de repartir au plus vite dans les meilleures conditions, la collectivité peut prévoir dans sa stratégie un plan d'accompagnement incluant le prêt de matériel ou de locaux, un soutien financier et le conseil d'experts.

Développement économique et attractivité

Cet accompagnement, qui pourrait être complété par une aide aux entreprises pour se protéger et s'équiper en solutions de sécurité adaptées, favorisera l'attractivité du territoire. Les entreprises y trouveront en effet les infrastructures pour se connecter et développer leur activité en toute confiance mais également un réseau de soutien en cas d'incident. Les entreprises du domaine de la cybersécurité et de la cyberdéfense pourront vouloir profiter de cet environnement pour inventer et tester des solutions innovantes qu'elles pourront proposer à un écosystème local mature sur ces questions, stimulant dans le même temps les organismes de recherche et d'innovation.

Dans le cadre d'une politique concertée et cohérente de gestion des emplois et des compétences une bourse à l'emploi pourra être mise en place, associée à une offre de formation capable de s'adapter rapidement aux besoins.

L'expérience montre néanmoins que cet enchainement ne se fait pas de manière naturelle et qu'il doit être accompagné par des dispositifs d'aide et de communication qui devront faire partie intégrante tant de la stratégie de cybersécurité territoriale que de la politique locale de développement économique.

Sensibilisation et accompagnement du territoire

La menace cyber concerne tous les acteurs d'un territoire. La sensibilisation et l'accompagnement de la population, des commerçants,

des artisans, des associations est indispensable pour assurer la résilience du territoire. La crise sanitaire de la Covid-19 a montré l'importance des services numériques pour permettre la continuité des activités, y compris pour les besoins essentiels tels que l'approvisionnement en nourriture.

En cela les collectivités territoriales peuvent s'emparer du sujet et mettre en œuvre une politique ambitieuse d'équipement et de formation. Néanmoins, afin de ne pas se contenter de passer de Charybde en Scylla, la connexion et la numérisation de l'activité socio-économique du territoire doit se faire de manière sécurisée et avec une bonne information des utilisateurs afin de développer une capacité de résilience en cas d'attaque.

De multiples initiatives existent déjà pour réaliser cette sensibilisation auprès des jeunes et des entreprises : Education nationale, Gendarmerie Nationale, DGSI, réserve de cyberdéfense, etc. De leur côté les collectivités peuvent activer les médias locaux ainsi que le dispositif des médiateurs numériques récemment renforcé dans le cadre du plan de relance, sans oublier les réseaux des bibliothèques, médiathèques et tiers-lieux.

L'accompagnement des plus jeunes et des plus démunis permettra notamment de lutter contre le cyberharcèlement, les escroqueries en ligne, la haine sur les réseaux sociaux, la divulgation de rumeurs et fausses informations, l'addiction aux écrans, l'exposition aux contenus violents ou inappropriés et d'aider à la protection de la vie privée et à la gestion de l'identité numérique.

L'accompagnement des entreprises, commerces et associations visera ces mêmes sujets en complétant avec les questions de protection des données à caractère personnel, de rançongiciels, d'escroquerie au Président, de gestion de crise, etc.

Le rôle de la stratégie sera de coordonner ces actions sur le territoire pour s'assurer de toucher tout le monde et de la complétude des messages passés. Des aides à l'achat de produits de sécurité (antivirus, VPN, etc.) pourraient également être mises en place comme cela se fait pour l'aide à l'équipement numérique ou pour le vélo.

Intégration de la cybersécurité dans les projets et dans les contrats

Le modèle mis en œuvre au sein des ministères et des opérateurs d'importance vitale a fait ses preuves. L'intégration, au travers d'une démarche structurée de gestion du risque, de la cybersécurité dans les projets, modifie en profondeurs les méthodes de travail mais renforce la qualité de gestion des projets, améliore la connaissance des systèmes et responsabilise les acteurs, y compris les décideurs.

Ce modèle ne s'est pas encore propagé dans les collectivités territoriales. En conséquence, les projets numériques sont souvent pilotés par les métiers avec le soutien de la direction des systèmes d'information et, éventuellement, du responsable de la sécurité des systèmes d'information (RSSI) et du délégué à la protection des données à caractère personnel (DPD) selon les processus propres à l'activité concernée qui, sauf rares exceptions, n'intègrent pas la menace cyber. Dans le meilleur des cas cette question est évoquée tardivement, sans moyen alloué pour la prendre en compte, ce qui conduit à un compromis minimal dont l'efficacité est faible.

Une révolution des méthodes de travail est nécessaire au sein des collectivités pour permettre une prise en compte adaptée du risque cyber. Chaque projet ayant une composante numérique devrait faire l'objet d'une démarche d'homologation de sécurité s'appuyant sur une analyse de risques. Il ne s'agit pas de mettre en place une démarche aussi complète que pour un système traitant du classifié de défense mais tout de même de considérer que la continuité du service public, le traitement des informations des usagers, la gestion de l'eau, de l'énergie, des transports, des hôpitaux, etc. nécessitent une maitrise des risques au bon niveau. Niveau qui doit être approuvé par une autorité représentative et bien informée.

Quelle politique territoriale pour l'Etat en matière de cybersécurité ?

Avec les lois de décentralisation, l'Etat n'a pas vocation à dicter aux collectivités territoriales comment mener leurs politiques publiques. Il

peut néanmoins les orienter et les conseiller et, s'agissant de sécurité, il conserve un rôle à jouer.

En premier lieu, au travers de ses actions de sensibilisation et d'accompagnement des victimes grâce, notamment, aux actions de la Gendarmerie Nationale, de la DGSI, de l'ANSSI et du dispositif Cybermalveillance.gouv.fr, ou encore aux formations de haut niveau pour les cadres dirigeants telles que la session « Souveraineté numérique et Cybersécurité » mise en place au sein de l'Institut des Hautes Etudes de Défense Nationale (IHEDN).

Il pourra soutenir la transition organisationnelle des collectivités en les aidant financièrement comme il a commencé à le faire via le plan de relance mais également accompagner le changement au moyen d'actions de formation des agents et des élus qui pourraient être confiées au Centre National de la Fonction Publique Territoriale (CNFPT).

Cette transition pourrait également être accélérée par la contrainte réglementaire, comme cela fut nécessaire pour les organismes de l'Etat et pour les opérateurs d'importance vitale.

Pour aider à la gestion d'une attaque qui toucherait tout un territoire, ses infrastructures les plus critiques ou certains de ses services les plus sensibles le plan Piranet pourrait être complété par des plans régionaux ou départementaux sur le modèle du dispositif ORSEC (Organisation de la Réponse de Sécurité Civile).

Enfin, pour renforcer son dispositif territorial, l'ANSSI développera peut-être un jour des agences régionales de sécurité des systèmes d'information, comme d'autres agences nationales ont pu le faire pour une meilleure efficacité de proximité.

Conclusion

La cybersécurité des territoires n'est pas une option. Elle est indispensable et se place dans le cadre de la sécurité globale.
La collectivité qui s'engagera dans une politique publique de cybersécurité,

cadrée par une stratégie ambitieuse et portée par un élu audacieux sera une pionnière qui attirera les regards et les talents et servira de champs d'innovation et d'expérimentation pour construire un modèle qui inspirera d'autres initiatives au niveau national mais également international. Il ne reste qu'à attendre de découvrir qui se lancera en premier.

[1] Computer security incident response team : équipe de sécurité opérationnelle et de réponse à incident.

La Caisse des dépôts, un tiers de confiance historique qui s'engage sur le terrain de la cybersécurité

FRANÇOIS CHARBONNIER
Investisseur Confiance Numérique
Banque des Territoires - Caisse des dépôts

La Caisse des dépôts et des consignations, tiers de confiance historique, s'engage sur le sujet de la confiance numérique. La cybersécurité est une problématique majeure de la confiance numérique, qui recouvre également de façon plus large le sujet de la bonne conception des systèmes, de la gestion éthique des données et de la souveraineté numérique.

Le présent article présente l'implication de la Caisse des dépôts en matière de confiance numérique et de cybersécurité.

La Caisse des dépôts et les territoires, une histoire de confiance

L'institution Caisse des dépôts

Créée en 1816 à la Restauration dans un contexte de dette publique critique héritée des campagnes napoléoniennes, la Caisse des dépôts et consignations a pour première vocation de restaurer le crédit financier de l'Etat. A cette fin, elle est directement placée sous la surveillance et la garantie de l'autorité législative, afin d'acquérir son indépendance par rapport au gouvernement, et obtient le statut d'établissement public assurant des missions au service de l'intérêt général.

Ce rôle de confiance de premier plan s'est enrichi au fil des années d'autres missions, qui ont fait de l'institution un grand outil de gestion de l'épargne nationale.

Aujourd'hui, outre les missions qu'elle assure directement grâce à ses 6 500 collaborateurs, la Caisse des dépôts est un groupe constitué de filiales et de participations stratégiques qui interviennent dans le domaine concurrentiel. Elle est la seule institution financière en Europe à pouvoir se prévaloir de la protection du Parlement.

Acteur responsable, la Caisse et ses filiales incarnent un groupe public, investisseur de long terme engagé à réduire les inégalités territoriales et sociales pour « faire grandir la France ».

Les métiers de la Caisse des dépôts

La Caisse des dépôts organise son action autour de cinq grands métiers : retraites et formation professionnelle, gestion d'actifs, suivi des filiales et participations, financement des entreprises et soutien aux projets des territoires.

Retraites et formation professionnelle : la Caisse des dépôts est un acteur majeur de la cohésion sociale, qui assure un rôle dans la qualification professionnelle de 33 millions de Français et contribue au défi du régime universel des retraites. Elle a aussi la charge du nouveau compte personnel de formation.
La gestion d'actifs de la Caisse des dépôts lui permet de financer et d'accompagner des projets d'intérêt général sur tous les territoires. La Caisse contribue au financement de l'économie française avec une prise en compte toujours plus forte des critères environnementaux, sociaux et de gouvernance.
Les filiales et participations stratégiques : les revenus tirés des filiales et les dividendes issus des participations stratégiques soutiennent les missions d'intérêt général de la Caisse des dépôts. Elle gère son portefeuille de filiales et participations sur la base de trois critères : son intérêt patrimonial, l'intérêt à long terme des entreprises, de leurs clients et de leurs collaborateurs, et l'intérêt général.
Le financement des entreprises : Bpifrance, la banque publique d'investissement détenue à parité par la Caisse et l'Etat, a pour mission de dynamiser et rendre plus compétitive l'économie française. Partenaire de confiance des entrepreneurs, elle est l'acteur public français

incontournable du financement des entreprises et de l'innovation. La banque intervient de multiples manières : prêts, garanties, prises de participations, conseil et accompagnement.
Le cinquième métier est le soutien aux projets des territoires, au travers de la Banque des Territoires.

La Banque des Territoires

La Banque des Territoires, créée en mai 2018, regroupe les offres de la Caisse des dépôts et de ses filiales au service des territoires. Elle ancre son action dans une perspective de long terme et promeut un développement économique soutenable, préservant les intérêts des générations futures. La Banque des Territoires conclut des partenariats au service du développement des territoires avec l'ensemble des acteurs publics et privés alignés avec sa mission d'intérêt général.

Cette nouvelle bannière, déployée dans les seize directions régionales et trente-cinq implantations territoriales, réunit quatre directions et deux filiales et propose des solutions sur mesure de conseil, financement en prêts et en investissement pour répondre aux besoins des collectivités locales, des organismes de logement social, entreprises publiques locales et professions juridiques (notaires et huissiers).

Tiers de confiance historique, elle a vocation à accompagner les transitions de tout type que ses clients traversent, en particulier la transition numérique : dans cette perspective, le thème de la confiance numérique s'impose naturellement comme une problématique majeure. La Banque des Territoires se positionne sur le sujet à travers trois axes principaux :
- L'investissement dans l'innovation technologique au service des territoires : cybersécurité, identité et signature numériques, souveraineté numérique, *legaltech* ;
- La sensibilisation des acteurs territoriaux, avec la réalisation fin 2020 d'un guide et de quatre vidéos dédiés aux élus des collectivités locales ;
- La gestion en 2021, d'un mandat d'appel à manifestation « Cybersécuriser les territoires » dans le cadre du Programme d'Investissements d'Avenir (PIA).

Cybersecurité et confiance numérique : une urgence pour les territoires

L'état de la menace

L'actualité quotidienne illustre la nécessité absolue pour les acteurs territoriaux d'une vraie maîtrise du numérique, plus particulièrement sous l'angle de la cybersécurité. On ne compte malheureusement plus les exemples de villes que des cyberattaques ont momentanément paralysées. En France, ce sont plus de 1200 collectivités qui ont été la cible d'attaques en 2019, et le nombre de cyberattaques par rançongiciel a plus que doublé en 2020. Le contexte sanitaire actuel, qui a considérablement augmenté le recours au télétravail, ne fait que renforcer ces fragilités.

Il n'est pas nécessaire de détailler davantage ce bilan, que l'ANSSI et Cybermalveillance.gouv.fr savent exposer avec beaucoup de justesse.

Grandes, médianes ou petites, toutes les villes et intercommunalités sont concernées par cette problématique de confiance numérique – il en est de même pour les régions et les départements. C'est notamment le cas au travers de leurs services déjà largement digitalisés comme le sont ceux d'état civil, d'urbanisme ou encore de gestion administrative.

Cela concernera bientôt la plupart des autres services proposés par les collectivités au fur et à mesure que s'informatiseront leurs infrastructures de transport, d'énergie, d'eau, leur signalisation routière, leur éclairage, leurs systèmes de vidéoprotection, etc. Il s'agit de sécuriser les systèmes industriels, l'internet des objets, l'intelligence artificielle, autant de technologies de plus en plus diverses et pointues – et de nouvelles fragilités potentielles.

Les autres acteurs territoriaux que sont les établissements de santé et les ports sont tout aussi concernés. De plus en plus numériques, ils voient leurs missions cruciales régulièrement mises en péril par un nombre croissant de cyberattaques.
Cette question de maîtrise numérique et de protection est ainsi de plus en plus prégnante pour les acteurs des territoires.

Le défi industriel de la sécurisation des collectivités et entreprises locales

Pour faire face à cette menace, les acteurs des territoires ont à s'emparer du sujet. Nous aborderons plus loin le détail les grandes actions que les élus doivent s'approprier et porter auprès des différentes parties prenantes.

Un élément fondamental consiste bien sûr à s'équiper de solutions de cybersécurité. Cependant, il s'agit parfois d'un véritable défi, car les acteurs des territoires manquent souvent de solutions de cybersécurité adaptées à leur profil. Cette carence s'explique en ce que les solutions disponibles ne couvrent que rarement les exigences suivantes :

- être maniables par des équipes non expertes ;
- être accessibles aux budgets de toutes les entités territoriales ;
- être mutualisables avec simplicité et souplesse entre différents acteurs territoriaux.

Dans ce contexte, il apparaît nécessaire que l'innovation puisse répondre à ces exigences, dans tous les compartiments de la cybersécurité – et qu'elle bénéficie, pour ce faire, d'une capacité de financement à laquelle participe la Caisse des dépôts dans son métier d'investisseur.

Agir pour la confiance numérique au profit des territoires

Gérer des participations stratégiques

La Caisse des dépôts assure un rôle d'investisseur institutionnel, à la fois dans une logique d'intérêt général et dans le cadre de missions publiques qui lui sont confiées par l'Etat.

Au travers de sa filiale La Poste, le groupe Caisse des dépôts s'implique dans le domaine de la confiance numérique au travers de deux acteurs de référence :

- Docaposte, qui s'illustre dans de nombreux segments autour des échanges professionnels de documents, dont l'identité numérique et la signature électronique ;
- Digiposte, un coffre-fort numérique et administratif du citoyen, qui s'inscrit notamment dans la dématérialisation des bulletins de paye.

Investir dans la confiance numérique

La direction de l'investissement de la Banque des Territoires répond aux besoins des territoires en appui des politiques publiques, en investissant dans des projets de développement aux côtés d'autres investisseurs publics ou privés. Elle propose une offre de financement en matière de développement économique, de développement urbain et touristique, de cohésion sociale et territoriale, de transition énergétique et numérique.
En matière de numérique, la Banque des Territoires investit historiquement dans des projets d'infrastructures : le très haut débit est au cœur de son action, aux côtés des acteurs publics et des industriels pour aider à son déploiement dans tous les territoires. Plus récemment, la Banque des Territoires s'est également mise à travailler à l'émergence et la structuration de projets de services numériques, au service des territoires. Elle investit ainsi dans des domaines aussi variés que les territoires intelligents et durables, les services publics numériques, la e-santé, le vieillissement, le e-tourisme, la culture et la confiance numérique.

En tant qu'investisseur dans la confiance numérique, la Banque des Territoires suit quatre grands axes :

1. La confiance dans la transition numérique des territoires et la cybersécurité ;
2. Le développement de services de confiance et de services juridiques innovants ;
3. Une économie de la donnée de confiance, dans le respect du principe de consentement.
4. Enfin, un critère transverse est le respect des principes de souveraineté numérique et d'intérêt général. Il s'agit principalement de répondre aux trois objectifs suivants :
    - Maîtriser la localisation, la gestion et la propriété des données et infrastructures sensibles, face aux velléités parfois intrusives des géants du numérique ;
    - Répondre à la logique d'intérêt général visant à garantir au citoyen un univers numérique de confiance ;
    - Maintenir l'emploi en France dans le secteur de la confiance numérique et de la cybersécurité, et favoriser la structuration d'un écosystème français et européen permettant d'offrir des solutions éprouvées aux acteurs publics.

Plus particulièrement en matière de confiance numérique, la Caisse des dépôts a notamment investi dans les sociétés suivantes :
IDnomic est l'un des leaders européens en matière de protection des identités des personnes et des objets, et sécurisation des documents et transactions numériques. La société dispose d'un portefeuille de qualifications et de certifications règlementaires délivrées par l'ANSSI, permettant ainsi d'asseoir sa position de leader français sur le marché de la signature électronique et des transactions sécurisées. En 2019, la société est cédée à ATOS.

Universign est une plateforme de signature électronique commercialisée sous forme d'abonnement, dont l'activité s'inscrit dans le cadre du règlement européen eIDAS. L'entreprise vise à proposer un outil à destination des administrations, entreprises, professions juridiques et citoyens en aidant au développement de la confiance numérique globale.

Dawex est une plateforme sécurisée de monétisation et d'échange de données (marketing, commerciales, industrielles, financières, administratives…). Elle automatise et industrialise le processus de transaction d'un point de vue technique, contractuel et règlementaire, et s'adresse à tout type de client, public ou privé. Le projet comporte un enjeu territorial important car il permet la monétisation des données issues d'entreprises ancrées dans les régions et de promouvoir la connaissance des territoires (les données étant très souvent géographiques). Le service porte une attention toute particulière à la protection des données personnelles.

Qwant est un moteur de recherche européen créé en 2011 et lancé en 2013. Il entend offrir une alternative éthique aux géants américains de la recherche, en proposant un modèle économique qui ne repose pas sur le profilage publicitaire de ses utilisateurs ou la monétisation des données personnelles. Qwant s'inscrit dans une logique de souveraineté européenne et d'intérêt général.

AgDataHub est une plateforme souveraine d'échange et valorisation de données agricoles créée dans le cadre de projets de recherches portés par les acteurs du secteur et le ministère de l'agriculture. AgDataHub s'inscrit

dans une éthique qui vise à laisser aux producteurs de données le contrôle sur ces données, dans l'esprit d'un « RGPD de la donnée agricole ».

S'adresser aux élus locaux

La Banque des Territoires a publié en novembre 2020 un guide sur la confiance numérique, pratique et pédagogique, à destination des élus des collectivités. Il vise avant tout à convaincre les élus du rôle crucial qu'ils ont à jouer en la matière, quel que soit leur niveau de connaissance du numérique, et à leur donner les principes clés à promouvoir auprès de leurs équipes et partenaires.

Le guide les informer et les plonger dans différentes situations pour leur permettre d'appréhender le sujet, les enjeux en matière de risques et de responsabilités juridiques, et les premiers réflexes à mettre en œuvre pour offrir aux citoyens des services de confiance. L'élu, plus spécifiquement, doit demander que la confiance numérique soit prise en compte selon les cinq grands axes suivants :

1. **Formation :** la formation ou la sensibilisation, non seulement des agents, mais également des élus ;
2. **Etat des lieux numériques :** l'entretien d'une connaissance à jour des systèmes et outils numériques auxquels recourt, directement ou indirectement, la collectivité ;
3. **Stratégie et priorités en matière de numérique :** une réflexion sur les nouveaux projets numériques à mener qui n'occulte pas les nécessités de mise à niveau du numérique existant ;
4. **Nouveaux projets numériques fiables et pérennes :** une exigence de fiabilité (qualité de conception, niveau de sécurité) et de pérennité (maintenance, maîtrise de la dépendance technologique à un ou plusieurs prestataires, capacité de réaction en cas de crise numérique, etc.) ;
5. **Préparation au pire :** se préparer à la crise numérique – que préparer pour mieux faire face au cas où les ordinateurs ne redémarrent plus, où des données sont volées, où des services municipaux ne fonctionnent plus, où des infrastructures (signalisation routière, eau, transport) dysfonctionnent ?

Ce guide a été conçu avec le soutien précieux d'associations d'élus, d'industriels et d'administrations, dont l'ANSSI et Cybermalveillance.gouv.fr.

S'impliquer dans la stratégie nationale pour la cybersécurité et le programme d'investissement d'avenir

Stratégie nationale pour la cybersécurité, un volet clé pour le renforcement des territoires

Le 18 février 2021, le Président de la République a annoncé une stratégie nationale pour la cybersécurité, qui mobilisera jusqu'à un milliard d'euros dont plus de sept cents millions portés par le financement public.

Déclinée en six objectifs clés, l'ambition de cette stratégie est de permettre une forte croissance de la filière française de cybersécurité, qui permettra de faire rayonner la France dans une concurrence internationale accrue, et de permettre le doublement des emplois de la filière.

Sans surprise, la stratégie vise notamment à stimuler la recherche et l'innovation industrielle françaises en matière de cybersécurité. En parallèle, la diffusion et une meilleure appréhension des enjeux de cybersécurité dans les entreprises et les administrations, adossée aux outils innovants dont l'émergence aura été favorisée par la stratégie, permettra d'optimiser leur sécurité numérique. Enfin, le renforcement de l'offre de formation des jeunes et des professionnels aux métiers de la cybersécurité est une priorité désormais clairement établie.

Les collectivités et acteurs des territoires ne sont pas délaissés. Deux actions clés sont à évoquer. La première consiste en un budget de 136 millions d'euros confiés à l'ANSSI, afin de renforcer la cybersécurité de l'Etat et des territoires sur la période 2021-2022. Un dispositif et des aides financières permettront d'améliorer la sécurisation des collectivités locales et établissements de santé, tandis qu'un accompagnement sera dispensé pour faire émerger des CSIRTs régionaux (Computer Security Incident Response Team), afin de mieux fédérer au niveau régional la réponse aux cyberattaques qui frappent les acteurs territoriaux.

Enfin, dans le cadre du Programme d'Investissement d'Avenir, un appel à manifestation d'intérêt « Cybersécuriser les territoires » est opéré par la Banque des Territoires pour le compte de l'Etat.

Appel à manifestation d'intérêt « Cybersécuriser les territoires »

L'objectif du projet global est de stimuler l'émergence d'une offre de cybersécurité adaptée aux besoins et spécificités des territoires.

Ce projet global s'échelonne en deux phases. La première, l'appel à manifestation d'intérêt (AMI), s'adresse aux collectivités locales, établissements de santé et infrastructures portuaires, pour qu'elles expriment des besoins de solutions innovantes de cybersécurité – c'est-à-dire, des solutions qui ne sont pas disponibles « sur étagère » à l'heure actuelle. Il n'y a pas de financement associé à cette phase, qui vise uniquement à sélectionner des besoins pertinents en matière de cybersécurité. Lancé le 18 mars 2021 et opéré par la Banque des Territoires, l'AMI devrait sélectionner au moins trois dossiers lauréats.

