2023

MISSION ECOTER
France et Territoires Numériques

CYBER MOIS

Paroles de Territoires

Livret

Octobre 2023

Mission Ecoter
France et Territoires Numériques

Depuis plus de 20 ans, Mission Ecoter-France et Territoires Numériques accompagne les collectivités locales françaises dans leur mutation organisationnelle et dans leur appropriation des technologies numériques, pour leur propre fonctionnement et pour le développement des services aux citoyens, avec des règles de fonctionnement simples et une accessibilité de toutes les collectivités à ses travaux.

Également organisme de formation, Mission Ecoter - France et Territoires Numériques propose des formations sur les données, sur l'économie numérique, la conduite et l'organisation des territoires, sur les politiques d'équipement numérique éducatif, sur les collectivités et leurs satellites, la réforme territoriale et les règles essentielles pour instaurer une relation de qualité et de confiance avec les décideurs locaux.

Mission Ecoter-France et Territoires Numériques est aujourd'hui présidée par Denis THURIOT, Maire de Nevers, Président de Nevers Agglomération et Conseiller régional de Bourgogne-Franche-Comté, et par un Président délégué, Bertrand RINGOT, Maire de Gravelines, Vice-Président de la Communauté urbaine de Dunkerque, Conseiller départemental du Nord.

Elle compte la Caisse des Dépôts et Consignations-Banque des Territoires parmi ses membres fondateurs et partenaires privilégiés.

L'Avant-propos de Denis THURIOT

Président de Mission Ecoter-France et Territoires numériques

Maire de Nevers et Président de l'Agglomération
Conseiller régional de Bourgogne-Franche-Comté

Mission Ecoter-France et Territoires Numériques agit depuis de nombreuses années pour apporter aux élus locaux les informations et les réflexions qui doivent leur permettre d'aborder le sujet complexe de la protection des données et la sécurisation des infrastructures numériques et des communications. La prise de conscience des cyberrisques et des cyberdangers est forte au niveau national et européen. La cybersécurité, la souveraineté numérique, les infrastructures et les usages, ou encore le métaverse, sont à la fois des thèmes passionnants et des sujets d'importance sur lesquels les dirigeants européens planchent afin de construire, d'ajuster une politique numérique européenne. Mais, au niveau infra-national, celui des villes médianes notamment, nos collectivités sont loin d'avoir le niveau requis de sécurité informatique. Pourtant, nos Mairies, nos Communautés de communes et même d'Agglomération, ou encore nos hôpitaux sont de plus en plus dans le viseur des cybercriminels. Le simple exemple des mises à jour (dangereuses parfois aussi…), qui ne sont pas toujours faites alors qu'elles assurent une meilleure protection, est révélateur et suffit à illustrer parfaitement le problème. Même si les élus, à l'instar de la très grande majorité des Français, sont conscients que l'usage des outils numériques comporte des risques, ces derniers restent majoritairement méconnus. « Hameçonnage » et « rançongiciel » sont des mots que les élus locaux connaissent mais ils sont finalement peu nombreux à pouvoir en donner une définition claire et précise.

Il est donc urgent d'accélérer l'accompagnement des élus, des agents des collectivités, de tous les acteurs publics et privés, institutionnels, économiques ou associatifs, afin qu'ils puissent comprendre, mesurer, anticiper les risques et réduire leur vulnérabilité. Même si le risque zéro n'existe pas, prévenir avant qu'il ne soit trop tard, en adoptant les bons réflexes pour nous assurer la meilleure sécurité numérique possible, n'est plus une option mais une exigence.

Pourtant, nos Mairies, nos Communautés de communes et même d'Agglomération, ou encore nos hôpitaux sont de plus en plus dans le viseur des cybercriminels

Les cyberattaques préoccupent effectivement les usagers car elles mettent généralement en péril leurs données personnelles. Dans cette optique, la coopération entre les territoires apparaît indispensable ; elle est la condition *sine qua non* d'une gestion complète de la cybervulnérabilité des réseaux. Elle peut aussi se mener à un niveau régional.

Cette réalité des risques est à prendre en compte également dans nos politiques de revitalisation : un territoire protégé est un territoire plus attractif… C'est la raison pour laquelle les villes innovantes, qui ont pris à bras le corps la transition numérique, les *smart cities*, ont tout intérêt à développer un axe *safe city* et mettre en œuvre des solutions pour se prémunir notamment des intrusions dans les systèmes d'information. Un axe qui doit aussi leur permettre d'accroître leur attractivité. La cybersécurité est, en outre, une formidable opportunité de développement économique et d'emploi dans nos territoires.

Nous sommes cependant, dans l'immédiat, tous porteurs de questions : comment protéger efficacement l'accès aux données personnelles ? Comment empêcher le piratage des infrastructures stratégiques ? Comment se prémunir contre la professionnalisation des cybercriminels dans un contexte de développement des objets connectés ? Et bien d'autres questions encore.

Créé en 2012, le Mois européen de la cybersécurité est une initiative voulue par l'Agence de l'Union européenne pour la cybersécurité (ENISA). Elle vise à sensibiliser aux enjeux de la cybersécurité à travers les pays de l'UE afin de permettre de mieux comprendre les menaces et les appréhender. En France, le Mois européen de la cybersécurité a été décliné en **« Cybermoi/s »**.

Mission Ecoter-France et Territoires Numériques est un relais nécessaire auprès des collectivités territoriales afin de sensibiliser, d'informer et de former les élus locaux à ce sujet majeur qui préoccupe l'ensemble des organisations publiques et privées.

La cybersécurité est bel et bien un enjeu citoyen, et fait désormais partie des enjeux de sécurité plus globale.

La Tribune de Bertrand RINGOT

Président délégué de Mission Ecoter-France et Territoires numériques

Maire de Gravelines
Vice-Président de la CUD
Conseiller départemental du Nord

La ville de Gravelines a été confrontée très tôt aux problèmes de cybersécurité, notamment avec l'attaque d'un cryptovirus qui a touché la médiathèque en 2013 et s'est propagé sur l'ensemble de la bureautique de la ville. Heureusement, grâce à des sauvegardes hors ligne, la situation a pu être rapidement restaurée, minimisant ainsi l'impact opérationnel de la mairie. Suite à cette expérience, la politique de sécurité de la ville a été renforcée par l'utilisation d'outils appropriés et une communication importante envers les agents de la collectivité.

Deux attaques de moindre ampleur ont également été maîtrisées en 2014 et 2015, en grande partie grâce à la vigilance des agents qui ont rapidement signalé des anomalies à la Direction des Systèmes d'Information et du Numérique (DSIN). Cependant, les attaques sont devenues plus sournoises, plus diversifiées et bénéficient même de l'aide de l'intelligence artificielle, ce qui donne une apparence de véracité aux documents envoyés. La sécurité est donc devenue un sujet majeur pour notre ville.

En 2023, près de 10% du budget de fonctionnement de la DSIN est consacré à la sécurité. Notre vigilance doit être décuplée, car après huit ans sans intrusion, l'un de nos sites web a été touché cette année par un script de minage de bitcoins opéré par une structure extérieure à l'Europe. Chaque jour, nos outils spécialisés détectent des centaines de menaces potentielles de plus en plus difficiles à identifier.

Nous révisons en permanence notre niveau de sécurité en prenant différentes mesures, telles que la réduction du temps de verrouillage des ordinateurs, le changement plus fréquent et la complexification des mots de passe, l'attribution de sessions aux stagiaires, et l'extinction automatique des ordinateurs la nuit pour s'assurer que les mises à jour se déroulent correctement. Cependant, la sensibilisation des agents aux nouvelles menaces reste l'élément clé de notre politique de sécurité.

En 2023, près de 10% du budget de fonctionnement de la DSIN est consacré à la sécurité

Nous privilégions trois axes : une communication interne régulière, la mise en place prochaine d'une campagne de phishing et la participation à des MOOC (formation en ligne différée) proposés par le CNFPT depuis cet été. Ces MOOC sont composés de trois modules visant à comprendre les principes généraux des cyberattaques, à agir pour valider et adopter les bonnes pratiques, et à saisir l'intérêt et la manière de transmettre ces valeurs.

Cependant, les cyberpirates ont souvent une longueur d'avance, ce qui oblige les collectivités à investir dans des logiciels de sécurité de plus en plus lourds et onéreux. Cette course en avant peut devenir difficile à suivre pour les budgets et les infrastructures internes.

Il est donc essentiel que les autorités compétentes prennent conscience de l'importance de la cybersécurité et fournissent les ressources nécessaires aux collectivités locales pour faire face à ces menaces grandissantes. La collaboration entre les différents acteurs, publics et privés, est également cruciale pour renforcer la sécurité de nos territoires. Ainsi, la DSIN de Gravelines aborde régulièrement ces sujets dans le cadre de rencontres trimestrielles des DSI des hauts de France.

En conclusion, la ville de Gravelines a su tirer les leçons de ses expériences passées en renforçant sa politique de sécurité et en sensibilisant ses agents aux nouvelles menaces. Cependant, il est important de rester vigilants et de continuer à investir dans des solutions de cybersécurité adaptées afin de protéger nos territoires contre les attaques toujours plus sophistiquées.

La collaboration entre les différents acteurs, publics et privés, est également cruciale pour renforcer la sécurité de nos territoires

Alain MELKA
Directeur Général des Services
Mission Ecoter-France et Territoires Numériques

Quentin MEULLEMISTRE
Directeur Général des Services Adjoint
Mission Ecoter-France et Territoires Numériques

La menace cyber

À l'heure du Big Data et de l'Open Data, les débats s'accroissent autour des questions liées au respect de la vie privée, de la protection de la liberté d'expression et des autres libertés individuelles.

Nous pourrions tenter de définir la cybersécurité comme un état recherché qui s'appuie généralement sur la mise en œuvre de mesures de protection et de défense contre une adversité.

Afin d'esquisser une définition de la « menace cyber », nous pouvons indiquer qu'il s'agit d'une potentielle utilisation malveillante de l'espace numérique. Elle prend forme lorsqu'une entité attaquante effectue un enchaînement d'action via des voies numériques ou physiques pour exploiter les propriétés de cyberespace, notamment ses vulnérabilités, techniques ou structurelles, afin de réaliser des impacts, eux-mêmes d'ordre numérique ou physique.

La Cybersécurité est l'affaire de tous

Ainsi, le cyberespace est une notion complexe à comprendre du fait de son caractère intangible et très technique, mais également en raison d'un grand flou lexical dans la littérature. En conséquence, il n'existe pas de définition universelle du cyberespace. Nous trouvons, bien au contraire, de nombreuses définitions en fonction des disciplines, des acteurs et des pays. Néanmoins, il est toutefois possible d'affirmer que le cyberespace est un espace intangible, dans lequel s'opèrent des échanges internationaux entre des internautes, à une vitesse tellement rapide, qu'il supprime toute notion de distance.

Il n'existe pas de définition universelle du cyberespace

Le Cybermoi/s

Le Cybermoi/s est une campagne de sensibilisation aux enjeux de la cybersécurité qui se tient chaque année au mois d'octobre. Elle est organisée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et fait intervenir de nombreux acteurs pour partager des conseils et bonnes pratiques à adopter à chaque instant de notre vie numérique.
La cybersécurité dans les collectivités territoriales est un enjeu majeur. En cette période de rentrée, alors que chacun reprend ses marques et de nouvelles résolutions, Mission Ecoter-France et Territoires Numériques s'associe au Collectif Cybermoi/s en lançant un appel afin que chacun se mobilise face à l'enjeu sociétal que constitue la cybersécurité.
Dans un monde de plus en plus digitalisé, les collectivités territoriales sont de plus en plus exposées aux cyberattaques. Ces dernières peuvent avoir des conséquences graves, tant sur le plan financier que sur le plan opérationnel.

