



**MISSION
ECOTER**



Parlons Territoires



CYBERMOIS
Octobre 2025



Depuis près de 30 ans, Mission Ecoter 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 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 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.

Mission Ecoter partenaire

Les jeunes, cibles privilégiées des cybermenaces

À l'occasion de la 13ème édition du Cybermois, Cybermalveillance.gouv.fr révèle les résultats de son 2ème baromètre avec IPSOS et part à la rencontre des Français dans les territoires

À l'occasion du Cybermois 2025, Cybermalveillance.gouv.fr, dispositif national d'assistance et de prévention, dévoile le programme de sa 13ème édition et les résultats de son 2ème baromètre sur la perception cyber des internautes, réalisé avec IPSOS*. Si les chiffres témoignent d'une évolution sensible de leur connaissance des menaces et de leurs comportements, les plus jeunes restent toutefois en première ligne. Face à cet enjeu crucial, le Cybermois s'impose comme le moment-clé de la mobilisation collective qui s'organise dans tous les territoires pour mettre la cybersécurité à l'honneur du 1er au 31 octobre prochains.

Maturité cyber des Français : vers une meilleure connaissance des menaces et des pratiques

De manière globale, l'étude 2025 met en évidence une bonne connaissance des pratiques cyber et 58 % des répondants considèrent être suffisamment informés des risques liés à l'utilisation d'Internet. En termes d'usages, les Français affichent également une meilleure compréhension des enjeux avec des gestes élémentaires de cybersécurité qui semblent s'affirmer : 55 % déclarent utiliser des mots de passe complexes et uniques pour chaque service, 68 % faire des vérifications avant un achat en ligne.

Une jeunesse qui reste surexposée et vulnérable face aux cybermenaces

L'étude révèle un contraste marquant entre les compétences numériques perçues des 18-34 ans et leur réelle exposition aux risques. Les usages de cette population ultraconnectée en font également des cibles idéales qui semblent réagir différemment face aux malveillances : moins de recours aux institutions, davantage d'auto-prise en charge, voire d'inaction. 29 % d'entre eux ont ainsi reçu un appel d'un faux conseiller bancaire (près de 4 fois plus que les 55-75 ans) ou ont été victimes d'un piratage de compte (20 % vs 7 % des 55-75), mais seuls 17 % ont alerté leur banque ou leur fournisseur (vs 34 % des 55-75 ans).

« Si les Français semblent gagner en maturité avec des comportements plus responsables au quotidien, trop peu d'entre savent encore comment réagir. Parmi eux, certains publics particulièrement exposés sont plus vulnérables, d'où la nécessité de les sensibiliser dès le plus jeune âge, pour les protéger et instaurer les bons réflexes durablement. C'est pourquoi nous souhaitons faire de la cybersécurité une priorité et poursuivre nos actions avec, entre autres, l'Éducation nationale. Face à cet enjeu sociétal, la mobilisation collective doit être massive et s'inscrire dans le temps, bien au-delà du Cybermois » a déclaré Jérôme Notin, Directeur Général de Cybermalveillance.gouv.fr

Cybermois 2025 : une mobilisation massive d'acteurs engagés

Fort de ce constat, Cybermalveillance.gouv.fr a décidé d'intensifier la mobilisation collective afin d'encourager tous les acteurs à sensibiliser leurs publics, notamment au travers de son collectif Cybermois constitué de plus de 1 300 membres entreprises, agglomérations, conseil départementaux, préfetures ou autres collectivités, administrations ou associations sur l'ensemble du territoire.

À cette mobilisation s'ajoute l'action spécifique de partenaires toujours plus nombreux. Outre le soutien de l'action par des structures gouvernementales (ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche, ministère de la Justice, Haut Commissariat de l'Enfance, ministère des Armées, ministère de la Culture, ministère de l'Agriculture et de la Souveraineté alimentaire, ministère chargé de l'Intelligence artificielle et du numérique, Cybermalveillance.gouv.fr), une action spécifique sera développée avec l'Éducation nationale pour sensibiliser les scolaires dès le plus jeune âge.

Cette sensibilisation s'appuiera également sur une campagne d'affichage nationale pédagogique à la tonalité volontairement décalée qui détourne des faits historiques emblématiques pour illustrer les bons réflexes cyber à adopter.

La campagne sera massivement relayée notamment au travers d'un partenariat avec France Messagerie, Culture Presse ainsi que le SNDP auprès de 15 000 marchands de presse et à travers une mobilisation de toutes les maisons France services de l'hexagone.

Cybermois 2025 : à la rencontre des territoires

L'ensemble des actions sera inscrit à l'agenda du Cybermois qui recensait plus de 400 événements lors de l'édition 2024. Pour les valoriser et souligner l'action des territoires, Cybermalveillance.gouv.fr a souhaité organiser cette année un CyberTour de France en s'appuyant sur les campus territoriaux (Bretagne, Nouvelle-Aquitaine, Hauts-de France, Normandie) et sur le campus national (Campus Cyber). Ainsi, le coup d'envoi de cette 13ème édition sera donné à Rennes, qui marquera la première étape de cette tournée : conférences, ateliers, expositions... De nombreuses séquences ouvertes au public sont prévues lors de 5 rendez-vous majeurs dans les régions.

Cybermois 2025 : une nouvelle ressource pour les 9-12 ans

Enfin, le Cybermois 2025 marque le lancement du livret de sensibilisation pour les 9–12 ans « le numérique, pas de panique ! », conçu en partenariat avec Bayard, et soutenu par l'AFNIC. Diffusé dans le magazine Astrapi à plus de 70 000 abonnés, ce guide illustré aborde la sécurité en ligne à hauteur d'enfant à travers différents thèmes (naviguer sur Internet, les jeux vidéos, les réseaux sociaux), des BD, conseils et jeux. Entièrement gratuit et téléchargeable en ligne, il sera également mis à disposition pour des distributions locales ou des expositions pédagogiques dès le 25 septembre. Enfin, il sera également largement diffusé auprès des scolaires par l'Éducation nationale et distribué lors des événements dans les territoires. L'objectif : faire de la prévention un réflexe dès le plus jeune âge.

**Étude Ipsos.Digital réalisée pour Cybermalveillance.gouv.fr du 16 au 26 mai 2025 juillet sur un échantillon de 2 000 Français de 18 à 75 ans.*

À propos de Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr est la plateforme du Groupement d'Intérêt Public Action contre la cybermalveillance (GIP ACYMA). Créé en 2017, ce dispositif national a pour missions l'assistance aux victimes d'actes de cybermalveillance, la protection des organisations, la sensibilisation aux risques numériques, et l'observation de la menace sur le territoire français, qui s'illustrent notamment au travers du service d'assistance 17Cyber.

Ses 64 membres issus du secteur public, du privé et du domaine associatif contribuent à sa mission d'intérêt général pour ses 3 publics : particuliers, entreprises et collectivités. En 2024, Cybermalveillance.gouv.fr a accueilli 5,4 millions de visiteurs uniques sur son site Internet et plus de 420000 personnes ont réalisé un parcours d'assistance. www.cybermalveillance.gouv.fr

Source : Cybermalveillance.gouv.fr – Septembre 2025



**L'Avant-propos de
Alain MELKA
Directeur Général des Services
Mission Ecoter**



La Mission Ecoter partenaire

Le Cybermois, organisé chaque année au mois d'octobre à l'échelle européenne, est devenu un rendez-vous incontournable pour rappeler à chacun que le numérique, tout en étant un formidable levier d'innovation et de développement, demeure exposé à des risques croissants. La cybersécurité n'est pas seulement une affaire de spécialistes : elle concerne désormais chaque citoyen, chaque entreprise, chaque administration.

Pour les collectivités territoriales, cette réalité est d'autant plus pressante que le numérique irrigue l'ensemble des politiques publiques locales. Les communes, intercommunalités, départements et régions portent aujourd'hui des responsabilités essentielles : éducation, mobilités, santé, gestion des infrastructures, accompagnement des transitions énergétiques et écologiques. Dans chacune de ces missions, les outils numériques jouent un rôle déterminant. Mais avec cette dépendance accrue vient également une exposition renforcée aux cyberattaques, aux tentatives d'intrusion, aux risques de paralysie des services publics.

Ces dernières années, plusieurs collectivités de toutes tailles ont déjà été touchées par des attaques informatiques d'ampleur, rappelant que nul n'est à l'abri. Les conséquences peuvent être lourdes : interruption de services, perte de données, coûts financiers considérables, atteinte à la confiance des habitants. Dans un monde interconnecté, la cybersécurité est devenue une composante stratégique de la résilience territoriale.

Le Cybermois a pour vocation de sensibiliser, d'informer et de mobiliser. Il s'agit non seulement de diffuser les bonnes pratiques, mais aussi de créer une véritable culture partagée de la cybersécurité au sein des collectivités. Car la sécurité numérique ne se limite pas à la mise en place d'outils techniques : elle repose sur une gouvernance adaptée, une vigilance de tous les instants, une coopération entre élus, agents, partenaires institutionnels et entreprises spécialisées.

La Mission Ecoter, fidèle à sa vocation d'accompagnement des territoires dans leurs transitions numériques, énergétiques et sociétales, s'associe pleinement à cette démarche, depuis plusieurs années. À travers ce livret, nous voulons rappeler que la cybersécurité est une condition indispensable de la transformation digitale réussie des collectivités. Protéger les systèmes d'information, sécuriser les données des citoyens, anticiper les menaces : autant de priorités qui doivent désormais figurer au cœur des stratégies locales.

Cet avant-propos est aussi un appel. Un appel à la mobilisation de toutes et tous, à la formation continue, au partage d'expériences, à l'entraide entre collectivités. C'est en conjuguant nos efforts que nous pourrons construire un numérique de confiance, au service des habitants et des générations futures.

En ce Cybermois, sachons faire de la cybersécurité non pas une contrainte, mais un levier de confiance, de responsabilité et d'innovation.