La seconde phase consistera, pour chaque besoin sélectionné dans le cadre de l'AMI, à monter un appel à projets adressé aux industriels pour répondre au besoin de l'acteur territorial. Les appels à projets seront co-construits par l'Etat et les candidats lauréats de l'AMI. Cette seconde phase repose sur une enveloppe d'une vingtaine de millions d'euros, qui serviront à financer sous forme de subvention jusqu'à 50 % des dépenses d'innovation des projets retenus.

Les candidats lauréats de l'AMI devront être prêts à porter le projet durant la deuxième phase, en co-construisant avec l'Etat les appels à projets qui suivront puis en participant au projet d'innovation avec le ou les industriels retenus.

Les enjeux de la sécurité numérique pour les collectivités françaises : prévenir, former et agir

MIREILLE CLAPOT
Députée de la Drôme
Présidente de la Commission Supérieure du Numérique et des Postes

Parce qu'elle est composée de députés et de sénateurs[1], élus de circonscriptions urbaines, de zones rurales ou de montagnes, la Commission supérieure du numérique et des postes (CSNP) est en prise directe avec les enjeux de la sécurité numérique dans nos territoires.

La CSNP est peu connue de nos concitoyens alors que notre Commission a pour mission de contrôler les activités liées au numérique et aux activités postales. Elle rend des avis et des recommandations, après audition, saisie ou mission d'information. Ses avis sont adressés au gouvernement, aux administrations et autorités indépendantes.
C'est à ce titre qu'elle a rendu un avis le 29 avril 2021 portant 27 recommandations dans le domaine de la sécurité numérique[2].

Alors que les attaques dans l'espace numérique se sont multipliées à un rythme quasi-exponentiel ces deux dernières années partout dans le monde et que tous les experts auditionnés par notre Commission nous ont fait part de leurs inquiétudes, les membres de la Commission supérieure ont souhaité que plusieurs mesures soient intégrées à la stratégie nationale pour la cybersécurité, présentée par le Président de la République le 18 février 2021, et pilotée par le Secrétaire d'État chargé de la Transition numérique et des communications électroniques.

Le plan d'accélération cyber apporte un certain nombre de réponses à des besoins identifiés en mobilisant des financements importants –1 milliard d'euros dont 720 millions de financements publics – qui devraient permettre de réduire les vulnérabilités des systèmes informatiques de nombreuses infrastructures publiques et privées.

Les membres de la CSNP considèrent qu'une stratégie nationale pour la sécurité dans l'espace numérique ne peut se limiter au seul plan d'accélération cyber, aussi nécessaire soit-il : le niveau global de la sécurité dans l'espace numérique dont l'État français, les services publics nationaux, les collectivités territoriales, les entreprises et nos concitoyens ont désormais une absolue nécessité de renforcer leurs capacités de lutte contre la cybercriminalité.

Compte tenu de la gravité d'une situation sécuritaire qui ne cesse de se dégrader dans l'espace numérique, la CSNP a souhaité formuler un certain nombre de recommandations concrètes portant sur les cinq champs de progrès identifiés :
• Le renforcement de la lutte contre la cybercriminalité ;
• Les points d'amélioration du plan cyber ;
• La stratégie de cyberdéfense de l'État français ;
• La sécurité des produits et services numériques ;
• Le développement du cloud de confiance.

Plusieurs recommandations concernent les collectivités locales parce qu'elles sont transversales (renforcement des moyens judiciaires et policiers, création d'un cloud de confiance, formation et renforcement de la filière sécurité) mais, encore une fois, parce que nos membres sont des élus de terrain, la CSNP s'est clairement exprimée pour un renforcement de la sécurité numérique des collectivités locales.

Un constat : aujourd'hui, la sécurité numérique des collectivités locales parait nettement insuffisante

En matière de cybersécurité et de sécurité numérique, le risque zéro n'existe pas et n'existera jamais.

Les géants du numérique sont eux même vulnérables : Microsoft a annoncé, en mars 2021, avoir été victime d'un groupe de hackers baptisé "Hafnium" qui a exploité les failles de sécurité dans ses services de messagerie Exchange pour voler les données de dizaines de milliers d'entreprises, villes et institutions locales aux États-Unis.

Côté pouvoirs publics, les réseaux les mieux protégés sont également victimes d'attaques en France ou à l'étranger.

Qu'en est-il des collectivités locales françaises ? La multiplication et l'ampleur des attaques récentes contre des métropoles ou des villes de taille moyenne (Marseille, Angers, …) laissent imaginer que les collectivités de tailles plus modestes sont également très vulnérables. Le profil de la cybercriminalité a évolué et toutes les collectivités locales sont potentiellement menacées. A l'heure où les rançongiciels se monnayent sur le *dark web*, particuliers, entités publiques ou privées peuvent être attaqués pour des motifs crapuleux.

Finalement la question n'est pas de savoir si une collectivité locale peut être victime d'une cyberattaque mais plutôt quand et, plus utilement, comment pourra-t-elle y répondre.

Jusqu'à présent les moyens de l'État et de l'ANSSI se sont concentrés sur la protection des opérateurs d'importance vitale (OIV) et des opérateurs de service essentiel (OSE).
Or, les collectivités locales ne font pas partie des OIV ni des OSE.

Dans le cadre de son plan de relance, l'État a mobilisé une enveloppe de 60 millions d'euros spécifiquement dédiés aux collectivités territoriales mais le dispositif ne concerne que les grandes collectivités : seules les collectivités qui disposent d'un responsable de la sécurité des systèmes d'information (RSSI) pourront bénéficier d'un appui de l'ANSSI. Une centaine seulement de collectivités locales répondent à cette exigence.

Pour les collectivités locales et les établissements publics dont les moyens humains, techniques et financiers sont limités, l'ANSSI les incite à "*mutualiser* " leurs ressources pour se doter de compétences en la matière et « *un plan de sensibilisation est en cours de finalisation avec l'appui de la Gendarmerie nationale* ». Les gendarmes du pôle national de lutte contre les cybermenaces, unité spécialisée créée en 2019 qui compte actuellement 5000 agents et qui pourrait passer à 7000 agents en 2022, devraient réaliser des actions de sensibilisation en collaboration avec l'Association des Maires de France (AMF).

Dans l'immédiat, l'État renvoie les élus locaux vers www.cybermalveillance.gouv.fr pour s'initier à la formation et à la sécurisation du système d'information.

Par ailleurs, le plan d'accélération cyber prévoit le déploiement dans chaque région d'un CSIRT (*Computer Security Incident Response Team* - équipe de réponse aux incidents informatiques) incubé avec le soutien de l'ANSSI. Ces CSIRT doivent permettre de réagir plus rapidement et efficacement aux incidents cyber qui peuvent frapper les collectivités territoriales, les structures du tissu sanitaire (hôpitaux, cliniques) et les acteurs du tissu économique local.

La CSNP recommande que la création des CSIRT en région se fasse en étroite concertation avec les collectivités territoriales à l'échelle régionale

Dans son avis n°03/2021 du 29 avril 2021, la CSNP recommande notamment la création dans chaque région d'un campus régional de la sécurité numérique capable de fédérer localement les acteurs de la sécurité numérique, de les faire travailler en réseau, et de sensibiliser l'écosystème public et privé à ces problématiques.
Ce campus pourrait héberger le CSIRT incubé par l'ANSSI et ainsi constituer un véritable relais de gouvernance régional pour l'ANSSI, au service de tous les départements d'une même région pour un maillage territorial efficace.

La création de ces campus régionaux pourrait s'appuyer sur l'article L4251-13 du Code général des collectivités territoriales portant sur la nouvelle organisation territoriale de la République, et être inscrite dans les schémas régionaux de développement économique, d'innovation et d'internationalisation.

Pour les membres de la Commission, cette proposition a vocation à constituer :
- Une ressource pour les élus en recherche de solutions opérationnelles,
- Une instance de gouvernance qui permet de capitaliser sur l'existence et le développement de ressources locales et régionales en matière de sécurité numérique et de cybersécurité,

- Une enceinte de coordination des différents services de l'État et des collectivités locales impliquées dans la sécurité numérique,
- Une instance de taille critique pour s'assurer du déploiement des solutions sur l'ensemble du territoire.

Nous ne pouvons pas laisser sans recours les millions de citoyens qui vivent en dehors de la centaine de municipalités pouvant recourir aux services de l'ANSSI.

La période pré-électorale de mai-juin 2021 se prêtait peu aux échanges sur ces schémas avec les principaux intéressés.

Pourtant il y a urgence et je me félicite que la plupart de ces recommandations de la CSNP aient été endossées début juin par nos collègues du Sénat[3]: au-delà des clivages partisans, il est important de ne pas perdre de temps dans la lutte contre le cybercrime.

Dès que les nouveaux exécutifs régionaux se mettront en place, il importera d'aborder ce sujet rapidement : si la région Ile de France pourra compter dès la fin de l'année sur le Campus Cyber qui sera installé dans le quartier de La Défense, des actions devront être entreprises sans attendre le déploiement de ses éventuels « satellites » en région.

La création du Campus Cyber, associant le public et le privé, permettra de présenter une véritable vitrine du savoir-faire français où les grands acteurs du secteur (Atos, Orange, Cap Gémini …) côtoieront des petites et moyennes entreprises, tout en favorisant la fertilisation croisée et l'émergence d'un écosystème avec des solutions souveraines.

L'idéal serait bien sûr que le Campus Cyber crée des émules et que chaque région puisse disposer d'un campus de la sécurité numérique ou, quel que soit le nom qui sera retenu, d'un lieu qui puisse réunir ou cordonner en région l'écosystème public et privé de la cybersécurité. L'initiative peut revenir aux collectivités les plus entreprenantes en la matière, sur la base de cette dynamique.

Un défi : une formation des élus et des agents des collectivités locales à la sécurité numérique

Pour lutter efficacement contre la cybercriminalité, la CSNP recommande qu'un effort tout particulier soit engagé en faveur de la sensibilisation et la formation aux enjeux de la sécurité numérique et de la cybersécurité au profit des élus et agents publics, notamment ceux qui sont employés dans les plus petites structures, particulièrement vulnérables.

A cette fin, les clés du succès seront, outre des ressources financières, la mise en place d'une offre de formation de qualité s'inscrivant aussi bien dans le cadre de la formation initiale que dans le cadre de la formation continue.

Les associations représentatives des collectivités locales se sont déjà engagées dans cette voie : les efforts doivent s'accélérer. Toutes les collectivités européennes doivent relever ce défi et le dialogue entre collectivités françaises mais également avec des collectivités européennes nous semble un facteur d'accélération absolument nécessaire : apprenons des succès et des échecs de chacun.

La commande publique des collectivités locales : un levier supplémentaire pour renforcer la sécurité numérique ?

Dans son avis du 29 avril 2021, la CSNP préconise que l'État prenne une part plus active à la consolidation de la filière cybersécurité française en mobilisant d'avantage le levier de la commande publique au niveau national et européen et propose même de modifier, si nécessaire, la directive 2014/25/UE du 26 février 2014 relative à la commande publique des opérateurs de réseaux. Il s'agirait notamment de permettre aux opérateurs de réseaux, dont les achats de produits et services de cybersécurité sont généralement soumis à cette directive, d'orienter leurs achats en la matière auprès de fournisseurs nationaux et européens.

A minima, les membres de la Commission considèrent que la cybersécurité pourrait entrer dans le champ d'exclusion de l'application

de la directive au profit des OIV (Opérateurs d'Importance Vitale) et OSE (Opérateurs de Services Essentiels) afin de leur permettre d'accéder à des solutions de confiance.

Cette recommandation formulée pour la commande publique de l'État est sans doute transposable à la commande publique des collectivités locales que ce soit dans la politique de choix du cloud, des datacenters, des logiciels…

A performance comparable, cette prise en compte de la souveraineté et de la sécurité peut constituer une solution renforçant notre souveraineté numérique et une promotion des entreprises françaises performantes dans le domaine de la cybersécurité et de la sécurité numérique.

En effet, l'accélération de la numérisation de nos territoires constitue un enjeu de sécurité mais également un enjeu économique fort avec des gains de performance et de compétitivité non négligeables pour les entreprises innovantes proches des territoires.

La question peut se poser par exemple pour les datacenters de proximité qui se développent sur notre territoire. Ce développement correspond à un besoin : le volume des données à conserver, traiter et exploiter décuple tous les six ans.

Selon Infranum[4], les élus locaux, en liaison avec les entreprises de leur territoire, sont ou seront amenés à étudier si un datacenter de proximité pourra répondre à un besoin exprimé localement. Tout ce qui peut préserver une plus grande sécurité et notre souveraineté nous semble devoir être encouragé.

Plusieurs options se présentent pour les collectivités : location de baies dans un datacenter existant, construction d'un datacenter public dédié aux collectivités et acteurs publics ou construction d'un datacenter public également ouvert aux acteurs privés.

Le législateur aura à se pencher sur les conséquences juridiques de ces choix, notamment au regard des règles de responsabilité et il conviendra

sans doute d'en préciser les contours, car les collectivités locales n'ont pas toujours les compétences et les outils pour effectuer les bons choix à long terme.

Le rôle des collectivités locales dans le renforcement du niveau de sécurité numérique global auprès de nos concitoyens

Par leur proximité évidente avec nos concitoyens, les collectivités locales sont des acteurs essentiels dans l'augmentation du niveau général de la culture numérique et donc de la sécurité numérique auprès de l'ensemble de la population.

C'est déjà le cas au sein des Espaces France Service qui vont pouvoir compter sur les 4000 conseillers numériques dont le gouvernement a annoncé le recrutement et la formation en novembre 2020, qui devraient être opérationnels au cours des prochains mois.

Au-delà de la détection et de l'accompagnement des 13 millions de français éloignés du numérique, les conseillers numériques et les agents des Maisons France Service, dès lors qu'ils sont eux-mêmes correctement formés, peuvent diffuser les bonnes pratiques et les bons réflexes auprès de nos concitoyens.

En liaison avec les chambres de commerce et d'industrie et les chambres des métiers et de l'artisanat qui mettent à disposition des boîtes à outils à destination des artisans et des petites et moyennes entreprises, les collectivités locales peuvent efficacement jouer un rôle de conseil auprès de leur tissu économique local.

Le développement des plateformes de e-commerce locales peut constituer des pistes de développement alternatives pour le tissu économique local. L'État s'est engagé à apporter un soutien immédiat de 20 000 € par commune[5], ce qui permettra d'accompagner les collectivités locales dans la mise en place de ces solutions, pour un montant total de 60 millions d'euros.

Nous ne disposons pas encore du recul nécessaire pour mesurer leur impact sur l'activité économique dans nos territoires mais il est certain que ces développements doivent se faire en intégrant d'ores et déjà des mesures suffisantes en termes de sécurité numérique.

A tous ces égards, la sécurité devrait être une préoccupation constante dès l'amont de l'accompagnement à la numérisation : acquisition de bons réflexes tels que changement régulier des mots de passe, choix judicieux des matériels et logiciels, sauvegardes régulières, prévention des hameçonnages, réactivité en cas d'attaque, … La collectivité locale, grâce au capital de confiance dont elle dispose, peut et doit transmettre les bonnes pratiques à ses administrés les plus éloignés du numérique, comme aux plus avertis, et être exemplaire en la matière.

En réalité, avec le développement sans précédent de la cybermenace, c'est un véritable changement de paradigme que nous devons adopter : au niveau individuel, en tant que citoyen, au niveau des acteurs économiques et politiques.

Les collectivités locales vont sans nul doute jouer un rôle essentiel dans cette transformation et doivent s'en donner les moyens.

Le cybercrime est international mais les cybervictimes sont locales : organisons-nous rapidement et efficacement !

[1] https://csnp.fr/composition/
[2] https://csnp.fr/wp-content/uploads/2021/05/Avis-n2021-03-du-29-avril-2021-portant-recommandations-sur-la-se%CC%81curite%CC%81-nume%CC%81rique.pdf
[3] Rapport d'information de MM. Sébastien MEURANT et Rémi CARDON, n° 678 (2020-2021) - 10 juin 2021
[4] https://infranum.fr/lancement-du-guide-pratique-le-datacenter-de-proximite/
[5] https://bpifrance-creation.fr/entrepreneur/actualites/aide-financiere-numerisation-petites-entreprises

Collectivités territoriales : le RGPD continue d'infuser…

FRANÇOIS COUPEZ
Avocat à la Cour
DPO certifié agrément CNIL

Devant l'explosion de la génération de données, aujourd'hui nécessaires à la conception, à la mise en œuvre et à l'évaluation des politiques publiques, les collectivités territoriales et leurs élus font face aux défis de l'utilisation efficace mais également licite de ces données, qu'elles soient nouvellement générées ou déjà existantes, mais nouvellement exploitées. Ces usages nécessitent d'abord et avant tout l'identification des données, leur catalogage et leur qualification juridique, afin de déterminer si et comment les règles concernant l'open data (Loi pour une république numérique, etc.) ou encore la protection des données à caractère personnel (RGPD, loi informatique et libertés, etc.) sont susceptibles de s'appliquer.

Si l'on se concentre sur ce dernier texte en particulier, on ne peut que constater que les effets de l'adoption du Règlement Général sur la Protection des Données (RGPD), qui vient de fêter ses 5 ans, ne cessent de s'amplifier et de concerner de plus en plus de situations opérationnelles.

Certains ont pourtant cru à l'époque que ce texte[1] ne changerait qu'à la marge la protection des données à caractère personnel, et que ces règles seraient vouées à une inobservation majoritaire, comme elles l'ont largement été depuis 1978.

Pourtant, cela n'a pas été le cas. Outre le montant important des sanctions prévues, le RGPD doit très certainement sa réussite au fait qu'il a été réfléchi et créé pour assurer une conformité en « halo », imposant en pratique aux différentes entités et acteurs économiques de n'interagir qu'avec des partenaires commerciaux (sous-traitants, etc.) eux-mêmes conformes. S'étendant en cercles concentriques au niveau des acteurs

concernés, il concerne des pans de plus en plus larges des activités économiques. L'actualité récente montre ainsi à quel point le monde de la publicité sur internet est percuté par ce texte alors, même que le RGPD n'était pas censé s'y appliquer directement. C'était en effet le rôle dévolu à sa sœur jumelle, le règlement eprivacy[2], qui devait plus spécifiquement concerner les courriers électroniques, les cookies et autres metadata et qui devait supposément être adopté en même temps que le RGPD. Privé de ce texte essentiel dont on annonce seulement sa négociation au niveau des trilogues européens, le RGPD n'en a pas moins continué seul son chemin et tracé de nouvelles voies, réécrivant les définitions structurantes et forçant les régulateurs européens à réinterpréter les règles existantes concernant les cookies.

Au niveau du secteur public en général et des collectivités territoriales en particulier, l'évolution issue du RGPD est là aussi en œuvre. Même si la conformité n'est pas encore généralisée et que de très importants efforts restent à faire, on ne peut que constater les années-lumière de progrès parcourues ces dernières années. Alors qu'avant, la loi de 1978 était souvent ignorée de nombre de décideurs et que l'on avait parfois la curieuse impression que son respect n'était assuré que par quelques moines-soldats ostracisés luttant contre des moulins à vent, force est de constater l'évolution considérable accomplie.

Les différents acteurs n'ont en effet pas ménagé leurs efforts pour faire en sorte que le texte « infuse » auprès de tous. En 2019, la publication par la Commission Nationale de l'Informatique et des Libertés (CNIL) du guide de sensibilisation au RGPD[3], auxquels ont participé de grands acteurs territoriaux et des associations essentielles en la matière (AMRF, AMF, ANDAM, ADF, Régions de France, la DGCL et l'AFCDP)[4], donnait une première vision transversale des problématiques à l'œuvre au niveau des collectivités locales.

En application du RGPD qui prescrit l'obligation de nommer un Délégué à la Protection des Données (ou DPO pour Data Protection Officer) pour chaque entité du secteur public, le nombre de DPOs effectivement nommés continue ainsi à augmenter. Le verre à moitié plein conduit à considérer qu'il est heureux que les collectivités nomment un tel DPO en

application de ce texte. À ce titre, il est heureux de constater qu'au niveau des départements en particulier, les désignations des DPOs sont aujourd'hui acquises ou sur la voie de l'être pour la totalité d'entre eux. Le verre à moitié vide est, quant à lui, lié au fait que l'on retrouve encore parfois à l'occasion des DPOs mutualisés auprès de plusieurs centaines de collectivités, faisant perdurer le mythe du DPO omniscient et omnipotent…

Quant à la CNIL, elle multiplie ou renouvelle ces dernières années les partenariats avec les associations d'élus pour promouvoir la culture « Informatique et libertés » et réhausser le niveau de conformité des collectivités territoriales : le 6 novembre 2019 avec l'Association des Maires de France et l'Assemblée des Communautés de France, le 16 septembre 2020 avec Régions de France, le 8 décembre 2020 avec l'Assemblée des Départements de France (renouvellement), etc.

Le but est de fournir un appui juridique et technique dans les situations les plus complexes et d'apporter son soutien de façon plus globale aux associations d'élus, charge à celles-ci d'apporter aux différentes collectivités territoriales qu'elles représentent les éléments centraux permettant la mise en conformité que sont :

- La définition de procédures de gouvernance et de pilotage de la conformité des acteurs impliqués dans la mise en conformité et le suivi dans le temps de celle-ci (relations DPO, Responsable des Systèmes d'information et Direction générale, conditions de réalisation d'audits internes, modalités de gestion des réclamations et des demandes des personnes exerçant leurs droits) ;
- La cartographie des traitements conduisant à produire des registres génériques recensant les traitements les plus usuels ;
- Et un guide pour les traitements les plus à risque (fiches méthodologiques, modèles d'analyse d'impact sur la protection des données/PIA, mise en place de modèles de conventions organisant les échanges de données entre les départements et des partenaires nationaux).

De façon plus globale, sur l'ensemble des éléments fondamentaux nécessaires à la mise en œuvre de la conformité en la matière, nous nous

permettons de reprendre ici ce que nous indiquions déjà dans notre article « Le RGPD : Acte II » en 2019[5] sur les piliers fondamentaux (organisationnel, technique et juridique) nécessaires à la mise en œuvre efficace des principes découlant du RGPD :

- cartographie des traitements existants ;
- identification des données traitées ;
- identification des acteurs de l'écosystème traitant les données (sous-traitants, fournisseurs, etc.), des lieux à partir desquels les données sont accédées et qualification de leur rôle au regard du traitement des données personnelles ;
- encadrement juridique approprié des relations économiques avec ceux-ci ;
- construction et sécurisation de traitements orientés « *privacy by design* » ;
- détermination des fondements légaux permettant leur traitement ;
- création / mise à jour d'un registre des traitements, d'un registre des sous-traitants et d'un registre des violations de données à caractère personnel ;
- transparence des informations à communiquer ;
- documentation de l'ensemble de la chaîne de traitement et des décisions prises ;
- nomination obligatoire de DPOs pour les entités du secteur public ;
- réalisation d'études d'impact sur la vie privée dans les cas où les traitements ont les conséquences les plus graves pour les personnes ;
- création des processus de notification des violations de données personnelles ;
- etc.

Depuis cette époque, il nous semble surtout important de préciser ici que l'appréciation de la conformité a indéniablement gagné en maturité : l'enjeu n'est heureusement plus de savoir si un fournisseur de service est nécessairement un « sous-traitant » au sens du RGPD[6], ni s'il peut n'être que responsable de traitement s'il n'est pas sous-traitant. L'appréciation plus précise des concepts conduit aujourd'hui à analyser de façon beaucoup plus approfondie les qualifications et déterminer en pratique ce qui était encore honni il y a quelques mois : y a-t-il des co-responsables de traitement dans la salle ?

Alors que de 2018 à 2020, nous constations en pratique que, dans les dossiers dans lesquels nous intervenions, les qualifications essentielles en

matière de traitement de données personnelles[7] n'avaient pas été analysées et que les mises en conformité réalisées s'avéraient en conséquence à reprendre en quasi-totalité, 2021 nous montre que les choses évoluent. Le constat, partagé par les praticiens, montre en effet que les fondamentaux sont peu à peu acquis et que la mise en conformité s'adresse aujourd'hui à des problématiques effectivement les plus complexes.