Les enjeux de la cybersécurité dans les collectivités territoriales

Les enjeux de la cybersécurité dans les collectivités territoriales sont nombreux :

La protection des données personnelles : les collectivités territoriales collectent et traitent de nombreuses données personnelles, notamment sur leurs citoyens, leurs agents et leurs partenaires. Ces données sont une cible privilégiée des cyberattaques, car elles peuvent être utilisées pour des activités criminelles, comme le chantage ou l'usurpation d'identité.
La continuité des services publics : les collectivités territoriales sont responsables de la fourniture de nombreux services publics, comme l'éducation, la santé ou la sécurité. Une cyberattaque peut perturber ou interrompre ces services, ce qui peut avoir un impact négatif sur la population.

L'atteinte à la réputation : une cyberattaque peut porter atteinte à la réputation d'une collectivité territoriale. En effet, les citoyens et les partenaires peuvent perdre confiance dans la capacité de la collectivité à protéger leurs données et leurs services.
Les mesures de cybersécurité à mettre en place

Pour se protéger des cyberattaques, les collectivités territoriales doivent mettre en place un ensemble de mesures de cybersécurité. Ces mesures doivent être adaptées aux besoins et aux ressources de chaque collectivité.

Parmi les mesures de cybersécurité les plus importantes, on peut citer :

La sensibilisation des agents : il est important de sensibiliser les agents aux risques de cybersécurité. Ils doivent être informés des menaces et des bonnes pratiques à adopter pour se protéger.
La mise en place d'une infrastructure sécurisée : les collectivités territoriales doivent mettre en place une infrastructure sécurisée, comprenant des pares-feux, des antivirus et des systèmes de détection et de réponse aux incidents (SIEM).
La mise en place d'une politique de gestion des accès : les collectivités territoriales doivent mettre en place une politique de gestion des accès qui définit les droits d'accès aux systèmes et aux données.
La sauvegarde des données : les collectivités territoriales doivent sauvegarder régulièrement leurs données pour pouvoir les restaurer en cas de cyberattaque.

L'État accompagne les collectivités territoriales dans leur démarche de cybersécurité. Il met à leur disposition des ressources et des outils, notamment le guide de la sécurité numérique des collectivités territoriales publié par l'ANSSI.

L'accompagnement des collectivités territoriales par l'État

En effet, l'État français s'engage à renforcer la cybersécurité française. Il a mis en place un ensemble de mesures, notamment :

La création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), chargée de coordonner les efforts de cybersécurité en France.
La mise en place d'un plan d'action national de cybersécurité, qui définit les priorités de la France en matière de cybersécurité.
Le financement de programmes de recherche et développement en cybersécurité.
Les perspectives

La cybersécurité est un domaine en constante évolution. Les cybermenaces sont de plus en plus sophistiquées et les solutions de sécurité doivent être régulièrement mises à jour pour y faire face.

La France est bien placée pour faire face à ces défis. Elle dispose d'un cadre réglementaire solide, d'un personnel qualifié et d'une industrie de cybersécurité dynamique. Cependant, il est important de poursuivre les efforts de sensibilisation et de formation pour que la cybersécurité soit une préoccupation de tous.

Notre pays accompagne les collectivités territoriales dans leur démarche de cybersécurité. Il met à leur disposition des ressources et des outils, notamment le guide de la sécurité numérique des collectivités territoriales publié par l'ANSSI.

Enfin, l'État participe au financement de la cybersécurité des collectivités territoriales, notamment au travers du plan France Relance.

En conclusion: la cybersécurité est un enjeu majeur pour les collectivités territoriales. En mettant en place des mesures de cybersécurité adaptées, les collectivités territoriales peuvent contribuer à protéger leurs données, leurs services et leur réputation.

Formation des élus et des cadres territoriaux à la cybersécurité, pas de temps à perdre !

FABIEN BAZIN
Président du Conseil départemental de la Nièvre,
Président de Nièvre Numérique

La cybersécurité : Impliquer les citoyens, première ligne de défense et premières victimes

La cybersécurité est un défi majeur qui transcende les frontières géographiques et touche chaque aspect de notre société. Il faut souligner l'importance cruciale de l'implication des citoyens dans la protection contre les menaces numériques. Les citoyens sont à la fois les premières portes d'entrée des attaques et les premières victimes potentielles, ce qui rend leur engagement actif essentiel, où qu'ils se trouvent.

Éduquer pour renforcer la résilience

L'éducation à la cybersécurité est un pilier essentiel de cette implication citoyenne. Les citoyens doivent être informés des risques et des bonnes pratiques pour se protéger en ligne. Ils doivent également apprendre à reconnaître les signes d'une cyberattaque en cours et à réagir rapidement. Cette vigilance citoyenne peut contribuer à minimiser les dégâts et à empêcher la propagation de l'attaque. Les cybercriminels vivent de la méconnaissance des utilisateurs des technologies numériques.

Depuis presque 20 ans le Conseil départemental de la Nièvre a mis en place un dispositif de médiation numérique permettant à la fois d'aider les personnes les plus éloignées du numérique et celles qui souhaitent faire évoluer leurs compétences pour franchir un cap vers l'autonomie numérique ou pour favoriser leur développement personnel ou professionnel.

En matière de sensibilisation et d'évolution des connaissances, les conseillers numériques, et plus largement les acteurs de la médiation et de l'inclusion numérique, jouent un rôle crucial.

Leur proximité est un atout essentiel leur permettant de s'adresser à tous les publics (professionnels y compris) d'un territoire. Au-delà de la prise de conscience des citoyens, ils peuvent également les accompagner techniquement dans la mise en place d'outils de protection et dans l'intégration des bons réflexes qui diminuent leur niveau de vulnérabilité.

Pour cette raison, et pour de nombreuses autres, les dispositifs d'aides aux usages numériques territoriaux jouent un rôle primordial dans l'intégration de pratiques numériques en constante évolution au sein de notre société.

Avoir les bons réflexes dès le plus jeune âge

Après avoir fait le constat que les pratiques numériques des moins de 15 ans étaient souvent à risque et une généralisation de l'usage des smartphones (souvent sans contrôle parental), de plus en plus tôt (parfois dès l'âge de 2 ou 3 ans), les médiateurs numériques ont intégré la cybersécurité dans leur offre d'accompagnement destinée à un public plus jeune, et aux parents.

Dans ce cadre, une nouvelle méthode de sensibilisation est en cours de construction et sera prochainement expérimentée dans un collège nivernais avec des élèves de 4ème. Cela se traduira par un ensemble d'ateliers et de discussions permettant d'aborder de façon ludique (sous la forme d'un cirque numérique, baptisé le « Numérik Circus ») le sujet des pratiques numériques sous toutes leurs formes.

Ce sera évidemment l'occasion d'aborder le sujet de la cybersécurité (notamment sous la forme d'un Escape Game) et de nombreux autres sujets connexes tels que le cyberharcèlement, la maitrise de ses données, etc…

Le signalement, un acte citoyen crucial

Une autre facette de l'implication citoyenne est le signalement des incidents de cybersécurité. Les citoyens doivent être encouragés à alerter de toute activité suspecte ou toute tentative d'attaque. Ils sont souvent les premiers à remarquer des comportements inhabituels sur leurs réseaux, et leur contribution est précieuse pour les autorités locales et les experts en sécurité.

La création de mécanismes de signalement simples et accessibles est essentielle pour faciliter cette démarche citoyenne. Les autorités doivent s'engager à traiter ces signalements de manière confidentielle et à agir rapidement pour protéger la communauté.

Sur ce point les équipes de médiation numérique du Département jouent également un rôle essentiel en diffusant des informations auprès de l'ensemble des publics qu'ils peuvent accompagner, relatives à des méthodes de repérage de mails ou de posts douteux, et en donnant des conseils précis pour les signaler.

L'implication active des citoyens est la clé de voûte de la cybersécurité. Éduquer, sensibiliser et encourager le signalement sont autant de moyens de renforcer la résilience de nos communautés face aux cyberattaques. En unissant nos forces, nous pouvons construire un avenir numérique plus sûr pour tous, où chaque citoyen joue un rôle actif dans la protection de notre patrimoine numérique commun.

Le signalement, un acte citoyen crucial

Éric BERLIVET
Maire de Roche-La-Molière

Renforcer la Cybersécurité des Collectivités Territoriales : Un Impératif pour Octobre, le Mois de la Sécurité, mais (surtout) pas que …

Octobre, le mois de la sécurité, nous offre l'occasion de nous pencher sur un sujet essentiel qui concerne l'ensemble de nos administrations locales : la cybersécurité.
En ma qualité de Maire Roche-La-Molière, une commune située dans la Loire (42), j'associe Nicolas Bard mon directeur du service informatique externalisé, pour vous sensibiliser à l'importance cruciale de renforcer la protection de nos infrastructures numériques.

La menace cybersécurité : une réalité incontournable

Dans un monde de plus en plus numérisé, nos collectivités territoriales deviennent des cibles privilégiées pour les cybercriminels. Les attaques informatiques visant les administrations locales se multiplient, et exposent nos services publics ainsi que les données sensibles de nos administrés à des risques considérables.
Les statistiques récentes sont alarmantes. Selon le Centre National de la Cybersécurité (CNC), en 2021, les attaques informatiques contre les collectivités territoriales avaient déjà augmenté de 47%. Cette tendance à la hausse montre clairement que la menace cybersécurité ne cesse de croître.

L'exemple récent de la mairie de Betton

Nous ne pouvons ignorer les événements très récents qui illustrent cette menace grandissante. Dans la nuit du 30 au 31 août 2023, la mairie de Betton, une petite commune de 12 000 habitants de la banlieue de Rennes, dans le département d'Ille-et-Vilaine, a été la cible d'une cyberattaque. Cette municipalité a été touchée par une attaque par rançongiciel, qui consiste à crypter les données et à exiger une rançon pour rétablir l'accès et éviter la publication en ligne des ~~les~~ fichiers récupérés.

Malgré des sauvegardes informatiques fiables qui ont permis de préserver des données cruciales, plusieurs services sont restés indisponibles, notamment les réservations pour la cantine scolaire et pour les centres de loisir. Il est également devenu impossible de contacter les services municipaux par e-mail.
Toutefois, des services tels que celui des cartes d'identité et des passeports sont restés opérationnels.

La surface d'attaque grandissante avec les objets connectés

Il est également crucial de noter que la surface d'attaque s'agrandit de manière exponentielle avec la prolifération des objets connectés. Comme l'a souligné Christian Estrosi, le président de Mission Ecoter France et Territoires Numériques, "Plus de 50 milliards d'objets connectés seront en circulation cette année." Cette explosion des objets connectés crée de nouvelles opportunités pour les cybercriminels de cibler nos collectivités territoriales. Des capteurs pour l'énergie thermique aux dispositifs de surveillance de la circulation, en passant par les systèmes de gestion des déchets, de nombreux équipements essentiels à nos services municipaux sont désormais connectés à internet, augmentant ainsi notre vulnérabilité.