L'Édito de
Quentin MEULLEMIESTRE
Directeur Général des Services Adjoint
Mission Ecoter



Le bouclier numérique des collectivités : une urgence vitale

Alors que notre pays s'appuie de plus en plus sur la **numérisation** pour moderniser ses services publics, les collectivités territoriales se retrouvent en première ligne d'un champ de bataille incontournable : celui de la **cybersécurité**. Souvent perçues comme des cibles moins stratégiques que les grandes entreprises ou les ministères, elles n'en sont pas moins des proies de choix pour les cybercriminels. Les chiffres récents sont alarmants : les attaques par **rançongiciel (ransomware)** contre les mairies, départements et régions se multiplient, paralysant les services, chiffrant les données des administrés et mettant à mal la continuité républicaine.

La vulnérabilité des collectivités s'explique par une convergence de facteurs techniques et organisationnels. D'abord, la **diversité et l'obsolescence des infrastructures informatiques**. Beaucoup de systèmes d'information sont hétérogènes, reposant sur des logiciels et matériels anciens, souvent non mis à jour, créant autant de **brèches** potentielles. On y trouve des serveurs sous d'anciennes versions de Windows Server, des applications métiers développées sans les meilleures pratiques de sécurité, et des réseaux internes mal segmentés, facilitant la propagation latérale des menaces.

Ensuite, la gestion des accès est un point noir. Les identifiants par défaut, le manque de politique de mots de passe forts et l'absence d'**authentification multifacteur (MFA)** sont encore monnaie courante. Ce sont autant d'invitations pour les attaquants. De plus, la surface d'attaque s'élargit avec le déploiement de l'**Internet des Objets (IoT)** dans les services urbains (éclairage intelligent, gestion des déchets, etc.), dont les équipements sont souvent mal sécurisés par défaut.

Par ailleurs, le facteur humain, quant à lui, est une porte d'entrée majeure. Le **hameçonnage (phishing)** et l'**ingénierie sociale** exploitent le manque de formation des agents sur les bonnes pratiques numériques. Un simple clic sur un lien malveillant peut compromettre un réseau entier.

Face à cette menace, il est urgent de passer d'une logique de correction des incidents à une approche de prévention et de **résilience**. L'État a mis en place des initiatives comme le programme "Cyber Malveillance" ou les aides de l'**ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)**, mais elles ne suffisent pas toujours à combler le retard.

Ainsi, les collectivités doivent considérer la cybersécurité comme un **investissement stratégique** et non comme une simple dépense. Cela passe par plusieurs chantiers prioritaires :

- **Réaliser un audit de sécurité complet** de l'infrastructure pour identifier et corriger les vulnérabilités les plus critiques.
- **Mettre en place une politique de mise à jour (patch management)** rigoureuse pour tous les logiciels et systèmes d'exploitation.



- **Segmenter les réseaux** afin de contenir la propagation des attaques. Un système d'information de collectivité est un écosystème. Il est impensable qu'un dysfonctionnement d'un point ait un impact direct sur la totalité du système.
- **Renforcer l'authentification** en généralisant le MFA, même pour l'accès aux services les plus basiques.
- **Former et sensibiliser** en continu l'ensemble du personnel, du secrétariat aux élus, aux risques cyber.
- **Établir un plan de continuité d'activité (PCA)** et un plan de reprise après sinistre (PRA) pour garantir la résilience des services en cas d'attaque.

Enfin, la cybersécurité est aujourd'hui une question de **souveraineté numérique** et de **confiance citoyenne**. En protégeant leurs systèmes, les collectivités ne se protègent pas seulement elles-mêmes, mais garantissent aussi la sécurité des données de leurs administrés et la continuité des services essentiels. Le temps de l'action est maintenant !

Devenez
#CyberEngagés

Inscrivez-vous

pour (re)découvrir
l'Histoire
le 1er octobre !

cybermois.gouv.fr

CYBER
MOIS

Denis THURIOT

Président de la Mission Ecoter
Maire de Nevers et Président de
l'Agglomération

Mickael AUDEGOND

Maire de Wailly

Fatima EL OUASDI

Adjointe au Maire déléguée au
Numérique et aux
Télécommunications de Rueil-
Malmaison

Serge ROCCHI

Conseiller Municipal chargé des
Nouvelles Technologies de
Rueil-Malmaison

Éric BERLIVET

Maire de Roche la Molière

Nicolas BARD

DSI Externe de la Mairie de
Roche-La-Molière

Communauté

d'agglomération Paris-
Saclay

Tony FLAHAUT

Directeur | Direction Mutualisée
du Numérique Communauté
d'Agglomération du Pays de
Saint -Omer

Lionel MONTILLAUD

Directeur | Direction Mutualisée
du Numérique Communauté
d'Agglomération du Pays de
Saint -Omer

Magali NOEGELIN

DPO et Responsable
Cybersécurité du Pays de
Montbéliard Agglomération

Nathalie POIGNON

Responsable du service
Communication de la Ville de
Marseillan

WALLIX

Devenez
#CyberEngagés

Inscrivez-vous



pour (re)découvrir
l'Histoire
le 1er octobre !

cybermois.gouv.fr



CYBER
MOIS

Devenez
#CyberEngagés

Inscrivez-vous



pour (re)découvrir
l'Histoire
le 1er octobre !

cybermois.gouv.fr



CYBER
MOIS

Denis THURIOT
Président de la Mission Ecoter
Maire de Nevers et Président de
l'Agglomération



L'IA dans les collectivités : priorité à la vigilance et à l'éthique

L'Intelligence Artificielle est en constante évolution depuis les années 1950 ; son adoption est aujourd'hui extrêmement rapide et elle influence désormais tous les secteurs, privés comme publics. Dans le secteur public, la défiance est encore présente car l'IA demeure mal connue et mal comprise. En outre, beaucoup de collectivités font face à l'insuffisance de moyens techniques, juridiques et humains pour déployer l'IA de manière sereine et maîtrisée. Pour pouvoir saisir pleinement les opportunités offertes par l'IA, notamment en termes d'amélioration de la productivité et d'efficacité des services publics, nos collectivités devraient être en mesure d'évaluer les risques particuliers (liés au rôle central des données qui pose des questions de confidentialité et d'intégrité) et connexes (liés à la cybersécurité). Elles devraient également, au préalable, penser leur stratégie de déploiement, d'utilisation, de contrôle et de protection, qui passe aussi par une réflexion sur la nécessaire « transparence » de l'IA.

En matière d'utilisation de l'IA, le risque cyber constitue un frein dans la réflexion des élus locaux. La question essentielle de la sécurisation des données personnelles et des données de la collectivité se pose bien évidemment, d'autant plus que la continuité du service public peut être fragilisée voire rompue. Les risques s'intensifient alors même que leur prise de conscience de la part des élus reste insuffisante faute de temps, de budget dédié, de compétences et de ressources humaines qualifiées. Fort heureusement, associations d'élus, organismes et institutions, à l'image de la Mission Ecoter, jouent un rôle significatif dans la cyber-protection des collectivités locales notamment en termes de sensibilisation, de partage des bonnes pratiques et d'accompagnement. L'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information, s'est également déployée progressivement dans les territoires pour accompagner plus largement l'ensemble des collectivités.

Au-delà des risques et de leurs conséquences, un aspect est trop souvent négligé : le régime de responsabilité dans le cadre du recours à l'IA. Peuvent ainsi voir leur responsabilité engagée, les collectivités en tant que personnes morales (si la collectivité a manqué à ses obligations, ou pour *faute de service* commise par l'un de ses agents), les élus et les agents publics (pour *faute personnelle*, imprudence, négligence, malveillance...). Il faut en être conscient sans toutefois se retrouver paralysé par la peur de la sanction et refuser toute utilisation de l'IA, car le lien entre la faute de service et le mauvais usage de l'IA reste toutefois à établir, et le régime de responsabilité doit être précisé par la jurisprudence.

Cette potentielle responsabilité doit surtout nous faire réfléchir aux précautions à prendre. La Commission nationale de l'informatique et des libertés a un rôle de conseil et d'accompagnement dans le déploiement de systèmes numériques et d'IA et suggère de combiner une analyse de sécurité classique avec une analyse des risques spécifiques. Nous pouvons aussi nous appuyer à la fois sur le Règlement Général sur la Protection des Données, qui a l'avantage d'avoir déjà bien implanté une culture de la protection des données, et le référentiel général de sécurité (RGS) qui a pour objectif de renforcer la confiance des usagers dans les téléservices. Depuis peu, les collectivités bénéficient aussi des recommandations prévues par le Règlement européen sur l'IA (RIA ou AI Act) qui s'applique aussi aux collectivités.

Il impose certaines obligations pour assurer la sécurité des systèmes mais il offre aussi les clés pour les sécuriser. Ce règlement européen représente surtout un véritable changement de paradigme en nous obligeant à nous mettre en conformité, une démarche assez nouvelle en France. Cette approche par la conformité pourrait même répondre au dilemme juridique concernant la responsabilité administrative, civile et pénale : le respect de l'obligation de conformité devenant le critère pour juger de l'engagement de la responsabilité d'une collectivité, de ses élus ou de ses agents. D'où l'enjeu de la formation des agents et des élus, car pour bien se conformer, il faut pouvoir se former. Il est important de consacrer du temps à l'information, à l'échelle intercommunale idéalement, et, pourquoi pas (c'est notre réflexion dans l'Agglomération de Nevers) de créer un poste mutualisé Cybersécurité et Intelligence Artificielle. Prendre le temps d'identifier les services adéquats où déployer les outils qui mettent en œuvre l'IA permet en outre un déploiement précis, sécurisé intelligible et progressif.