De même, alors qu'une pénurie de DPOs était apparue et que la conformité demandait des bras :

- les régulateurs des pays européens étaient moins regardants sur le niveau de qualification réelle, comptant sur leur montée rapide en compétence,
- ou encore reconnaissant qu'un DPO puisse réaliser des registres de traitements ou prendre la responsabilité des notifications de violation, faisant fi du texte pourtant extrêmement clair du RGPD redéfinissant le rôle des anciens CILs « faiseurs » en DPO « contrôleurs ».

Là également, le gain en maturité conduira les DPOs nommés à peu à peu voir leurs fonctions se redessiner pour intégrer pleinement leur rôle d'auditeur de la conformité, sous peine de voir les sanctions pour conflits d'intérêts se multiplier (cf. par analogie avec la décision du régulateur belge du 28 avril 2020).

Et les exemples de ce type sont encore nombreux, allant du registre de traitement dont la seule existence était saluée comme un accomplissement à un registre exhaustif accompagné le cas échéant d'un registre de sous-traitance et du registre de notification des violations de données. La question de la réalisation des Analyses d'Impact relative à la Protection des Données (AIVP ou PIA pour Privacy Impact Assessment) en est une des dernières illustrations en date. Il est malheureux que des instruments aussi utiles pour la conformité n'aient été que trop souvent mis de côté en raison d'une complexité supposée (découlant seulement du fait qu'un PIA bien réalisé est souvent le signe d'une conformité solide et approfondie et qu'en bâtir depuis une conformité mal maîtrisée est un dangereux exercice d'équilibrisme).

À cet égard, on rappellera que la CNIL a officiellement sifflé la fin de la récréation pour fin mai 2021, mettant fin à sa période de tolérance en la

matière. On ne peut que souhaiter la systématisation de ces PIA et donc leur réalisation effective quand ils sont rendus nécessaires, soient très fréquemment en pratique.

Si la conformité au RGPD ne doit pas être vue à notre sens comme une fin en soi, loin de là, elle conduit à s'interroger sur la relation entretenue avec la « personne concernée », soit la personne dont on collecte et traite les données personnelles. Là encore, certaines notions qui restent encore solidement ancrées brouillent la perspective, telle que la notion de « data owner », d'origine organisationnelle, mais qui laissent supposer de façon parfaitement erronée qu'une entité serait « propriétaire » des données à caractère personnelles de ses clients ou salariés par exemple, alors que ces données ne lui ont été que confiées.

Heureusement, pour les collectivités territoriales, ce biais semble moins fréquent que pour les entreprises de droit privé, du fait sans doute de la relation habituelle avec l'administré et de la relation citoyen qui doit être à l'origine du traitement des données de celui-ci. D'autant que l'e, axe important de modernisation de l'action publique, répond a`une demande effective des citoyens dans le cadre de l'e-deḿocratie, et que le respect des regl̀es de protection des donneés a`caracterè personnel par les collectiviteś est un facteur fondamental de transparence et de confiance a`l'eǵard des usagers, mais aussi du personnel qui y travaille.

En 2019 dans notre article précité, nous soulignions le fait que l'engagement dans un process de conformité au RGPD nécessitait une dynamique portée par les élus, un chef de projet référent, un travail en collaboration avec l'ensemble des services, parfois l'accompagnement d'experts extérieurs de confiance, et un engagement sur le long terme afin de faire de cette réglementation un véritable atout pour les collectivités, et que tout le monde (administrés et collectivités territoriales) devait sortir gagnant de cette conformité.

Force est de constater que la dynamique est enclenchée dans un nombre toujours plus important de collectivités territoriales et que chaque acteur semble s'y atteler avec toujours plus d'énergie. Il n'en reste pas moins que des efforts importants demeurent nécessaires et qu'une composante

importante de la conformité ne semble pas aussi avancée que ceux que nous avons pu mentionnés aussi, au moins si l'on en croit l'actualité médiatique récente. Ainsi, la sécurité des systèmes d'information, pierre angulaire du dispositif, est encore très souvent perfectible. Et alors que les téléservices administratifs ouverts aux citoyens ne font que se multiplier, le Référentiel Général de Sécurité (RGS), cadre règlementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens, applicable depuis déjà de nombreuses années[8], n'est encore que très peu respecté à l'heure actuelle. Or, juridiquement, il est parfaitement possible de considérer que des manquements aux règles de sécurité minimale prévue par le RGS puissent être sanctionnés comme des manquements aux règles de sécurité dont le principe est prévu par le RGPD[9]…

Dès lors, les collectivités territoriales qui n'auraient pas encore pris à bras le corps l'importance de la sécurité des systèmes d'information sont le signe que le RGPD a besoin d'infuser plus longtemps chez certains que d'autres pour être compris et (parfaitement ?) intégré. D'autant qu'en embuscade, les nouvelles thématiques juridiques sont nombreuses (intelligence artificielle, etc.) et s'appuient, elles aussi, sur les mêmes fondamentaux.

[1] Adopté le 27 avril 2016, le RGPD est applicable depuis le 25 mai 2018 en remplacement de la directive 1995/46 du 24 octobre 1995 « *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* ».

[2] Ce projet de réglementation, prévu pour être adopté à l'origine en même temps que le RGPD, n'en est, cinq ans plus tard, qu'au tout début de l'étape des trilogues au niveau européen.

[3] https://www.cnil.fr/sites/default/files/atoms/files/cnil-guide-collectivite-territoriale.pdf.

[4] Rappelons que l'AMRF est l'Association des maires ruraux de France, l'AMF est l'Association des maires de France, l'ANDAM est l'Association nationale des directeurs d'associations de maires, l'ADF est l'Assemblée des départements de France, la DGCL est la Direction générale des collectivités locales et l'AFCDP est Association française des correspondants à la protection des données à caractère personnel.

[5] Publié dans la Lettre Territoires de Projet n°5 Hiver 2019, édité par l'ANPP.

[6] cf. en ce sens la fiche « l'impact du RGPD sur le droit de la commande publique » du 25 octobre 2018 émanant de la Direction des affaires juridiques (DAJ) du ministère de l'économie (https://www.economie.gouv.fr/files/files/directions_services/daj/marches_publics/conseil_acheteurs/fiches-techniques/preparation-procedure/impact_RGPD_droit_Commande_Publique.pdf) qui ne mentionnait que l'hypothèse d'un fournisseur forcément « sous-traitant » au sens du RGPD. En ce sens, les nouveaux CCAG publiés au JO du 30 mars 2021 tels que le CCAG-TIC prévoit de nouvelles dispositions sur le RGPD en leur article 5.2, mais ne mentionnent jamais clairement que le « prestataire » peut être « responsable de traitement » tel que défini dans le RGPD !

[7] Quel est l'un des six fondements légaux utilisés pour le traitement ? Qui est responsable de traitement, sous-traitant, responsable conjoint, responsable disjoint, tiers autorisé ? etc.

[8] Le référentiel général de sécurité est pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives.

[9] Contrairement à la majorité des sanctions financières prévues dans le RGPD d'un montant de 4% du Chiffre d'Affaires globales mondialisé ou 20 Millions d'euros (le plus important des deux montants étant retenu), la sanction maximale serait ici de 2% du Chiffre d'Affaires globales mondialisé ou 10 Millions d'euros (le plus important des deux montants étant retenu).

La cybersécurité n'est plus une option pour nos Territoires de projet !

JOSIANE CORNELOUP
Présidente
Association Nationale des Pôles d'équilibre territoriaux
et ruraux et des Pays (ANPP)
Députée de Saône-et-Loire

Sarrebourg, Évreux, Bayonne, La Rochelle, Angers, Houilles, Annecy, Aix-Marseille-Provence… autant de collectivités qui ont été victimes de cyberattaques ces derniers mois. La liste ne cesse de s'allonger à un rythme qui s'accélère depuis un an, notamment avec la digitalisation accentuée de nos modes de travailler, de consommer, de produire, de vivre tout simplement. Paralysie des services, pertes et fuites de données, rupture du lien de confiance avec les citoyens, image dégradée… autant d'impacts majeurs qu'une cyberattaque réussie entraîne pour une collectivité.

Aujourd'hui, la question n'est donc plus de savoir "si" les collectivités seront la cible d'une cybermalveillance, mais "quand" : toutes sont concernées par cette menace en plein développement, quelles que soient leur taille et leur localisation géographique. Il est donc aujourd'hui indispensable de se doter d'une politique de cybersécurité cohérente et d'en faire un axe de leur culture, afin de sécuriser leurs missions au service des citoyens et habitants et des acteurs économiques présents sur leur territoire.

Alors même que le numérique devient de plus en plus omniprésent dans nos sociétés, la crise sanitaire que nous traversons actuellement a accéléré ce phénomène de transformation profonde, auquel n'échappent pas les collectivités. Nombre d'entre elles se sont engagées dans un processus de modernisation continue de leur administration et des services qu'elles délivrent. Que ce soit sous l'impulsion des citoyens ou de la réglementation, elles sont au tournant de la numérisation de la "relation

citoyen" : l'e-administration (numérisation des démarches administratives, à laquelle s'ajoute une recherche de simplification) est un axe important de la modernisation de l'action publique et répond à une demande effective des citoyens dans le cadre de l'e-démocratie. Elles détiennent par ailleurs une masse importante de données, parmi lesquelles des données à caractère personnel, dont la divulgation, la suppression, l'altération, le vol, la mauvaise utilisation sont susceptibles de porter atteinte aux droits et libertés des personnes ou à leur vie privée, ou à une mauvaise gestion de l'ensemble des responsabilités sociétales dont les collectivités ont la charge : état-civil, justificatifs de domicile, données fiscales, sociales, inscriptions en établissement scolaire, résultat de vote électronique, études foncières, projets de délibérations, schémas d'aménagement, documents budgétaires… En dehors de la réglementation, notamment le RGPD, la protection de ces données est ainsi non seulement un facteur de bon fonctionnement de la société mais aussi un élément de transparence et de confiance à l'égard des citoyens.

Au-delà de cet enjeu de protection des données, la cybersécurité est également au cœur des infrastructures que gère une collectivité : gestion de l'eau, des déchets, des systèmes de l'éclairage public, des infrastructures sportives, vidéosurveillance, mobilité intelligente, écoquartiers… autant de systèmes gérés par le numérique et le développement d'objets connectés qui se doivent d'être sécurisés, car exposés. Par exemple, la tentative récente avortée de sabotage via une attaque informatique du réseau de distribution d'eau de collectivités aux Etats-Unis en février dernier montre s'il en était besoin combien l'enjeu de la sécurisation de tels systèmes est impérieux.
Au-delà, les collectivités se sont lancées dans des plans de développement via le numérique au service des acteurs présents sur leur territoire : plan d'accompagnement à la transformation numérique des acteurs économiques, des commerçants aux industries, de développement de la e-santé ou de l'industrie 4.0, programmes d'inclusion numérique, création de tiers lieux, accompagnement au déploiement du télétravail… Autant d'actions fondamentales aujourd'hui pour l'attractivité et le développement des territoires, mais qui constituent autant d'espaces vulnérables.

Cette transformation numérique profonde des collectivités opérée pour

leurs propres infrastructures, induit de fait de nouveaux risques : face aux menaces numériques, la cybersécurité n'est plus une option. Or, la dimension sécuritaire n'est généralement pas suffisamment prise en compte dans les démarches de transformation numérique des collectivités, qui ne sont souvent orientées que vers les usages.

L'enjeu est donc de mieux sensibiliser et surtout éclairer sur les enjeux liés à cette menace, de faire de la sécurité un pilier majeur de la transformation numérique des collectivités et de leurs plans d'actions, et d'hisser cet enjeu comme étant un élément phare de la culture numérique de l'ensemble des élus et des collaborateurs.

La cybersécurité souffre en effet de son image technocratique et lointaine, jusqu'au jour où l'on est concerné. Elle est souvent vue comme un sujet purement technique, réservé à des experts. Cependant ce sujet, quand il est pris en compte et anticipé par les collectivités, est souvent enfermé dans la tour d'ivoire du service informatique, qui a bien souvent du mal à mettre ses recommandations en œuvre tant cette dimension est perçue au mieux comme accessoire ou frein à la mise en œuvre du développement des projets, au pire comme un seul facteur de coût.

Or la sécurité numérique n'est pas uniquement un sujet technique. Elle repose avant tout sur de la gouvernance, du management, de l'organisation, de la sensibilisation, de la formation, du juridique, de relations avec l'ensemble de l'écosystème d'une collectivité : prestataires, partenaires… autant de dimensions qui sont hors de la simple sphère "informatique". Elle repose sur le facteur humain et à ce titre concerne l'ensemble des collaborateurs d'une structure : en matière de cybersécurité, l'adage veut que le maillon faible se situe entre le clavier et la chaise. Plus de 80% des incidents de sécurité relèvent d'une erreur humaine. Mais ce qui montre aussi que l'humain bien formé peut devenir le maillon fort de la cybersécurité.

Face à ce phénomène de transformation numérique des collectivités, au recours au numérique comme facteur de développement des territoires, la sécurité numérique doit devenir un élément clef au cœur de l'action des collectivités, avec deux impératifs : que l'ensemble des élus s'approprient

cette dimension dans leur vision stratégique de l'avenir des collectivités qu'ils dirigent, seuls capables d'insuffler l'impulsion nécessaire pour une politique de sécurité numérique transverse ; qu'elle devienne un des piliers de la culture de chaque agent, dans les missions qu'il conduit ou de ses usages des outils numériques.

Aujourd'hui, il ne peut y avoir de développement responsable et d'attractivité des territoires sans numérique, pas de numérique pérenne sans confiance numérique, et pas de confiance numérique sans sécurité numérique. C'est bien là que réside l'un des enjeux majeurs d'une transition numérique responsable.

La réussite de la transformation numérique des collectivités, c'est la cybersécurité

DR MICHEL DUBOIS
Directeur scientifique et technique
Groupe La Poste

Samedi 12 octobre 2019, il est 1 heure du matin. Dans la salle serveur, un équipement se met à clignoter plus rapidement : un processus vient de s'activer. En quelques minutes le ransomware se propage de serveurs en postes de travail, chiffrant tous les fichiers qu'il croise sur son passage. Samedi 12 octobre 2019, il est 1h10. L'agglomération Grand Cognac a perdu près de 400 postes de travail.

Ce scénario pourrait appartenir au monde des séries policières. Même s'il a été volontairement romancé, il relève de la vraie vie et de vrais attaques subies par de plus en plus de communes françaises. Ainsi, et pour ne retenir que les attaques les plus médiatiques, ce sont les villes du Grand Annecy, de La Rochelle, de Marseille, de Martigues, de Besançon, de Vincennes et d'Angers qui subiront un sort similaire en 2020 et en 2021. A leur corps défendant, les directeurs des systèmes d'informations (DSI) et les responsables de la sécurité des systèmes d'information (RSSI) de ces communes sont aujourd'hui familiers de concepts comme bitcoins, demande de rançons, rançongiciel, plan de continuité d'activité (PCA), résilience, Pyza, Mespinoza...

Etant donné l'étendue des dégâts causés et l'importance de l'impact sur la vie des citoyens de ces communes, nous pouvons légitimement nous demander si ces attaques sont évitables. La réponse est sans appel : non, ces attaques ne sont pas évitables. Aujourd'hui, il s'agit plus de se demander "quand allons-nous être la cible d'un ransomware" que "vais-je être la cible d'un ransomware". Ce raisonnement étant malheureusement valable pour les menaces les plus courantes que sont le phishing, le ransomware, l'arnaque au président ou le vol de données...

Cet état de fait est concomitant à la transformation numérique, souvent à marche forcée, de notre société.

En 2013, dans un rapport intitulé "les territoires numériques de demain", le président de l'Association des départements de France, Claudy Lebreton, pointait l'étendue des champs de l'action publique pour lesquels le numérique apporterait des évolutions marquantes : développement économique des territoires, méthodes de travail dans la fonction publique, efficacité énergétique, éducation et enseignement, santé, accès aux services publics... Aujourd'hui, le numérique s'est imposé partout et il a d'une manière ou d'une autre, transformé le domaine dans lequel il est intervenu, parfois même de manière fondamentale.

Pour les collectivités publiques, le numérique est un nouveau levier pour le pilotage des politiques publiques et il facilite leur adaptation à la variété des situations rencontrées. En particulier, il offre de nouvelles formes d'accès aux services et enrichit la relation aux citoyens : il rend possible la mise en oeuvre d'une relation omnicanale, en proposant un accès renouvelé par tous les canaux disponibles (physique, numérique, itinérant). Il ouvre également des opportunités de maîtrise accrue des services publics en transformant les dispositifs de gouvernance, de contrôle et de suivi.

En février 2018, le Gouvernement s'est engagé à promouvoir cette transformation afin qu'à l'horizon 2022 toutes les démarches administratives soient accessibles par le canal numérique. Ainsi, pour atteindre une administration numérique et inclusive à cette échéance, le moment est venu pour toutes les communes, quelle que soit leur taille, de bâtir et de proposer une relation omnicanale aux citoyens.

Le numérique est un levier pour transformer la relation aux citoyens en apportant son lot de défis et d'opportunités.

En effet, les champs d'application du numérique ne cessent de s'étendre tant les bénéfices de ses technologies sont capables de faciliter notre vie quotidienne. Aussi, l'action publique s'est-elle emparée de cette ressource

en tant que levier d'un renouvellement de son organisation, puis d'amélioration des services proposés aux citoyens. Mais ce mouvement laisse aussi entrevoir des situations contrastées, car l'appropriation de ces outils numériques n'est pas homogène. Au risque de nouvelles inégalités, ce sont de nouvelles fractures qui apparaissent avec le développement du numérique. Ainsi, 70% des Français jugent prioritaire le développement de l'e-administration et 88% se disent prêts à utiliser les services en ligne de l'administration (Source : Baromètre Digital Gouv' 2017 d'IPSOS pour Sopra-Steria). Mais, dans le même temps, près de 40% des Français se trouvent toujours en difficulté face aux outils numériques (Source : WeTechCare et Capgemini - décembre 2017).

Dans notre organisation administrative, la porte d'entrée de proximité dans l'univers administratif, pour les citoyens, c'est en tout premier lieu la mairie. Au moment ou`certaines collectivités modifient l'amplitude horaire d'accès à leurs lieux d'accueil, il y a un intérêt évident à accroitre l'accessibilité aux services en recourant au numérique. C'est d'ailleurs le choix que nombre d'entre elles sont amenées à faire. De fait, grâce au numérique, les administrations publiques deviennent des opérateurs omnicanals. La gestion de cette relation devient plus complexe et le besoin d'accéder à des outils performants de gestion cette relation se fait jour. D'ores et déjà, les budgets des DSI traduisent cette évolution puisqu'ils sont en croissance marquée : ils auraient augmenté de plus de 5 % en 2018.

Pour permettre le développement du numérique dans les services publics, les collectivités doivent prendre en compte de nouveaux paradigmes : open-data, code des relations entre le public et l'administration (CRPA), saisine par voie électronique, dématérialisation des actes et documents administratifs, paiement dématérialisé, intelligence artificielle, smart city... Autant de défis nécessitant de s'approprier un environnement numérique en transformation, de gérer ses impacts sur l'organisation des services et de transformer le service rendu aux citoyens.

Aujourd'hui, force est de constater que la transition numérique des communes est déjà bien engagée. Ainsi, 57,2% des communes disposent d'un site Web sur Internet avec un taux d'équipement allant de 50,5%

pour les communes de moins de 2000 habitants à 91,3% pour les établissements public de coopération intercommunal (EPCI). Or, le site internet est la première brique fonctionnelle qui permet à une collectivité de rendre accessibles des services par voie dématérialisée. Le critère du site internet représente donc un premier niveau d'équipement permettant à une collectivité de se conformer au principe de saisine par voie électronique (SVE), puisqu'il permet d'offrir aux usagers du service public local une voie d'accès et de saisine dématérialisée de l'administration.

Au-delà du site internet, l'accessibilité des services en ligne sur des smartphone ou des tablettes doit être garantie. En effet, les études relatives aux usages d'Internet montrent que les Français sont désormais plus nombreux à utiliser un terminal mobile plutôt qu'un ordinateur pour accéder à des services en ligne. Or, pour garantir la pleine accessibilité d'un site internet sur un terminal mobile, le site doit offrir une consultation confortable, sur des écrans de tailles très différentes, sans avoir recours au défilement horizontal ou au zoom avant/arrière. Cette capacité, offerte par les technologies de responsive web design (RWD), sont peu implémentées par les sites internet des communes avec seulement 48% des sites pleinement accessibles sur un terminal mobile.

Autre domaine d'importance concernant les sites internet des communes : l'attention particulière qui doit être portée à l'hébergement des données publiques. En effet, les données des collectivités territoriales sont soumises, dès leur création, au régime particulier des archives publiques. Cela recouvre notamment : les supports papier numérisés, les documents bureautiques issus de logiciels de traitement de texte, le contenu des bases de données et les courriels reçus ou transmis par l'administration. En outre, les archives publiques ont qualité de trésor national, ce qui leur impose un régime de circulation contraignant : elles ne peuvent sortir du territoire douanier français. Or, les collectivités locales sont nombreuses à recourir à un hébergement non sécurisé avec des situations à risque liées au nom de domaine et à l'hébergement des données.

Ainsi, plus de trois communes sur dix ont un hébergement qui présente des risques ou qui s'avère non conforme du point de vue des règles applicables aux données publiques. Ces non-conformité sont par exemple :

l'utilisation de sous-domaines appartenant à des tiers, l'absence de traçabilité sur les données hébergées en ligne, l'absence d'information légale sur l'hébergement des données, le recours à des serveurs basés en dehors du territoire national. Dans ces situations, la collectivité n'est pas en mesure de contrôler la gestion ou le stockage des données qui sont publiées et hébergées via son site internet.

Au travers de ce rapide focus sur l'hébergement des sites internet, nous commençons à apercevoir les enjeux et à la complexité de la transformation numérique des collectivités locales. Héberger un site Web est un premier pas, les étapes suivantes de la délivrances de téléservices, de la mise en oeuvre du télépaiement, du déploiement du compte citoyen, sont autant d'enjeux complexes et néanmoins cruciaux de cette transformation numérique.

Une transformation numérique réussie est un processus qui maintient le lien de confiance entre le citoyen et sa collectivité. Cette confiance numérique ne peut exister sans la garantie de la sécurité des services numériques. En un mot, la réussite de la transformation numérique c'est la cybersécurité.

La cybersécurité se décline en trois volets. La cyberprotection décrivant les mesures de sécurité à mettre en oeuvre pour protéger le système d'information. La cyberdéfense qui traite des mécanismes de réponses aux incidents survenant sur le système d'information. Et enfin, la cyber-résilience qui regroupe les concepts de plan de continuité informatique (PCI) et plan de reprise informatique (PRI), tout partie intégrante des plan de continuité et de reprise d'activité (PCA et PRA).

En résumé, la cybersécurité a pour but de protéger le patrimoine informationnel de la collectivité. La valeur du patrimoine informationnel peut être appréciée au regard des opportunités qu'il offre quand on l'utilise correctement et des conséquences négatives dans le cas contraire. Le patrimoine informationnel naît, vit et disparaît dans le cadre des différents systèmes d'information qui le traitent. Ceux-ci ont un but, des moyens, et sont organisés pour créer, exploiter, transformer et communiquer le savoir (informations) et le savoir-faire (fonctions, processus...). Ils sont par

nature complexes, changeants et interfacés avec d'autres, chacun ayant ses propres contraintes. Enfin, ces systèmes d'information sont confrontés à des vulnérabilités (configuration, bugs...), ils évoluent constamment et sont liés les uns aux autres. Il est donc nécessaire d'employer des moyens rationnels pour appréhender la protection du patrimoine informationnel de manière à la fois globale et dynamique.

Pour la collectivité locale, la mise en oeuvre de la cybersécurité doit donc débuter par une analyse des risques pesant sur son patrimoine informationnel. Le risque zéro n'existant pas, cette analyse des risques est fondamentale. En informatique, le risque est la possibilité de survenue d'un événement indésirable qui génère un préjudice portant atteinte à l'un des composants du système d'information ou de son environnement, par exemple : la perte ou le vol de données, la dégradation d'un service pouvant aller jusqu'à l'arrêt du système, les conséquences juridiques ou en termes d'image.