L'engagement de la Mairie de Roche-La-Molière dans la cybersécurité

Concernant la Mairie de Roche-La-Molière, nous avons pris des mesures concrètes pour renforcer la cybersécurité de nos infrastructures numériques depuis plusieurs années. Cela inclut la mise en place d'un plan d'amélioration continue, avec un budget spécifiquement dédié au système d'information, afin de maintenir et d'améliorer en permanence la sécurité de nos systèmes. Nous sommes engagés à protéger nos données, nos services municipaux, et par-dessus tout, nos citoyens.

Dans un monde de plus en plus numérisé, nos collectivités territoriales deviennent des cibles privilégiées pour les cybercriminels

Agir de concert pour renforcer la cybersécurité

Face à cette menace grandissante, il est impératif que nous unissions nos efforts. Les collectivités territoriales, avec le soutien de nos collaborateurs et administrés, doivent investir de manière proactive dans la cybersécurité, former nos équipes aux meilleures pratiques, et mettre en place des protocoles de protection rigoureux. La sécurité informatique doit devenir une priorité incontournable, et ce mois d'octobre est l'occasion idéale pour passer à l'action.

L'engagement de la Mairie de Roche-La-Molière dans la cybersécurité :

La Mairie de Roche-La-Molière, consciente des défis posés par la cybersécurité, juge impératif la mise en œuvre des mesures suivantes pour protéger son système d'information :

- Audit de sécurité régulier : Nous recommandons la réalisation régulière d'audits de sécurité pour évaluer les vulnérabilités potentielles de nos systèmes et réagir rapidement aux menaces.
- Plan de réponse aux incidents : La mise en place d'un plan de réponse aux cyberattaques est essentielle pour réagir rapidement et efficacement en cas d'incident, minimisant ainsi les dommages potentiels.
- Formation continue de notre personnel : Nous insistons sur la nécessité de former nos équipes aux dernières techniques de cybersécurité et aux bonnes pratiques en matière de protection des données.
- Renforcement de la collaboration avec des experts en cybersécurité : Nous préconisons la collaboration avec des professionnels de la cybersécurité pour évaluer et renforcer notre infrastructure numérique.
- Sensibilisation de nos administrés : Informer nos citoyens sur les enjeux de la cybersécurité et les bonnes pratiques à adopter pour leur propre protection reste une priorité.

Formation continue de notre personnel

Ensemble, nous pouvons renforcer la cybersécurité de nos collectivités territoriales, quelle que soit leur taille, et assurer un avenir numérique plus sûr pour nos administrés.

Ce mois d'octobre, en tant que Mois de la Sécurité, est une opportunité pour chacun de réfléchir à notre rôle dans la protection de nos collectivités. La cybersécurité ne concerne pas seulement les spécialistes en informatique, mais tous les élus et dirigeants des collectivités territoriales.
Ensemble, nous pouvons faire en sorte que nos collectivités territoriales soient des exemples de préparation et de résilience face aux menaces. Nous vous remercions pour votre engagement envers la sécurité de nos collectivités et nous sommes impatients de collaborer pour atteindre cet objectif vital.

Face à cette menace grandissante, il est impératif que nous unissions nos efforts

Luc BOUARD

Maire de La Roche-Sur-Yon
Président de La Roche-Sur-Yon Agglomération
Conseiller départemental de Vendée

L’ère de la donnée à l’épreuve de la cyber sécurité

Une Ville-Préfecture comme La Roche-sur-Yon dépend de manière croissante du numérique. Que ce soit pour gérer les services publics, dématérialiser les procédures via les services en ligne apportés aux citoyens, mais également avec le déploiement des nombreuses infrastructures dont nous avons la gestion quotidienne. Cette tendance s’accélère avec le déploiement de la ville intelligente et une gestion décentralisée de plus en plus nécessaire.

Si nous pouvons nous réjouir du progrès et des avancées technologiques, cette dépendance accrue rend les territoires comme le nôtre plus vulnérables aux cyberattaques. D’autant plus vulnérables que les collectivités comme celles de La Roche-sur-Yon, où la majorité des services de la Ville et de l’Agglomération sont mutualisés, collectent et gèrent une grande quantité de données sensibles : notamment des informations personnelles sur les citoyens, des données financières, médicales, techniques, etc. Et ces données sont extrêmement précieuses pour les cybercriminels, ce qui fait des collectivités des cibles de choix !

Des cyberattaques récentes ont généré la diffusion ciblée de données personnelles de citoyens, nuisant à la réputation des administrations locales, perturbant gravement et durablement des services publics essentiels. Les citoyens doivent pourtant pouvoir faire confiance à leur collectivité pour protéger leurs données personnelles. Les cyberattaques érodent cette confiance essentielle, et peuvent avoir des conséquences désastreuses, telles que l’usurpation d’identité et bien sûr la divulgation d’informations.

Le respect du RGPD est une chose maintenant acquise par les collectivités. La protection des données personnelles est essentielle pour garantir la vie privée. Elle est également nécessaire pour promouvoir des pratiques responsables dans la collecte et l'utilisation des données personnelles. La protection des données est son nécessaire corollaire. Et comme la cyber sécurité des données territoriales est cruciale pour maintenir la confiance des citoyens, nos administrations doivent être proactives, mais aussi conscientes des enjeux d’une bonne gestion de la donnée dans leur approche de la cyber sécurité. C’est tout à la fois une question aussi technique qu’éthique.

C’est pourquoi à La Roche-sur-Yon nous gardons à l’esprit que renforcer la cyber sécurité au sein de notre administration est essentiel. C’est également une nécessité de prendre conscience qu’il s’agit tout à la fois de protéger l’intégrité de nos équipements techniques que de protéger chaque citoyen.

A La Roche-sur-Yon nous gardons à l’esprit que renforcer la cyber sécurité au sein de notre administration est essentiel

François CHARBONNIER

Directeur d'Investissement Cybersécurité et Souveraineté numérique – Banque des Territoires

Grandes, médianes ou petites, toutes les villes et intercommunalités sont sous le feu des cyberattaques – il en est de même pour les régions et les départements. On ne compte malheureusement plus les annonces spectaculaires en la matière, qui mettent en péril la continuité du service public sur les territoires. C'est notamment le cas lorsque sont touchés des services déjà largement digitalisés comme le sont ceux d'état civil, d'urbanisme ou encore de gestion administrative.

La tendance n'est pas près de s'inverser au fur et à mesure que s'informatisent et se connectent les infrastructures de transport, d'énergie, d'eau, la signalisation routière, l'éclairage, les systèmes de vidéoprotection, etc. : le défi devient alors 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.

La cybersécurité, question de maîtrise et de protection du numérique, est ainsi de plus en plus prégnante pour les acteurs des territoires. La cybersécurité représente même un véritable enjeu de confiance du citoyen dans son rapport à l'Etat sur les territoires. **La Banques des Territoires en est convaincue : au service des régions, elle mène d'importantes actions de financement de la cybersécurité, dans le cadre de France 2030 pour faire émerger des démonstrateurs territoriaux de cybersécurité adaptés aux contraintes des collectivités, et en tant qu'investisseur en entrant au capital des startups les plus prometteuses à même d'apporter des solutions aux collectivités territoriales et établissements de santé souhaitant se protéger des cyberattaques** : Yes We Hack (campagnes de chasses de failles par des *hackers* éthiques), Hackuity (gestion optimisée des vulnérabilités par lesquelles attaquent les pirates), Egerie (analyse des risques), Sesame-IT & Sekoia (détection de dernière génération des cyberattaques) sont des pépites couvrant différents pans majeurs de la cybersécurité.

… il est de la responsabilité des élus, des DGS et DGA d'impulser la dynamique qui seule permet à la collectivité de mettre en place un projet cohérent, maîtrisé et sûr

Mais l'innovation, seule, ne suffit pas. **Face à l'enjeu crucial qu'est la cybersécurité, il est de la responsabilité des élus, des DGS et DGA d'impulser la dynamique qui seule permet à la collectivité de mettre en place un projet cohérent, maîtrisé et sûr. A cette fin, il n'est nul besoin qu'ils comprennent les rouages techniques du sujet : ils doivent même accepter de ne pas être un expert. Il leur faut cependant définir le cap et mobiliser ses cadres et agents territoriaux.**

La Banques des Territoires souhaite ainsi, par cette tribune, remettre l'accent sur l'engagement nécessaire des élus, DGS et DGA, devant un sujet qui, suscitant l'angoisse et le doute, peut parfois sembler inabordable. Elle vous invite à redécouvrir à cette fin son guide paru à la toute fin de 2020, passé dans l'angle mort de la crise sanitaire mais toujours pleinement d'actualité : pensé comme un **véritable guide de survie de l'élu, il n'est en rien technique ou jargonnant, mais synthétique, pédagogique et pratique, avec les zooms incontournables sur les notions élémentaires à appréhender – et leurs enjeux – et les questions juridiques qui concernent nos collectivités. Il a été conçu en coopération avec l'AMF, l'AdCF, la FNCCR, France Urbaine, l'ANSSI et Cybermalveillance.gouv.fr.**

=> https://www.banquedesterritoires.fr/guide-pratique-pour-une-collectivite-et-un-territoire-numerique-de-confiance

Joël DUQUENOY

Président de la Communauté d'Agglomération du Pays de Saint-Omer

A l'heure où les technologies numériques transforment notre quotidien et où nos territoires sont de plus en plus connectés, il est impératif de reconnaître que la cybersécurité est devenue une préoccupation majeure pour chacun d'entre nous. En ce Cybermois, nous souhaitons mettre en lumière l'importance cruciale de la cybersécurité dans la préservation de nos territoires, de nos infrastructures et de notre manière de vivre.

Les enjeux sont multiples. Les attaques, de plus en plus sophistiquées, ne connaissent pas de frontières. Elles peuvent toucher aussi bien les grandes métropoles, que les collectivités rurales. Les services publics, les entreprises locales, les écoles, les hôpitaux, et même nos maisons, sont devenus des cibles potentielles pour les cybercriminels.

La cybersécurité n'est plus seulement une affaire de technologie, elle est une question de sécurité nationale et locale. Elle doit être abordée avec une approche holistique, en tenant compte des spécificités de chaque territoire. Il est temps de mettre en place des stratégies de cybersécurité adaptées à nos réalités locales, en collaboration étroite avec les acteurs publics et privés.

A la CAPSO, nous avons eu l'opportunité de nous inscrire dans le cadre du plan France Relance cybersécurité. Dans sa phase initiale, cette action nous a permis d'obtenir un état de notre « cyberscore » par le biais d'un audit.

La cybersécurité n'est plus seulement une affaire de technologie, elle est une question de sécurité nationale et locale

La première mesure à prendre au sein de nos territoires est de multiplier les actions de sensibilisation. Les citoyens, les entreprises et les administrations locales doivent être conscients des risques et des bonnes pratiques pour se protéger. La formation des professionnels de la cybersécurité doit également être renforcée pour assurer une protection efficace. Sur cette thématique, nous mettons en œuvre depuis quelques jours une solution innovante et ludique mêlant tests de phishing et sensibilisation à la cybersécurité.

Dans une démarche d'inclusion, des actions doivent également être menées via les centres de médiation afin de se prémunir. Nous avançons sur cette voie et inscrivons cette dimension dans notre stratégie numérique.

~~L~~es collectivités territoriales ont un rôle essentiel à jouer en investissant dans des infrastructures sécurisées. Les villes intelligentes, les réseaux électriques, les systèmes de transport, et bien d'autres, sont de plus en plus interconnectés. Nous devons veiller à ce que ces systèmes soient robustes et résilients face aux menaces numériques.