Dans ce développement vigilant de l'IA, l'angle éthique devrait être une préoccupation première, un pré-requis à la conception de chaque projet intégrant l'IA. D'une part, en raison de la défiance exprimée par nos concitoyens et, d'autre part, au vu du risque de détournement de l'IA (images et vidéos truquées par exemple). Les collectivités acheteuses de produits IA se trouvent parfois démunies face à des *entreprises qui sont les seules à savoir ce qui se trouve dans le code*. Nous devrions pouvoir exiger une logique d'« explicabilité », c'est-à-dire la capacité d'un système d'IA à expliquer de manière claire et compréhensible ses actions.

L'échelle de la collectivité territoriale apparaît comme un niveau approprié de réflexion sur la dimension éthique. A condition, là encore, d'organiser des formations et des actions de prévention à destination des agents sur les risques de l'utilisation des outils. Des chartes éthiques peuvent même être élaborées pour fixer les principes, les valeurs et les normes auquel tout projet d'IA doit se conformer : transparence, qualité des données, sécurité des systèmes d'information, gouvernance, implication des citoyens, etc. Les élus et les agents doivent pouvoir rester maîtres de la technologie, pouvoir la contrôler et en signaler les dysfonctionnements. Vigilance et éthique semblent donc bien être les ingrédients nécessaires à un développement en confiance de l'IA et, surtout, accepté par nos concitoyens. Elle doit rester un outil, et non pas un substitut de la plus-value humaine.

The logo for 'CYBER MOIS' features a stylized 'S' shape on the left, composed of a blue top half and a green bottom half. To the right of this symbol, the words 'CYBER' and 'MOIS' are stacked vertically in a bold, dark blue, sans-serif font.A promotional graphic for Cyber Mois with a dark teal background. At the top, the text 'Devenez #CyberEngagés' is displayed in white and green. Below this, 'Inscrivez-vous' is written in large, light blue letters. To the right, a woman in 18th-century attire is shown holding a smartphone. Further right, the text 'pour (re)découvrir l'Histoire le 1er octobre !' is written in white. At the bottom, there is a white search bar containing the URL 'cybermois.gouv.fr' and a magnifying glass icon. The 'CYBER MOIS' logo is positioned at the bottom center.

Devenez
#CyberEngagés

Inscrivez-vous

pour (re)découvrir
l'Histoire
le 1er octobre !

cybermois.gouv.fr

CYBER
MOIS



Mickael AUDEGOND
Maire de Wailly



Cyber sécurité et collectivités : Et si on défrichait le terrain avant même de s'armer pour éteindre le feu ?

Le sujet est désormais partagé, la question de la cybersécurité est un viatique indispensable en amont de toute réflexion autour du numérique. Que ce soit pour les systèmes d'informations, pour les systèmes d'intelligence artificielle et pour tous les projets qui déploient de l'IoT sur les territoires. La réflexion sur la sécurité est un préalable indispensable sans lequel tout projet crée ou créera des failles de sécurité qui permettront à des assaillants d'infiltrer nos systèmes.

Les chiffres sont éloquentes, la dernière étude de cybermalveillance.gouv.fr le confirme. Une collectivité sur 10 a été victime d'attaques dans les 12 derniers mois. L'ANSSI nous apprend aussi que 14 % des incidents traités par l'agence sont des incidents qui concernent des collectivités territoriales. Et dans le principe de cette pêche au chalut adopté par le cybercrime la petite taille des collectivités n'est pas une protection contre la menace. Alors que dans le même temps, elles sous-estiment leur exposition, tout comme elles manquent de moyens mais aussi de compétences spécialisées.

La culture du risque indispensable à cette situation chemine néanmoins dans les têtes de beaucoup ce qui se concrétise par la mise en place de réelles gouvernances CYBER par de nombreux exécutifs.

Une prise de conscience s'est engagée afin de pouvoir répondre à la course lancée par les dernières technologies, je pense en particulier aux intelligences artificielles génératives qui vont déployer des périmètres et des axes d'attaque beaucoup plus nombreux et beaucoup plus puissants.

Face à ce crime désormais organisé au niveau mondial et prenant ma casquette de maire d'une commune de 1100 habitants, on ne peut pas non plus sous-estimer les freins observés encore en 2025.

Le premier est que les petites communes sous-estiment leur vulnérabilité. Plus de 40% s'estiment faiblement exposées, trop d'entre elles n'engagent même pas ce sujet dans les débats...

Les budgets restent trop limités, quelques milliers d'euros sont consacrés à la cybersécurité annuellement alors que les communes souhaitent de plus en plus avoir des capteurs, mettre en place des systèmes d'intelligence artificielle en oubliant ce fondamental de la sécurité.

Le dernier frein demeure un manque cruel de compétences et de sensibilisation qui voit par exemple encore trop souvent des élus ou des agents ne pas rendre étanche leur usage du numérique entre ce qui concerne la collectivité et ce qui concerne leur vie privée

Se former et s'outiller pour parer une attaque, installer des systèmes résilients de protection sont des indispensables pour contre attaquer et se préparer au pire.

N'y a-t-il pas des périmètres de l'anticipation qui restent en friches ?

La clé de lecture proposée dans cet article ne concerne pas directement cette course à la contre-offensive mais plus à la connaissance de ce qui est ciblé par les hackers du monde entier.

Dans une attaque les principales conséquences sont les interruptions de service, des atteintes à la réputation, des pertes financières et aussi pour quasiment 1/4 des cas le vol ou la destruction de données. Et revoilà la question de la DATA qui se pose.

Et si en même temps que nous nous équipions de pare-feu et de systèmes résilients, un travail en amont était mené sur la création d'une cartographie de la donnée avant qu'elle ne soit volée.

Quelle collectivité sait exactement quelles données elle a en sa possession, quelles données elle offre à l'Open data, quel sont les lieux de leur stockage, le traitement de leur archivage, la question de leur destruction

Pourtant, ces données sont devenues un élément essentiel du patrimoine des collectivités tout comme un bâtiment, tout comme une route, tout comme un éclairage public ou un espace naturel protégé.

Ce n'est pas parce qu'il ne se voit pas que ce patrimoine ne doit pas être analysé et connu. Et pourtant, il est encore souvent inconnu, négligé voire totalement ignoré.

La cartographie des données, processus qui consiste à recenser, localiser, classer les données selon leur criticité, leur sensibilité, leur usage et leur accès présente plusieurs atouts pour toutes les collectivités territoriales

Le premier concerne l'identification des actifs critiques.

Elle permet de savoir quelles données sont réellement sensibles. Quelles sont les données personnelles de ses agents ou de ses administrés en sa possession. Quelles sont les données stratégiques pour la fiscalité et son budget, le développement économique ou l'urbanisme. Le travail sur la criticité en amont d'une attaque permet de prioriser les mesures de sécurité.

Un autre atout de cette démarche est la détection des vulnérabilités dans les flux.

Qui est capable aujourd'hui de reconstituer un parcours de données (celui qui accède, quand il peut le faire, comment il peut y accéder, à partir de quel support, ...)

Et pourtant, cela permet de repérer les points faibles concernant les accès restreints, les questions de stockages dans le chiffrement et la question des sauvegardes. Elle peut permettre aussi d'identifier l'utilisation de logiciels métiers mal ou pas mis à jour tout comme la question des accès à distance qui mettent à mal la sécurité d'une collectivité sans que personne n'en prenne vraiment conscience.

Atout dans un aspect opérationnel, si jamais la catastrophe arrive, cette cartographie permet aussi la réduction drastique du temps de réaction.

En cas d'incendie dans un bâtiment, vous m'avouez qu'il est plus simple de savoir gérer la crise si on a connaissance du mobilier ou des documents qui se trouvent dans ce bâtiment ou plus grave de savoir combien de personnes sont présentes ? Cela revient à poser la question de qu'est-ce qui doit être sauvé en priorité ? Qu'est-ce qui doit être préservé en priorité ?

Et bien c'est exactement la même chose pour le numérique et il faut se poser les mêmes questions.

En cas de cyberattaque connaître l'emplacement, la nature, le propriétaire des données, permet d'évaluer l'impact de l'incident très rapidement. Cela permet aussi de rendre étanche plus facilement des systèmes concernés ou ceux avec des données plus sensibles. Il permet enfin d'informer les agents les structures partenaires qui devront elles aussi réagir de manière efficace.

Pour prendre une dimension plus juridique, cette démarche permet aussi de répondre plus rapidement et plus efficacement à la mise en place de la réglementation RGPD. Dans ce cadre réglementaire les collectivités doivent démontrer qu'elles ont pris des mesures proportionnées. Pour protéger les données en fonction de leur criticité la cartographie est donc un élément indispensable et devient un levier essentiel pour bien appliquer ce texte.

De plus, pas besoin d'être une métropole pour s'engager dans cette démarche. Cette procédure est adaptée pour toutes les collectivités y compris les plus petites. Un simple tableur permet avec quelques critères (sensibilité, accès, sauvegarde, fréquence de mise à jour, ...) d'avoir une vision assez claire des données propriété de la collectivité.

Dernier élément de réflexion qui est horizontal au sujet, cet outil renforce la culture de la sécurité.

En effet, ce processus implique tous les acteurs, élus, agents, services informatiques, DPO, prestataires partenaires externes, ... Il sensibilise d'une part à la sécurité mais aussi à la question de la DATA trop souvent oubliée dans nos politiques publiques.

Elle permet de structurer une gouvernance autour de la sécurité informatique et numérique sur les rôles et les responsabilités de chacun. Elle outille les collectivités dans une meilleure connaissance de leur propre fonctionnement.

Entrer dans cette démarche est aussi une manière de démontrer que la gestion de la cybercriminalité n'est plus et ne doit plus être juste une question technique, juste une question d'experts, juste une question de RSI.

Elle doit devenir une question politique et les exécutifs dans les prochains mandats devront s'en emparer pour mettre ce sujet au cœur de leur réflexion et pour porter une gouvernance résiliente si nous voulons assurer une vraie transition numérique rassurante et de confiance pour nos concitoyens.