Une analyse de risques est un processus d'identification, d'évaluation et d'estimation de chaque composante du risque - vulnérabilité, menace, impact et probabilité - liée au système d'information. Cette analyse permet à la collectivité de déterminer quel niveau de risque est acceptable pour elle au regard des impacts de la concrétisation d'une menace. Elle peut alors prendre les mesures adéquates pour couvrir les risques jugés inacceptables et protéger ainsi ses biens et services essentiels, à commencer par les données.

Une fois ces bases théoriques posées, il reste la mise en pratique effective. Réaliser une analyse des risques sur un système d'information est relativement facile à conceptualiser mais bien plus complexe à mettre en oeuvre. Un serveur est un système d'information, le service Web ou la base de données qu'il héberge sont également des systèmes d'information. Le réseau qui interconnecte les postes de travail au serveur est à son tour un système d'information. Nous voyons bien que la dimension fractale de la notion de système d'information peut très vite devenir insurmontable. D'où l'importance de définir précisément le périmètre sur lequel notre analyse des risques va porter. Heureusement, il existe des méthode facilitant le déroulement du processus d'analyse des risques. La norme

ISO/CEI 27005 décrit les grandes lignes d'une gestion des risques. De même, la méthode d'expression des besoins et identification des objectifs de sécurité (EBIOS) est un outil complet de gestion des risques informationnel.

Une collectivité qui a cartographié ses systèmes d'information et en a réalisé l'analyse des risques dispose d'un excellent niveau de maturité en cybersécurité. Il ne lui reste plus qu'à obtenir la certification ISO 27001 et elle sera parée à contrer toutes les cyberattaques. Malheureusement ce graal est rarement atteint et semble difficilement accessible au regard de la prise en compte réelle du risque informationnel.

En revenant à l'exemple des ransomwares cités en introduction, nous prédisions que la survenue des cyberattaques était inévitable. Au regard de la complexité et de la criticité des systèmes d'informations des collectivités locales, il apparaît que le risque est bien réel et que le manque de prise de conscience de ce risque est grave. Heureusement, la situation peut rapidement s'améliorer par l'application de principes aussi simples que cruciaux.

En tout premier lieu, la cybersécurité, comme tous les autres domaines de la sécurité, est un processus dynamique d'amélioration continue basé sur l'humain. L'humain est le maillon fort de la cybersécurité car c'est sur son intelligence, sa conscience professionnelle, sa vigilance et sa sagacité que repose l'efficacité des mesures de sécurité. S'appuyant sur une gouvernance forte, il est donc fondamental que, de l'édile à l'agent de la voirie, tous les agents de la collectivité soient sensibilisés et formés aux enjeux de la cybersécurité.

Après le volet organisationnel et humain, **le deuxième élément de prise en compte du risque informationnel est éminemment technique.** Nous l'avons abordé, le domaine des systèmes d'information est le royaume de la technique. Il est donc tout naturel que les processus visant à sécuriser ces systèmes d'information le soient également. Cependant, un principe prévaut en cybersécurité, c'est le retour aux fondamentaux. En paraphrasant Nicolas Boileau, nous pourrions dire que "ce qui se conçoit bien se construit simplement, et les mesures pour le sécuriser arrivent

aisément". Autrement dit, plus une architecture est complexe, plus elle est difficile à sécuriser, ou encore, une bonne politique de mots de passe vaut mieux que toutes les appliances achetées à prix d'or. En résumé, appliquer les règles d'hygiène de l'ANSSI suffit à sécuriser efficacement un système d'information.

Quand nous parlons de cybersécurité, le décalage entre l'impact dramatique d'une cyberattaque et la simplicité des mesures de sécurité à mettre en oeuvre, choque souvent. Ce décalage est inhérent au monde du numérique, tout y est plus immédiat, plus facile et plus interconnecté : le simple clique d'un agent sur la pièce jointe d'un email semblant être légitime, suffit à déployer le ransomware qui va se propager sur le réseau et le rendre indisponible pendant des semaines. Et pourtant, la mesure de sécurité est simple, il eut suffi que l'agent, correctement sensibilisé, ne clique pas.

Remettre le citoyen au centre des échanges : un impératif pour réussir la transformation numérique des collectivités, en confiance

FABIEN FERRAZZA
Directeur secteur public
Docaposte

Au cours de mes années opérationnelles passées au service de l'État et de collectivités territoriales, j'ai acquis la conviction forte que seule une combinaison intelligente des services numériques et physiques permettra de relever le défi numéro 1 de la transformation de l'action publique : remettre le citoyen au centre des échanges et lui simplifier la vie, tout en facilitant le travail des agents. La crise sanitaire récente et la démocratisation du télétravail n'ont fait que renforcer cette conviction.
C'est dans cet objectif que Docaposte, référent de la confiance numérique en France, accompagne l'État, les opérateurs spécialisés, les organismes sociaux et les acteurs du secteur public local (collectivités territoriales, bailleurs sociaux, chambres consulaires) dans la mise en œuvre de grands chantiers de modernisation de l'action publique. Nous sommes également leur partenaire au quotidien pour adapter les services aux nouveaux usages, aux nouvelles organisations et aux changements réglementaires.

Les enjeux du secteur public

Le secteur public, à tous les échelons, se transforme pour répondre à 4 enjeux principaux :
- optimiser la dépense publique,
- simplifier et donner plus de flexibilité à l'organisation interne au bénéfice des agents qui rendent le service public,
- améliorer la qualité du service apporté aux citoyens
- contribuer à l'inclusion numérique.

Les problématiques peuvent varier car chacun des trois versants de la

fonction publique – Etat, Territoriale et Hospitalière – avance à sa vitesse, en fonction de son budget, des ressources déployées et de son métier. Cependant, de manière générale, ils partagent les mêmes attentes.

En effet, le fonctionnement des administrations françaises coûte plus cher que celui d'autres pays européens qui obtiennent pourtant des résultats équivalents ou supérieurs aux nôtres. C'est pourquoi l'un des grands enjeux est de faire de la France l'un des États numériques les plus armés en termes de technologies, d'efficacité et d'agilité mais aussi de compétitivité. Bien sûr, les acteurs publics attendent une réduction des coûts mais celle-ci ne peut se faire sans embarquer les agents de la fonction publique. La force de frappe de notre administration ce sont eux, pas seulement les technologies ! Il n'y a pas de digital sans humain et inversement. D'où l'importance, au sein des administrations, d'impliquer les ressources humaines et les agents et d'adopter une réelle conduite du changement.

Enfin, il est essentiel d'inclure les citoyens dans cette transformation en assurant l'accessibilité des services numériques publics. Ces derniers ne sont pas encore assez inclusifs et les citoyens le constatent. Selon le dernier bilan de l'Observatoire de la qualité des démarches en ligne, sur 250 démarches administratives, 25% ne sont pas réalisables en ligne. De même, il faut répondre à la problématique de complexité des démarches. C'est pour lever ce frein que l'État a prévu le dispositif « Dites-le nous une fois », qui a le mérite d'être clair : dès lors qu'une des branches de l'État dispose d'une information sur l'usager (coordonnées le plus souvent), l'échange doit se faire directement entre les services publics concernés pour éviter aux utilisateurs de ressaisir les mêmes données à chaque connexion. Pour les services publics, le gain économique est aussi un argument, la multiplication des étapes impliquant l'ajout de modules de vérification d'identité représente un coût non négligeable. Ainsi, tout le monde y gagnera : les coûts pourront être rationalisés et la relation avec le citoyen n'en sera que plus fluide.

Cependant, force est de constater qu'il subsiste des freins internes à cette mutation. D'une part, certains services en ligne ne se démocratisent pas car ils sont jugés trop compliqués ou fastidieux par les agents (pour

s'authentifier par exemple). D'autre part, il n'existe pas encore de cohérence nationale en ce qui concerne l'attribution des ressources des différentes administrations : d'aucuns ont tendance à éviter l'externalisation quand d'autres, en particulier la fonction publique territoriale et les agences sous tutelle, vont, au contraire avoir tendance à externaliser les ressources. Le cas échéant, il est essentiel que l'externalisation de ces ressources bénéficie à des acteurs européens, garantissant une conformité réglementaire et une souveraineté des données, ce qui est encore loin d'être le cas.

Notre engagement est donc de simplifier la vie des citoyens et le travail des agents grâce à une offre complète de solutions phygitales couvrant l'ensemble de la chaîne de confiance numérique, pour une administration et un service public repensés, s'appuyant sur des solutions de dématérialisation omnicanal, sur mesure ou prêtes à l'emploi, faisant appel à tout le panel des savoir-faire de Docaposte.

Pour ce faire, nous nous appuyons sur une double proposition de valeur :

- **Optimiser le fonctionnement interne des administrations** par des solutions numériques et physiques, éprouvées et robustes, garantissant une maîtrise des coûts et une haute qualité de service.

- **Améliorer la gestion de la relation citoyen** en proposant des solutions digitales et physiques aux opérateurs publics nationaux et locaux pour délivrer des services de proximité assistés par des outils numériques, avec la garantie de service d'un tiers de confiance.

L'exemple du numérique éducatif

Pour illustrer ce propos, je vous propose d'aborder l'exemple du numérique éducatif.
Avec l'accélération des usages numériques, les acteurs de la communauté éducative, qu'ils soient élèves, professeurs, parents, agents ou personnels d'encadrement, sans oublier les collectivités territoriales, les associations et tous les autres acteurs éducatifs, doivent répondre à de nouvelles attentes et relever de nouveaux défis. Docaposte a prouvé sa légitimité sur le terrain

de l'éducation en mettant en place au mois de mars 2020, en un temps record, un dispositif complet pour assurer la continuité pédagogique des 200 000 élèves en situation de déconnexion numérique « Devoirs à la maison ». Ce dispositif comprenait une plateforme numérique et documentaire sécurisée d'envoi des devoirs et une solution de numérisation des devoirs retournés par courrier, pour en permettre la consultation par les établissements pendant la période du confinement. 50 000 familles ont pu bénéficier de ce dispositif.

Avec l'acquisition d'Index Éducation, éditeur du logiciel PRONOTE et premier partenaire numérique de l'Éducation nationale, Docaposte a poursuivi sa diversification dans le secteur de l'EdTech pour accompagner l'accélération des usages numériques à l'école. Dédié aux établissements de l'enseignement secondaire, PRONOTE est aujourd'hui utilisé par plus de 16 millions de personnes, soit 2 milliards de connexions en 2020. A destination à la fois des enseignants et des familles, PRONOTE gère toute la vie scolaire : cahier de texte, compétences, absences, QCM, notes, infirmerie, sanctions, stages, messagerie…

Docaposte accélère également le déploiement du numérique dans l'enseignement du premier degré en permettant, grâce à PRONOTE Primaire, à la direction de l'école et aux enseignants de se libérer des tâches administratives chronophages, d'accéder rapidement aux informations essentielles, et surtout de centraliser la communication avec les familles : gestion de l'emploi du temps, des plannings, des absences et des résultats scolaires… . PRONOTE et PRONOTE Primaire sont donc deux outils à double vocation : simplifier le travail des enseignants et fluidifier les relations avec les familles.
Au-delà, PRONOTE Primaire est le lien direct entre les parents d'élèves, l'école et leur commune. Via PRONOTE Primaire, la mairie (globalement, les collectivités sont pleinement impliquées, au-delà de l'Éducation Nationale) peut diffuser des informations aux parents d'élèves et échanger des données avec l'école : inscriptions périscolaires, demandes de travaux de l'école, etc. Ainsi, l'ensemble des services scolaires, périscolaires et de cantine sont mis à la disposition des parents.

Avec ces solutions, Docaposte veut garantir un numérique responsable et

souverain, l'égalité des chances par l'inclusion numérique et la confiance dans le système éducatif.

La confiance au cœur des usages

En effet, dans un contexte où le numérique est devenu incontournable pour toutes les organisations et où il s'inscrit dans le quotidien des citoyens, garantir la confiance sur l'ensemble de la chaîne de valeur dans le traitement de la donnée, est au cœur des enjeux numériques.

Les enjeux de la confiance :
- Réconcilier, sécuriser et pérenniser la donnée physique et digitale
- Opérer la donnée dans un environnement organisationnel, humain, technologique, juridique, sécurisé, maintenu et pérenne
- Prévenir le risque lié à la gestion des données et aux exigences règlementaires, juridiques et normatives

3 étapes fondamentales composent cette chaîne de valeur :
- l'identification : assurer la fiabilité d'une identité
- la transaction : assurer la sécurisation des flux
- la conservation : assurer l'hébergement des données et leur pérennité

La confiance ne peut pas être une option, elle est le socle de toute proposition de la part des prestataires de services de confiance qui évoluent dans le monde numérique.

Docaposte prolonge dans le monde numérique la promesse de la confiance portée historiquement par La Poste dans le monde physique, en mettant sa chaîne de services de confiance au service des entreprises et des institutions publiques, pour qu'elles puissent disposer d'un ensemble de solutions numériques interopérables facilitant la vie digitale de leurs clients et administrés.

Face aux enjeux de la transformation numérique qui sont ceux des collectivités aujourd'hui, Docaposte s'affirme comme un acteur de confiance grâce à une infrastructure "Made in France", une offre numérique et documentaire adaptée à leurs besoins, et un dialogue de proximité.

Cybersécurité : les collectivités territoriales face à quatre défis majeurs

RÉMY FÉVRIER
Maître de Conférences au CNAM
Ancien officier supérieur de la Gendarmerie Nationale

Longtemps les collectivités territoriales se sont très clairement estimées à l'abri de cyberattaques, qui étaient envisagées par la plupart des élus locaux comme des menaces lointaines et exclusivement tournées vers les grandes entreprises ou les administrations centrales, notamment en lien avec la Défense Nationale. Après avoir décliné en 2010, pour la première fois, le concept d'Intelligence Economique à destination des collectivités territoriales afin de les encourager à s'approprier les outils et concepts afférents pour mieux valoriser leurs atouts[1], sans toutefois rencontrer le moindre écho de la part de l'ensemble des pouvoirs publics, nous récidivions en alertant, dès 2013, sur l'impréparation flagrante de ces mêmes collectivités face aux menaces cyber[2], sans plus de succès… Mais il est vrai qu'à l'époque aucune cyberattaque d'envergure n'avait encore ciblé ce type d'organisation. Ce qui ne manqua pourtant pas d'arriver quelques années plus tard avec deux cyberattaques massives contre les villes de Baltimore[3] et Florida Beach en 2019. Il est triste de constater que dans notre pays, la notion d'anticipation tend à disparaitre et que l'on agit essentiellement *a posteriori*, une fois le péril survenu alors même qu'il eut été plus cohérent, mais aussi plus économique, de prendre véritablement en compte l'ensemble des signaux faibles. Or, si les crises ont toujours constitué des opportunités majeures pour des escrocs et malfaisants de toute nature, force est de constater que la crise du Covid-19 constitue un véritable changement de paradigme en matière de cyberattaques[4].

En janvier 2015 déjà, dans la droite ligne des attentats contre Charlie Hebdo et l'Hyper Cacher, plus de 20 000 portails web, dont plusieurs centaines de sites Internet de collectivités, avaient fait l'objet d'attaques de la part de hackers sympathisants d'organisations terroristes jihadistes.

Toutefois, dans l'immense majorité des cas, ces intrusions se trouvaient limitées à des attaques de bas niveau (défacement de sites). Seules des collectivités ne disposant pas d'un suivi que l'on pourrait qualifier de minimal furent touchées et virent leur page d'accueil remplacée par des messages à la gloire des terroristes. Cette première alerte demeura également lettre morte et ces dernières se trouvèrent donc fort dépourvues lorsque la Crise du Covid-19 entraina une vague d'attaques sans précédent contre les centres de soin et les collectivités territoriales. Ainsi, en l'espace de quelques mois, des collectivités aussi dissemblables que Besançon, Toulouse, la Métropole Aix-Marseille-Provence, Angers, Douai, Chalon-sur-Saône, La Rochelle, Houilles ou plus modestes comme Argenton-sur-Creuse et Morières-Lès-Avignon ont toutes été victimes d'attaques informatiques plus ou moins sophistiquées. Force est donc de constater qu'aujourd'hui, profitant de l'absence d'anticipation évoquée plus haut, les collectivités territoriales de toutes nature (Communes et EPCI[5]) sont dorénavant devenues des cibles de choix pour un ensemble de cyberpirates. Toutefois, il serait erroné et contre-productif de réduire ce phénomène, qui selon toute vraisemblance n'est pas près de s'arrêter, à de « simples » attaques de type ransomware (rançongiciel), de défaçage. Selon nous, il ne s'agit là que de la partie visible d'un spectre d'attaques bien plus large et il convient de prendre en compte le fait qu'une collectivité territoriale moderne se doit de relever quatre défis majeurs en termes de sécurisation de ses Systèmes d'Information (SI) sous peine de connaître des désagréments bien pire que ceux connus depuis plusieurs mois.

Le premier défi relève de l'évidence et revient à optimiser la sécurisation des SI internes afin d'éviter les attaques virales susceptibles de provoquer le chiffrement des unités de stockage (ransomware) ou encore les attaques par déni de service distribué (DDoS) qui visent à saturer les capacités de connexion des serveurs distants afin de les rendre inaccessibles.
Ce type d'attaque, devenu classique, se traduit par la prise de contrôle à distance de plusieurs centaines de milliers, voire de millions d'ordinateurs à travers le monde, à l'insue de leur propriétaire : le virus va utiliser une très faible partie des ressources des ordinateurs connectés de manière à demeurer indétectable. Une fois l'infection réalisée, un ordre d'attaque

(préprogrammé ou non) part de l'ordinateur du pirate, agissant comme un serveur « Command & Control » à destination de l'ensemble des ordinateurs « zombies » et qui va provoquer l'attaque finale, à savoir la saturation d'un serveur cible incapable d'absorber un nombre de requêtes simultanées aussi élevé. Face à cette menace, en plus d'indispensables précautions d'ordres matériels ou logiciels (à l'image de la mise en place d'une DMZ[6] ou encore d'IDS[7]), il existe des services spécialisés auxquels n'importe quelle organisation publique ou privée peut faire appel. Ainsi, le Centre de lutte contre les criminalités numériques (C3N) de la Gendarmerie Nationale a désinfecté à distance plus de 85 0000 ordinateurs zombies corrompus par le malware « Retadup » en 2019. Ces exemples d'attaques devenues classiques doivent faire l'objet de toute l'attention des DSI des collectivités, y compris dans les cas où la Sécurité des Systèmes d'Information (SSI) est confiée à un prestataire extérieur, qu'il soit privé (SSII) ou public (DSI d'un EPCI en charge des SI de collectivités de taille plus modeste et dans l'incapacité financière d'assumer seule la sécurisation de leurs SI respectifs). Malheureusement, une collectivité territoriale moderne doit faire face à d'autres menaces et cet état de fait est largement ignoré de nombreux dirigeants d'exécutifs locaux, alors même que ces dernières sont de nature à induire leur mise en cause personnelle sur le plan civil, voire pénal…

Le deuxième défi auquel sont confrontées les collectivités territoriales est étroitement corrélé à l'appétence des Français pour la démocratie électronique.

D'après un sondage commandé par le Secrétariat d'Etat au numérique en 2016, plus de la moitié des personnes interrogées considérait que le niveau de prise en compte de l'avis des citoyens dans les décisions politiques locales n'était pas satisfaisant. Ces derniers appelaient par conséquent à une meilleure consultation des administrés, que ce soit au travers des portails web des collectivités, des réseaux sociaux ou encore d'outils numériques dédiés. Si cette « soif » démocratique, encore renforcée à l'issue de la crise des « gilets jaunes » semble de bonne augure en termes de réappropriation de l'espace public par les citoyens, elle pose directement le problème de la sécurisation des données personnelles échangées dans le cadre de l'E-démocratie. En effet, comme le montre une enquête réalisée

par la Commission Nationale de l'Informatique et des Libertés (CNIL) en 2018, les Français apparaissent de plus en plus préoccupés quant au niveau de protection accordé à leurs données numériques personnelles. Or, les collectivités territoriales se trouvant au premier rang des prestataires de démocratie électronique, il convient donc qu'elles soient inattaquables en matière de SSI relativement aux services proposés à leurs administrés, eu égard au caractère « sensible » des informations échangées.

La sécurisation des données à caractère personnel des citoyens constitue également un « nœud gordien » pour le troisième défi numérique auquel sont confrontées les collectivités territoriales : l'administration électronique. Comme l'enseigne le sondage « Digital Gouv' » (réalisé annuellement) de 2018, les services administratifs dématérialisés constituent une priorité pour une large majorité de citoyens (67%). Il serait d'ailleurs très intéressant de connaitre l'évolution de cette tendance à l'issue de la crise du Covid-19 durant laquelle les périodes de confinement successives ont fait que l'un des seuls liens demeurant possible entre les Français et la plupart des services publics se trouvait être réduit aux ressources administratives en ligne. Or, parallèlement à ce tropisme affirmé, les internautes demeurent très inquiets quant à la sécurisation des données dématérialisées qu'ils sont amenés à partager avec l'administration. Si, dès 2012, la peur de se voir dérober des informations à caractère personnel représentait une menace majeure pour 42% d'entre eux (Sondage IFOP/Generix group), cette méfiance n'a fait que s'amplifier depuis lors. Ainsi, l'édition 2019 de l'enquête « Digital Gouv' » montre que plus de 70% des personnes interrogées redoutent non seulement le vol de données, mais également que celles-ci soient utilisées pour leur nuire. Cette dichotomie amène à une conclusion simple : il est loisible de considérer que les Français ne pardonneront pas à leurs collectivités respectives une compromission de leurs données à caractère personnel, *a fortiori* si ces dernières devaient faire l'objet d'une utilisation illicite ultérieure. Selon toute vraisemblance, le phénomène de judiciarisation accru de la société moderne les incitera par ailleurs immanquablement à se retourner contre les membres d'exécutifs locaux jugés incapables d'assurer la sécurité de leur SI. Ces actions auront des conséquences potentielles d'autant plus dommageables pour les collectivités visées et leurs dirigeants qu'elles coïncideront avec la montée en puissance du

Règlement Général sur la Protection des Données (RGPD) adopté par l'Union Européenne en 2016. Cette législation induit un renversement de paradigme dans la mesure où elle repose intrinsèquement sur la prédominance nouvelle du principe de conformité ainsi que sur une volonté avérée de mieux responsabiliser les responsables de traitements, y compris en cas de faute avérée d'un de leurs sous-traitants.

En plus des trois défis précédemment évoqués, avec leurs implications potentielles en matière de SSI pour les collectivités territoriales, **il en est un dernier qui, bien que moins médiatisé, s'avère tout aussi délicat : la dématérialisation des appels d'offres publics.** A l'origine issue d'une volonté de l'Union Européenne de moderniser les commandes publiques des états membres, cette dématérialisation devait permettre d'en optimiser l'efficacité au travers d'une meilleure fluidité des traitements administratifs afférents ainsi que d'une plus grande capacité de disposer de comparatifs détaillés des différentes offres reçues. Si l'objectif le plus immédiat de la dématérialisation était d'optimiser les processus d'achats publics afin de réduire les coûts relatifs à des appels d'offres diffusés sous format papier et engendrant de nombreuses opérations lourdes et coûteuses, cette dernière procédait d'une volonté plus large. Des appels d'offres informatisés devaient permettre une amélioration bienvenue des procédures d'achat, la réduction des durées des procédures de passation des marchés publics souvent considérées à juste titre comme peu compatibles avec une nécessaire réactivité, mais également et peut-être surtout de diversifier les sources d'approvisionnement des collectivités territoriales (représentant en 2019, plus de 60% de la commande publique nationale) au travers du recours à des PME jusqu'alors incapables de répondre à des appels d'offres publics par manque de ressources disponibles pour soumissionner selon des règles fastidieuses et extrêmement chronophages. Mais la condition première de réussite de cette dématérialisation des appels d'offres résidait dans la mise en place d'un SI dédié et capable d'assurer une totale confidentialité relativement aux échanges entre la collectivité et ses partenaires, tout en sécurisant l'ensemble des documents fournis afin de ne pas induire de rupture d'égalité entre les concurrents préalablement au choix final des commissions d'appels d'offres. Cette obligation a donc conduit le gouvernement à définir un cadre légal spécifique, déclinable en outils

juridiques et techniques d'identification, de nature à permettre de tisser un véritable lien de confiance entre la puissance adjudicatrice (en l'occurrence les collectivités territoriales) et les soumissionnaires. Or, la mise en place d'une dématérialisation sécurisée implique d'engager des moyens humains et financiers souvent situés au-dessus des ressources des petites collectivités qui représentent l'immense majorité (91%) de l'ensemble des 34 965 communes françaises recensées au 1er janvier 2021[8], à moins de transférer cette obligation à un échelon supérieur (EPCI).