Enfin, les territoires doivent pouvoir accompagner les communes autant que possible face à cet enjeu majeur. L'investissement de moyens humains, matériel et logiciels, la mutualisation des compétences dans ce domaine, permettra aux communes les plus modestes de se doter d'une sécurité optimale. Dans le cadre de notre « Service Commun Numérique » nous proposons à l'ensemble des communes de notre territoire de bénéficier de la résilience de notre infrastructure, des sécurités mises en place sur nos postes de travail et de notre support. C'est par ailleurs ce qui a été réalisée suite à l'attaque d'une des communes de l'agglomération en juin dernier.

En conclusion, la cybersécurité est un défi collectif qui concerne l'ensemble de nos territoires. En ce Cybermois, et au-delà, engageons-nous à renforcer notre vigilance pour garantir la sécurité de nos infrastructures et de nos données. La cybersécurité est un pilier de notre souveraineté et de notre qualité de vie, ne laissons pas nos territoires vulnérables aux menaces numériques.

Fatima EL OUASDI
Adjointe au Maire de Rueil-Malmaison déléguée au Numérique
Vice-Présidente de Mission Ecoter-France Territoires Numériques

Face à la menace durable de cyberattaques, une urgence à mutualiser les moyens pour garantir une continuité d'activité

Alors que la numérisation des services publics est toujours plus importante, à la fois par souci d'efficacité et de discipline budgétaire, les collectivités et services publics ont récemment été les cibles de cyberattaques d'ampleur, paralysant les systèmes d'information et par conséquent la continuité d'activité. Ces cyberattaques détruisent des données, avec comme conséquence une lente reprise d'activité : il faut parfois plusieurs mois pour retrouver un fonctionnement normal.

Pour nos Collectivités, la question à se poser n'est plus de savoir quand nous allons être attaqués, car nous le sommes tous les jours, mais de savoir quelle politique est mise en place, collectivité par collectivité, pour qu'en cas d'attaque, les services publics ne soient pas perturbés.

Pour cela, il est indispensable de mettre en place un plan de défense associé à une politique de sécurité du système d'information (PSSI), avec quatre points d'attention majeurs :

- Établir un **plan de de continuité de l'activité** (PCA) et de gestion de crise
- Sensibiliser et former les agents et les élus à ces risques. **Tous les utilisateurs connectés font partie du rideau défensif**
- Prévoir les **moyens humains et financiers** pour faire face au risque Cyber
- Réaliser périodiquement des **exercices de cyberattaques**

Les maires doivent pouvoir compter sur les syndicats et intercommunalités, départements, régions et métropoles pour obtenir des subventions ou bénéficier de soutiens opérationnels

Néanmoins, la mise en place de PSSI est exigeante, tant en termes financiers qu'opérationnels. En effet, l'inquiétude majeure des élus à ce jour est dans la difficulté à attirer les talents nécessaires pour se préparer aux risques cyber et à conjuguer les budgets toujours plus contraints.

En effet, la maille d'une mairie est trop petite pour attirer des RSSI. C'est pour cela qu'au sein de l'établissement public territorial (EPT) de Paris Ouest la Défense, qui rassemble 11 communes des Hauts-de-Seine, nous avons recruté et mutualisé un RSSI pour pouvoir protéger nos communes et se mettre en conformité des recommandations de l'ANSSI.
Les maires doivent pouvoir compter sur les syndicats et intercommunalités, départements, régions et métropoles pour obtenir des subventions ou bénéficier de soutiens opérationnels.
Des organisations de l'État comme**, l'**Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) est également disponible pour aider les collectivités par une offre large de formations et contenus gratuits.

A Rueil-Malmaison, la Direction des Systèmes d'Information, très mobilisée, sollicite à ce titre dès qu'il est possible, le soutien financier et opérationnel de l'État via le Plan France Relance, du POLD pour le RSSI, et de la Métropole du Grand Paris pour le PCA.

Les collectivités ne peuvent rester seules face au risque cyber. Le cyber est à la fois un impératif et une urgence, il faut les aider.
C'est en ce sens que l'association Villes Internet représentant près de 500 collectivités, petites et grandes, a également mis en lumière l'urgence Cyber dans sa Motion 2023, présentée mi-octobre à Dominique Faure, Ministre des Collectivités Territoriales et de la Ruralité.

André FIGOUREUX

Maire de la commune de West-Cappel

Président de la Communauté de Communes des Hauts de Flandre

La Cybersécurité, un enjeu stratégique pour la Communauté de Communes des Hauts de Flandre

A l'heure où nos missions de services publics dépendent de plus en plus du numérique, la cybersécurité est devenue une préoccupation incontournable pour la Communauté de Communes des Hauts-de- Flandre. Comme toutes collectivités, la CCHF regorge de données numériques sensibles et de systèmes qui ne peuvent être compromis. Nous le savons, les cyberattaques peuvent causer des dégâts considérables, non seulement sur le plan économique mais aussi sur la vie quotidienne des administrés. C'est dans ce contexte qu'il y a quelques mois, nous nous sommes saisis de la question en initiant un audit de cybersécurité, accompagné par un prestataire spécialisé et avec l'appui de l'ANSSI.

Le plan d'actions qui en découle nous amène aujourd'hui à renforcer nos compétences en matière de cybersécurité et à mener auprès de tous les agents de la collectivité, des campagnes de sensibilisation aux menaces existantes et aux bonnes pratiques d'hygiène numérique. Les efforts menés dans ce domaine par la CCHF devront également bénéficier aux 40 communes qui la composent, la mutualisation des ressources, la collaboration avec les acteurs spécialisés (Conseil régional Hauts-de-France, gendarmerie…) et la coopération permettront la mise en place de stratégies adaptées et l'élaboration de politiques de cybersécurité efficaces pour notre territoire.

Nos entreprises, quelle que soit leur taille, sont également des cibles potentielles pour les acteurs malveillants c'est pourquoi nous nous devons de les accompagner dans leur transition numérique. En CCHF des intervenants locaux et régionaux, experts en digitalisation des entreprises ou en cybersécurité, sensibilisent les acteurs économiques du territoire lors d'ateliers et évènements qui leurs sont dédiés.

Sur le plan politique, la cybersécurité est devenue une question transversale essentielle, les responsables politiques, tant au niveau régional que national, reconnaissent la nécessité d'investir dans la protection des infrastructures critiques et des données sensibles contre les cybermenaces. En outre, l'ouverture d'un centre de réponse à incident cyber (CSIRT) dans la région Hauts-de-France démontre la volonté forte d'accompagner les victimes de cyberattaques (PME, ETI, collectivités et associations).

La cybersécurité est notre responsabilité à tous et nous devons la prendre au sérieux.

Il y a quelques mois, nous nous sommes saisis de la question en initiant un audit de cybersécurité

Olivier GACQUERRE
Maire de Béthune
Président de la Communauté d'Agglomération Béthune-Bruay-Artois-Lys-Romane

La commune de Béthune a participé au titre de France Relance à un parcours visant à prendre en compte la menace « cyber » dans la collectivité. La supervision de cette démarche a été confiée à l'ANSSI.

Ainsi, avec le soutien de l'Etat et le recours à l'expertise de Pilliot Cybersécurité, les élus et agents de la Ville de Béthune ont été sensibilisés aux risques « cyber ». Une feuille de route a été élaborée dans l'objectif de réduire la vulnérabilité de la collectivité. Celle-ci permet désormais d'objectiver, évaluer et in fine de piloter l'atténuation des risques au quotidien.

A titre d'exemple, un « antivirus intelligent » afin de détecter les comportements anormaux et d'en atténuer les effets a été installé. L'accès aux outils numériques depuis l'extérieur a été renforcé et des formations pointues sur « l'hygiène numérique » ont été dispensées à notre direction de la transformation numérique.

Par ailleurs, le premier vecteur d'attaque restant le mail, la commune a limité les risques d'attaque vers les boites aux lettres en mettant en place un anti-spam. Nous procédons à des exercices en interne afin de tester nos agents sur la réception de courriels malveillants. L'exercice permet de réaliser une analyse des pratiques, de faire évoluer les mentalités sur le risque numérique et de renforcer la sensibilisation.

Enfin, nous profiterons du cybermois (octobre), pour mettre en œuvre le nouveau process trimestriel de sécurisation et de changement des mots de passe pour les agents et les élus et pour enclencher une réflexion commune avec la Communauté d'Agglomération sur ce sujet de la cybersécurité.

La commune de Béthune, Smart City, fait de la sécurité numérique une de ses priorités pour permettre aux usagers et aux partenaires d'interagir en toute confiance avec notre collectivité.

L'exercice permet de réaliser une analyse des pratiques, de faire évoluer les mentalités sur le risque numérique et de renforcer la sensibilisation

Nadège HORNBECK

Adjointe au Maire de Sélestat chargée de la Communication et du Numérique
Vice-Présidente de la Région Grand Est chargée de la Santé et du Handicap
Vice-Présidente de Mission Ecoter-France et Territoires Numériques

Penser global, agir local, chacun doit y prendre sa part

Notre économie, et plus largement notre société, intègrent désormais nativement les usages du numérique en matière d'accès à l'information, de transmission, de traitement de données et d'interconnexion des réseaux de données.

La sécurisation des systèmes d'information est devenue une condition *sine qua non* de l'établissement de la confiance numérique, de la stabilité des acteurs institutionnels, de la protection des citoyens et du développement de notre économie et de notre société. Le sujet est complexe dans la mesure où il relève de technologies de plus en plus sophistiquées, mais également de la prise de conscience collective et individuelle, comme de l'évolution des comportements induits.

Si la notion de sécurisation des systèmes d'information était dans les années 2000 l'apanage des acteurs étatiques dans une approche de cyberguerre et de cyberespionnage, on observe, depuis une décennie, l'émergence d'une cybercriminalité organisée et professionnalisée qui aborde le piratage de données comme une entreprise économique. À travers des attaques plus ou moins automatisées, ciblées ou aléatoires, les cybercriminels cherchent à prendre le contrôle partiel ou total d'un système d'information. Le gain financier est obtenu par la vente de données et/ou le rançonnage.

À cela s'ajoutent des attaques plus stratégiques, de la part d'acteurs idéologiques ou étatiques, destinées bien souvent à affaiblir les États qui en sont la cible. Les motivations sont variées, parfois combinées : espionnage industriel, perturbation ou neutralisation des services essentiels, influence, atteinte à la crédibilité d'un État, d'un gouvernement, d'un dirigeant ou d'une grande entreprise nationale.
Pour tenir compte de ces différentes évolutions, la France a actualisé en février 2021 sa stratégie en matière de cybersécurité, en cohérence avec les politiques européennes. L'État a identifié le niveau régional comme le plus pertinent pour garantir une bonne mise en œuvre des initiatives nationales et une adaptation aux contextes et spécificités de chaque territoire.
La Région Grand Est a lancé en mars 2023 un plan régional pour la cybersécurité qui vise à prévenir les cybermenaces par la sensibilisation de tous les acteurs régionaux et leur permettre de réaliser un diagnostic pour évaluer le niveau de maturité en cybersécurité de leur organisation et définir un plan d'actions.
Au-delà de la strate régionale, ce sont toutes les collectivités qui doivent mettre en leur sein une politique de cybersécurité.
A titre d'exemple, la commune de Sélestat dispose déjà de plusieurs solutions permettant de protéger l'infrastructure informatique de la collectivité et poursuit un travail de mise en œuvre de modes de supervision et de lutte contre les cyber-attaques.
L'enjeu numérique de demain est d'inscrire notre économie et notre société dans la responsabilisation individuelle et collective.
Penser global, agir local, chacun doit y prendre sa part.