Il est d'ailleurs assez surprenant que dans ce domaine, les collectivités ont souvent tendance à tendre vers l'excellence et désirer un dispositif parfait (très complexe à imposer ou à mettre en place) et finalement finissent trop souvent pour de multiples raisons (loin de moi l'idée de juger ou de critiquer) par ne rien faire ou ne pas faire grand-chose.

Comme tous les autres sujets qui concernent la cybersécurité, le plus important est de ne pas rester immobile mais d'améliorer et acculturer en fonction de ses capacités.

Si je voulais reprendre une analogie avec la sécurité incendie, mettre en place des équipements de sécurité de haut niveau revient à acheter des véhicules dernier cri doté de toute la technologie pour lutter contre le feu. Cartographier sa donnée et savoir ce qui peut être la cible du cybercrime est un défrichage indispensable pour limiter l'incendie. Il permettra même très certainement de mettre en place des parades ou de nouvelles réponses.

Bien évidemment, cette mise en place a un coût initial en temps et en ressources. Elle doit être réalisée de manière complète car une cartographie mal tenue va donner un faux sentiment de sécurité. Elle entraîne aussi des conséquences indirectes (néanmoins fortes utiles) comme celle de se poser la question sur les données anciennes inutilisées ou sur les anciens accès de collaborateurs partis en retraite ou dans d'autres structures. Autant de microsujets qui sont autant de failles et de vulnérabilités.

Ne tombons pas sous le charme de la solution unique solution à tous les problèmes. Mettre en place une cartographie de ses données est un outil et seulement un outil.

L'humain restant central, rien ne remplacera pas la sensibilisation, la formation et la rigueur dans les usages des outils numériques.

Je prends conscience en rédigeant ce texte qu'il faudra prolonger cette réflexion en apportant des propositions concrètes pour les communes de ce sujet. Cet article à la modeste ambition de poser ce débat dans le débat politique pour un début de prise de conscience et pour changer réellement nos pratiques ;

Vous savez tout comme moi que l'anticipation, d'une cyberattaque est la première étape d'une bonne gestion de celle-ci. La cartographie de vos données devient quasiment une démarche indispensable de cette prévention.

Elle travaille sur la gestion du risque, priorise les mesures, renforce les préparations et limite les conséquences et d'exposition en cas d'attaque.

Cette démarche est applicable par les grandes collectivités comme par les petites. Un simple travail d'inventaire de classification de mesures de protection et de plan de réponse est déjà une grande étape dans la gestion du cyber risque pour une petite collectivité.

Protéger ses données en apprenant à les connaître et les maîtriser, c'est aussi protéger ses administrés et le bon fonctionnement de nos services publics indispensables à nos habitants. C'est indispensable dès maintenant.

Éric BERLIVET
Maire de Roche la Molière
Nicolas BARD
DSI Externe de la Mairie de Roche-La-Molière



Cybersécurité et Territoires : une responsabilité partagée au service du citoyen

La cybersécurité n'est plus seulement une affaire d'État ou de grandes entreprises. Chaque collectivité territoriale, quelle que soit sa taille, est désormais en première ligne.

À Roche-la-Molière comme dans toute collectivité, nos systèmes d'information soutiennent des services essentiels : état civil, restauration scolaire, équipements publics, associations... Autant de briques qui font battre le cœur de la vie locale.

1. Une menace bien réelle, même pour les petites communes

Contrairement aux idées reçues, les cyberattaques ne ciblent pas uniquement les grandes métropoles. Les petites et moyennes collectivités sont des cibles idéales : elles gèrent des données sensibles, mais disposent de moyens plus limités.

- **1 collectivité locale sur 10** déclare avoir été victime d'une cyberattaque au cours des 12 derniers mois ([Tyrex Cyber](#)).
- En 2023, **24 % des victimes de ransomware en France étaient des collectivités territoriales** ([CERT-FR](#)).
- L'ANSSI a géré **plus de 4 300 incidents en 2024**, soit une hausse de 15 % par rapport à 2023, dont **1 361 attaques confirmées** et **144 cas de ransomware** ([C-Risk](#)).

Les conséquences sont lourdes : interruption de services publics, pertes financières, et surtout perte de confiance des citoyens.

2. Construire une cybersécurité du quotidien

À Roche-la-Molière, nous avons choisi une approche pragmatique, fondée sur trois piliers :

- **Prévenir** : former nos agents aux bons réflexes (mots de passe robustes, vigilance face aux mails suspects, mises à jour régulières).
- **Protéger** : sécuriser les postes et serveurs, cloisonner les accès, mettre en place la double authentification.
- **Réagir** : disposer de sauvegardes fiables et de procédures de continuité pour limiter l'impact en cas d'attaque.

3. La force du collectif : Loire et Métropole

La cybersécurité est un défi trop vaste pour être relevé seul. C'est pourquoi nous nous appuyons sur une dynamique de coopération :

- Avec le **Département de la Loire**, nous bénéficions de campagnes de **tests de phishing** et d'expérimentations partagées, afin de sensibiliser efficacement nos agents.
- Avec la **DSI de Saint-Étienne Métropole**, nous trouvons un accompagnement précieux : conseils, mutualisation des moyens et partage de bonnes pratiques.

Cette logique de réseau illustre une conviction forte : c'est en mutualisant nos forces locales que nous augmentons la résilience numérique de tout un territoire.

4. La cybersécurité, une culture humaine avant tout

La technologie ne suffit pas. La cybersécurité est avant tout une affaire d'humains. À Roche-la-Molière, chaque agent est considéré comme un **maillon essentiel** de la chaîne de protection : ateliers de sensibilisation, exercices pratiques, réflexes répétés.

Former, expliquer, répéter : c'est la clé pour bâtir une vraie culture de vigilance.

Conclusion

La cybersécurité est désormais une condition de la continuité du service public. En combinant **formation des agents**, **sécurisation technique** et **coopération territoriale**, nous protégeons non seulement nos systèmes, mais surtout la confiance de nos habitants.

C'est collectivement, entre communes, départements et métropoles, que nous construirons des territoires numériques plus sûrs et plus résilients.





Communauté d'agglomération Paris-Saclay

**PARIS
SACLAY**
Communauté d'agglomération

**CYBER
MOIS**

La souveraineté numérique, un enjeu stratégique

Un territoire d'excellence et de responsabilité

Avec ses 27 communes, 320 000 habitants, et un écosystème unique regroupant 20 % de la recherche académique française et 15 % de la R&D nationale, Paris-Saclay porte une ambition forte : faire du numérique un levier de transformation territoriale, tout en garantissant la maîtrise de ses données et infrastructures.

L'enjeu est comment faire du numérique et de l'innovation, en s'appuyant sur les atouts et les richesses de notre territoire.

La souveraineté numérique, un enjeu stratégique

Face aux enjeux posés par le numérique, l'agglomération Paris-Saclay s'engage dans une démarche affirmée pour garantir un usage maîtrisé du numérique.

Il s'agit notamment de

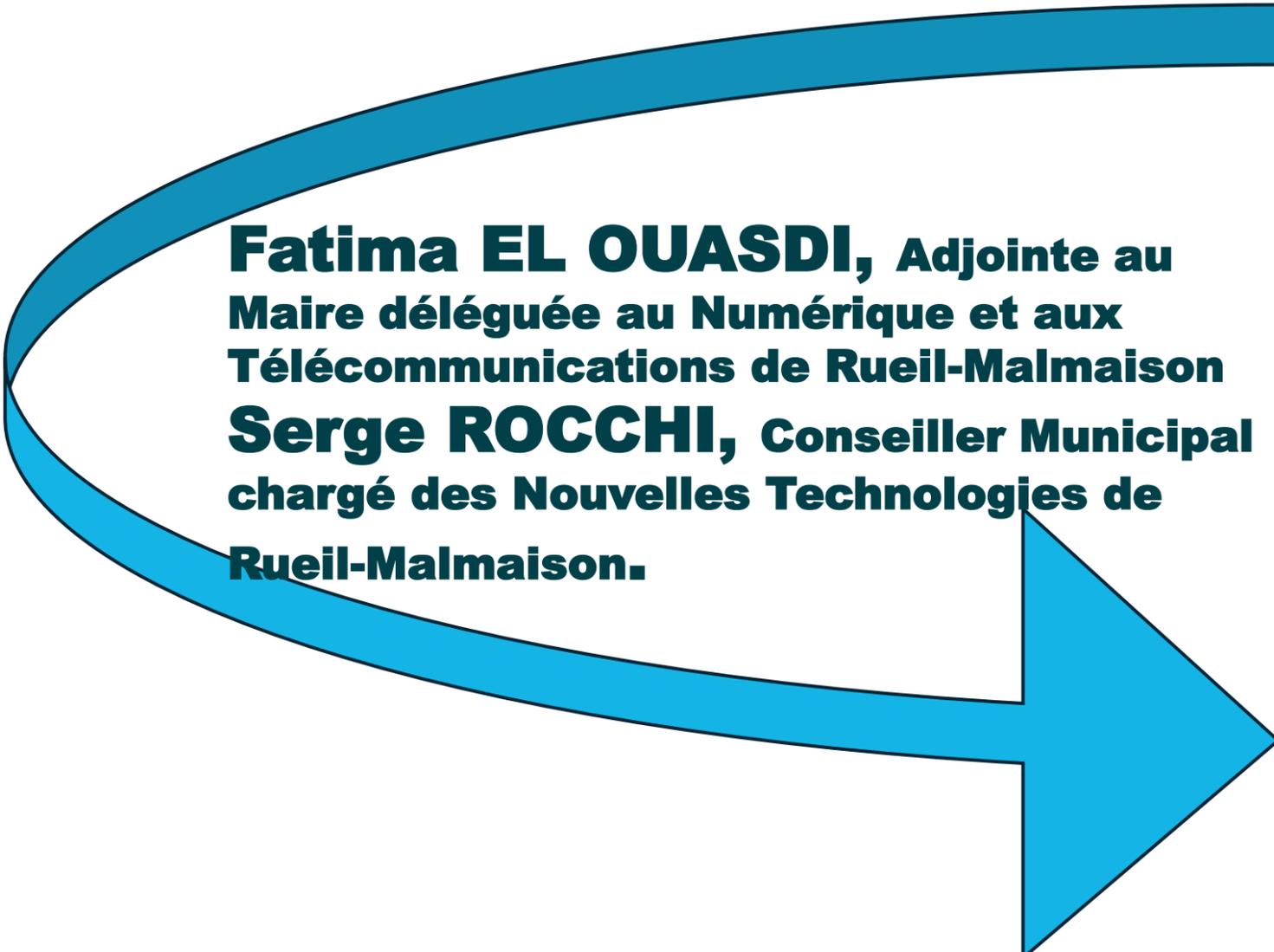
- Maîtriser les données territoriales : en les collectant, structurant et valorisant localement.
- Sécuriser les infrastructures : en s'appuyant sur des solutions cloud souveraines hébergées en France.
- Privilégier des outils conformes au RGPD et non soumis au Cloud Act.
- Renforcer la résilience numérique : face aux cybermenaces croissantes, avec l'appui de l'ANSSI et des dispositifs comme le WAAP souverain
- S'assurer des usages de l'IA : L'intelligence artificielle ouvre de nouvelles perspectives pour l'urbanisme et la gestion des territoires, tout en soulevant des enjeux éthiques cruciaux.