Face des cybermenaces qui selon toute vraisemblance ne feront que croître, les collectivités se doivent donc de réagir sous peine, non seulement de voir les membres de leurs exécutifs respectifs mis en cause personnellement en cas d'atteinte aux données, mais également de perdre toute crédibilité auprès de leurs administrés, ce qui peut s'avérer extrêmement problématique en ces temps de méfiance citoyenne généralisée. La vulnérabilité des SI des collectivités territoriales constitue un enjeu dépassant largement le simple cadre local. Les mesures à mettre en place ne peuvent s'établir qu'au travers d'une action concertée impliquant à la fois les élus locaux et les administrations de l'Etat. La conjonction d'une situation budgétaire souvent très tendue et d'une absence de ressources humaines adéquates, notamment dans les collectivités de taille modeste, fait qu'il serait illusoire de penser que ces dernières puissent procéder à un niveau de sécurisation suffisant de leurs SI sans une aide étatique - qui pourrait se traduire, par exemple, par une vaste politique publique de sécurisation des SI territoriaux. On pourrait objecter avec raison qu'une telle ambition serait de nature à grever encore davantage des finances publiques largement sollicitées durant la crise de la Covid-19. Toutefois, ce serait oublier que le fait de relever les quatre défis cyber auxquels sont confrontées les collectivités territoriales s'insère entièrement dans un ensemble d'actions régaliennes visant à assurer un développement harmonieux du territoire ainsi qu'à favoriser la compétitivité d'un tissu économique majoritairement constitué de PME. Un usage optimal des nouvelles technologies, en tant que vecteurs privilégiés d'un nouveau type de rapports sociaux, administratifs ou économiques, procédera, avant tout, de la capacité des pouvoirs publics à garantir à l'ensemble des citoyens, ainsi qu'au monde économique, une sécurisation maximale de leurs échanges électroniques.

Webographie

Cyberattaque contre la Ville de Baltimore (Maryland) :
https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html

Cyberattaque contre la Ville de Florida Beach (Floride) :
https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html

Cyberattaques contre plusieurs milliers de sites français (Janvier 2015) :
https://www.01net.com/actualites/plus-de-20-000-sites-francais-pirates-par-des-hackers-anticharlie-hebdo-641277.html

Cyberattaque contre la ville de Besançon :
https://www.besancon.fr/actualite/le-systeme-dinformation-de-grand-besancon-metropole-de-la-ville-et-du-ccas-de-besancon-victime-dune-cyberattaque-dampleur/

Cyberattaque contre la ville de Toulouse :
https://www.lejournaltoulousain.fr/societe/site-de-la-mairie-de-toulouse-pirate-les-cyberattaques-sintensifient-79867/

Cyberattaque contre la Métropole Aix-Marseille-Provence :
https://www.laprovence.com/article/papier/5965065/comment-des-hackers-ont-failli-mettre-marseille-a-genoux.html

Cyberattaque contre la ville d'Angers :
https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/video-a-angers-une-cyberattaque-paralyse-les-services-de-la-ville_4266933.html

Cyberattaque contre la ville de Douai :
https://www.lavoixdunord.fr/979090/article/2021-04-09/la-mairie-de-douai-victime-d-une-cyberattaque-dans-la-nuit-de-jeudi-vendredi

Cyberattaque contre la ville de Chalon-sur-Saône :
https://www.usine-digitale.fr/article/la-ville-de-chalon-sur-saone-et-l-agglomeration-du-grand-chalon-sont-victimes-d-une-cyberattaque.N1063299

Cyberattaque contre la ville de La Rochelle :
https://www.sudouest.fr/charente-maritime/la-rochelle/la-rochelle-la-ville-et-l-agglo-victimes-d-une-cyberattaque-1624489.php

Cyberattaque contre la ville de Houilles :
https://www.ville-houilles.fr/news/2021/cyberattaque-contre-la-ville-de-houilles

Cyberattaque contre la ville d'Argenton-sur-Creuse :
https://france3-regions.francetvinfo.fr/centre-val-de-loire/indre/propagande-islamiste-site-mairie-argenton-creuse-indre-victime-pirates-informatiques-1890440.html

Cyberattaque contre la ville de Morières-Lès-Avignon :
https://www.ledauphine.com/faits-divers-justice/2021/04/11/vaucluse-la-ville-de-morieres-les-avignon-victime-d-une-cyber-attaque

Neutralisation à distance de 850000 ordinateurs infectés par les services de la Gendarmerie Nationale :
https://www.lemonde.fr/pixels/article/2019/08/28/la-gendarmerie-a-neutralise-un-reseau-de-850-000-ordinateurs-infectes-par-le-meme-virus_5503771_4408996.html

Résultats du sondage « Numérique et Démocratie » réalise pour le Secrétariat d'Etat au Numérique (2016) :
https://www.economie.gouv.fr/files/files/PDF/sondage-numerique_et_democratie-2016.pdf

Résultats du sondage Ifop « Les Français et la protection des données personnelles » réalisé pour la CNIL (2018) :
https://www.cnil.fr/sites/default/files/atoms/files/barometre_ifop_rgpd-2018.pdf

Résultats du baromètre « Digital Gouv' 2018 » :
https://www.ipsos.com/fr-fr/barometre-digital-gouv-2018-le-developpement-numerique-des-services-publics-prioritaire-pour-les

Résultats du sondage « Les français face à la dématérialisation » (IFOP/ Generix Group, 2012) :
https://pnr-files.pro1.gus.wdc.dianum.io/globenewswire/articles/1659461/fr/generix-group-stop-a-la-paperasse-les-francais.pdf

Résultats du baromètre « Digital Gouv' 2019 » :
https://www.soprasteria.com/docs/librariesprovider2/sopra-steria-corporate/publications/digital-gov2019-booklet_fr-v5-hds.pdf?sfvrsn=97b35edc_3

Part des collectivités territoriales dans la commande publique en 2019 :
https://www.banquedesterritoires.fr/forte-progression-de-la-commande-publique-en-2019

Statistiques 2021 sur les Collectivités territoriales françaises (DGCL) :
https://www.collectivites-locales.gouv.fr/collectivites-locales-chiffres-2021

[1] Ouvrage « Intelligence Economique et collectivités territoriales : *Des stratégies innovantes pour une meilleure valorisation des territoires*, Paris : Ed. Ellipses, 264 p.
[2] Ouvrage « Les collectivités territoriales face à la cybercriminalité », Paris : Ed. Eska, 312 p.
[3] L'ensemble des évènements évoqués fait l'objet d'une webographie située en fin d'article
[4] R. Février (2020), « Covid-19 et cyberattaques : Vers une nécessaire évolution du paradigme dominant en management stratégique ? », Revue Française de Gestion, n°293, p. 81-94.
[5] EPCI : Etablissement Public de Coopération Intercommunale
[6] Zone démilitarisée : sous-réseau contenant l'ensemble des machines nécessitant d'accéder à Internet au sein d'une organisation et isolé du reste du réseau local.
[7] Intrusion Detection System : Système de détection d'intrusion. Il en existe différents types (NIDS, HIDS, Hybrides…), toutefois des techniques appelés IDS Evasions Techniques permettent de contourner ces dispositifs.
[8] Source : Direction Générale des Collectivités Locales (DGCL).

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 des 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 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.
- **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** 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.
- **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** 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 :** 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
https://www.ssi.gouv.fr/uploads/2020/01/anssi-infographie-les_collectivites_face_aux_enjeux_de_cybersecurite.pdf

Rapport d'activité 2020 – Kit de sensibilisation aux risques numériques / Cybermalveillance
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2020

L'essentiel de la sécurité numérique pour les dirigeants et les dirigeantes / Challenge
https://www.nxtbook.fr/newpress/CEIDIG/l_essentiel-de-la-securite-numerique-pour-les-dirigeants-et-les-dirigeantes-2eme-edition/index.php?utm_source=medef#/p/Couverture

Quels sont les axes majeurs pour lutter contre les cyberattaques ? / L'usine digitale
https://www.usine-digitale.fr/article/budget-comex-donnees-quels-sont-les-axes-majeurs-pour-lutter-contre-les-cyberattaques.N1077979

Cybersécurité : comment former les télétravailleurs pour réduire les vulnérabilités comportementales / IT Social
https://itsocial.fr/enjeux-it/enjeux-strategie/dsi/cybersecurite-comment-eduquer-les-teletravailleurs-pour-reduire-les-vulnerabilites-comportementales

Vigilance face aux cyberattaques : les collectivités sont toutes concernées ! / Cybermalveillance
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/vigilance-cyberattaques-collectivites-toutes-concernees

"Au moins 4% des communes françaises ont été piratées en 2020" Jérôme Notin - Cybermalveillance / Journal Du Net
https://www.journaldunet.com/economie/services/1497637-jerome-notin-cybermalveillance/

Le rapport Fujitsu sur la cyberculture
https://www.fujitsu.com/global/services/security/insights/cybersmart-culture/

Le secteur public français doit mettre sa cybersécurité en ordre de marche

LOÏC GUÉZO
Directeur Stratégie Cybersécurité SEMEA
Proofpoint

Hôpitaux, universités, communes, communautés de communes ou d'agglomérations… Depuis le début de la pandémie, le rythme des cyberattaques visant les organisations du secteur public ne cesse de s'accélérer. Les rançongiciels ont déjà causé de nombreux dommages et aucun profil n'est épargné. La situation est particulièrement préoccupante, et d'après de nombreux experts, elle devrait même continuer à se dégrader dans les prochains mois.

Pour un secteur quasi étranglé par la pression des cybercriminels, il apparaît donc urgent de prendre la mesure du risque sécuritaire et d'adopter des mesures concrètes et fortes pour éviter de sombrer dans le chaos numérique. Mais par où commencer pour organiser la riposte ? Comment rattraper un retard de près de 15 ans par rapport aux entreprises en matière de cybersécurité ? Proofpoint partage son éclairage sur ces questions et sur les actions concrètes permettant de renforcer la posture en cybersécurité dans le secteur public.

Un secteur pris dans le tourbillon des rançongiciels

En mars 2020, la Métropole de Marseille s'est retrouvée paralysée par une cyberattaque massive et généralisée. L'attaque a chiffré la quasi-totalité des serveurs contre une demande de rançon. De la stupeur à la remise en marche des services, stylos et papiers ont remplacé claviers et ordinateurs pour assurer un semblant de continuité de service auprès des citoyens. Mais pendant près d'un mois et dans un contexte sanitaire tendu, toutes les déclarations de naissances ou décès ont par exemple dû être enregistrées manuellement…

Loin d'être un cas isolé, ce scénario s'est depuis répété pour de nombreuses autres organisations du secteur public : Vincennes, Alfortville, Angers, La Rochelle, Aulnoye-Aymeries… Selon un récent rapport publié conjointement par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et l'Association des Maires de France et Présidents d'Intercommunalité (AMF), un incident cyber sur quatre remonté en France affecte directement les communes et intercommunalités. La transformation numérique de ces organisations est à la fois une source d'opportunités formidables en faveur de l'action publique, mais de facto un réel facteur de risque.

Au total l'an dernier, 159 collectivités ont officiellement déclaré une cyberattaque auprès du portail cybermalveillance.gouv.fr, soit une hausse de 50 % par rapport à 2019. D'après l'étude MIPS 2020 menée par le CLUSIF, les attaques par rançongiciel ont commencé à toucher de manière beaucoup plus systématique les collectivités depuis 2018, avec près de 30 % des conseils territoriaux et des villes impactés. Les décomptes restent encore aujourd'hui très certainement sous-évalués.

Les organisations publiques dans le secteur de la santé sont également dans le viseur des cybercriminels : après l'Assistance Publique Hôpitaux de Paris, c'est au tour des établissements de Dax (Landes), de Villefranche-sur-Saône, Tarare et Trévoux (Auvergne-Rhône-Alpes) d'être victimes d'une cyberattaque. Bref, c'est tout un secteur qui se retrouve fragilisé, sur l'ensemble du territoire.

Car dans tous les cas, l'interruption de service est dramatique et se fait au détriment du citoyen, jusqu'à mettre en danger sa santé. Le risque de perte de confiance dans la numérisation des services publics est également fort. Tout comme l'impact sur l'image de marque de l'établissement… et de ses dirigeants ; une cyberattaque pouvant finalement être utilisée comme un argument politique contre les élus en place.

Connaître l'ennemi pour mieux le combattre

L'ennemi à abattre : les rançongiciels, ces logiciels malveillants qui rendent illisibles les données d'un ordinateur ou d'un serveur et exigent le

paiement d'une rançon en cryptomonnaie contre leur restitution. Plus de neuf fois sur dix, le point de départ d'une telle attaque est un email piégé qu'un collaborateur n'a pas su identifier comme frauduleux. Il clique sur un lien ou une pièce-jointe d'apparence légitime, ouvrant la porte à un logiciel malveillant qui vient ensuite s'infiltrer profondément dans le système d'information de l'organisation. A l'activation à distance du logiciel par les attaquants, chaque ordinateur se chiffre et devient totalement inopérant. Ce genre d'attaque est souvent lancé en début de week-end, lorsque la vigilance est abaissée et que les équipes de supervision ne sont plus là pour constater que quelque chose d'anormal est en train de se produire. Les cybercriminels font ensuite chanter leurs victimes en demandant le paiement d'une rançon.

Dans le cadre d'une plongée dans les coulisses de l'écosystème cybercriminel menée par un groupe de travail de l'Institut Montaigne, il a été établi que le retour sur investissement d'une attaque par rançongiciel se situerait entre 232 % et 880 %. On comprend donc aisément les motivations des criminels à poursuivre voire intensifier le rythme de leurs attaques cyber. Les rançongiciels sont si rentables que leurs auteurs n'ont aucune raison de lever le pied.

Alors ne suffirait-il pas de ne pas payer la rançon pour enrayer le phénomène ? Si la recommandation officielle reste de ne pas payer, la réalité est qu'environ une victime sur cinq paierait la rançon qui lui est réclamée. Dans le secteur public, certaines collectivités se retrouvent complètement démunies face à une cyberattaque de cette ampleur. Et même si le prix à payer est élevé, cette solution peut apparaître, à tort, comme plus accessible que de devoir reconstruire tout un système d'information. Vice du système actuel, les victimes seraient assez souvent incitées à payer par les sociétés d'assurance elles-mêmes. Une situation jugée inacceptable, car elle n'a bien évidemment pour conséquence que de nourrir et perpétuer la cybercriminalité.

Mais les lignes sont en train de bouger. Aux Etats-Unis, le paiement des rançons dans le cadre de cyberattaques est déjà considéré comme une atteinte à la souveraineté nationale, et en France, il est devenu un sujet parlementaire, depuis que Johanna Brousse, vice-procureur chargée des

dossiers de cybersécurité au parquet de Paris, a déclaré lors d'une audition au Sénat le 15 avril dernier que la raison principale du nombre d'attaques par rançongiciel en France se justifiait par la forte propension des entreprises à payer les rançons sous couvert d'un remboursement par leur assurance. Les débats ont depuis été animés autour de ce jeu parfois trouble des assureurs, menant Axa à suspendre sa garantie « cyber rançonnage ». Une décision qui ouvre la voie à une attitude plus responsable de certaines organisations qui — si d'autres assureurs emboîtent le pas à Axa — se devront d'investir davantage dans leur cybersécurité.

Et il ne s'agit pas seulement d'assurer des sauvegardes efficaces. La capacité des cybercriminels à propager des attaques informatiques s'est tellement professionnalisée et industrialisée qu'elle croît plus rapidement que celle de leurs victimes à se protéger. C'est une réalité, les collectivités ne sont aujourd'hui pas prêtes à faire face à ce type d'attaque.

Une cybersécurité nationale en chantier

Prenant la mesure d'un risque auquel nous sommes collectivement confrontés, le gouvernement a mis sur pied une stratégie nationale d'accélération de la cybersécurité. Présenté par le Président de la République le 18 février dernier, ce plan d'actions ambitieux prévoit de mobiliser 1 milliard d'euros pour renforcer le niveau global de sécurité au sein de l'espace numérique de l'Etat français, des services publics nationaux, des collectivités territoriales, des entreprises et des citoyens. Comme le souligne l'avis N°2021-03 du 29 avril 2021 de la Commission Supérieure du Numérique et des Postes (CSNP), ce plan n'est certes pas parfait, car encore insuffisant ou incomplet sur certains aspects, mais il a le mérite d'exister et de proposer des actions pertinentes.

Sur cette base, la CSNP a émis une série de recommandations complémentaires portant sur différents champs de progrès, comme par exemple le renforcement de la lutte contre la cybercriminalité avec de nouveaux moyens judiciaires et policiers pour surmonter les défis techniques, la sensibilisation et la formation à la sécurité numérique ou encore la consolidation de la filière cybersécurité, aujourd'hui encore trop

morcelée entre de nombreuses PME et quelques grands industriels très spécialisés. Sur ce dernier volet, le Campus Cyber, initié par le Président de la République en 2019, est en train de devenir un lieu emblématique pour rassembler les principaux acteurs de la cybersécurité et développer des synergies entre eux ainsi que des partenariats avec des pôles de cybersécurité en région.

Un véritable maillage régional de la cybersécurité serait un atout indéniable pour atteindre les plus hautes ambitions en matière de protection de l'espace numérique national. Le plan d'accélération cyber prévoit à cet effet le déploiement dans chaque région d'un CSIRT (Computer Security Incident Response Team - équipe de réponse aux incidents informatiques) incubé avec le soutien de l'ANSSI. Ces entités de terrain doivent permettre de réagir plus rapidement et efficacement aux cyberattaques qui peuvent frapper les collectivités territoriales et autres structures locales, ainsi que les établissements de santé (hôpitaux, cliniques).

En France, n'oublions pas que nous avons également la chance d'avoir de longue date un cadre réglementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens. Porté par l'ANSSI, ce référentiel général de la sécurité (RGS) a pour objectif d'aider les collectivités dans l'évolution de leur cybersécurité, avec notamment une cartographie des risques, la mise en place d'un dispositif de gouvernance avec une commission pour éclairer les décisions, et un partage de bonnes pratiques dans une démarche d'amélioration continue. Ce dispositif n'est pas nouveau, mais reste encore méconnu et peu appliqué. Car même s'il reste obligatoire, à la différence du RGPD, il est purement incitatif et ne comporte pas de sanction en cas de non-respect. Or pour changer de paradigme, il apparaît crucial que chaque organisation puisse s'emparer du RGS. Qui plus est quand on ne sait pas par où commencer pour développer sa maturité en cybersécurité, ce texte se révèle être un guide très pragmatique, qui encourage à la mise en œuvre de bonnes pratiques. C'est finalement tout le rôle d'un Responsable de la Sécurité du Système d'Information (RSSI) : le RGS doit être bien pris en compte par l'ensemble des décideurs du secteur public.

Car avec une accélération de leur transformation numérique et une migration certes progressive mais avérée vers le cloud, les organisations du secteur public voient leur surface d'attaque potentielle s'étendre, et avec elle des préoccupations se marquer plus sensiblement que pour leurs homologues du secteur privé sur les questions de stockage, d'accès ou encore de sécurisation, compte tenu de la valeur et de la nature de leurs données. Trois mois après le lancement de son plan cybersécurité, le gouvernement vient en réponse à ces inquiétudes de présenter sa stratégie nationale en matière de cloud souverain, avec le lancement d'un label « Cloud de confiance » qui reposera sur le visa « SecNumCloud » délivré par l'ANSSI pour contribuer à la mise en œuvre d'un véritable bouclier numérique.

La réalité à l'échelle des organisations

Si les cadres d'action et les dynamiques évoluent, il apparaît aujourd'hui pourtant encore légitime de se demander qui est aux commandes de la cybersécurité au sein des organisations du secteur public. Quand certaines collectivités n'ont même pas de Service Informatique digne de ce nom, il semble en effet compliqué d'organiser un plan de bataille à la hauteur des enjeux. En outre, il est bien évident que la taille des organisations influe sur la dotation de ressources dédiées à la sécurité de leur système d'information : les plus importantes s'organisent pour allouer des moyens humains internes, tandis que les plus petites feront davantage le choix de l'externalisation auprès de partenaires privés ou de structures de mutualisation.

Dans tous les cas, l'objectif est de garantir un pilotage de la cybersécurité, et il est primordial de nommer des responsables pour l'assurer. Plusieurs postes externalisés ou partagés ont d'ailleurs commencé à émerger dans le secteur public, du RSSI au délégué à la protection des données (DPO), notamment dans le cadre de la mise en œuvre du RGPD au sein des collectivités. Mais la pénurie de talents dans le domaine de la cybersécurité à l'échelle nationale constitue un véritable problème. Cette discipline complexe exige des connaissances pointues que peu de personnes sur le marché de l'emploi possèdent, et en proposant des salaires plus élevés, les entreprises sont donc mieux placées pour attirer les talents que les organismes publics qui ne peuvent malheureusement rivaliser.

Mais finalement peu importe leur taille, et avec une dotation de compétences encore insuffisante, le niveau de maturité des organisations du secteur public en matière de cybersécurité est actuellement trop disparate, et globalement assez bas. Pour l'illustrer de façon assez provocatrice, partons du postulat que le niveau de maturité actuel en cybersécurité dans le secteur public en France est l'équivalent de celui des entreprises… il y a 15 ans ! Principal écueil : le manque de perception du risque cyber. Beaucoup d'organisations se sont en réalité davantage concentrées sur le fait d'augmenter les services numériques pour la population qu'au fait de protéger l'architecture même de ces systèmes. Les efforts sur la sécurité ont été systématiquement sous-dimensionnés.

Ces manquements sont d'ailleurs assez flagrants en matière de lutte contre la fraude email. Selon une enquête Proofpoint, seuls 5 des 14 ministères français ont mis en œuvre DMARC, le standard d'authentification des emails pourtant recommandé par l'ANSSI. Et sur les 5 organisations de services publics clés (considérées comme des infrastructures critiques), seule 1 est protégée contre les attaques par usurpation de domaine (Les Impôts). Mais son domaine associé utilisé pour envoyer des emails au contribuable (DGFIP) est lui laissé sans protection active…

Une plus grande prise de conscience est aujourd'hui nécessaire pour inverser la tendance et instaurer une hygiène numérique, comme point de départ d'une riposte organisée contre le cybercrime. Pour y parvenir, la transparence des organisations victimes de cyberattaques est fondamentale. Même si trop peu de plaintes sont encore déposées, élus et agents acceptent de plus en plus de partager leur expérience. Et pas seulement pour des raisons juridiques. Angers par exemple a organisé une communication en janvier dernier suite à une cyberattaque ayant paralysé ses systèmes et contraint ses agents à retourner au fax et au papier pour poursuivre leur mission. La vidéo décryptant les coulisses de cette attaque et les réactions qui se sont enchaînées est précieuse pour toutes les autres collectivités. C'est cette transparence qui favorise la sensibilisation et donc la prévention possible face à un risque croissant.

Transparence et mutualisation sont clés. Dès lors que les responsables de la sécurité sont nommés, ils doivent se regrouper pour partager les bonnes

pratiques et veiller à la mise en œuvre de moyens à disposition des autres organisations. D'où l'émergence d'initiatives, comme le groupe CoTer du CLUSIF qui favorise l'échange de savoir-faire et le retour d'expériences.