Au-delà de la strate régionale, ce sont toutes les collectivités qui doivent mettre en leur sein une politique de cybersécurité

Frédéric LAFFORGUE

Maire de Castelnau-Le-Lez
Vice-président de Montpellier Méditerranée Métropole
Conseiller régional d'Occitanie

Le risque cybersécurité est un des risques majeurs de toutes les entreprises et collectivités. Les menaces cyber de toutes sortes ne cessent de se développer et leurs conséquences sur le fonctionnement des organisations sont difficiles à anticiper. Elles peuvent prendre la forme d'interruptions des services administratifs, de fuites de données à caractère personnel, de risques juridiques ou encore d'inaccessibilité des documents financiers ou administratifs.

Castelnau le Lez, 25 000 habitants, 2ème ville de la Métropole de Montpellier, s'est engagée dans une transformation numérique profonde, à la fois pour rendre un meilleur service aux citoyens et pour répondre aux obligations réglementaires.

Pour répondre à ce double défi, élus et Direction des Services Informatiques ont entamé conjointement depuis 3 ans une action volontariste en impliquant l'ensemble des acteurs dans une démarche d'amélioration continue.

Nous avons récemment procédé à l'évaluation de notre sécurité numérique par un organisme externe aux compétences techniques, fonctionnelles et métiers éprouvés pour ainsi mieux assurer notre cybersécurité du quotidien et adopter les bons réflexes face à une potentielle cyber attaque.

En 2020, la pandémie de COVID-19 a considérablement accéléré la progression du numérique, principalement en raison de la généralisation du télétravail, qui aujourd'hui est devenue une pratique courante. Avant cela, Castelnau s'était déjà engagée dans l'accompagnement à la transformation numérique, aussi bien pour ses agents que pour ses administrés.

Nous disposons d'ailleurs actuellement de cinq Maisons des Proximités qui offrent une variété d'ateliers axés sur le numérique et finançons également une Maison France Services qui est un dispositif de l'État visant à réduire la fracture numérique et garantir l'accès pour tous aux services publics. Nous reconnaissons donc forcément l'importance cruciale de la cybersécurité pour assurer la fiabilité de notre service public et maintenir la confiance des administrés.

En effet, il y a là la question cruciale de la protection des données sensibles. Les mairies gèrent un grand nombre d'informations confidentielles, depuis les données personnelles des citoyens jusqu'aux dossiers des employés municipaux et il est impératif de les sécuriser contre tout accès non autorisé.

La transversalité est en effet un élément clé de notre approche en matière de cybersécurité, l'objectif est commun et concerne tous les services sans exception. Cette coordination permet une approche plus complète de la cybersécurité, que ce soit au niveau de la prévention des menaces ou de la gestion des incidents. L'aspect humain est crucial et tous les agents doivent être bien informés des meilleures pratiques en matière de sécurité informatique et être capables de reconnaître les signes précurseurs d'une tentative d'attaque. Nous organisons plusieurs fois par an des campagnes de sensibilisation et des formations aux bonnes pratiques sous différentes formes.

Nous avons abordé la notion de transversalité interne, mais il est essentiel de souligner que la cybersécurité nécessite une approche globale. Il est donc impératif d'engager toutes les parties impliquées, qu'il s'agisse des agents de la Ville ou des intervenants externes tels que les prestataires de services.

Nous devons constamment nous adapter pour faire face à ces nouvelles réalités

Depuis plus de dix ans maintenant, nous travaillons sur notre Plan de Reprise d'Activité (PRA) / Plan de Continuité d'Activité (PCA). Initialement, la DSI a entrepris un audit de l'ensemble des services pour évaluer leur capacité à maintenir une continuité de service en l'absence de système informatique. Nous avons examiné les délais d'interruption acceptables et la durée de perte de données en cas de restauration d'une sauvegarde. À l'époque, une journée d'interruption était la limite acceptable, car nous n'étions pas encore très éloignés du papier. Aujourd'hui, il semble impensable d'accepter une telle période d'interruption, étant donné l'explosion du numérique.

Un PRA/PCA doit évoluer en permanence. Lorsque nous évaluons les risques actuels, il est évident qu'ils diffèrent considérablement de ceux d'il y a dix ans, notamment en ce qui concerne la cybersécurité mais aussi l'approvisionnement en électricité. **Nous devons constamment nous adapter pour faire face à ces nouvelles réalités.**

La prise de conscience est bien ancrée aujourd'hui. Les élus sont bien au fait de l'actualité et il n'est plus nécessaire de consulter la presse spécialisée pour comprendre les enjeux liés à la cybercriminalité. Les problématiques des communes sont avant tout liées aux moyens dont elles disposent et à leurs contraintes budgétaires.

La principale vulnérabilité réside effectivement dans les comportements humains plutôt que dans la technologie elle-même. Les erreurs humaines, la méconnaissance des menaces et la négligence des pratiques de sécurité sont des facteurs majeurs de risque en cybersécurité.

La solution passe inévitablement par la formation, la sensibilisation et la responsabilisation de tous pour renforcer la sécurité numérique.

Il y a là la question cruciale de la protection des données sensibles

Yves MICHEL
Maire de Marseillan

« Cybersécurité et Territoires » le retour d'expérience de la commune de Marseillan

La commune de Marseillan est sensibilisée au problème de la Cybersécurité car elle a été confrontée lors de la dernière décennie à des hackings et à un cryptovirus.

... il convient d'agir sur la modification des comportements des agents et des élus

Ainsi, les bonnes pratiques ont été mises en place depuis plusieurs années. Ces pratiques sont à plusieurs niveaux. En premier lieu, le système : pour cela nous avons fait appel à un professionnel Xefi qui nous assure une double sauvegarde (site de l'entreprise et salle blanche dans une grande ville française) avec un maintien des données sur le sol français. Nous avons mis en place des pare feux et des annuaires de confiance. Ainsi, les boites mails avec extensions @marseillan.com sont obligatoires dans les échanges internes pour éviter les boites mails non gérées par notre dispositif informatique.

En deuxième lieu, il convient d'agir sur la modification des comportements des agents et des élus. Ainsi, la commune a limité les risques de contagions virales pour les boites aux lettres en mettant en place un anti-spam, pour ne pas le citer, mail in black. Ensuite, nous obligeons à un changement de mot de passe tous les six mois. Nous allons prochainement procéder à un exercice pour simuler l'envoi d'un mail vérolé pour constater qui ouvrait le mail, la pièce jointe. L'exercice permettra de réaliser une analyse des pratiques et faire évoluer les mentalités sur le risque informatique. La commune souhaite tendre vers le "zéro trust" et s'assurer ainsi que ceux qui ont accès aux données internes suivant leur niveau d'accréditation. L'objectif est de bien faire comprendre aux utilisateurs qu'ils sont les premiers concernés par la sécurité numérique de leur collectivité.

Lionel MONTILLAUD
Maire de Sainte-Hélène

« Nous sommes tous vulnérables ! »

La menace cyber n'est plus une surprise pour personne. Encore moins pour les collectivités locales qui sont devenues une cible privilégiée des cyberattaques en raison du grand nombre de données qu'elles possèdent suite à la transformation des services publics numériques. En 2022, une collectivité sur trois a été victime d'une tentative d'intrusion. Hameçonnage, rançongiciels ou piratage de compte mail…, les hackers débordent d'imagination et utilisent toutes les brèches possibles. Le phénomène se multiplie d'année en année ! Et pour les collectivités de toutes tailles !

Les petites communes se pensent souvent à tort, à l'abri. Elles sont, au contraire, encore plus exposées aux risques que les grandes villes dans la mesure où celles-ci disposent de moyens humains et techniques pour se prémunir au mieux des attaques. Maire d'une commune de 3 000 habitants, je sais qu'à notre échelle, les moyens de défenses sont beaucoup plus compliqués à mettre en place car, bien souvent, les budgets, les compétences manquent et nos priorités quotidiennes sont ailleurs.

Pourtant, nous sommes tous vulnérables ! Et il est temps de prendre conscience de notre retard (65%* des collectivités pensent que le risque est faible, voire inexistant, ou ne savant pas l'évaluer) et de trouver des solutions rapides et efficaces pour nous protéger et éviter de perturber voire d'interrompre les services rendus à nos administrés. D'autant que les conséquences peuvent être lourdes : perte irrémédiable de données informatiques ou financières, mise au chômage technique d'agents de mairie, altération du lien de confiance avec les citoyens…

Parmi les signes encourageants pour répondre à ce défi majeur, on peut noter que le RGPD a servi d'accélérateur dans la mise en place de dispositifs de sécurité. Comme de nombreux élus locaux, j'ai bien sûr veillé à la mise en place de ces règles de sécurité pour tous nos outils web mais c'est loin d'être suffisant. Les politiques de sécurité restent encore peu structurées, souvent par manque de culture cyber.

Les petites communes se pensent souvent à tort, à l'abri

Peu de communes utilisent des mots de passe complexe, sensibilisent leurs personnels au sujet de la cybersécurité ou pensent à la gestion des droits d'accès lors de changement de personnel. Progresser au niveau communal, passera nécessairement par la mutualisation. Que ce soit pour acheter de systèmes de protection, recruter des profils adaptés et accompagner nos agents à adopter les bons réflexes dans leurs pratiques numériques.

L'état s'empare de ce sujet mais l'Agence Nationale de la Sécurité des Systèmes d'Information mérite d'être mieux connue et doit développer des actions innovantes de sensibilisation et de formation pour accompagner les collectivités notamment, encore une fois, les plus petites et créer un environnement national technique et industriel permettant à la France d'assurer elle-même sa sécurité.

La cybersécurité est désormais l'affaire de tous. Et face à des pirates informatiques opportunistes, les collectivités ne doivent surtout pas baisser la garde mais au contraire poursuivre leurs efforts et muscler leurs défenses numériques pour ne plus être les cibles les plus faciles. Protégeons-nous !

**Etude 2021 cybermalveillance.gouv.fr auprès des collectivités de moins de 3500 habitants qui représentent 91% des communes en France)*

Mauna TRAIKIA
Conseillère territoriale Plaine Commune-Grand Paris
Vice-Présidente de Mission Ecoter-France et Territoires Numériques

Le CyberMois en octobre, le mois de la sensibilisation aux enjeux de la cybersécurité, c'est sain. Mais toute l'année, c'est mieux !

Le CyberMois en Octobre le mois de la sensibilisation aux enjeux de la cybersécurité c'est sain mais toute l'année c'est mieux : rendez-vous sur cyberbienveillance.org. Et si nous protégions notre CyberMoi pour mieux protéger notre Cyber NOUS.

L'élu face à une crise Cyber Quelques reflexes ? Comment réagir ? Les collectivités : sont les proies parfaites des cybermalveillants, prédateurs du 21ème siècle. Que les collectivités soient petites ou grandes, elles sont les grandes victimes des Cyberattaques.

« La question n'est pas de savoir si je vais être attaqué mais quand et suis-je suffisamment préparé » General Boget Gendarmerie nationale lors des secondes rencontres cybersécurité de Plaine commune.

Depuis plusieurs années, les cyberattaques sont devenues récurrentes dans l'actualité. Les élus de collectivités de toute taille ne sont pas épargnés et ont pour responsabilités légales entre autres : la protection des données de leurs administrés, la continuité des services publics et la préservation de la confiance citoyenne en leurs élus.