La qualité et la souveraineté des données, ainsi que la transparence des algorithmes, sont essentielles pour garantir la fiabilité et la légitimité des outils d'IA dans le secteur public.

La souveraineté numérique ne se limite pas à la technologie : elle implique l'accompagnement et la formation des citoyens, des agents et la mobilisation des acteurs locaux.

La formation des agents au numérique et aux technologies d'IA est un investissement stratégique pour moderniser l'administration, développer les compétences nécessaires et accroître sa performance comme son attractivité. Cette montée en compétences est cruciale pour exploiter le potentiel du numérique tout en respectant le cadre éthique et réglementaire. Ainsi le règlement intérieur a été amendé pour prendre en compte les enjeux de sécurité numérique et d'usage de l'IA

La vulgarisation de l'IA auprès du grand public renforce l'engagement citoyen en rendant les informations politiques et les processus décisionnels plus accessibles. Elle facilite la participation citoyenne aux débats, enrichissant ainsi la réflexion collective sur l'avenir de nos territoires, comme cela a été fait lors des concertations territoriales de l'IA



Fatima EL OUASDI, Adjointe au Maire déléguée au Numérique et aux Télécommunications de Rueil-Malmaison
Serge ROCCHI, Conseiller Municipal chargé des Nouvelles Technologies de Rueil-Malmaison.



**CYBER
MOIS**

Cybersécurité : une priorité politique pour les communes et une opportunité de combiner des dispositifs pour se protéger

La cybersécurité est désormais au cœur des priorités des territoires, car elle conditionne la continuité des services publics essentiels comme l'état civil, l'éducation et la vie scolaire et la sécurité. La cybersécurité n'est plus seulement technique : elle est devenue stratégique et politique, car elle touche aux données des administrés.

Pourtant, de nombreuses collectivités, notamment les petites communes, manquent de moyens humains et financiers, rendant la mutualisation et les dispositifs de soutien de l'État indispensables. Le facteur humain demeurant la première vulnérabilité, les élus et agents sont les cibles privilégiées. Par ailleurs, les systèmes informatiques, matériels et logiciels, parfois obsolètes, nécessitent a minima des mises à jour régulières, voire une modernisation pour réduire les risques.

Face à ces dangers, les obligations réglementaires (RGPD, directive NIS2, loi de programmation militaire) accentuent la pression juridique et la responsabilité des collectivités en cas de manquement.

Selon leur taille, leur poids économique et politique, les territoires ne partent pas tous avec les mêmes cartes en main. Les plus petites communes manquent souvent de personnel et de budget pour renforcer leurs défenses alors que les menaces deviennent toujours plus sophistiquées. Les élus comme les agents peuvent se sentir esseulés, voire abandonnés.

Aussi, la coopération entre communes, intercommunalités, départements, régions et métropoles, ainsi qu'avec les services de l'État (*préfectures, ANSSI, Cybermalveillance.gouv.fr, la CNIL*) et les associations de collectivités (*AMF, AMIF, Mission ECOTER, Association Villes Internet, syndicats...*) est devenue indispensable.

Au regard de ces enjeux, et pour compléter toutes les actions relatives aux systèmes d'information déjà entreprises, la ville de Rueil-Malmaison a décidé d'inclure le risque cyber dans le plan communal de sauvegarde (PCS), pour permettre à chaque direction de disposer d'un plan de continuité d'activité en cas d'attaque.

Enfin, nous avons bénéficié de l'aide de l'ANSSI pour mettre en œuvre un exercice de gestion de crise cyber afin de tester l'ensemble de notre organisation en situation d'attaque. Ce parcours a été possible grâce à la mise en œuvre de plusieurs dispositifs parmi tous ceux listés ci-après (liste non exhaustive).

Cybersécurité : des leviers disponibles quelle que soit la taille de la collectivité

1) Financements & cadres nationaux

Rueil Malmaison a pu bénéficier du Plan France Relance – volet cybersécurité (ANSSI). Le plan a consacré 176 M€ à la cybersécurité publique, dont 100 M€ pour les Parcours de cybersécurité pilotés par l'ANSSI. L'objectif était clair : réaliser des diagnostics, mettre en place une mise à niveau priorisée et proposer des accompagnements concrets pour les collectivités, en particulier les petites et moyennes. Le bilan 2025 est significatif puisque 75 % des bénéficiaires sont des collectivités. La démarche passait par un contact avec le référent régional (*préfecture ou Région*) et/ou avec le CSIRT territorial, puis par une candidature aux vagues régionales correspondant à des lots de prestations prédéfinies. Les avantages étaient multiples : un cofinancement fort, un cadrage assuré par l'ANSSI, des livrables standardisés et un accès facilité à l'écosystème régional. En contrepartie, les collectivités s'engageaient sur un plan d'actions priorisé et devaient partager les résultats du diagnostic avec leurs partenaires publics (*Cyber Sécurité+, Banque des Territoires*).

Pour cadrer **la gouvernance et la conformité**, plusieurs références sont disponibles. Le guide de l'ANSSI intitulé "*Sécurité numérique des collectivités territoriales – l'essentiel de la réglementation*" et ses infographies, ainsi que le guide Cybermalveillance.gouv.fr et CNIL, détaillent les obligations et les responsabilités des collectivités, notamment en matière de protection, de continuité et d'information. Ces documents constituent une aide précieuse lors de l'élaboration d'une PSSI et dans la préparation des budgets (Cybermalveillance.gouv.fr).

Les CSIRT territoriaux (*Computer Security Incident Response Team*), créés dans le cadre de France Relance, jouent un rôle essentiel. Ces équipes régionales assistent les communes et EPCI en apportant un conseil de premier niveau, une orientation vers des prestataires qualifiés et une réponse aux incidents. Ces centres de réponse aux incidents cyber représentent une porte d'entrée opérationnelle pour les collectivités dépourvues de RSSI interne (cert.ssi.gouv.fr).

Le dispositif **MonAideCyber**, porté par l'ANSSI, propose un accompagnement progressif qui permet d'avancer pas à pas dans la sécurisation de son système d'information grâce à des diagnostics simples et des recommandations concrètes, déployées avec le soutien des CCI.

Enfin, **la sensibilisation et la formation des agents** reposent sur des outils gratuits et accessibles. La plateforme PIX Cybersécurité permet d'évaluer et de renforcer les compétences numériques, tandis que la SecNumAcadémie, le MOOC officiel de l'ANSSI, offre un contenu complet et structuré pour acquérir une véritable culture en cybersécurité. Ces démarches viennent compléter les supports déjà bien connus de Cybermalveillance.gouv.fr.

2) Solutions "métropolitaines" & territoriales

La Métropole du Grand Paris (MGP), en partenariat avec le Campus Cyber, propose un programme gratuit d'accompagnement destiné aux 130 communes de son territoire. Ce dispositif comprend des évaluations, des ateliers et des actions d'acculturation, ainsi qu'un appui à la continuité de service, avec la force de frappe du Campus Cyber. L'approche est concrète puisqu'elle permet de passer du diagnostic plan d'actions, tout en faisant progresser la maturité des collectivités sans alourdir leurs budgets (*Campus Cyber, Métropole du Grand Paris*). À ce titre, Rueil-Malmaison a pu bénéficier d'un cofinancement de la MGP pour réaliser son étude PCS cyber.

L'EPT Paris Ouest La Défense) (*POLD* a mutualisé un RSSI commun pour 11 communes, dont Rueil-Malmaison. Le *POLD* organise également l'initiative CyberÉco et s'appuie sur les ressources du Campus Cyber. Le retour d'expérience met en lumière les bénéfices d'une telle mutualisation : outillage partagé, sensibilisation conjointe des élus et agents, et expérimentations innovantes telles qu'un bug bounty territorial (*Paris Ouest La Défense*).

Enfin, la Région Île-de-France a déployé la plateforme Urgence Cyber Île-de-France, afin d'apporter un soutien direct aux collectivités et associations franciliennes face aux menaces. Cette plateforme s'appuie sur un numéro vert (0800 730 647) offrant orientation, premiers secours numériques et assistance en cas d'incident. Elle constitue une véritable "porte d'entrée" locale pour l'organisation de la réponse à incident et l'utilisation de fiches réflexes (Urgence Cyber Île-de-France).