Sensibilisation et formation

De manière intéressante, les initiatives de partage de retour d'expériences tels que celui du CLUSIF montrent déjà que si le sujet de la cybersécurité revêt une dimension hautement technique, il ne doit pas être l'apanage des RSSI. Certaines collectivités proposent désormais des séances de sensibilisation à la sécurité numérique pour l'ensemble de leurs agents. C'est une excellente chose. Mais il faut professionnaliser et systématiser la pratique auprès de l'ensemble des publics : élus, décideurs, agents mais aussi citoyens. L'humain étant historiquement considéré comme le maillon faible de la chaîne de cybersécurité, alors il est évident que toute stratégie cyber doit se centrer sur les individus si elle veut être pertinente et surtout efficace en en faisant le dernier rempart ...

Et sur ce point, les entreprises de sécurité elles-mêmes ont forcément un rôle à jouer. Notamment en faisant un pas vers les organisations les plus sensibles et en développant des solutions en réelle adéquation avec leurs besoins. Chez Proofpoint notamment, nous souhaitons prendre pleinement notre part dans le projet d'amélioration de la posture cybersécurité des organisations du secteur public, en y insufflant une culture de la sensibilisation et de la formation à l'hygiène numérique. La dimension pédagogique pour y parvenir est essentielle, la composante organisationnelle, fondamentale. En raison de la pénurie de compétences en cybersécurité dans l'hexagone (et en Europe), la formation au sein des organisations est en effet la condition sine qua non de la mise en œuvre opérationnelle du plan d'accélération cyber du gouvernement.

D'après nos analyses, 94% des cybermenaces actuelles passent par les boîtes email et 99% d'entre elles nécessitent une interaction de la part des utilisateurs pour se déclencher. Il faut donc transformer tous les utilisateurs « passifs » en acteurs de la protection de l'espace numérique collectif. Les moyens existent déjà. Outre les solutions techniques de type passerelles de messagerie sécurisées, les solutions pédagogiques comme les packs

PSAT (Proofpoint Security Awareness Training) offrent un niveau de protection supplémentaire. En misant sur l'interactivité et la formation en continu (simulations d'attaques réelles, modules d'information et de sensibilisation, …), la méthodologie PSAT permet d'évaluer les connaissances des utilisateurs, de les sensibiliser aux dernières tendances en matière de menaces et surtout de créer et renforcer leur capacité à détecter une intention malveillante pour pouvoir réduire le nombre d'attaques qui aboutissent.

Au-delà de ces efforts internes, il faut que la sécurité numérique soit mieux comprise par l'ensemble de la population. Les citoyens doivent être massivement instruits des menaces auxquelles ils peuvent être confrontés dans leurs usages du numérique, tant à titre privé que professionnel, et des mesures permettant de s'en prémunir pour éviter de compromettre leurs données personnelles. La meilleure approche consisterait à lancer des campagnes nationales de sensibilisation pour vulgariser le sujet et partager des bonnes pratiques. Cela peut sembler anodin, mais parvenir à faire douter chaque usager de la réelle légitimité d'un email (voire le signaler aux autorités compétentes) serait finalement déjà une grande victoire sur la cybercriminalité.

La protection des systèmes d'information, une nécessité à tous les niveaux

CHRISTOPHE GUILLOTEAU
Président
Département du Rhône

Dans le Rhône, le 15 février 2021, le centre hospitalier de Villefranche-sur-Saône a été la cible d'une cyberattaque.
Ce jour-là, le centre hospitalier de Villefranche-sur- Saône a été la cible d'une cyberattaque d'une grande ampleur, paralysant une grande partie de son système d'information et provoquant le report de plusieurs interventions. Il aura fallu plus de 15 semaines pour un retour à la normale.

Les attaques informatiques se multiplient : pas une seule semaine sans information sur une attaque majeure.

Escroqueries en ligne, cyberattaques, hameçonnages ou rançongiciels : quelles que soient les formes qu'elles prennent, les criminalités numériques font désormais partie de notre quotidien.
Et pire encore, elles ne cessent de se multiplier dans le contexte de crise sanitaire actuel avec une augmentation significative en 2020 liée aux confinements (télétravail, achats en ligne…).

En deux ans, le nombre d'attaques informatiques par des pirates réclamant une rançon a explosé en France comme dans le reste de l'Europe. Selon l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), en 2020, le nombre de ces attaques aux « *rançongiciels* » aurait augmenté de 255% rien que sur les grandes entreprises publiques et privées y compris celles qui relèvent de la sécurité nationale, selon l'AFP.

Les attaques informatiques constituent donc aujourd'hui un vrai fléau qui touche aussi bien les particuliers que l'ensemble des entreprises ou administrations.

Face à ce contexte, la cyberdéfense est devenue une priorité pour les collectivités territoriales.

Rappelons que les collectivités traitent de nombreuses données fiscales, sociales et gèrent de nombreuses prestations… La divulgation ou le vol de ces données serait une atteinte majeure à la vie privée des citoyens, une atteinte très dommageable.
À titre d'exemple le Département du Rhône traite environ 25 000 prestations par mois.

Pour faire face de manière efficace aux nombreuses menaces qui pèsent sur les données dématérialisées, les collectivités territoriales ont l'obligation de se soumettre à un cadre réglementaire solide de protection des données des usagers.

Ce cadre légal a sensiblement évolué depuis 2018, afin de prendre en compte les avancées digitales et une multitude et variété de canaux de diffusion (réseaux sociaux, cloud, etc..).

De plus les collectivités ont entrepris elles-mêmes une transformation numérique profonde.

En effet elles ont besoin de ces nouveaux moyens pour moderniser leurs actions, pour accompagner le développement de leur territoire et améliorer la qualité de service aux usagers : accès facilité aux services, efficacité et gain de temps dans le traitement des dossiers…
Ces mutations impliquent une augmentation des services en ligne, impliquant plus de risques, plus de répercussions sur le fonctionnement de l'administration et sur le service à l'usager.

Enfin, force est de constater que les données du territoire sont de plus en plus nombreuses et variées du fait d'une multiplication des sources (smartphone et réseaux sociaux, capteurs …). Ces nouvelles données sont difficilement exploitables avec les outils informatiques traditionnels.

Tout cela nous amène à repenser notre schéma de systèmes d'information pour nous moderniser tout en assurant la protection des données.

Pour répondre à cette nécessité, les collectivités doivent être en capacité de se défendre, d'assurer la souveraineté des données pour lutter contre les cybermenaces. Trouvons une alternative en nous dotant d'outils innovants, en sensibilisant et formant les agents.

L'arrivée massive de nouveaux moyens de communication et le développement de l'internet ont nécessité une refonte complète de nos usages numériques en 2017.

Le Département de Rhône applique en son sein une stratégie transverse de cybersécurité et de protection des systèmes d'informations et des données afin de protéger les données des agents, des collaborateurs, des citoyens, et de maintenir l'exploitation des services en ligne et de son système d'information.

Au Département du Rhône nous avons mis en place un dispositif de cyberdéfense technique, opérationnel et organisationnel. Nous complétons actuellement ce plan d'actions en élaborant une politique globale de sécurité pour protéger nos systèmes d'information.

Dans ce cadre nous avons produit un livret des usages numériques.

Ce document, que nous réactualisons périodiquement, est la charte d'utilisation des outils informatiques mis à disposition des agents pour exercer leurs missions.

Parallèlement à ces bons usages, nous avons mené une campagne de sensibilisation auprès de l'ensemble des agents. Dans ce cadre, une base documentaire est accessible à tous les agents sur l'intranet du Département avec des fiches pratiques adaptées aux situations.

Plus concrètement, le Département met en avant sur son site intranet les gestes simples (choix des mots de passe, séparation données personnelles et privées, utilisation restreinte de la messagerie électronique) qui permettent d'accroitre de manière significative la sécurité des données professionnelles de l'ensemble des agents départementaux.

Nous poussons également les agents intéressés par le sujet à s'inscrire sur la plateforme de l'ANSSI pour suivre une formation d'initiation à la cybersécurité.
Enfin, nous veillons à la pertinence des systèmes de protection en les faisant évoluer selon l'état de l'art et les préconisations de l'ANSSI.

Le monde de la cybersécurité et de la cybercriminalité évolue sans cesse et très rapidement.
Dans la démarche d'amélioration continue de ses outils de protection face aux cybermenaces, le Département du Rhône, comme d'autres collectivités territoriales, étudie de près l'usage de solutions de protection et de défense « nouvelles générations » tirant partie des avancées technologiques apportées par l'univers de l'informatique en Nuage telles que l'Apprentissage Machine et l'Intelligence Artificiel.

Incontestablement, cette sensibilisation à la cybersécurité ne pourra se mettre en place sans l'appui de sociétés prestataires de confiance certifiées pour le choix et l'intégration de ces outils, et grâce à une formation poussée de tous les agents concernés par ce secteur aux enjeux considérables dans un monde 2.0 qui ne cesse de s'agrandir.

La Région Auvergne-Rhône-Alpes pleinement mobilisée pour le renforcement de la cybersécurité

JULIETTE JARRY
Ex Vice-présidente déléguée au Numérique
Région Auvergne-Rhône-Alpes

Les outils numériques ne cessent de se multiplier et de se diversifier, touchant de plus en plus de pans de nos vies, tant personnelles que professionnelles. Ordinateurs, téléphones portables et autres objets connectés sont progressivement devenus le prolongement voire l'auxiliaire de notre corps ou de notre mémoire. Précieux au quotidien sur de nombreux aspects, ils sont aussi une porte d'entrée sur nos données privées ou professionnelles, très convoitées par les pirates informatiques. Dans le monde des entreprise, les chiffres sont éloquents : 40% d'entre elles ont déjà subi une ou plusieurs attaques ou tentatives d'attaques informatiques alors que 17% seulement sont assurées contre ce risque, selon une enquête nationale de la CPME.

La cybersécurité est devenue d'autant plus cruciale que le contexte de crise sanitaire a obligé bon nombre d'entreprises à revoir leurs modalités de travail pour basculer dans des délais très courts vers une solution à distance. Le manque d'anticipation dans la mise en œuvre d'outils de sécurisation des flux de données mais aussi de sensibilisation et de formation des collaborateurs aux risques cyber ont fragilisé les entreprises face à ce nouveau contexte et à l'accroissement du niveau de menaces. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) estime ainsi que le nombre de cyberattaques a été multiplié par 4 en 2020 par rapport à l'année précédente. Il est, plus que jamais, temps de s'intéresser à la protection de ses données.

Ce manque de préparation et de capacité d'intervention s'explique en partie par les conditions pénuriques sur le marché de l'emploi et par les contraintes budgétaires qui en découlent. Du fait de sa rareté, l'expertise

en sécurité informatique, qu'elle soit en interne ou en externe, peut s'avérer relativement coûteuse. Après avoir interrogé plus de 3 000 responsables informatiques dans 12 pays dont la France, le cabinet Vanson Bourne[1] a constaté que 79% des responsables informatiques déclaraient qu'il était difficile de recruter des professionnels possédant les compétences en cybersécurité dont ils avaient besoin.

Consciente de cette problématique, la Région Auvergne-Rhône-Alpes a souhaité dès 2017 se mobiliser sur cette question en adoptant une Feuille de route stratégique en matière numérique qui intègre dans ses grands principes celui de la confiance numérique. Cette question touche à la fois le citoyen dans sa vie quotidienne, le salarié dans sa vie professionnelle, les entreprises dans leur activité économique et les collectivités locales.
La mise en œuvre de la stratégie régionale en matière de cybersécurité s'articule en lien avec le Campus Région du numérique qui a récemment ouvert ses portes à Charbonnières-les-Bains, à proximité de Lyon. Lieu-ressource et outil au service des transitions économiques, industrielles et environnementales, ce hub permet de traiter à 360° les enjeux du numérique dans ses 3 composantes : formation, transformation des organisations, innovation, particulièrement sur l'industrie du futur. C'est sous ces 3 angles que nous avons voulu aborder la question de la cybersécurité.

Le Campus propose une riche offre de formation avec les modules proposés par l'Esisar, les formations Simplon à l'Université Lyon II, le Mastère Spécialisé Data Scientist de Sigma Clermont, la IT Academy, ou encore la formation Data Analyst de la Wild Code School, qui sont destinées à des étudiants mais aussi à des professionnels qui souhaiteraient se perfectionner sur cette thématique. Sur sa plateforme web https://campusnumerique.auvergnerhonealpes.fr, le Campus propose également un MOOC de l'ANSSI intitulé « se former à la cybersécurité » ainsi qu'un dossier complet de sensibilisation des petites entreprises aux risques de la cybercriminalité.

Un programme « Caractériser la valeur de mon entreprise face aux-cyber menaces » opéré par la CPME est également disponible sur le portail « Ambition Eco » de la Région. Il présente une offre d'accompagnement

aux entreprises pour la mise en place d'une culture et d'un savoir-faire lié à la cybersécurité.

Les partenaires de la Région tels que Minalogic, l'ENE, Digital League, le CyberCercle et la CCI de Savoie s'inscrivent dans une démarche de démocratisation des enjeux de la cybersécurité auprès de leurs réseaux en organisant régulièrement des ateliers, séminaires, formations en ligne et des événements autour de cette thématique. L'ENE, à travers son programme « Usine Numérique Régionale » permet aux entreprises d'auditer la sécurité de leurs systèmes informatiques et d'identifier ainsi les risques de cyber-attaques et de proposer des mesures correctives. Le dispositif Atouts Numériques accompagne quant à lui les entreprises de moins de 50 salariés du territoire vers les usages du numérique dont la sécurité des infrastructures informatiques.

La composante innovation du Campus se matérialise quant à elle par un espace de près de 3 000 m2 nommée « l'Usine ». Elle porte les sujets de la transformation des modèles industriels vers la « Smart Factory ». L'Usine est composée de plateformes technologiques à échelle 1 qui permettent de découvrir, tester les technologies de l'industrie du futur et d'être accompagné dans son projet, quel que soit son niveau de maturité. Il est à noter que l'Usine sera équipée en 5G début mars 2021. Des expérimentations de 5G industrielle seront ainsi possibles. En ce sens, l'interopérabilité des systèmes industriels et leur cybersécurité seront au centre des activités des plateformes technologiques. Par sa vocation de travail en réseau, l'Usine s'appuie sur les forces d'Auvergne-Rhône-Alpes, région qui concentre 20% des effectifs nationaux de recherche et d'innovation en matière de cybersécurité avec des travaux de premier plan en matière de sécurité des objets connectés (dont industriels), de prévention et réaction aux cyberattaques, d'analyse de vulnérabilités logicielles et de sécurité des infrastructures critiques.

En complément, un démonstrateur des technologies du numérique récemment installé au Campus vient pousser les entreprises à se transformer et innover en se dotant de nouveaux outils numériques : il présente, de manière accessible à tous, les 4 technologies d'excellence de la région Auvergne-Rhône-Alpes, que sont l'intelligence artificielle, le

calcul haute performance, les systèmes cyber-physiques et la cybersécurité. Cette dernière technologie est présentée au travers d'exemples d'entreprises de notre région qui l'utilisent au quotidien : concrètement, leurs dirigeants expliquent en quoi la sécurisation des données et des process est fondamentale pour la bonne marche de leur entreprise, et leurs professionnels expliquent en quoi consiste leur métier de data scientist, ingénieur vision, responsable sécurité des réseaux…

A travers ces différents dispositifs, la Région Auvergne-Rhône-Alpes s'est dotée ces dernières années d'une vraie stratégie numérique de confiance que nous vous invitons à venir découvrir à Charbonnières-les-Bains selon nos 3 axes de sensibilisation : formation, transformation des entreprises et innovation.

[1] Etude réalisée en juin 2019 pour le compte de l'éditeur de logiciels de sécurité Sophos dans 12 pays : Etats-Unis, Grande-Bretagne, Allemagne, Inde, Canada, Brésil, Colombie, Mexique, Australie, Japon, Afrique du Sud.

Cybersécurité et Collectivités : un enjeu de sécurité nationale

WILLIAM LECAT
Coordinateur Plan de Relance Cybersécurité
Secrétariat Général pour l'Investissement

La diversité de tailles et de maturités, complexe pour la cybersécurité

Le sujet de la cybersécurité pour les collectivités dans leur ensemble est complexe. En effet, le terme de collectivité adresse des entités autant géographiquement dispersées que variées en terme de taille. Cela induit naturellement une diversité de maturité sur les problématiques cyber mais aussi, du point de vue des fournisseurs de sécurité, une difficulté à les adresser commercialement. Sur bien des aspects, les problématiques de cybersécurité des collectivités rejoignent celles des TPE et des PME, ne serait-ce que sur les questions de dimensionnement, de compétence et de sensibilisation.

De manière générale, il semblerait que l'investissement dans l'informatique relativement à la taille d'une structure est plus faible pour les petites entités. La part de l'investissement cyber est encore plus sensible à ce phénomène. En caricaturant, plus une entité est petite plus son équipement informatique risque d'être désuet et la cybersécurité absente. Cette non linéarité a plusieurs conséquences en fonction de la taille. Tout d'abord, de manière négative, elle rend difficile la communication sur ces sujets entre les entités de différentes tailles et a tendance à accroitre les écarts avec le temps. De plus, cela affecte l'impact des investissements et donc la spontanéité avec laquelle ils sont faits. Sans surprise, plus une entité est mature en cyber, moins un investissement, relativement à sa taille, a d'impact. En effet, plus une structure est sécurisée, plus l'augmentation de son niveau de sécurité est coûteuse. De manière plus étonnante, il apparait que les acteurs partant de très bas au niveau cyber

nécessitent un investissement important (toujours relativement à leur taille) pour amorcer leur sécurisation. Dans ces conditions, la rentabilité immédiate d'un investissement en cybersécurité représenterait plus ou moins une gaussienne fonction de la maturité (et souvent de la taille) de l'entité. Dans une volonté de tirer la sécurité de chacun des acteurs vers le haut, il apparait donc que pour les plus petites entités (souvent moins matures en cyber), l'impact observable émergera à moyen terme et nécessitera un investissement relativement à leur taille plus important que pour les acteurs moyennement matures. Les acteurs matures en cyber, quant à eux, sont relativement rares. Néanmoins, la criticité de ces entités n'est pas toujours fonction de leur taille.

Une menace principalement cybercriminelle pour le moment

La cybercriminalité correspond aujourd'hui à la grande majorité des attaques de manière générale. Les collectivités n'échappent donc pas à cette menace qui constitue à l'heure actuelle l'un de leurs risques principaux. Le ransomware, très visible en ce moment, est certainement une source d'inquiétude majeure. Néanmoins, pour des raisons qui devraient paraitre évidentes par la suite, les collectivités pourraient présenter une cible de choix pour les menaces étatiques plus ciblées, à des fin d'espionnage ou de déstabilisation. Il est d'ailleurs important de noter que si beaucoup s'inquiètent déjà de la menace « systémique » que représente la cybercriminalité, elle est pour le moment très sporadique. Seule une menace étatique pourrait avoir un impact systémique sur une typologie de victimes aussi diverse et dispersée ne serait-ce qu'en raison des moyens à déployer. Ce type de menace pourrait de surcroit rester invisible pendant plusieurs années avant d'être découverte ou de se manifester. Néanmoins, la prépondérance et la visibilité du ransomware de nos jours font de la cybercriminalité la crainte d'aujourd'hui, repoussant potentiellement à plus tard les inquiétudes vis-à-vis d'autres menaces cyber. Il faut tout de même garder à l'esprit que si les cybercriminels capitalisent sur la nuisance que peut représenter une attaque isolée sur une collectivité, une action coordonnée sur de multiples collectivités pourrait avoir un effet dévastateur.

Pourquoi les collectivités peuvent représenter une cible de choix pour les cybercriminels ?

La numérisation de notre société et de tous ses secteurs s'est accrue rapidement depuis des années. La crise sanitaire n'a fait qu'amplifier ce phénomène. Le numérique fait partie intégrante de notre vie sur de nombreux aspects, même si l'on ne le remarque pas ou plus, que ce soit dans les transports, dans la vie professionnelle ou même dans nos logements. Malheureusement, un tel rythme nécessite un effort considérable d'un point de vue cybersécurité pour garder la maitrise de la sécurité des différents réseaux et équipements. Sans surprise, la convergence des différentes connectivités vers les technologies de l'Internet a permis aux menaces de se répandre à moindre coût sur les domaines nouvellement connectés. Depuis la crise sanitaire, la conjonction de l'augmentation des attaques et de la numérisation en marche forcée nous amène face à une possibilité de décrochage, le rattrapage au niveau cyber risquant de prendre plusieurs années. Il en ressort que, tristement, les cybercriminels ne peinent pas à trouver des cibles au maximum de leur capacité d'exploitation, attirant ainsi constamment de nouveaux acteurs. Il y a quelques années encore, ce phénomène était décrit comme anecdotique mais aujourd'hui les États s'interrogent à juste titre sur l'impact de la cybercriminalité sur leur croissance économique. Même si le secteur de la cybercriminalité est relativement opaque, il n'y a aucun doute sur l'accélération de son industrialisation, sur l'augmentation de son niveau de technicité et de sophistication, voire de spécialisation. Une ingénierie spécialisée a émergé, bénéficiant du marché noir du « dark web », vendant des outils d'attaque de plus en plus automatisés et performant permettant à des acteurs avec un niveau technique relativement commun de réaliser des opérations de compromission de grande ampleur. Néanmoins, ce type d'opération, même en mutualisant les infrastructures pour faire levier sur les coûts fixes et en optimisant les processus, présente une source de dépense. Les cibles se présentant par milliers, voire millions, les cybercriminels auront naturellement tendance à se focaliser sur celles présentant le moins de résistance ou la meilleure espérance de revenu. Il s'agit ici d'un aspect très important du problème mais aussi potentiellement de la solution. Beaucoup d'éléments laissent à penser que les compromissions sont principalement opportunistes, les attaquants

n'ayant pas d'idée a priori des typologies exactes des cibles. Il est même possible que certains acteurs se soient spécialisés dans la phase de première compromission uniquement et revendent massivement et de manière indifférenciée les accès illicitement acquis à d'autres criminels qui déploient ensuite toutes sortes de ransomware et demandent des paiements aux victimes. Il existe donc toute une chaine de valeur de la cyberattaque. Cet aspect est particulièrement inquiétant, plus encore que la recrudescence des attaques observées. En effet, dans ce scenario, il est possible que des millions d'accès illégitimes soient en attente de revente et d'exploitation (l'exploitation étant plus chronophage que la compromission initiale). Les premiers confinements en 2020 ont forcé de très nombreux acteurs à ouvrir numériquement leurs portes, portes que l'on commence à peine à sécuriser. Il y a donc eu une très longue période d'opportunité pour des compromissions massives et indiscriminées. Malheureusement, les collectivités tombent dans une catégorie d'acteurs particulièrement exposés à ce risque et peu équipés pour y faire face.

Pourquoi les collectivités sont-elles peu équipées ?

Au-delà du fait que peu d'acteurs sont très bien équipés en cybersécurité dans l'absolu, les collectivités, en tant que petite structure, souffrent de plusieurs facteurs aggravants. Tout d'abord, elle se tournent massivement vers la numérisation qui amène des perspectives très importantes fonctionnellement mais aussi au niveau de la réduction des coûts dans bien des cas. Paradoxalement, alors que ce type d'acteurs est massivement attiré par le numérique, la cybersécurité actuelle reste largement inadaptée pour lui. Les solutions actuelles restent très complexes à déployer, techniques à opérer et coûteuses à maintenir, autant d'inadéquation avec les petits acteurs qui n'ont que peu de budget et pas vocation à internaliser systématiquement une compétence cyber. La question tourne donc beaucoup autour du coût et de la compétence (elle-même coûteuse et rare). Du point de vue des offreurs de solutions, un produit sur-mesure vendu à un client techniquement compétent à un prix élevé est plus attractif. En effet, le célèbre ratio du 80/20, où 80% des fonctionnalités représentent 20% d'efforts alors que les 20 derniers pourcents fonctionnels coûtent 80% d'efforts supplémentaires, semble très vrai en cybersécurité. Or, ce sont bien ces 20 derniers pourcents fonctionnels, le packaging,

l'automatisation et la facilité d'utilisation, dont les petites structures ont besoin… à un coût réduit. Il y a donc la nécessité d'un passage à l'échelle commerciale, d'un « mass market » pour que ce type de produit puisse exister à des prix abordables tout en rentabilisant les coûts de développement. A l'opposé, les petites structures peuvent également tenter de se regrouper, sous réserve que leurs problématiques soient similaires, et de mutualiser les coûts liés à la cybersécurité pour accéder aux solutions actuelles. Ces deux actions, allant l'une vers l'autre, doivent être menées en parallèle pour accélérer leur rencontre (des solutions relativement simples et à prix moyens pour de petits acteurs rassemblés pour former un groupe de taille moyenne).