Que ce soit le secteur privé ou le secteur public nous sommes toutes et tous concernés. Que la proie soient les Hôpitaux ou collectivités, rien n'arrête les cybercriminels. Ils sont dénués d'éthique ou de sentiment car seul le gain compte.

Pour une collectivité cela peut aller de l'arrêt complet des services publics, comme a pu le connaître la Mairie d'Angers au vol de données des concitoyens pour les revendre sur la partie obscure du Web (DarkWeb) comme a pu le vivre la Mairie de Betton.

Les cybercriminels sont organisés. Ils ont leurs propres modèles économiques et ne reculent devant rien. Ils ne prennent pas de vacances et ne cessent d'innover.

Dernièrement, un chiffrage inédit en France a permis d'estimer le coût des cyberattaques à deux milliards d'euros en 2022.

D'après cette estimation réalisée par le cabinet d'études économiques Asterès pour le compte du CRiP, une association regroupant 13 000 responsables d'infrastructure et de technologie, plus de 40% de cette somme a été destinée au paiement de rançons.
Je pourrais évoquer des discussions avec des Maires de ville de toute taille dont l'idée même du téléphone qui sonnerait dans la nuit pour annoncer la cyberattaque les effraie au quotidien.
De nombreux exemples : Mairie de Lille, Mairie de Marseille, Mairie d'Angers et plus récemment La cyberattaque de la Mairie de Betton en Ille et Villaine où RIB, factures… et données personnelles d'habitants ont été rendues publiques suite au refus de payer la rançon de 100 000 dollars pour les récupérer.
Les collectivités possèdent les informations personnelles les plus qualifiées pour ainsi dire les plus vraies et des informations ultra confidentielles concernant la vie personnelle des administrés.
Les collectivités sont le garant des services publics essentiels au quotidien à leurs administrés.

Les élus de collectivités de toute taille ne sont pas épargnés et ont pour responsabilités légales entre autres : la protection des données de leurs administrés, la continuité des services publics et la préservation de la confiance citoyenne en leurs élus

Ce qui implique donc que ces données et services sont très attractifs, précieux et hors de prix pour les cybercriminels.
Un simple clic dans un mail peut permettre une infection du système d'information, bloquer toute une collectivité et les données dérobées peuvent même avoir des impacts à long terme comme entre autres l'usurpation d'identité et la perte de confiance citoyenne.

Que faire en cas de cyberattaque ? Faut-il payer la rançon ? qui contacter ? Quels sont les premiers gestes de secours à prodiguer ?

En France, nous avons un dispositif remarquable dédié et les collectivités ne sont pas seules

- Anssi : Agence nationale de la sécurité des systèmes d'information (https://www.ssi.gouv.fr/), de nombreux guides techniques et publications

- ComCyberGEND Commandement de la Gendarmerie dans le cyberEspace (https://www.gendarmerie.interieur.gouv.fr/)

- Cybermalveillance.gouv.FR : fiches pratiques, diagnostic en ligne, …

Si vous pensez être victime d'une cyberattaque ou si vous avez un doute vous pouvez utiliser le diagnostic en ligne sur le site de https://www.cybermalveillance.gouv.fr/diagnostic/accueil .

Ce diagnostic pourra vous aider à déterminer la marche à suivre et vous conseiller des prestataires.
Si l'attaque est avérée, heureusement les collectivités ne sont pas seules.

Tout d'abord **le sujet de la rançon** :

La question récurrente faut-il payer la rançon ? Les acteurs ci-dessus conseillent de ne pas céder au paiement de la rançon pour ne pas continuer à alimenter un système.

Pour les grandes étapes simplifiées :

1/ **Alerter le Service informatique** s'il existe et oui pour les plus petites collectivités cela peut être problématique. Dans ce cas faire déconnecter le réseau pour éviter la propagation de la cyberattaque.

2/ **Porter plainte** et préserver les preuves car cela va permettre de lancer une enquête.
Rendez-vous au commissariat ou à la gendarmerie la plus proche.
Vous pouvez toutefois communiquer avec un gendarme 7jours/7 24h/24 sur le site (https://www.gendarmerie.interieur.gouv.fr/contact/discuter-avec-un-gendarme) ou via l'application Ministérielle : Ma Sécurité disponible sous IOS et Android qui regorge d'informations précieuses aussi pour les élus locaux et un guichet unique de l'offre numérique sécuritaire)

3/ **Déclarer à la CNIL** : Si des données personnelles ont été dérobées, une déclaration à la CNIL dans un court délais s'impose.

Si vous n'êtes pas en mesure d'évaluer l'atteinte à des données personnelles, la CNIL peut enregistrer des déclarations préalables d'incident.

(https://www.cnil.fr/fr/notifications-dincidents-de-securite-aux-autorites-de-regulation-comment-sorganiser-et-qui-sadresser)

4/ **Communiquer en interne /externe** afin que les collaborateurs et les personnes concernées puissent être informés des risques de sollicitations frauduleuses et maintenir la confiance des habitantes et habitants...

Les enjeux de la cybersécurité font que nous devons toutes et tous être responsables individuellement pour nous protéger collectivement.
Il est toutefois préférable d'anticiper, de former aux risques cybersécurité et de sensibiliser afin de lutter en amont notamment agir sur la faille humaine.
La peur n'ayant jamais fait fuir le danger, il est essentiel de se préparer et investir dans un plan cybersécurité.
Mettre en place a minima :

- des instances de gouvernance de la crise,
- plan de continuité de services,
- plan sauvegarde des données et de
- plan de communication interne/externe essentiel.

Un simple clic dans un mail peut permettre une infection du système d'information, bloquer toute une collectivité et les données dérobées peuvent même avoir des impacts à long terme comme entre autres l'usurpation d'identité et la perte de confiance citoyenne

La faille humaine est aussi un des points d'entrée des cybercriminels à ne pas négliger. Il est nécessaire et indispensable de former tous les collaborateurs pour la détection de mails frauduleux notamment pour « réfléchir avant de cliquer » et éviter le pire.

Chacune et chacun de nous est donc concerné, aussi bien collectivité, entreprise ou habitant.
Chacune et chacun de nous est concerné dans sa vie professionnelle ou personnelle.
C'est pour cela que vous pouvez rejoindre le collectif de la communauté des cyberbienveillantes et cyberbienveillants sur le site www.cyberbienveillance.org* afin de partager nos expériences, nous entraider et faire que chacune et chacun de nous œuvre pour une société numérique durable, éthique, sociale, responsable, et inclusive.

Protégeons ensemble notre CyberMoi pour protéger notre CyberNous : rendez-vous sur Cyberbienveillance.org 1er réseaux citoyens, collectivités et entreprises unis face aux risques cyber.

**Cyberbienveillance.org en partenariat avec la Mission Ecoter France Territoires numérique.*

Dernièrement, un chiffrage inédit en France a permis d'estimer le coût des cyberattaques à deux milliards d'euros en 2022

Cybermoi/s 2023

Entreprises

Thierry ELKAIM

Directeur du Développement
Cisco France

Octobre, mois européen de la cybersécurité et 2024 année française de la cybersécurité… ?

Bien plus que l'effort de sensibilisation du très utile mois européen de la cybersécurité, c'est une mobilisation totale des collectivités territoriales sur l'année à venir qui est nécessaire, à l'approche des Jeux Olympiques et Paralympiques qui font peser sur la France entière une forte menace cyber.

Ce cybermois, organisé chaque année en octobre à l'initiative de l'Agence de l'Union européenne pour la cybersécurité (ENISA), en association avec la Commission européenne et les États membres, a pour objectif de promouvoir la cybersécurité à travers d'actions de sensibilisation. Si le thème pour 2022 était les rançongiciels et l'hameçonnage, l'ENISA a souhaité faire de la fraude par ingénierie sociale le thème principal de 2023, face à la multiplication des fraudes par ingénierie sociale. (Abus de confiance où les cybercriminels soutirent argent et informations personnelles sur les réseaux sociaux aux particuliers).
Mais attention ! Il serait contreproductif de n'attirer l'attention uniquement des citoyens et que sur la fraude sur les réseaux sociaux, pour cette 11ème édition.
En effet, le fléau des cyberattaques demeure un phénomène durable bien plus large, qui nous concerne tous : administrations, entreprises, nécessitant des actions immédiates de chacun.
Par exemple, les collectivités ont en leur possession un grand nombre de données personnelles de leurs administrés (y compris avis d'imposition, fiches de paie,) qui représentent une cible juteuse pour les attaquants .(lesquels sauront par la suite d'autant mieux personnaliser leurs tromperies).

Aussi la politique de cybersécurité d'une collectivité à destination de ses administrés, revêt 3 dimensions :

- Politique (élus),
- Organisationnelle et financière (direction générale des services),
- Technique (services informatiques et DPO).

Face à l'actualité, passer de la sensibilisation à l'action…

Avec les Jeux Olympiques, les régions, les départements et villes hôtes sont en première ligne, mais ne seront pas les seuls en France à être menacés.
En effet n'oublions pas que les attaquants multiplient leurs attaques sur de nombreuses cibles de manière aléatoire « à l'aveugle » via des robots, ville hôte ou non. (On peut donc être victime de « balles perdues » aussi en cyberattaques ...)

C'est donc le moment ou jamais, à cette occasion, pour les collectivités de se doter de moyens adaptés et durables, pour assurer leur sécurité, face à ces attaques avec lesquelles elles devront s'habituer à vivre. Il s'agit là aussi d'un héritage pour le futur, issu du passage des Jeux Olympiques en France.

Le bon moment ...

C'est aussi le bon moment car de nombreux obstacles ont été levés ces derniers temps, et la situation s'éclaircit. Pendant bien longtemps le progrès en cyber a été freiné pour de nombreuses raisons- toujours très bonnes- notamment :

- Les élus ne voyaient pas l'intérêt pécuniaire des cyberattaquants à s'attaquer à leur collectivité et vivaient dans l'insouciance,
- Les directeurs des services n'attribuaient pas les budgets suffisants à la cybersécurité, n'ayant pas conscience des coûts énormes et des préjudices subis en cas d'attaques,
- De ce fait, les directeurs informatiques n'avaient pas toujours l'écoute suffisante des élus et des directeurs des services face ce sujet ingrat :

- Les mesures de sécurité qu'ils prenaient étaient impopulaires, car elles rendaient moins bonnes les performances du réseau et l'expérience utilisateur,
- La pénurie de compétences et la pénibilité des tâches à assurer en interne pour lutter contre les menaces, leur étaient pénalisante

- Les discours souvent ésotériques des fournisseurs de solutions multiples et variées, plus ancrés dans la complexité que dans la vulgarisation et la pédagogie, n'encourageaient pas à l'adoption de ces technologies pourtant nécessaires.

Vous pouvez aisément comprendre que les collectivités ont perdu du temps face à l'avancée des cyber malfaisants, et qu'il s'agit de reprendre l'avantage face à eux.

L'accélération est cette fois possible car…

- Les Jeux Olympiques sont un véritable catalyseur, qui demande aux collectivités une réponse urgente à une pression externe qui pousse à l'action, dans un délai défini avec les conséquences connues de l'inaction.
- Face à l'actualité, les élus et les directeurs des services ont pleine conscience des dangers et des coûts des cyberattaques et dialoguent davantage avec les services informatiques pour trouver des solutions, en dépit de l'inflation, de la hausse des prix de l'énergie ou de la transformation énergétique qui sont également leur priorité.
- Enfin le marché de la cybersécurité est bien plus lisible que dans le passé, les offres de plus en plus intégrées et les bonnes pratiques de plus en plus accessibles.