3) Ressources nationales "prêtes à l'emploi"

Cybermalveillance.gouv.fr (*ACYMA*) met à disposition des kits de sensibilisation prêts à diffuser, ainsi que des programmes pour les élus et agents en trois étapes. Une liste complète de ressources comprend des affiches, des vidéos, des fiches ainsi qu'un guide pour les collectivités (cadre juridique, responsabilités, plan d'action). Ces contenus couvrent 80 % des besoins d'acculturation et de communication interne.

Les guides opérationnels de l'ANSSI complètent ce dispositif. Au-delà du cadrage réglementaire, le document "42 mesures pour un SI sain" propose un socle technique (*MFA, sauvegardes hors ligne, cloisonnement, supervision, PRA/PCA*) à utiliser comme check-list dans les chantiers MCO/MCS. L'InterCERT France met également à disposition des fiches réflexes claires et pragmatiques, utiles en cas de *phishing, ransomware* ou compromission de comptes, permettant d'adopter immédiatement les bons gestes, d'alerter les bons acteurs et de limiter l'impact d'un incident.

4) Rôle des départements & préfectures

Les préfectures et les SGAR (*Secrétariat Général aux Affaires Régionales*) sont les relais des dispositifs France Relance et de la doctrine ANSSI (guides, notes aux maires, sessions de sensibilisation). Elles renvoient vers les CSIRT et coordonnent la diffusion des appels et guides. À titre d'exemple, la préfecture des Hauts-de-Seine (92) a animé un événement cyber pour sensibiliser et partager des bonnes pratiques. Le département des Bouches-du-Rhône (13) a, de son côté, développé un kit de réaction à un incident cyber.

Les conseils départementaux, selon les territoires, peuvent également être sollicités : cellules d'appui numérique, marchés cadres (*socles techniques partagés*), relais vers l'écosystème régional (*CSIRT, gendarmerie, 17Cyber*).

5) Tissu privé & Campus Cyber

Le Campus Cyber (*et son programme CYBIAH*) agrège éditeurs, intégrateurs, blue teams, red teams (*nota: l'équipe blue team est chargée de défendre les systèmes et réseaux; l'équipe red team simule des attaques pour identifier des vulnérabilités et renforcer la résilience en testant les défenses d'une organisation*), cabinets de conseil et écoles. Pour une commune, c'est une place de marché qualifiée permettant de cadrer un diagnostic (*audit ciblé, EBIOS-RM, trajectoire 12-18 mois*), de sourcer des prestataires de réponse à incident et SOC/EDR compatibles avec les contraintes publiques, d'expérimenter des exercices de crise et campagnes de sensibilisation "clé en main" ou encore de mutualiser des retours d'expérience d'autres collectivités (*MGP, POLD*) et PME locales du territoire. Rueil-Malmaison est contributrice dans ce cadre, en partageant ses bonnes pratiques et retours d'expérience.

(*nota: le SOC Security Operations Center est un centre de supervision piloté par des analystes en Cybersécurité; il interprète les alertes remontées par 'EDR; l'EDR Endpoint Detection and Response protège tous les terminaux. Il repose sur l'intelligence artificielle pour analyser tes comportements suspects et détecter les attaques en temps réel en s'appuyant sur des signaux faibles, l'apprentissage automatique et l'analyse comportementale*)

Des analyses privées (ex. La société de Cybersécurité Almond) documentent par ailleurs la résilience territoriale et les mécanismes de financement (croisement subventions + budgets locaux + aides à l'innovation), avec des cas réels et des plans de remédiation post-incident pour des communes.

6) Focus associatif & cohésion-solidarités

La cybersécurité n'est pas qu'un sujet de systèmes d'informations, c'est aussi un levier de cohésion. Les outils Cybermalveillance.gouv.fr sont pensés également pour les associations locales (culture, sport, social) et les citoyens. Une commune peut s'en saisir pour animer des "mois cyber" avec des ateliers et des kits, en s'appuyant sur des labels et communautés (ex. Villes Internet) pour rayonner au-delà de la DSI.

En combinant ces différents leviers, les collectivités disposent aujourd'hui d'un écosystème d'accompagnement robuste qui leur permet non seulement de renforcer leur résilience face aux menaces, mais aussi de structurer progressivement une véritable politique de cybersécurité locale.

En conclusion, la clé du succès pour minimiser le risque cyber est de ne pas s'isoler, mais bien de se préparer en amont et de tirer parti des dispositifs territoriaux, nationaux et de coopérer entre collectivités et associations.





Tony FLAHAUT
Directeur | Direction Mutualisée du
Numérique Communauté
d'Agglomération du Pays de Saint -Omer



CYBER
MOIS

« L'IA générative accroît le risque de fuite de données sensibles... »

À l'ère de la transformation numérique, la cybersécurité s'impose comme un pilier fondamental de la continuité des missions de service public au sein des territoires. La recrudescence des menaces informatiques, qu'il s'agisse de ransomwares, de tentatives de fraude ou de vol de données, rappelle que la cybersécurité n'est plus uniquement l'affaire de l'État ou des grandes entreprises, mais concerne directement chaque collectivité territoriale.

Celles-ci sont particulièrement exposées en raison de la diversité de leurs missions, de l'externalisation croissante des services numériques et de la masse de données sensibles qu'elles manipulent au quotidien. D'après un rapport de Cybermalveillance.gouv.fr, une collectivité sur dix a déjà été victime d'attaque ces douze derniers mois. Les conséquences ? Blocage de services essentiels, vols de données, pertes financières importantes et atteintes à la confiance des administrés.

Les infrastructures des collectivités locales peuvent supporter des activités vitales : gestion de l'eau, transports, écoles, services sociaux... Les cyberattaques visent à la fois des profits rapides et à déstabiliser durablement l'action publique. Parallèlement, l'entrée en vigueur de la directive européenne NIS2 en octobre 2024, doit être transposée dans le droit français avant décembre 2025. Elle viendra intégrer les collectivités dans son périmètre, imposant de nouvelles obligations : sécurisation des réseaux essentiels, gestion des incidents, politiques de formation et audit régulier des systèmes. L'arrivée de l'intelligence artificielle complexifie la sécurisation des infrastructures.

Les outils d'IA générative, employés par les agents publics, offrent des gains d'efficacité administrative, mais doivent être déployés dans des environnements maîtrisés et sécurisés.

Les cybercriminels exploitent aussi l'IA pour automatiser et sophistication leurs attaques, par exemple avec des hameçonnages ultra-ciblés, des malwares adaptatifs, ou la falsification de données pour tromper les systèmes protecteurs.

L'IA générative accroît le risque de fuite de données sensibles, car des informations confidentielles peuvent être traitées ou stockées dans des outils non maîtrisés.

De nouveaux enjeux apparaissent autour de l'intégrité et de la fiabilité de l'information, de l'audit des algorithmes et de la lutte contre la manipulation automatisée (deepfakes, usurpation d'identité, désinformation automatisée).

Contraintes budgétaires, complexité administrative, hétérogénéité des systèmes, multiplication des prestataires, utilisation de l'IA : telles sont les réalités auxquelles sont confrontées les équipes informatiques des collectivités. La cybersécurité exige la mobilisation de tous : élus, directions, agents, partenaires. Le maintien et le développement des compétences internes restent un défi clef face à la rapidité des évolutions numériques et à la pénurie d'experts sur le marché.

Pour relever ces enjeux, plusieurs leviers sont à privilégier :

- Mettre en place une gouvernance dédiée, intégrant la cybersécurité dans la stratégie numérique de la collectivité et favorisant la mutualisation avec l'échelle intercommunale ou régionale, ce qui peut permettre par ailleurs la demande de financements européens FEDER ;

- Déployer des actions continues de sensibilisation et de formation de l'ensemble des agents, en utilisant des ressources nationales comme celles du Cybermois, ou en s'appuyant sur des partenaires comme nous le faisons avec KAMAE ;
- Assurer la mise à jour régulière des systèmes d'information, et élaborer des plans de continuité et de reprise d'activité adaptés à chaque contexte local. A la CAPSO, nous nous engageons dans cette démarche afin de pouvoir s'assurer d'apporter la meilleure des réponses en cas d'attaque ;
- S'appuyer sur des partenariats avec les centres régionaux ou sectoriels de cybersécurité (CSIRT) et d'autres collectivités, pour partager expériences, outils et réponses face aux incidents.

Sur le volet IA :

- La définition de stratégies combinant souveraineté numérique, maîtrise de la donnée et sécurisation des usages,
- La formation des agents et élus à l'usage responsable de l'IA et à l'identification des risques nouveaux,
- L'encadrement réglementaire et technique de l'IA en cybersécurité, dans le respect des principes éthiques et des obligations européennes (RGPD, future réglementation IA).

Assurer la cybersécurité de la collectivité, c'est protéger la capacité à offrir un service public fiable et continu, garantir la sécurité et l'intégrité des données et préserver la confiance des citoyens. Profiter du Cybermois pour mobiliser l'ensemble des parties prenantes constitue une occasion privilégiée d'ancrer une vraie culture de la sécurité numérique. Alors que les cadres réglementaires et les menaces évoluent, cette mobilisation doit s'inscrire dans la durée.



Devenez
#CyberEngagés

Inscrivez-vous

pour (re)découvrir
l'Histoire
le 1er octobre !

cybermois.gouv.fr 🔍

CYBER MOIS

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



Bâtir une armure numérique

Les cyberattaques ne sont plus une menace invisible, elles sont une réalité pour ¼ des collectivités en 2024 ! En menaçant notre quotidien, elles bloquent la continuité de nos services publics et nuisent à la confidentialité des données que nos habitants nous ont confié.

Face à cette réalité, la Ville de Béthune a fait un choix clair : renforcer sa résilience numérique pour assurer la fiabilité et la continuité des services publics du quotidien.

Bâtir une armure numérique

Labellisée Smart City, Béthune s'est engagée dans une démarche ambitieuse, accompagnée par l'ANSSI et soutenue par l'État dans le cadre du programme France Relance 2030. Concrètement, la Ville a construit une solide armure numérique avec un plan de 230 actions visant à identifier les failles, réduire les risques et sécuriser les usages.