Les collectivités, des acteurs particulièrement sensibles ?

Rien de tel qu'une « smart city », étendard de la modernité, pour augmenter la visibilité d'une commune, d'un département ou d'une région. Tout est connecté ou le sera bientôt permettant l'apparition de nouveaux usages très rapidement devenus indispensables. Face à ce phénomène, on visualise rapidement le niveau d'exposition croissant à la menace cyber. On peut déjà imaginer des ports, des aéroports, des axes routiers, des réseaux électriques ou de distribution d'eau bloqués par une attaque informatique. Les impacts seront indéniables et très problématiques. Néanmoins, inutile d'attendre l'émergence de ces nouvelles technologies pour se rendre compte des conséquences d'une attaque sur une collectivité. A l'heure où les fuites de données personnelles se multiplient et interrogent de plus en plus, doit-on se poser la question des données personnelles que détient une collectivité ?

Peut-on sécuriser les particuliers ?

Les problématiques des petites structures sont exacerbées chez les particuliers. Or, ils sont également massivement victimes de cybercriminalité. Une des pistes de solution évoquée consisterait donc à les regrouper pour atteindre une taille critique sur une même typologie de besoin. Les collectivités pourraient choisir de se positionner sur ce point de regroupement pour tenter de fournir un service public de cybersécurité tant pour ses citoyens que pour ses entreprises (TPE et PME en

particulier). Il y aurait donc un deuxième enjeu cyber au niveau des collectivités : d'abord leur sécurité puis leur rôle dans la cybersécurité de leur territoire. Le besoin de produits simples, voire transparents, à l'utilisation serait néanmoins toujours plus présent mais la concentration pour atteindre une taille critique permettrait de supporter un coût potentiellement plus élevé et la complexité de la mise en place. Il s'agit typiquement de la cible technologique des projets sélectionnés dans le Grand Défi cyber dans le cadre du troisième axe de la feuille de route : « protection des petites structures contre la cybercriminalité ». Le premier frein à la baisse des prix de ce type de solutions étant le coût de leur développement (cf. règle des 80/20 ci-dessus) avant leurs coûts d'opération, le Grand Défi a investi plus de 4M€ pour financer la R&D sur les aspects de sécurité de la navigation web et de l'email pour avancer vers la sécurisation de ces petites entités et des particuliers. En effet, le mail et le web représentent 95% des vecteurs d'attaques cybercriminelles. Ces investissements seront poursuivis dans le cadre de la Stratégie Nationale cyber.

Ce type de mesures, même si elles sont loin de sécuriser intégralement un territoire, pourrait avoir un impact majeur. En effet, comme mentionné précédemment, pour être moins attractif pour le cybercriminel, il « suffit » d'être plus dur à attaquer (même légèrement) que d'autres et de donner des perspectives de revenu faibles. Sur ce dernier point, le non-paiement des rançons et l'affichage clair de cette politique semblent être essentiels. Ainsi, en combinant le non-paiement généralisé des rançons et le déploiement massif de solutions de cybersécurité simples pour élever même légèrement le niveau de sécurité globale, on peut s'attendre à « un effet d'éviction » où les cybercriminels déporteraient leurs activités vers d'autres cibles plus attractives.

Des territoires de cybersécurité

A l'heure où l'Union Européenne se consolide en cybersécurité et où la France lance une Stratégie Nationale cyber plus ambitieuse que jamais, les territoires feront la différence pour l'atteinte des objectifs fixés. En effet, la structuration de l'écosystème cyber doit passer par une polarisation thématique, sectorielle et régionale. Que ce soit au niveau de la stimulation

de l'entreprenariat, de l'émergence de centres d'excellence et de recherche régionaux ou de la formation, le rôle des collectivités est central. C'est l'objet en particulier des projets de Campus Cyber régionaux qui ont vocation à former un véritable réseau en France et en Europe. Il en va de même de l'initiative de Startup Studio cyber qui, bien qu'en cours de lancement à Paris et à Rennes, a vocation à pouvoir être étendue dans différentes villes et régions.

La cybersécurité est un enjeu majeur pour les territoires et les collectivités. A ce titre, près d'un tiers du budget mis en œuvre par les puissances publiques dans la Stratégie Nationale cyber y est dédié. Dans ce cadre, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) bénéficie spécifiquement d'un budget de 136M€ issu du Plan de Relance avec pour objectif un fort impact sur le niveau de cybersécurité des collectivités. La Stratégie met également en œuvre un budget de 20M€ pour financer le développement de démonstrateurs territoriaux répondant aux besoins spécifiques identifiés. Enfin, l'effort de soutien au développement de solutions pour les petites structures se poursuivra dans le prolongement des actions du Grand Défi cyber. Néanmoins, pour que ces mesures puissent être exploitées au maximum, un effort important de communication devra être fait afin de généraliser la connaissance de l'existence de ces dispositifs et exprimer clairement leurs objectifs.

Collectivités : vous disposez d'un levier de performance trop souvent méconnu ! Et si vous osiez la « protection des informations et du numérique » ?

PHILIPPE LOUDENOT
Délégué cybersécurité, Région des Pays de la Loire
Administrateur, CESIN

Les collectivités territoriales sont des acteurs trop méconnus. Ce sont des structures administratives françaises, distinctes de l'administration de l'État, qui doivent prendre en charge les intérêts de la population d'un territoire précis. Il y a trois catégories de collectivités : les communes, les départements, les régions. Nous comptons aujourd'hui en France un peu plus de 35000 collectivités territoriales (tableau 1) se décomposant comme suit :

	2020
Communes	**34 968**
Dont : France métropolitaine	34 839
Outre-mer	129
Conseils départementaux	**96**
Dont : France métropolitaine	94
Outre-mer	2
Conseils régionaux	**14**
Dont : France métropolitaine	12
Outre-mer	2
Collectivités à statut particulier	**5**
Collectivité territoriale de Corse	1
Collectivité de Corse	1
Métropole de Lyon	1
Martinique	1
Guyane 1	
Département de Mayotte	1

Tableau 1 : Les collectivités territoriales en France métropolitaine et dans les départements d'outre-mer (en nombre de collectivités) - Source : Insee, Code officiel géographique.

Logement, action sociale, urbanisme, environnement, aménagement du territoire, développement économique, culture, sport, tourisme, transport scolaire, etc. dans tous ces domaines, les collectivités disposent chacune de compétences administratives différentes et complémentaires de celles de l'État. Afin de répondre à ces missions, les collectivités sont engagées dans une profonde transformation numérique, notamment leurs échanges dématérialisés avec leurs concitoyens, les acteurs économiques et les administrations publiques qui se sont ainsi multipliés. L'e-administration (simplification administrative) est un axe important de la modernisation de l'action publique et répond à une demande effective des citoyens dans le cadre de l'e-démocratie. De même s'est accélérée la mise en place de sites « vitrines », proposant de présenter la vie de la collectivité et le champ des possibles sur une commune, une communauté de communes, un département ou une région.

L'augmentation de la population urbaine, les contraintes sur les finances publiques, la transition énergétique induisent le besoin de réinventer le lien entre le service public et l'usager, au service de l'augmentation du confort de vie des habitants. Autant de problématiques que les « Smart Cities » peuvent contribuer à adresser et qui poussent les collectivités à investir dans cette direction. De nombreuses collectivités en France se sont ainsi emparées du sujet Smart City pour faire face aux défis énoncés précédemment : de grandes métropoles bien sûr, mais également des villes de tailles plus modestes.

Une condition de réussite : la transformation numérique doit être intégrée et les directions numériques être forces de propositions et porteuses des politiques publiques en la matière, au regard des champs d'intervention des collectivités.
Que ce soit au niveau national, avec des compétences différentes selon la collectivité en question :

- pour les communes : enseignement primaire et scolarisation, logement, action sociale, culture, etc.
- pour les départements : action sociale et sanitaire (loi du 22 juillet 1983), éducation (collèges), culture, patrimoine, etc.
- pour les régions : développement économique, aménagement du territoire et développement durable, éducation (lycées), formation professionnelle, culture et santé, etc.

Ou au niveau international, en agissant dans le cadre de la coopération décentralisée.

Les collectivités possèdent, parfois sans le savoir ou l'avoir appréhendé, des informations qui peuvent être éminemment sensibles. D'une part, les applications ou fichiers utilisés par les collectivités recensent de nombreuses informations sur les particuliers, administrés ou autres usagers : données individuelles, état civil, sociales (aides sociales, données médicales, régime alimentaire, handicap, etc.), financières (revenus fiscaux, quotient familial, redevances, etc.), d'urbanisme, de police, etc. D'autre part, pour leur fonctionnement en propre : elles détiennent ainsi des données concernant leurs personnels (CV, position, ancienneté, statut, absences, maladies, arrêts, etc.), des données financières, stratégiques (travaux préparatoires à une délibération, résultat de vote électronique, études foncières, projets de délibérations, schémas d'aménagement, documents budgétaires), etc.
C'est donc une quantité d'informations sur lesquelles un acte de cybermalveillance ou un piratage est susceptible de porter atteinte aux droits et libertés des personnes ou à leur vie privée, mais également d'engager la responsabilité des élus.

Au-delà des données, les systèmes numériques doivent également faire l'objet d'une attention particulière. Quand il est ici fait mention de systèmes numériques, il est bien sûr fait allusion à ce que traditionnellement l'on qualifie de systèmes informatiques : réseaux, serveurs, applications, postes de travail. Mais la cible est beaucoup plus large : vidéosurveillance, centres d'appels, smart cities (avec une quantité de dispositifs permettant la gestion de l'énergie, de l'eau, panneaux d'affichages, circulation, etc.). Cela augmente donc de façon significative les surfaces d'attaque.

Ajoutons à ce constat, la crise liée à la COVID-19 qui a entraîné le développement du télétravail rendu indispensable pour assurer la continuité des services publics, et auquel les collectivités, comme de nombreuses entreprises d'ailleurs, n'étaient pas préparées.

Accompagnant ces mouvements de fond vers plus de numérique dans l'organisation des collectivités, on observe depuis ces dernières années une augmentation importante des attaques et des incidents notables impactant

ces dernières. Le nombre de cyberattaques contre les collectivités locales a ainsi augmenté de 50 % en 2020. Le chiffrement des données suivi d'une tentative d'extorsion de fonds est la technique employée la plus courante. Longtemps touchées à la marge par rapport aux acteurs privés ou étatiques, les collectivités sont devenues des cibles privilégiées des cybercriminels, comme récemment La Rochelle, Angers, Suze sur Sarthe, Douai…
La question n'est donc pas, et cela s'applique à n'importe quel type de structure entrée dans le monde numérique, de savoir « si » l'on peut être la cible d'une cybermalveillance, mais « quand » on sera la cible d'une cybermalveillance.

Parallèlement, par manque de connaissance ou de prise en compte, certains fondamentaux « oubliés » de protection peuvent entrainer une atteinte grave sur les informations, que ce soit sur la disponibilité des données, leur intégrité ou leur confidentialité.

La protection de l'information et sécurité du numérique, ou cybersécurité, est encore souvent une thématique que les collectivités ont du mal à appréhender. Ce n'est pas dans leur ADN et cela n'est que rarement l'objet de leurs préoccupations. Inscrites dans un processus de modernisation continue de leur administration et des services qu'elles délivrent, elles sont au tournant de la numérisation de la « relation citoyen », avec au cœur de leur action la simplification des usages, demandée par les habitants eux-mêmes.

Or, un défaut de prise en compte du risque numérique peut avoir des conséquences pouvant être dramatiques. A titre d'illustration, l'incendie qui a détruit le centre de données strasbourgeois de l'entreprise OVHcloud, leader européen de l'hébergement de sites internet, dont de nombreux services utilisés par des collectivités, a impacté un certain nombre de collectivités mais également de petites entreprises de leur territoire : un des fondamentaux de la sécurité en numérique, la sauvegarde, avait été oublié ou méconnu. Pour certaines, l'impact immédiat est malheureusement des pertes de données irrémédiables.

Cependant, si le tableau fait apparaître de nombreuses zones grises, il n'est pas si sombre mais à la condition de prendre en compte le risque numérique,

de valoriser les actions en matière de protection, véritable fondation de toute transformation. Il s'agit de s'appuyer sur les différents leviers permettant d'agir.

Au profit des collectivités, un certain nombre d'actions de sensibilisation, de partage de bonnes pratiques ou d'appui en matière de cybersécurité sont déjà mises en œuvre.

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. Si elle apporte son expertise et son assistance aux administrations centrales et aux opérateurs d'importance vitale, il lui est toutefois impossible d'adresser l'ensemble de la Nation. En 2017, issu de la Stratégie numérique du Gouvernement, dont les objectifs ont été ensuite détaillés dans la Stratégie Nationale pour la Sécurité du Numérique, le GIP ACYMA (Cybermalveillance.gouv.fr) a été ainsi mis en place. L'État est à l'époque parti du constat que, s'il était plutôt en mesure de protéger ses propres infrastructures ou les infrastructures vitales du pays, il se devait d'apporter une réponse structurée aux autres composantes de la société, souvent désarmées face à une cybercriminalité en plein essor. Le GIP ACYMA (cybermalveillance.gouv.fr) agit ainsi contre la cybermalveillance au sens large pour les structures hors du périmètre d'intervention de l'ANSSI.

Différentes actions de sensibilisation existent, notamment :

- Une série de vidéos mettant en scène des collectivités face aux risques numériques, réalisée par Cybermalveillance.gouv.fr en partenariat avec la Banque des Territoires (Groupe Caisse des Dépôts). Dans chaque scénario, un maire est présenté comme une victime d'une cyberattaque avec ses conséquences. Quatre menaces y sont abordées : le rançongiciel, la fuite de données, le piratage de l'arrosage public et le piratage des feux de circulation.
- Il est impossible ici de ne pas citer le Tour de France de la Cybersécurité lancé en 2018. Sur le terrain, ce sont des événements fédérateurs au service du développement des territoires, qui réunissent experts et non experts, acteurs nationaux, européens et locaux, autour de thématiques de sécurité numérique en adéquation avec les enjeux de développement du tissu économique local.

La crise sanitaire sans précédent vécue par tous a également été accompagnée, sur le volet numérique, par une explosion d'attaques et actes de cybercriminalité. Ainsi la nécessité de démultiplier les actions en cybersécurité est désormais prise en compte à tous les niveaux avec différentes propositions.

Dans le cadre du plan de relance, sont mises en œuvre :

- Un appel à manifestation d'intérêt sur la thématique de « sécuriser les territoires » qui s'adresse à trois types d'acteurs du territoire (collectivités territoriales, établissements de santé et infrastructures portuaires) souhaitant expérimenter des démonstrateurs de cybersécurité qui répondent à leurs besoins. Au-delà du cœur du système d'information (réseau, ordinateurs et applications), il s'agit donc de sécuriser l'ensemble des infrastructures numériques territoriales : véhicules connectés, feux de circulation, lampadaires, capteurs et autres mobiliers urbains communicants… ;
- L'offre de l'ANSSI, ouverte à toutes les collectivités, qui propose une phase diagnostic dont la réalisation est confiée à des prestataires labellisés et intégralement prise en charge financièrement par l'ANSSI. Ce diagnostic proposera à la collectivité une feuille de route pour sécuriser son système d'information ;
- Appel à projets pour la création de CSIRT régionaux (Computer Security Incident Response Team), centre de réponse aux incidents cyber, dont la mission sera de soutenir et d'orienter collectivités, TPE/PME, ETI et victimes d'attaques ou d'incidents numériques "de premier niveau". Ils traiteront les demandes d'assistance et les mettront en relation avec des partenaires de proximité : prestataires de réponse à incident et partenaires étatiques, en coordination avec l'ANSSI et Cybermalveillance.gouv.fr, mais également les différents représentant de l'État, notamment la police et la gendarmerie ;
- La proposition de mettre en place un centre d'appel.

Une prise en compte des risques cyber est ainsi aujourd'hui incontournable pour les collectivités : elle ne peut plus être oubliée ou mise de côté. Et, au-delà de sa dimension technique, la cybersécurité est un véritable sujet de gouvernance dont la responsabilité relève du plus haut niveau des organisations. Il est de la responsabilité des élus de s'emparer de la maîtrise des risques pesant sur les données et des systèmes d'information numériques, non pas dans leur dimension technique, mais bien en termes d'enjeux de

développement à travers la transformation numérique que vivent aujourd'hui les collectivités et les politiques publiques locales qui s'appuient sur le numérique. Cette prise en compte permettra ainsi de proposer des systèmes de confiance vertueux au niveau des écosystèmes locaux tout en favorisant le développement de solutions, qui elles-mêmes permettront de générer de l'attractivité sur un territoire. Cette prise en compte doit être accompagnée par un changement de paradigme en démontrant que la protection des données et la sécurité du numérique ne sont pas qu'un centre de coûts : elles constituent véritablement un investissement pour un développement pérenne et un fantastique levier de performance.

L'assistance aux collectivités, une cible prioritaire du dispositif Cybermalveillance.gouv.fr

JÉRÔME NOTIN
Directeur Général
Cybermalveillance.gouv.fr

Les collectivités sont l'un des publics principaux pour lequel le dispositif national de prévention et d'assistance aux victimes Cybermalveillance.gouv.fr a été créé il y a maintenant bientôt quatre ans. Son directeur général Jérôme Notin, revient sur l'offre de service de ce dispositif, ainsi que sur les services et action qui sont développés pour ce public.

Origine, missions et services offerts par Cybermalveillance.gouv.fr

Lancé fin 2017, notre dispositif est la réponse voulue par l'État pour faire face à la croissance de la cybercriminalité et répondre au besoin de la population qui en est victime pour l'aider à s'en prémunir et y faire face.

Créé conjointement par l'Agence nationale de sécurité des systèmes d'information et du ministère de l'Intérieur, notre dispositif vise à apporter une information et une aide concrète aux publics.

Cybermalveillance.gouv.fr rassemble dans un groupement d'intérêt public plus de 50 acteurs étatiques et de la société civile engagés à ses côtés pour contribuer à sa mission. On retrouve ainsi parmi nos membres des ministères et agences, des associations professionnelles, de consommateurs ou encore d'aide aux victimes, des opérateurs, des éditeurs, des assureurs …

Les services offerts par Cybermalveillance.gouv.fr s'adressent à tous les types de publics qui ne sont pas couverts par les autres dispositifs de l'État. Il s'agit donc des particuliers, des entreprises, des associations, des administrations et des collectivités, et en particulier pour ceux d'entre eux

qui ne disposent pas de connaissances ou de moyens suffisants en cybersécurité.

Nos missions s'articulent en trois axes qui s'alimentent entre eux dans une boucle vertueuse.

En premier lieu, il y a l'observation de la menace qui vise à avoir la vision la plus précise possible des phénomènes cybercriminels afin d'adapter au mieux nos services aux besoins de nos publics, ainsi que de pouvoir alimenter en informations les acteurs étatiques qui luttent contre la cybercriminalité (ministères de l'Intérieur et de la Justice en particulier). Fort de cette connaissance, vient ensuite la prévention, avec la diffusion de nombreux supports sur les bonnes pratiques à adopter pour se protéger et faire face aux différentes formes que la cybercriminalité peut revêtir. Cette prévention passe par la mise à disposition sur notre plateforme de nombreux contenus pédagogiques (articles, vidéos, infographies…), d'alertes et de campagnes de sensibilisation menées avec nos membres et partenaires diffusées dans les médias dont des spots télévisés.

Arrive enfin au cœur de notre action, l'assistance aux victimes en leur permettant sur notre plateforme d'obtenir un diagnostic en ligne de leur situation et les conseils adaptés pour y remédier. Cette assistance va jusqu'à la possibilité d'une mise en relation avec un des plus de 1 100 prestataires spécialisés de proximité référencés par notre plateforme qui pourront apporter leur aide aux victimes qui ne sont pas en mesures d'appliquer seules nos conseils.

À l'exception du recours à un prestataire spécialisé, tous les services offerts par Cybermalveillance.gouv.fr sont gratuits. En 2020 la plateforme a reçu plus de 1,2 million de visiteurs.

Les collectivités - cibles de choix pour les cybercriminels

Les collectivités ont longtemps pu penser qu'elles pourraient rester épargnées par les cyberattaques ou du moins que si elles l'étaient leurs impacts pourraient rester mineurs.

Il est vrai qu'il y a quelques années encore, les principaux risques auxquels elles pouvaient être confrontées touchaient leur seul site Internet qui pouvaient se retrouver saturé ou modifié par des pirates aux compétences limitées et agissant avec des motivations idéologiques ou ludiques.

Mais aujourd'hui la situation a bien changé. Depuis plus d'un an, il ne se passe plus une semaine sans qu'une métropole, une commune, un conseil régional ou départemental ne soit frappé avec des conséquences particulièrement graves dans la réalisation de leurs missions de service public.

L'écosystème cybercriminel s'est considérablement développé et « professionnalisé » et les collectivités sont à présent confrontées à des niveaux de sophistication d'attaques proches de celles qui pouvaient être réalisées autrefois par des États.

Suivant le rythme de la société, les collectivités ont considérablement développé leur numérisation ces dernières années, tant pour optimiser leur fonctionnement que pour offrir de nouveaux services à leurs usagers.
Ne percevant pas qu'elles augmentaient dans le même temps considérablement leur surface d'attaque, la criticité des services et informations qu'elles détenaient, et le niveau de menace qui allait peser sur elles, les collectivités, et en particulier les plus petites et donc les plus fragiles d'entre-elles, n'ont bien souvent pas réalisé les investissements nécessaires pour pouvoir y faire face.

Cette situation de fragilité n'a pas échappé aux cybercriminels qui ont fait des collectivités des cibles prioritaires dans un combat devenu très inégal. En 2020, plus de 2 000 collectivités sont venues chercher de l'assistance sur la plateforme Cybermalveillance.gouv.fr dont 159 suite à une attaque par rançongiciel.

En augmentation de 54 % par rapport à l'année précédente, cette menace a pris la première place des cybermalveillances en 2020 pour les collectivités.

Dans ce type d'attaque qui est aujourd'hui la principale menace auxquelles les collectivités sont confrontées, les cybercriminels vont essayer de s'introduire dans le réseau de la collectivité.

Pour cela, ils peuvent compromettre un premier poste qui aura ouvert une pièce-jointe dans un message malveillant et ensuite chercher à se propager dans le réseau. Ils peuvent également pénétrer le réseau via ses accès extérieurs en exploitant une vulnérabilité non corrigée ou encore en « forçant » un mot de passe trop faible.

Une fois dans le réseau de la collectivité, les cybercriminels vont chercher à détruire toutes les sauvegardes, voler toutes les données qui peuvent avoir à leurs yeux de la valeur et enfin saboter tout le système en chiffrant les fichiers dont les bases de données.

La collectivité se retrouve alors paralysée et confrontée à une demande de rançon pour pouvoir retrouver ses informations et en empêcher la divulgation.

Dans ce type de scénario malheureusement fréquent, la collectivité prend immédiatement conscience de sa dépendance et sa fragilité numérique quand il faut revenir au papier-crayon et parfois fax, ce que l'on ne sait parfois même plus faire.

La collectivité frappée se retrouve alors à devoir gérer une crise qu'elle n'a généralement pas anticipée.
Son fonctionnement se retrouve à l'arrêt et il lui faudra des semaines, voire des mois pour revenir à une situation normale, si tant est que des données n'aient pas été irrémédiablement détruites.

La responsabilité de la collectivité et de ses élus se trouve directement engagée, non seulement parce que le service aux usagers se retrouve interrompu, mais aussi parce qu'elle n'a pas su protéger les informations de ses agents et administrés qui peuvent à leur tour se voir personnellement impactés.