Les problèmes à régler restent les mêmes…

Que ce soit pour le comité d'organisation de l'évènement le plus menacé au monde, ou pour une collectivité territoriale, les menaces à affronter restent les mêmes et sont connues :

- Usurpation d'identités, intrusion dans un système d'information, via les réseaux ou un terminal (y compris les objets connectés), vols de données personnelles, rançongiciels, hameçonnage, , etc.

Quelles nouvelles réponses ? Comment la situation peut-elle s'améliorer face à la menace… : processus, bonnes pratiques et technologies…

- Dans un certain nombre de collectivités, des progrès ont été accomplis, que ce soit en **sensibilisation** des équipes au danger, ou en processus d'**organisation**, (analyse de risque, sécurité by design…,)
- En termes de **bonnes pratiques** à adopter :
  - Le fameux « la question n'est pas de savoir si on va être attaqués mais quand on va être attaqués » doit être aujourd'hui dans tous les esprits.
  - Les plans d'action doivent autant traiter la prévention, que la détection et la réponse aux menaces, conduisant à **un plan de résilience** en cas d'attaque et à des exercices réguliers d'anticipation.
  - Mettre au rebus les produits obsolètes (logiciels et matériels) qui ne sont plus supportés, , véritables aubaines pour les attaquants et **gérer les vulnérabilités de son parc** pour bénéficier des dernières mises à jour des fournisseurs,.
  - **Face à la pénurie de compétences**, avoir une réflexion de « make or buy » et décider de la partie à traiter en interne et de celle à externaliser dans des centres opérationnels de sécurité (Security Opération Centers). **Favoriser l'automatisation** (cf plus oin)
  - Ne faire confiance à personne **(Zero Trust**) pour les accès aux réseaux et aux informations.
- Le moment est aussi venu d'investir, alors quels sont les **nouveaux services rendus par la technologie ?**
  - Grâce aux nouvelles architectures, il est possible d'apporter de la sécurité à l'utilisateur sans nuire à sa performance où qu'il soit (travail hybride, nomade, cloud, …)
  - Le temps des antivirus est révolu, passer à des outils de **détection et réponse (DR) aux menaces** (réseaux, postes de travail,…)
  - **Simplifier** : Il existe désormais des plateformes intégrées couvrant les différents domaines de la cybersécurité (réseaux, terminaux, applications, données, cloud) permettant de restreindre le nombre de fournisseurs et diminuer les coûts d'intégration et de formation.

La question n'est pas de savoir si on va être attaqués mais quand on va être attaqués

- Face à la complexité, **automatiser** reste la réponse :
  - Il est aujourd'hui plus facile de collecter des informations, grâce à des sondes réparties sur les réseaux et les terminaux, détecter automatiquement les situations anormales grâce à l'intelligence artificielle, remonter ces informations en temps réel dans des tableaux de bord faciles à exploiter, le tout nécessitant moins de main d'œuvre que dans le passé.
    - Face à une suspicion, il est ainsi possible en temps réel de demander un verdict à des bases de données de renseignement accessibles, et décider de la suite à donner.
- Face à l'infobésité des remontées d'alerte du passé, **l'intelligence artificielle générative** va accélérer les temps de réponse des équipes cyber et augmenter leur efficacité, tout en allégeant leur charge de travail.

Donc, vive le mois européen de la cybersécurité, il est le bienvenu !
Il doit encourager les collectivités territoriales, à faire face dignement aux menaces qui risquent de monter dans les mois qui viennent, avec l'arrivée des Jeux Olympiques et Paralympiques, en adoptant les processus et la technologie nécessaires, et se constituer un héritage pour le futur.

Cisco est partenaire officiel de Paris 2024 pour les infrastructures de cybersécurité, les équipements réseaux et les logiciels de visioconférence.
La stratégie de Cisco consiste à proposer à ses clients des solutions logicielles et matérielles de connectivité (équipements de tous types de réseaux), qui sont sécurisées par nature, et observables.
Pour répondre aux attentes du marché, Cisco fournit une plateforme étendue permettant de gérer à la fois la sécurité du réseau, du poste de travail, des applications et du cloud. Elle reçoit des remontées de tous ces éléments et les intègre à un tableau de bord intelligent facile d'utilisation permettant une grande réactivité.

Cisco est partenaire officiel de Paris 2024

Vous -ou votre partenaire- êtes ainsi alerté en cas de détection de problème de manière automatique et pouvez corriger.
Cisco s'appuie également sur son service mondial de renseignement sur l'état de la menace (Talos), qui permet aux clients de s'appuyer sur cette connaissance des menaces déjà connues pour pouvoir les traiter avec efficacité.
Cisco France est particulièrement à l'écoute des collectivités territoriales en vue de leur partager ses multiples expériences sur l'approche de la cybersécurité, en termes de technologie, de process et de gestion des compétences (signature de convention de formation gratuite Netacad)

Pour répondre aux attentes du marché, Cisco fournit une plateforme étendue permettant de gérer à la fois la sécurité du réseau, du poste de travail, des applications et du cloud

Frank MOSSER

Président MGDIS

Cybersécurité et Territoires : MGDIS s'engage envers la Sécurité du Service Public

Chers adhérents de la Mission Ecoter-France et Territoires Numériques,

Au nom de MGDIS, je suis honoré de vous adresser cette tribune sur un sujet qui nous tient particulièrement à cœur : **la cybersécurité et son impact sur nos territoires.** MGDIS, en tant qu'acteur investi dans le domaine des solutions logicielles pour les collectivités territoriales, considère la sécurité comme une priorité absolue. Nous souhaitons partager avec vous nos convictions, nos bonnes pratiques et notre engagement indéfectible en matière de cybersécurité.

Aujourd'hui, la transformation numérique est une réalité incontournable pour l'ensemble des acteurs publics. **Le Gouvernement Français a fait du Cloud un élément central de sa stratégie, visant à accélérer la modernisation de l'administration tout en garantissant la sécurité des données des citoyens et des entreprises.** MGDIS est pleinement aligné avec cette vision, et nous soutenons cette politique Cloud avec détermination.

En 2020, près de 60 % des victimes de cyberattaques étaient des PME et des collectivités territoriales. En 2021 et 2022, ce chiffre a continué d'évoluer, démontrant que la protection des PME/TPE/ETI et des collectivités face à ces menaces est plus cruciale que jamais.

Le temps n'est plus aux constats et aux promesses mais aux actes avec la mobilisation de moyens proportionnés pour répondre à cet enjeu. La mobilisation de MGDIS se mesure par :

- 2 experts dédiés à notre pôle RSSI,
- 1 juriste spécialisé dans la sécurité,
- Formations spécifiques pour nos équipes techniques, de développement et tests et le MOOC de l'ANSSI obligatoire pour tous nos collaborateurs,
- 2 audits de sécurité réalisés chaque année par une société certifiée PASSI,
- Plus de 100 000 contrôles de vulnérabilité effectués annuellement,
- Des dizaines de correctifs de sécurité appliqués chaque année suivant les évolutions des menaces,
- L'exploitation de plus de 250 environnements sécurisés,
- Le déploiement et pilotage d'un Système de Management de la Sécurité de l'Information (SMSI),
- Une démarche de certification ISO 27001 en cours,
- MGDIS lauréate du dispositif d'accompagnement à la qualification SecNumCloud,
- Aucune faille de sécurité exploitée à ce jour.

Dans notre démarche de développement, **la sécurité est une priorité absolue**, suivant le principe du "**Security by Design**". Nous intégrons les exigences de sécurité dès la conception de nos produits, grâce à des analyses de risques méthodiques. Notre architecture micro-services à base de containers garantit une sécurité distribuée et une protection des communications.

Aujourd'hui, la transformation numérique est une réalité incontournable pour l'ensemble des acteurs publics

La cybersécurité est un engagement continu, avec une détection précoce des vulnérabilités tout au long du processus de développement et de la production logicielle. Nos solutions sont soumises à une surveillance constante, avec une attention particulière aux attaques potentielles. Notre **Plan d'Assurance Sécurité (PAS)**, conforme au CCSC, couvre tous les aspects de la sécurité, de la politique à la résolution des différends.

Par ailleurs, MGDIS est fière de collaborer avec différentes écoles et d'accueillir des alternants. Cette démarche nous permet d'apporter un regard neuf et de contribuer à la formation des futurs experts en sécurité (interventions en 2023, notamment, à l'ENSIBS, l'ESNA, l'ISTIC, l'IRIAF…).

Nous ne nous contentons pas de garantir la sécurité de nos produits, mais nous étendons notre engagement à nos services en ligne. Notre solution logicielle "**Portail Aiden**" est reconnue comme une **solution de confiance par OVH**. L'hébergement est réalisé dans un datacenter respectant la réglementation européenne, notamment le "code de conduite" européen CISPE sur la protection des données et celui sur la réversibilité des données, facilité par la Commission Européenne. **MGDIS bénéficie du label OpenTrustedCloud.**

Nous travaillons main dans la main avec nos clients, en collaborant étroitement, en toute transparence avec leurs équipes RSSI. Nous participons activement aux homologations RGS, aidons à l'analyse des risques, et facilitons la réalisation de tests d'intrusion ou de configuration en mode service en ligne.

Une illustration concrète de notre engagement est le récent **Bug Bounty** mené en partenariat avec le **Conseil Départemental de la Haute Garonne, l'association COTER Numérique et le Club des RSSI des collectivités territoriales**. Cette initiative a permis de détecter des vulnérabilités et d'intégrer leur résolution dans notre processus de correction et dans le cycle des sorties des versions mensuelles, illustrant notre **engagement envers une amélioration continue de la sécurité de nos logiciels.**

Madame Marilyne Boubée, RSSI du Conseil Départemental de la Haute Garonne, témoigne de notre engagement en affirmant que « *MGDIS est un éditeur mature qui intègre les exigences de sécurité à tous les niveaux de son processus d'édition logicielle. Les résultats du Bug Bounty démontrent une prise en compte totale de ces exigences.*

Au sein du Club RSSI, nous croyons en une démarche constructive et collaborative avec les éditeurs de logiciels. Nous sommes convaincus que cette transparence peut bénéficier à l'ensemble des collectivités territoriales. »

La sécurité est un objectif stratégique de MGDIS et les moyens humains et financiers nécessaires sont mobilisés pour le tenir.

Nous sommes convaincus que les acteurs du numérique qui n'ont pas pris la mesure de cet enjeu auront disparu dans les 3 années à venir. Chacun à son niveau doit s'assurer de limiter les d'impacts potentiels d'une attaque sur son système en vérifiant qu'au-delà des promesses écrites dans un contrat de partenariat ou une réponse à un appel d'offre, les moyens humains et financiers mis en œuvre sont réels et proportionnés. La sécurité représente une responsabilité collective, et les acteurs qui refusent ou négligent d'assumer le coût associé, mettent en péril l'ensemble du groupe.

Ensemble soyons vigilants pour bâtir un avenir numérique plus sûr et plus prospère pour tous.

La sécurité est un objectif stratégique de MGDIS et les moyens humains et financiers nécessaires sont mobilisés pour le tenir

Charles MURE

COO CYBERSHEN

Changer de perspective sur la cybersécurité

Il est aujourd'hui indéniable qu'un nombre grandissant de services proposés aux citoyens par les collectivités territoriales reposent sur la disponibilité de services numériques.