Ainsi, les messageries professionnelles sont protégées par des systèmes de filtrage renforcés, les postes de travail sont équipés d'antivirus intelligents et les accès numériques sont strictement sécurisés.

Grâce à un diagnostic précis pour connaître nos vulnérabilités, à une feuille de route claire pour prioriser les réponses et à une gouvernance partagée nous faisons de la sécurité numérique une priorité politique !

Sensibiliser et former nos agents : les « ambassadeurs du numérique »

La cybersécurité pour nos collectivités ne dépend pas seulement de logiciels ou de pare-feu : elle repose avant tout sur une vigilance et une mobilisation de chaque instant.

C'est pourquoi nous avons créé un réseau d'« ambassadeurs du numérique » afin d'accompagner les agents dans la sécurité informatique du quotidien.

Ainsi, nos agents sont régulièrement formés et testés pour reconnaître les tentatives de fraude et la culture du mot de passe a été repensée pour que chacun devienne acteur de la sécurité de la collectivité.

Faire de la cybersécurité un réflexe permanent

Les menaces cyber évoluent et nous devons sans cesse adapter notre réponse. Simulations, sensibilisations, harmonisation des politiques de sécurité et des ressources avec la Communauté d'agglomération : nous faisons de la cybersécurité un réflexe permanent.

La cybersécurité n'est pas qu'une affaire technique : elle est un enjeu politique, un gage de confiance et de continuité pour l'exercice de nos missions de services publics.

Ma conviction est claire : en protégeant nos systèmes informatiques et en sécurisant nos pratiques, nous protégeons les données personnelles de nos citoyens !



Lionel MONTILLAUD
Maire de Sainte-Hélène
Vice-Président de la Mission Ecoter



Cyberfiabilité, le bouclier numérique de la démocratie locale

Quand les serveurs nationaux des cartes d'identité ou des passeports tombent, ce sont des milliers de citoyens qui se retrouvent bloqués dans leurs démarches. Quand les flux informatiques de La Poste sont paralysés, impossible de suivre un courrier, de recevoir un transfert d'argent, de percevoir certaines prestations. Et quand, dans une mairie, l'accès au logiciel comptable ou RH dysfonctionne, ce n'est pas seulement une gêne technique : c'est la vie de la collectivité qui s'arrête.

Ces exemples montrent que la cybersécurité ne se limite pas à contrer les pirates informatiques. Elle doit s'accompagner d'une autre exigence : la **cyberfiabilité**. La sécurité protège, la fiabilité rassure. Ensemble, elles garantissent la continuité du service public, la stabilité des institutions locales et la confiance des citoyens. Car derrière chaque panne ou attaque, ce n'est pas seulement la technique qui est en cause : c'est le fonctionnement même de notre démocratie locale.

Dans un monde où tout transite par le numérique – de la scolarité à la santé, du courrier aux démarches administratives – la cybersécurité et la cyberfiabilité deviennent un **nouveau pilier démocratique**. Elles sont le socle invisible qui permet aux droits d'être exercés, aux prestations d'être versées, aux projets d'avancer. Sans elles, c'est la confiance dans l'action publique qui vacille.

Mais pour les communes rurales, investir dans cette double exigence est un défi immense. Nous n'avons ni directions des systèmes d'information, ni armées d'experts, ni budgets extensibles. Dans une petite mairie, « l'informaticien » est souvent un agent polyvalent, parfois même un élu. La moindre attaque, la moindre panne peut tout bloquer : état civil, paie des agents, délibérations, subventions aux associations.

C'est pourquoi la **mutualisation** est la seule voie crédible. Mutualiser les achats pour faire baisser les coûts. Mutualiser les expertises rares qu'aucune commune ne peut financer seule. Mutualiser la formation des agents pour créer une culture commune du réflexe numérique. Cette coopération doit se jouer à toutes les échelles : intercommunale, départementale, régionale, nationale. L'État, de son côté, doit assumer sa responsabilité en rendant ces solutions accessibles, lisibles et soutenues.

C'est tout l'enjeu de bâtir ce que j'appelle un **bouclier numérique territorial**. Un dispositif de protection, de vigilance et de continuité, pensé collectivement, qui couvre aussi bien les communes que les acteurs économiques, agricoles, associatifs ou de santé de nos territoires. Car une attaque sur une maison de santé, une exploitation agricole ou une PME locale peut avoir autant de conséquences pour la vie d'un territoire qu'une attaque sur une mairie.

Nous avons appris à protéger nos écoles avec des plans de mise en sécurité, à équiper nos forêts de dispositifs DFCl, à installer des caméras pour sécuriser nos espaces publics. Il est temps d'acquiescer le même réflexe pour nos systèmes informatiques. Parce que la prévention coûte toujours moins cher que la réparation. Et parce que la cyberfiabilité est désormais une condition de la confiance entre élus, agents et citoyens.

La cybersécurité et la cyberfiabilité ne sont pas des dépenses de luxe. Elles sont des **assurances démocratiques**. Elles garantissent que l'école est bien administrée, que les paies sont versées, que les courriers circulent, que les projets d'urbanisme avancent. Elles garantissent, tout simplement, que nos collectivités fonctionnent au quotidien.

Protéger nos territoires, c'est les rendre cyberfiables.

Et cela, nous ne pourrions le réussir qu'ensemble.





Magali Noegelin

**DPO et Responsable Cybersécurité du
Pays de Montbéliard Agglomération**



Cybersécurité et Territoires : renforcer ensemble la résilience numérique

La cybersécurité est aujourd'hui un enjeu majeur pour notre collectivité. Les établissements publics sont en effet en première ligne face aux menaces numériques. Nous devons protéger nos données tout en assurant la continuité de nos missions de service public.

L'avant-projet

Une stratégie soutenue par France Relance et l'ANSSI.

En 2022, grâce au plan **France Relance**, nous avons pu initier une politique de sécurisation de notre Système d'Information. Ce soutien national nous a permis de mettre en place des ateliers avec un prestataire et de structurer nos priorités pour traiter les mesures urgentes.

Un appui fort de l'**ANSSI**. Notre correspondante régionale est intervenue sur 2 jours dans nos locaux pour sensibiliser les agents de la collectivité. La Directrice Générale des Services de notre collectivité a souhaité que tous les agents puissent s'inscrire afin de bénéficier de conseils et de points de vigilance tant sur les usages professionnels que personnels.

En 2024, nous avons bénéficié du second pack France Relance pour déployer des solutions concrètes et durables, en phase avec les réalités notre collectivité.

Notre ambition : des actions communes avec des partenaires spécialisés.

Au-delà des outils et procédures, nous accordons une importance majeure à la coopération multipartenaires afin de permettre une efficacité des expertises. Nous pensons qu'en cas de crise, la résilience de notre SI sera dépendante de la collaboration de l'ensemble des acteurs.

Un outillage renforcé et l'élaboration d'une méthodologie innovante et multi-partenariale

Pour prévenir, détecter et répondre efficacement aux incidents, nous avons structuré notre dispositif autour de plusieurs outils complémentaires :

- **Varonis** : Supervision, centralisation, détection des alertes comportementales sur le SI (signaux faibles)
- **NXO Cyber Protect** - Solution globale WithSecure : Protection des postes et des serveurs.
- Processus de gestion des accès et authentification renforcée pour les télétravailleurs (OpenVpn).
- Sauvegardes sécurisées et automatisées.
- PCA (Plan de Continuité d'Activité): système de réplication / redondance du SI sur un site distant.

Ces éléments constituent notre première ligne de défense et garantissent une vision consolidée de notre exposition aux menaces.

Un élément majeur : la mise en place d'un SOC

Un SOC (Security Operations Centers) a été progressivement mis en œuvre. Sa mission : centraliser la surveillance, corréler les événements et déclencher des mesures rapides en cas d'incident. C'est un levier essentiel pour anticiper les menaces et améliorer la réactivité opérationnelle.

Le SOC est actuellement opéré par notre partenaire **NXO**.

Sensibilisation des agents : exercices de phishing

La sécurité repose aussi sur les usages, 80% des cyberattaques proviennent d'un e-mail de phishing.

Pour impliquer les agents, nous avons mis en place un programme de sensibilisation avec notre partenaire « **Avant de cliquer** ».

L'apprentissage par la pratique est efficace. Des exercices de simulation de phishing automatiques ont lieu plusieurs fois par an. Cette pédagogie innovante passe aussi par des séances d'E-learning courtes. Chaque agent piégé doit suivre une micro-formation. Ces campagnes permettent de mesurer la vigilance, de renforcer les bonnes pratiques et de développer une culture de sécurité à l'ensemble des agents de la collectivité.

Une PSSI comme cadre de gouvernance

Toutes ces actions s'articulent autour d'une Politique de Sécurité des Systèmes d'Information (PSSI). Celle-ci fixe les règles de contexte, les responsabilités et la gouvernance, garantissant une cohérence entre aspects techniques, organisationnels et humains.

SPIE ICS est notre partenaire dans cette démarche.

Conclusion

Impulsée par France Relance, notre démarche en cybersécurité se poursuit sans relâche, étape après étape, pour renforcer durablement notre résilience numérique. Chaque partenaire joue un rôle essentiel dans cette dynamique collective. Chaque prestataire, chaque agent, chaque collaborateur est un maillon essentiel à cette protection collective.



Devenez
#CyberEngagés

Inscrivez-vous

pour (re)découvrir
l'Histoire
le 1er octobre !

cybermois.gouv.fr 🔍





Nathalie POIGNON
Responsable du service Communication
de la Ville de Marseillan



La mairie de Marseillan s'engage pour une cyber-sensibilisation collective

En octobre 2024, la mairie de Marseillan a lancé une initiative innovante pour sensibiliser ses agents aux enjeux de la cybersécurité. En cette période de forte dépendance numérique, il est devenu indispensable de comprendre les risques auxquels nous sommes exposés et d'adopter les bonnes pratiques pour garantir la sécurité de nos informations et de nos infrastructures.