Peuvent s'ensuivre des mouvements sociaux ou même des poursuites engagées contre la collectivité pour manquement à ses obligations de protection des données personnelles, sans compter l'altération de la nécessaire confiance que les citoyens se doivent d'avoir dans leurs pouvoirs publics et leurs élus.

Face à une telle pression, la tentation peut être grande de payer la rançon demandée. Mais cela ne résout rien car non seulement cela alimenterait les réseaux cybercriminels avec des fonds publics les incitant à poursuivre leurs activités, mais dans tous les cas des efforts considérables seront à réaliser pour reconstruire les systèmes impactés. Et surtout il faut comprendre comment l'attaque a pu se produire, afin de pouvoir corriger ce qui doit l'être au risque d'une récidive.

La sensibilisation pour éveiller les consciences

Prévenir les populations contre les risques liés à la cybermalveillance et les bonnes pratiques à mettre en œuvre pour les palier constitue l'une des principales missions du dispositif Cybermalveillance.gouv.fr.

La sécurité est généralement vécue comme une contrainte et n'est donc efficace que si elle est comprise et acceptée. La défaillance humaine étant la principale cause des cyberattaques réussies, c'est par la sensibilisation et la formation des acteurs que l'on pourra minimiser les risques.

L'humain doit donc être mis au cœur du dispositif de détection, de réaction et de préservation de la sécurité de l'organisation. Mais l'humain est souvent résumé à l'utilisateur lambda, ce qui est une grave erreur. Certes, cet utilisateur a toute sa place dans cette démarche, mais pas moins que les techniciens et les informaticiens, fréquemment oubliés mais sur lesquels repose pourtant une grande partie de la sécurité.

Sans compter les cadres et élus qui sont d'autant plus des cibles de choix qu'ils peuvent avoir tendance à éluder les mesures de sécurité qu'ils ont eux-mêmes édictées.

Pour sensibiliser ses publics, et avec le concours de ses membres, Cybermalveillance.gouv.fr propose gratuitement sur son site de nombreux supports pédagogiques originaux et accessibles à tous, sous différents formats destinés à toutes les catégories de publics, tels des fiches pratiques pour apprendre les gestes essentiels pour se sécuriser ou réagir face à une attaque, mais aussi des vidéos didactiques, des infographies.… Ces supports sont également destinés aux organisations pour répondre à leur

demande de sensibilisation de leur personnel.

Mais pour ce qui concerne la situation particulière de fragilité et d'exposition au risque des collectivités, cela ne semblait pas suffisant. Cybermalveillance.gouv.fr a donc entrepris un programme de sensibilisation spécifique adressé aux collectivités et à leurs élus. Ce programme qui a démarré en 2020 et se poursuit en 2021 a été élaboré par un groupe de travail rassemblant nos membres et partenaires impliqués sur ce thème, dont des associations d'élus.

Ce programme s'est déjà concrétisé par une campagne d'information visant à s'adresser directement aux collectivités, pour leur présenter les risques auxquels elles étaient exposées, les bonnes pratiques de cybersécurité à mettre en œuvre, les services que Cybermalveillance.gouv.fr pouvait leur offrir, les actions internes qu'elles pouvaient engager. Tout cela assorti de témoignages d'élus et de cas concrets ciblant particulièrement les collectivités. On peut noter par exemple des vidéos co-réalisées avec la Banque des territoires1 où des élus vivent des cyberattaques dans leur collectivité, ainsi que la publication d'un guide pratique.

Ce programme se poursuivra en 2021 avec la réalisation de nombreux supports et actions de sensibilisations afin de porter les messages essentiels et éveiller les consciences sur les risques et moyens d'y faire face.

La cybersécurité est souvent perçue comme un sujet technique réservé aux techniciens. Or il s'agit bien au contraire d'un sujet stratégique, car une cyberattaque peut impacter le fonctionnement des services publics délivrés par les collectivités et même la sécurité des informations personnelles qui leur sont confiées par leurs administrés.

Bien entendu, il ne s'agit pas de transformer les élus en experts de la cybersécurité, mais de leur donner les clés sur les enjeux et les actions à entreprendre à leur niveau pour y faire face, telles par exemple les garanties à demander à leur support ou prestataire informatique, ou encore sur les actions à piloter à leur niveau en cas de cyberattaque.

Avant d'envisager des solutions de protection coûteuses et techniquement complexes à gérer, les collectivités doivent avoir conscience qu'une grande majorité d'attaques pourrait être évitée par l'application de mesures simples et peu onéreuses comme la bonne gestion des mots de passe, des sauvegardes efficaces et sécurisées, ou encore des systèmes tenus régulièrement à jour. On peut ajouter une bonne sensibilisation des agents, cadres et informaticiens aux différentes menaces et aux réactions à avoir lorsqu'on y est confronté.

De nouveaux services pour aider les collectivités à se sécuriser

Cybermalveillance.gouv.fr proposait déjà un service d'assistance en cas d'attaque au travers des conseils dispensés sur sa plateforme et de son réseau de prestataires référencés sur le territoire national au plus près des victimes.

Un autre besoin d'assistance a toutefois été identifié pour accompagner les publics professionnels et notamment les collectivités dans leur sécurisation afin d'éviter les attaques ou se donner les moyens de les contenir.

En effet, un système informatique qui fonctionne et rend son service n'est pas toujours un système sécurisé pour faire face aux attaques.
Sécuriser un système ou une infrastructure numérique requiert des compétences spécifiques dont les collectivités ou leurs prestataires de développement et maintenance informatique ne disposent que rarement en interne.

Comme dans d'autres domaines comme la médecine, l'informatique recouvre un ensemble de spécialités qui ne sont pas interchangeables et la cybersécurité est une spécialité à part entière. Si l'on veut poursuivre l'analogie par une métaphore : quand on a mal aux dents, il faut consulter un dentiste, pas un cardiologue.

Qu'il s'agisse donc de faire un état des lieux de sa sécurité numérique, de sécuriser ses systèmes ou de détecter les attaques, ou encore d'intervenir

pour y faire face quand elles se produisent, les collectivités doivent savoir se faire accompagner par des prestataires spécialisés en cybersécurité. Mais par où commencer ? À qui s'adresser ?

Pour répondre à ce besoin, Cybermalveillance.gouv.fr a créé en 2020, avec le soutien de l'AFNOR et en partenariat avec des organisations professionnelles, un label destiné à donner un premier niveau de reconnaissance des compétences des prestataires de cybersécurité dans la sécurisation des systèmes numériques, leur maintien en condition opérationnelle de sécurité et le traitement des incidents.

En juin 2021, 80 prestataires en cybersécurité ont déjà obtenu ce label baptisé ExpertCyber. Le service d'accès à ces prestataires ExpertCyber a été ouvert sur la plateforme Cybermalveillance.gouv.fr dans le cadre des annonces du Président de la République sur la stratégie nationale de cybersécurité de février 2021.

Ces prestataires labellisés ExpertCyber, qui verront leurs compétences réévaluées tous les deux ans, sont qualifiés pour accompagner les collectivités dans leurs projets de sécurisation afin d'assurer la protection de leurs informations et des services qu'elles délivrent.

Qu'il s'agisse d'aider les collectivités à sensibiliser leurs agents et même leurs administrés aux risques et bonnes pratiques de cybersécurité, de sécuriser leurs services et informations, ou même de réagir en cas de cyberattaques, les collectivités ne sont pas seules. Cyermalveillance.gouv.fr développe en permanence toutes une gamme de services accessible gratuitement pour répondre aux besoins des collectivités.

[1] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/programme-sensibilisation-risques-numeriques-collectivites-territoriales

Collectivités territoriales et systèmes de santé : cibles des cyberpirates

VINCENT TRELY
Président
Association Pour la Sécurité des Systèmes d'Informations de Santé (APSSIS)

Aulnoye-Aymeries, ville de 9 000 habitants, puis son CCAS et son EHPAD, Vincennes, Alfortville, Charleville-Mézières, Marseille métropole, la Région Grand-Est font partie de la longue liste des collectivités attaquées par des groupes de cyberpirates en 2020, selon un mode opératoire bien connu : le rançongiciel. Celui-ci, avec plus ou moins de virulence, bloque les systèmes informatiques en les chiffrant, rendant inopérants les services numériques et les accès aux fichiers de travail des agents, et détaille les modalités de paiement d'une rançon en cryptomonnaie censée offrir le retour à la normale. Guillaume POUPARD, Directeur général de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), rattachée au Premier Ministre, s'exprimant devant le Sénat, a déclaré que « la sécurisation des collectivités territoriales serait une priorité de 2021 ». En parallèle des ennuis rencontrés par nos communes, les établissements de santé subissent la même punition : les Centres Hospitaliers de Villefranche-sur-Saône, de Dax, d'Oloron-Sainte-Marie, de Narbonne, de Montpellier font partie des dizaines de structures de santé publiques ou privées attaquées ces douze derniers mois.

Alors pourquoi un tel engouement des criminels pour notre secteur public ? Pour quelles raisons s'en prendre à une ville, à un hôpital, à une maison de retraite ? Décryptage.

Des systèmes fragiles et des pirates fainéants

La croissance du cybercrime n'est pas un phénomène récent. Dès les prémices de la troisième révolution industrielle, celle des technologies

numériques, l'écosystème de la criminalité internationale s'est très vite adapté et organisé, comprenant que « le business » du futur se ferait via les réseaux d'échanges de données, les plates-formes de services informatisées et que l'or du 21ème siècle serait « la data », les milliards de données produites et stockées par des systèmes déployés partout sur la planète. Plusieurs études, dont celle du Club des juristes publiée en 2021, estiment que la cybercriminalité est déjà la 3ème économie mondiale, derrière la Chine et les États-Unis, et que son volume financier dépassera les 10 500 milliards de dollars en 2025. Quel est aujourd'hui l'intérêt d'aller braquer une agence bancaire, de risquer dix ans de prison et une balle dans la peau pour quelques milliers d'euros ? L'argent n'est plus « réel », il est dématérialisé.

Les secteurs de la banque / assurance, de l'industrie de pointe et des grands groupes du CAC 40 ont connu leurs premiers déboires dans les années 2000 et en ont tiré les leçons. Les récentes attaques du Groupe Bouygues Construction, de COVEA ou de la Banque Centrale Européenne rappellent que le risque zéro n'existe pas, mais pour autant, s'attaquer à ces mastodontes devient complexe et coûteux. Plusieurs mois de préparation, des équipes de hackers très performants et une organisation bien huilée sont nécessaires, pour des résultats toujours aléatoires, alors qu'une collectivité ou un hôpital sont des cibles bien plus faciles. Les fragilités de ces institutions s'expliquent par trois principaux facteurs : une surface de numérisation plus récente, avec le déploiement massif de l'informatique sur les quinze dernières années sur pratiquement tous les métiers et la mise en œuvre de multiples services communicants vers les citoyens et les patients, des investissements techniques et humains qui n'ont pas suivi, laissant la part belle à des matériels vieillissants, voire totalement obsolètes et truffés de failles de sécurité connues et documentées, et un manque de sensibilisation des personnels, rarement formés aux bons usages du numérique, à l'hygiène informatique et aux « gestes barrières ». Ces trois facteurs connus des criminels les orientent naturellement vers ces systèmes, plus poreux, plus fragiles et tout aussi lucratifs. N'oublions pas que les cybercriminels, en bons chefs d'entreprises, recherchent eux-aussi le meilleur retour sur investissement possible !

Des systèmes remplis de données sensibles et monnayables

Si les grands groupes sont aujourd'hui mieux protégés contre les attaques informatiques, à la fois grâce à des investissements plus soutenus et des politiques de sécurité matures, ils ne sont pas pour autant sans intérêt pour le cybercrime, et en particulier pour le volet cyber espionnage consistant à dérober tout type d'information stratégique dans le cadre de la guerre économique qui fait rage ! Mais c'est une affaire d'agences de renseignements, les Américains, les Chinois et les Russes se partageant les trois premières places du podium, ce qui n'est pas nouveau. Soyons heureux de savoir que l'Europe est en train de se doter, elle aussi, d'une force cyber offensive afin de pouvoir enfin jouer d'égal à égal avec nos alliés ou nos ennemis, en fonction de contextes géopolitiques instables.

Il serait très naïf de croire que l'intérêt croissant pour les collectivités ou le système de santé ne se base que sur leurs faiblesses. Les deux secteurs sont très attractifs en termes de contenus ! Remplis de données à caractère personnel, administratives, de santé, de situation, ils constituent une mine d'or intarissable pour le crime organisé. Le Règlement Général sur la Protection des Données, mis en application par la Loi le 25 mai 2018, impose aux organisations, dans son article 32, de mettre en œuvre toutes les mesures de sécurité relatives à la protection des données, afin de protéger les citoyens contre la fuite, la destruction ou la corruption de leurs données. Les amendes en cas de manquement sont non négligeables (entre 400 000 et 600 000 euros prononcés contre des Hôpitaux européens, 30 000 euros contre l'Office HLM de la Métropole de Rennes, 204 millions d'euros pour British Airways, 20 millions d'euros pour le Groupe Marriott…).

Alors quels intérêts pour les pirates ? Ils sont multiples : extraire les données pour les revendre sur le marché noir de l'internet (et rassurez-vous, il y a de nombreux acheteurs !), exercer un chantage financier sur l'institution dont les données ont été volées (et qui pèsera le pour et le contre entre le paiement du chantage ou celui de l'amende, de l'atteinte à l'image et des éventuelles poursuites engagées par des citoyens fâchés de voir leur vie privée s'étaler sur les réseaux sociaux), utiliser les données dérobées pour fabriquer de fausses identités, de faux documents, voire

pour s'en prendre directement aux personnes physiques (le vol de plus de 25 000 dossiers de psychiatrie en Finlande en 2020 a donné lieu à des prises de contacts et à des chantages directs auprès des patients, sur le mode « j'ai votre dossier psychiatrique devant moi, alors c'est 1 000 euros ou je le publie et informe votre famille et votre employeur »). Comme le disait Claude LELOUCH : « Le pire n'est jamais décevant ».

La riposte du système de santé : un modèle clonable

L'article L.1111-8-2 du code de la santé publique institue l'obligation de signalement des incidents de sécurité des systèmes d'information. Le décret d'application n°2016-1214 du 12 septembre 2016 précise que les incidents graves de sécurité des systèmes d'information du secteur santé doivent être signalés sans délai à compter du 1er octobre 2017 pour les établissements de santé, les hôpitaux des armées, les centres de radiothérapie et les laboratoires de biologie médicale. Enfin, l'arrêté du 30 octobre 2017 présente les modalités de signalement et de traitement des incidents graves de sécurité des systèmes d'information. L'objectif de ce processus de signalement est double : recenser les incidents et leur typologie afin de factualiser la situation et d'adapter la riposte, accompagner, le cas échéant, les structures en difficulté, comme cela a pu être le cas pour le CHU de Rouen ou l'Hôpital de Villefranche.
Il est plus que probable que ce dispositif s'étende à l'ensemble des institutions publiques et aux collectivités (villes, métropoles, départements, régions), ce qui serait normal, tant pour la surveillance cyber de nos institutions que pour l'information transparente des usagers.

En complément de ces dispositions, le Président de la République a annoncé, en février 2021, l'accélération du déploiement du « service national de cyber surveillance en santé » en partenariat avec l'Agence du Numérique en Santé (ANS) et le développement des moyens du dispositif « cyber veille en santé » pour augmenter les capacités de réaction et d'appui aux structures en cas d'incidents ou de cyberattaques. Encore trop d'établissements restent « frileux » à déclarer un incident de sécurité, habités par un sentiment de honte ou d'une peur de mauvaise publicité. Il faut dépasser ce sentiment naturel et entrer définitivement dans une dynamique de transparence et de coopération. Ce qui arrive aux uns

arrivera aux autres et aucune autorité ne considère aujourd'hui qu'une cyberattaque est la conséquence a priori d'un manquement. Les déclarations constituent un indicateur factuel et performant, et contribuent clairement à faire progresser l'écosystème.

Lors des annonces du Président de la République, la formation des professionnels de santé aux bons usages des technologies numériques et à la cybersécurité est annoncée comme essentielle et prioritaire. La sensibilisation à la cybersécurité sera intégrée dans tous les cursus de formation des acteurs en santé afin de conforter les pratiques « d'hygiène numérique » dans un contexte de renforcement de la convergence et de l'interopérabilité des systèmes d'information comme de la fluidité du parcours ville-hôpital. Il est grand temps de corriger cette anomalie qui a consisté depuis quinze ans à mettre entre les mains des soignants et des agents publics en général des voitures de course sans leur avoir fait passer ni le code, ni le permis. L'humain est et restera le meilleur moyen d'assurer au système un haut niveau de sécurité, en le formant à la vigilance, un juste milieu entre la naïveté et la paranoïa !

Le RSSI : une pièce centrale enfin reconnue !

Longtemps considéré comme un « geek » un peu paranoïaque, le Responsable de la Sécurité des Systèmes d'Information (RSSI) est en passe d'être enfin reconnu comme pièce maitresse du dispositif de maîtrise du système d'information et de lutte contre les multiples menaces internes et externes. Il devient essentiel de lui donner une existence et un soutien, par un courrier de nomination explicite, signé de la Direction Générale et largement diffusé, une indépendance, par son rattachement à une Direction « neutre » (Qualité, Juridique ou DG), et des moyens, avec le souhait ministériel d'une meilleure prise en compte de la cybersécurité dans tous les projets de systèmes d'information.

Dans sa communication du 22 février 2021, le Ministère des Solidarités et de la Santé précise : « Face à l'augmentation de la menace, il n'est plus possible de faire de la cybersécurité une variable d'ajustement des projets informatiques des établissements de santé. Ainsi, aucun projet ne pourra désormais faire l'objet d'un soutien de la part de l'Etat si une part de à

5 à 10% de son le budget informatique n'est pas dédiée à la cybersécurité. » Après tout, lorsque l'on achète une voiture, les freins et les ceintures de sécurité ne sont pas des options ! Cette règle devrait naturellement s'imposer à tout projet numérique, quel que soit son porteur.

Les discussions sur le positionnement du RSSI datent du moyen-âge, et ce dans tous les secteurs d'activité. On peut raisonnablement acter deux principes : le RSSI doit pouvoir exercer, c'est-à-dire travailler pour le compte de l'institution qu'il sert avec tout le soutien nécessaire des autorités administratives et cœur de métier ; le RSSI doit pouvoir assurer un rôle de conseil et de contrôle des pratiques de la DSI, en bonne intelligence et dans le cadre d'objectifs partagés.

L'analyse des risques et la certification des systèmes d'information

Politique de Sécurité (PSSI) et analyse des risques constituent les deux fondements de la mise en œuvre stratégique et opérationnelle d'un programme de sécurité global. En ce qui concerne les analyses des risques, la réalité impose la nécessité de faire évoluer les modèles existants, basés sur des fichiers EXCEL et la méthode EBIOS 2010, et de mettre en œuvre un cycle de vie opérationnel et efficient. L'ANSSI recommande maintenant l'usage de la méthode EBIOS Risk Manager, qui adopte une approche de management du risque numérique partant du plus haut niveau (grandes missions de l'objet étudié) pour atteindre progressivement les fonctions métier et techniques, par l'étude des scénarios de risque possibles. C'est une petite révolution conceptuelle et les structures publiques vont devoir réviser ce volet de la gestion des risques, en intégrant cette nouvelle méthode et en s'outillant avec des outils labellisés et adaptés aux enjeux.

PSSI, analyse des risques, chartes, gestion des habilitations, puis des droits, traçabilité, supervision, sauvegardes testées, plan de continuité d'activité, intégration de la sécurité dans les projets sont autant d'items que l'on retrouve dans l'ISO 27001. Si l'on ajoute le respect non négociable du RGPD, qui exige des mesures de sécurité adaptées à la criticité des données et des traitements, donc des processus, et les textes français et européens

qui qualifient les données à caractère personnel d'ultra-sensibles, on flirte avec la nécessité d'une certification officielle. Alors pourquoi ne pas aller au bout de la démarche, et exiger des systèmes d'information des structures publiques qu'ils soient certifiés ISO 27001 (et ISO 27701), pour le moins sur le périmètre d'exploitation ? Le SI serait ainsi certifié, comme d'autres processus et soumis à un plan d'amélioration continu régulièrement challengé.

Je ne veux pas m'occuper de sécurité ! Ni d'informatique d'ailleurs.

Lors du discours que l'on peut qualifier d'historique du 17 mai 2021, les trois ministres Bruno LEMAIRE, ministre de l'Economie, des Finances et de la Relance, Amélie de MONTCHALIN, ministre de la Transformation et de la Fonction publiques et Cédric O, Secrétaire d'Etat chargé de la Transition numérique et des Communication électroniques ont décliné la stratégie Cloud de l'Etat. A l'intérieur même de la révolution numérique, il existe des « sous-révolutions ». La première fut l'avènement du PC, la seconde celle de l'Internet et la troisième est celle du cloud computing, c'est-à-dire de l'informatique en nuage. Lors de cette intervention très écoutée, les ministres ont posé la doctrine et déclaré : « Cette nouvelle doctrine s'applique aux ministères et organismes placés sous leur tutelle, et s'incarnera dans une circulaire. Le Cloud devient dorénavant la méthode d'hébergement par défaut pour les services numériques de l'Etat, pour tout nouveau produit numérique et pour les produits connaissant une évolution substantielle. Les recrutements et les programmes de formation continue destinés aux agents de l'Etat dans la filière numérique comporteront un volet cloud ».

On peut aisément en déduire que l'État en général et les collectivités territoriales dans la continuité vont entrer dans un processus d'externalisation de leur informatique traditionnelle, et donc sous-traiter l'ensemble des couches informatiques : hébergement du hardware et donc des données auprès d'opérateurs spécialisés et reconnus, usage de logiciels métiers à distance en mode SaaS, utilisation de technologies de sécurité externalisées. Une mairie, un conseil départemental ou régional n'aura plus à gérer qu'un parc d'ordinateurs et d'imprimantes, une liaison réseau

fibre optique de qualité, et l'ensemble des services sera opéré par des industriels dont c'est le métier. Nous suivrons ainsi le modèle des États-Unis, du Canada, du Royaume-Uni, de la Corée du sud… où l'immense majorité des entreprises privées, des hôpitaux et des collectivités ont depuis longtemps procédé à un recentrage sur leurs cœurs de métiers et ont confié la gestion de leurs systèmes d'information à des opérateurs privés. C'est alors que le débat sur notre souveraineté prend tout son sens, avec le nécessaire recours à des opérateurs français (ou européens), malgré les offres alléchantes et parfois, disons-le, efficaces et modernes des géants américains et chinois.

Table des matières

CyberCercle - 18 rue Tronchet, 69006 Lyon
contact@cybercercle.com - cybercercle.com

« Sécurité numérique & Collectivités » est le deuxième opus de notre Collection CyberCercle - Regards croisés lancée fin 2020.

Des livres collectifs, dont chaque édition associe des auteurs représentant différentes organisations, publiques et privées, autour d'une thématique déterminée dans le champ de la confiance et de la sécurité numériques.

Des livres collectifs qui peuvent se lire de la première à la dernière page, ou de façon séquencée, par des entrées « auteur » ou « thématique ».

Ces ouvrages n'ont pas l'ambition d'être exhaustifs. En revanche, grâce à des contributions de personnalités expertes complémentaires, ils ont pour vocation d'apporter aux lecteurs des éléments d'analyse de confiance, propres à enrichir leur appréhension du sujet et leur réflexion.

La Collection CyberCercle - Regards croisés s'inscrit ainsi, à travers ses deux publications annuelles, comme une référence dans le panorama français de réflexion sur les sujets de confiance et de sécurité numériques, un outil de travail au service de la décision.

Ce deuxième opus est consacré aux collectivités, un des axes majeurs de la réflexion et de l'action du CyberCercle depuis 2015, et dont les enjeux en matière de sécurité numérique sont à la hauteur des défis de la transformation numérique dans laquelle elles sont aujourd'hui engagées.

Cet ouvrage a été réalisé avec le soutien de

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

BANQUE des TERRITOIRES
Caisse des Dépôts Groupe

proofpoint.

LE GROUPE LA POSTE

CERTitude NUMERIQUE

AvantdeCliquer.com
L'humain au cœur de la cybersécurité