A l'ère de la multiplication de ces usages, une cyber-attaque peut mettre à mal un nombre important de services publics essentiels à la vie de la cité. Assurer la résilience des systèmes informatiques devient un enjeu majeur pour les territoires.

Malheureusement, depuis quelques années, la menace s'est intensifiée. Une collectivité sur dix a déjà été victime d'un rançongiciel selon les données de juin 2023 issues des diagnostics Di@GoNal (menés par la Gendarmerie auprès de 965 collectivités, et 769 communes de moins de 5 000 habitants).

Ce nombre grandissant d'attaques s'explique notamment par le fait que les acteurs malveillants se sont structurés et ont automatisés leurs opérations, leur permettant désormais de **cibler tout type de structures sans avoir besoin de démultiplier leurs efforts.**

Citoyens, protection des données personnelles et lien de confiance

Dans le même temps, les citoyens deviennent de plus en plus exigeants sur les sujets de **protection de leurs données personnelles**, **mettant la confiance dans les systèmes au cœur du sujet**. En effet, au-delà de l'incapacité à fournir un service pendant une cyber-attaque, une attaque réussie menant à un vol de données personnelles détériore immanquablement lien de confiance construit avec les citoyens. Et cette confiance sera d'autant plus dure à reconstruire si des manquements sérieux dans la protection des données sont exposés à la suite de l'attaque.

Changer de perspective pour passer à l'action

Mais cette situation ne devrait pas rester une fatalité. Ce mois d'octobre marque le début du cyber-mois. Et au-delà d'être un mois marqué par les traditionnelles sensibilisations sur les risques d'hameçonnages, ce mois est aussi l'occasion de **changer sa perspective sur la cybersécurité.**

Pour mieux prioriser les sujets de cybersécurité, nous sommes convaincus que nous devons **arrêter de voir la cybersécurité seulement comme un moyen de se protéger contre des menaces obscures**, mais plutôt comme **un outil efficace pour renforcer les liens de confiance sur son territoire**, d'autant plus à l'heure où ceux-ci tendent à se fragiliser.

En prenant cette perspective, la cybersécurité s'intègre désormais dans un projet plus large et plus motivant pour les parties prenantes, permettant in fine de faciliter la communication et de mieux valoriser les actions prises.

Bien sûr, l'objectif n'est pas de transformer du jour au lendemain toutes les structures en forteresses inviolables, mais plutôt de se mettre dans une démarche d'amélioration continue, avec motivation et engagement, et **devenir pro-actif de sa cybersécurité pour renforcer les liens de confiance.** Quelle que soit le niveau de maturité actuel sur ce sujet, seule la progression compte.

Dernièrement, plusieurs initiatives ont été lancées pour accompagner ce passage à l'action sur les sujets de cybersécurité. Par exemple, nous pouvons citer le réseau **Communes Cyber-dynamique**, le développement de **cyber-malveillance.gouv.fr,** ou encore le "**Grand Défi Cyber**" permettant le financement d'innovation critique sur la cybersécurité.

Malheureusement, depuis quelques années, la menace s'est intensifiée

Enfin, si vous souhaitez passer à l'action rapidement, il existe déjà de nombreuses approches pragmatiques qui fonctionnent, et qui permettent de prendre les bonnes décisions dès aujourd'hui pour améliorer sa posture cyber sans avoir à rediriger tout son budget informatique/système d'information vers la cybersécurité.

En voici quelques exemples concrets :

- Se former et nommer un référent cyber dans sa collectivité, et s'assurer qu'il dispose des sponsors et des moyens suffisants pour mener des actions à impact.
- S'acculturer aux attaques en organisant des exercices "Incendie Cyber". Il s'agit d'évoquer dans chaque structure les conséquences envisageables d'une cyberattaque, grâce à une simulation conduite une fois par an (sur le modèle de l'alerte incendie).
- Anticiper l'interruption d'activité : Préparer et diffuser une liste de bonnes pratiques à la suite de l'alerte incendie cyber.
- Organiser la sauvegarde de ses données critiques sur un support hors-ligne.
- Sécuriser les postes de travails de son SI (qui représentent la porte d'entrée principale des attaques modernes) et demander des engagements en termes de sécurité informatique auprès de son infogérant.
- Vérifier les configurations de ses applications hébergées sur le Cloud, notamment la configuration de l'authentification double facteur pour tous les utilisateurs dès qu'elle est disponible.

Bon Cybermois à toutes et à tous !

A propos

CYBERSHEN est une plateforme 100% souveraine « tout-en-un », hébergée en France, basée sur des technologies européennes pour apporter un niveau de protection essentiel à tous. Innovation technologique majeure (DeepTech), CYBERSHEN est soutenu par BPI France, le Campus Cyber, Systematics, l'incubateur de Telecom Paris, ainsi que la Banque de territoires. Cybershen est membre de la Mission ECOTER.

CYBERSHEN est issue des expériences terrains d'un ancien RSSI Santé et d'un expert cyber, agissants au service du bien commun.

Pour mieux prioriser les sujets de cybersécurité, nous sommes convaincus que nous devons arrêter de voir la cybersécurité seulement comme un moyen de se protéger contre des menaces obscures, mais plutôt comme un outil efficace pour renforcer les liens de confiance sur son territoire, d'autant plus à l'heure où ceux-ci tendent à se fragiliser

Édouard de RÉMUR

Co-fondateur d'Oodrive

Cybersécurité et Territoires : Bâtir la confiance numérique pour un avenir durable

Dans l'épopée numérique qui façonne notre époque, les territoires se trouvent au cœur d'une révolution inédite. Cette transformation, portée par la numérisation croissante, est un moteur puissant de progrès, mais elle s'accompagne d'une réalité obscure : les menaces et ingérences cyber. En ce mois dédié à la sensibilisation à la cybersécurité, il est crucial de plonger dans les enjeux de cette mutation numérique et d'explorer les voies qui conduisent à la Confiance Numérique. Le cloud de confiance, inscrit dans la Doctrine Cloud de l'État, se positionne comme la pierre angulaire de la résilience des territoires et des collectivités.

La Confiance Numérique : Garant de la Sécurité et de l'Indépendance Numérique

Alors que les collectivités s'orientent résolument vers le numérique, cette connectivité accrue expose à de nouvelles vulnérabilités. La confiance numérique émerge comme un élément vital pour le bon fonctionnement des territoires et la satisfaction de leurs citoyens. Au cœur de cette quête, la souveraineté numérique évolue vers une vision plus inclusive : le cloud de confiance. Cette confiance repose sur deux piliers fondamentaux. D'une part, la sécurité technologique garantit la protection des données, et d'autre part, la sécurité réglementaire écarte la menace des lois extraterritoriales.

Un acteur de confiance dans ce contexte doit posséder ces deux piliers. La sécurité technologique assure la robustesse des infrastructures et inspire confiance en protégeant les données. La sécurité réglementaire offre une protection juridique contre les lois extraterritoriales, préservant ainsi la confidentialité des informations sensibles. Cette souveraineté nationale, promue par la Doctrine Cloud de l'État, suppose un contrôle total des infrastructures et des données en France, réduisant les risques d'ingérence extérieure.

Le Cloud de Confiance : Fondement de la Résilience Territoriale

Dans ce paysage complexe, où les cyberattaques peuvent paralyser l'accès aux services publics essentiels, la confiance numérique s'appuie sur des infrastructures sécurisées, une gouvernance transparente et participative, ainsi qu'une utilisation éthique et responsable des technologies. Les mesures de sécurité, incluant le chiffrement et la gestion des identités numériques, se présentent comme des remparts indispensables.

La collaboration entre les acteurs de la filière devient cruciale pour concevoir des solutions fiables. Investir dans une infrastructure numérique fiable garantit des villes intelligentes durables, offrant une meilleure qualité de vie et une efficacité accrue des services pour tous les citoyens.

Le Cloud de Confiance : Bouclier des Intérêts Nationaux et Citoyens

Le cloud de confiance devient également le bouclier protecteur des intérêts nationaux et citoyens. Dans un monde où les menaces numériques et les lois extraterritoriales se multiplient, la maîtrise des données sensibles devient un impératif de sécurité nationale.

Cette indépendance numérique n'est pas simplement un rempart défensif, mais aussi un catalyseur pour la transition numérique. Elle optimise les coûts, simplifie l'organisation et améliore la qualité de service, façonnant ainsi un avenir numérique plus résilient et durable.

La souveraineté numérique évolue vers une vision plus inclusive

La collaboration entre les acteurs de la filière devient cruciale pour concevoir des solutions fiables

Accompagner la Transformation Numérique du Secteur Public : Un Impératif Financier et Stratégique

Au-delà des défis de sécurité, la collaboration sécurisée devient une nécessité urgente. Comment partager des données sensibles avec des organisations publiques et des partenaires externes sans compromettre l'intégrité du système d'information ? Des cas d'usages concrets et des témoignages clients émergent comme des preuves tangibles de faisabilité.

Cependant, les chiffres révèlent des disparités inquiétantes : seulement 21% des PC utilisés par les collectivités sont chiffrés, contre 43% dans le secteur privé. Les signalements à l'ANSSI s'élèvent à 2296, avec 370 incidents identifiés, dont 9 qualifiés de majeurs. Dans ce contexte, 18% des collectivités ont augmenté leur enveloppe budgétaire pour renforcer leur politique de sécurité.

Répondre aux Enjeux Actuels : Accompagner la Transformation Numérique du Secteur Public

Répondre aux enjeux de la cybersécurité signifie également accompagner la transformation numérique du secteur public. Bien plus qu'une nécessité sécuritaire, cette approche se positionne comme un levier stratégique pour optimiser la dépense publique. La modernisation des infrastructures, la rationalisation des processus et la sécurisation des données convergent vers une gestion plus efficiente des ressources, assurant ainsi une pérennité financière.

En conclusion, la cybersécurité, ancrée dans la confiance, n'est pas simplement un rempart contre les menaces, mais un catalyseur pour la transformation positive des territoires. En investissant dans des pratiques avancées, une collaboration sécurisée et une confiance numérique affirmée, les territoires édifient non seulement une résilience numérique, mais également les fondations d'une société numérique éthique, transparente et prospère.

[Téléchargez ici la Brochure d'Oodrive : "Une sécurité sans faille pour collaborer en totale confiance" - Nos solutions]

Au-delà des défis de sécurité, la collaboration sécurisée devient une nécessité urgente

Directeur de la publication

Alain MELKA

Ligne éditoriale

Quentin MEULLEMIESTRE

Contributeurs

Denis THURIOT
Bertrand RINGOT
Alain MELKA
Quentin MEULLEMIESTRE
Fabien BAZIN
Éric BERLIVET
Luc BOUARD
François CHARBONNIER
Joël DUQUENOY
Fatima EL OUASDI
André FIGOUREUX
Olivier GACQUERRE
Nadège HORNBECK
Frédéric LAFFORGUE
Yves MICHEL
Lionel MONTILLAUD
Mauna TRAIKIA
Thierry ELKAIM
Frank MOSSER
Charles MURE
Édouard de RÉMUR

Contacts Mission Ecoter-France et Territoires Numériques :
Alain MELKA – Directeur Général des Services
+33 (0)6 33 75 13 60
alain.melka@ecoter.org

Quentin MEULLEMIESTRE – Directeur Général des Services Adjoint
+33 (0)6 04 08 38 16
quentin.meullemiestre@ecoter.org

Maquette : M.E.F.T.N

2023

CYBER MOIS

MISSION ECOTER
France et Territoires Numériques

Paroles de Territoires

Livret

Octobre 2023