La digitalisation des services (portails en ligne, gestion des données personnelles des citoyens, etc.) amplifie les risques, en particulier pour les agents municipaux qui utilisent quotidiennement des informations cruciales.

Face à cette menace croissante, la mairie de Marseillan a pris des mesures concrètes pour sensibiliser ses agents. Pour rappel, en 2024, le service communication a proposé de mettre en avant les employés municipaux à travers une série de petits clips de sensibilisation. Ces clips, dont les acteurs sont les agents eux-mêmes, alertent de façon humoristique les risques de cyberattaques.

En 2025, la mairie de Marseillan organise un forum pédagogique. Ce forum proposera une série de 7 ateliers interactifs visant à sensibiliser, initier et former les 200 agents dans un cadre convivial et propice aux échanges.

Les ateliers se déclineront comme suit :

Atelier 1 & 2 : Sensibilisation aux risques cyber professionnels et personnels

Organisés par les entreprises XEFI et SNS, ces ateliers aborderont les risques auxquels sont confrontés les professionnels au quotidien. Grâce à des quizz et des jeux interactifs (Kahoot), les participants pourront tester leurs connaissances tout en découvrant les pièges à éviter dans la gestion de leurs données personnelles et professionnelles.

Atelier 3 : Réalité virtuelle, immersion dans des scénarios cyber
Cet atelier innovant proposera aux participants une expérience immersive avec des casques de réalité virtuelle.

Atelier 4 : Découverte de la littérature autour de la cybersécurité
En collaboration avec la médiathèque, cet atelier offrira une perspective culturelle sur les enjeux de la cybersécurité à travers la littérature et les ouvrages spécialisés.

Atelier 5 : Escape Game Cyber, une aventure pour se former
Inventé par la médiathèque, cet escape game autour du thème de la cybersécurité offrira aux participants une immersion ludique dans un environnement virtuel.

Atelier 6 : Le coffre-fort électronique Kalydian
Dans cet atelier, les agents découvriront l'outil Kalydian, une solution de coffre-fort électronique sécurisée permettant de stocker et protéger les données sensibles.

Atelier 7 : Découverte des grands principes de la Charte informatique
Enfin, un atelier sera dédié à l'apprentissage des règles fondamentales de la Charte informatique, qui régit l'utilisation des outils numériques au sein des collectivités.

Pour 2025, la mairie de Marseillan espère que chaque agent repartira non seulement avec des connaissances accrues sur les bonnes pratiques à adopter, mais aussi avec un sentiment d'appartenance à une démarche collective de protection des données et de la sécurité des systèmes d'information. Avec le forum dédié à cette thématique et les ateliers interactifs proposés, Marseillan donne l'exemple d'une collectivité très active dans la gestion des risques numériques.



Cybersécurité et Territoires : protéger les infrastructures et les citoyens à l'ère du numérique

Introduction

La transformation numérique bouleverse en profondeur la manière dont les territoires fonctionnent. Les collectivités s'appuient de plus en plus sur des technologies connectées pour améliorer la qualité de vie, fluidifier les services publics et optimiser la gestion des infrastructures. Villes intelligentes, réseaux d'énergie connectés, systèmes de transports automatisés, bâtiments intelligents : ces innovations sont au cœur de la modernisation des territoires.

Mais cette interconnexion croissante a un revers : elle expose les territoires à des risques cyber sans précédent. Un incident de cybersécurité ne se limite pas à une perte financière : il peut paralyser des services essentiels, mettre en danger la vie des citoyens et fragiliser la confiance des usagers envers leurs institutions. Dans ce contexte, la cybersécurité devient un pilier central de la stratégie de résilience des territoires.

1. Des territoires connectés, mais vulnérables

Les collectivités locales et régionales gèrent aujourd'hui une multitude de systèmes critiques. Ces environnements ne se limitent plus à l'informatique classique (IT), mais incluent désormais des systèmes opérationnels (OT) :

- Réseaux d'énergie et d'eau potable.
- Transports publics et signalisation.
- Systèmes de chauffage, ventilation et climatisation (CVC) dans les bâtiments.
- Vidéosurveillance et dispositifs de contrôle d'accès.

Avec la généralisation de l'Internet des Objets (IoT), chaque capteur, caméra ou automate devient un point d'entrée potentiel pour une attaque. Or, la convergence entre IT et OT brouille les frontières traditionnelles de la sécurité : un attaquant qui infiltre un simple poste de travail peut remonter jusqu'à un système industriel critique.

Les exemples ne manquent pas : attaques contre des hôpitaux entraînant l'arrêt de services d'urgence, cyberattaques contre des collectivités locales provoquant l'indisponibilité de services administratifs, ransomwares paralysant des réseaux de transport. Ces scénarios, autrefois exceptionnels, se banalisent et rappellent à quel point les territoires sont devenus des cibles privilégiées.

2. Les enjeux de sécurité pour les collectivités

Face à ces menaces, les territoires doivent répondre à plusieurs défis majeurs :

1. Garantir la continuité de service

L'interruption d'un service public, même temporaire, a un impact direct sur les citoyens : impossibilité de prendre un transport, coupure d'électricité, services hospitaliers inaccessibles. La cybersécurité devient un enjeu de résilience.

2. Protéger la vie privée des citoyens

Les territoires collectent et stockent des quantités massives de données personnelles : informations administratives, données de santé, géolocalisation, vidéosurveillance. Une fuite ou un vol de données entraîne une perte de confiance immédiate.

3. Assurer la conformité réglementaire

Les collectivités doivent se conformer à des cadres réglementaires exigeants : RGPD pour la protection des données personnelles, directives européennes (NIS, NIS2), obligations nationales spécifiques à certains secteurs critiques.

4. Maintenir la confiance des usagers et partenaires

Une cyberattaque médiatisée peut ternir durablement l'image d'une collectivité. À l'inverse, une stratégie proactive de cybersécurité renforce la crédibilité et la confiance.

3. Vers une approche intégrée de la cybersécurité

La cybersécurité des territoires ne peut plus se limiter à des actions ponctuelles. Elle doit reposer sur une approche intégrée et proactive, articulée autour de quatre piliers :

- **Anticiper** : évaluer les risques, identifier les vulnérabilités, sensibiliser les équipes.
- **Protéger** : mettre en place des solutions adaptées de contrôle d'accès, de chiffrement, de segmentation réseau.
- **Détecter** : surveiller les accès et comportements inhabituels grâce à des outils de monitoring en temps réel.
- **Réagir** : disposer de procédures claires de réponse aux incidents et assurer la traçabilité des actions.

Au cœur de cette approche se trouve la **gestion des identités et des accès**. Les collectivités doivent maîtriser qui accède à quoi, quand et comment. Ce contrôle est d'autant plus critique pour les **accès à privilèges**, qui donnent à un utilisateur (interne ou externe) le pouvoir de modifier ou contrôler des systèmes sensibles.

4. La réponse WALLIX pour les territoires

WALLIX accompagne les collectivités et territoires dans leur transformation numérique sécurisée grâce à une suite de solutions centrées sur la **sécurisation des accès et des identités**.

WALLIX PAM (Privileged Access Management)

- Garantit un contrôle strict des accès à privilèges.
- Enregistre et trace toutes les sessions sensibles.
- Permet de limiter les droits en fonction des besoins réels (principe du moindre privilège).

Access Manager & Web Session Manager

- Simplifient et sécurisent les accès distants, par exemple pour les prestataires externes qui interviennent sur des systèmes critiques.
- Offrent une traçabilité complète sans complexité technique.

Solutions OT (PAM4OT)

- Adaptées aux environnements industriels et aux infrastructures intelligentes.
- Fonctionnent même dans des contextes où l'Active Directory n'est pas présent.
- Répondent aux besoins spécifiques des territoires connectés : transport, énergie, bâtiments intelligents.



Exemple d'usage

Une collectivité doit permettre à un prestataire de maintenance d'accéder à distance à un système de chauffage urbain.

- Sans contrôle : l'accès ouvre une porte à des intrusions.
- Avec WALLIX : l'accès est sécurisé, limité dans le temps, surveillé en temps réel, et toutes les actions sont enregistrées pour audit.

Ce type de dispositif réduit considérablement les risques, tout en facilitant la collaboration entre collectivités et partenaires.

5. Les bénéfices pour les collectivités et territoires

Mettre en place une cybersécurité intégrée avec des solutions comme celles de WALLIX apporte de nombreux avantages :

- **Continuité de service** : les infrastructures critiques restent opérationnelles, même en cas de tentative d'attaque.
- **Réduction des risques** : les cybermenaces sont contenues avant d'avoir un impact majeur.
- **Conformité renforcée** : les collectivités respectent les exigences réglementaires.
- **Traçabilité et transparence** : chaque accès et chaque action est documenté, permettant de répondre aux audits et d'améliorer la gouvernance.
- **Protection des citoyens** : les données personnelles sont sécurisées, renforçant la confiance dans les institutions.

Conclusion

La cybersécurité des territoires n'est plus une option. Elle est devenue une condition sine qua non de la modernisation numérique et de la résilience des collectivités. Dans un monde où chaque capteur, chaque automate et chaque accès distant peut être la cible d'un attaquant, il est urgent d'adopter une stratégie globale de protection.

En plaçant la gestion des accès et des identités au cœur de leur politique de cybersécurité, les territoires se donnent les moyens de protéger efficacement leurs infrastructures, de garantir la continuité des services publics et de préserver la confiance des citoyens.



**MISSION
ECOTER**



Directeur de la publication :
Alain MELKA – Directeur Général des Services
+33 (0)6 33 75 13 60
alain.melka@ecoter.org

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

Parlons Territoires

**CYBER
MOIS**

CYBERMOIS
Octobre 2025

