MISSION ECOTER

NOUS SOMMES #CYBERENGAGÉS

DU 1ER AU 31 OCTOBRE 2024

CYBER MOIS

Parlons Territoires

Livret CYBERMOI/S

Octobre 2024

MISSION ECOTER

Depuis plus de 20 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.

À propos du Cybermoi/s

Créé en 2012 , le Mois européen de la cybersécurité (European Cybersecurity Month – ECSM) est une initiative conçue par l'Agence de l'Union européenne pour la cybersécurité (ENISA). Elle vise à promouvoir le sujet de la cybersécurité à travers les pays de l'UE pour permettre de mieux comprendre les menaces et les appréhender.
En France, le Mois européen de la cybersécurité a été décliné en « Cybermoi/s » et est piloté par Cybermalveillance.gouv.fr.
Face à la multiplication des fraudes par ingénierie sociale, ces attaques au cours desquelles les cybercriminels manipulent les victimes et abusent de leur confiance pour leur soutirer de l'argent ou des informations personnelles, l'ENISA a souhaité faire de la fraude par ingénierie sociale auprès des jeunes via l'intelligence artificielle le thème principal du Cybermoi/s 2024.
Tout au long du mois d'octobre 2024, des activités vont être organisées en France et en Europe autour des enjeux de cybersécurité : événement de lancement, événements de sensibilisation, campagnes vidéo… Comme chaque année, un panel d'acteurs publics, privés et associatifs se mobiliseront pour proposer un programme de sensibilisation pédagogique à destination de tous les publics et ainsi développer une culture européenne cyber commune.

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.

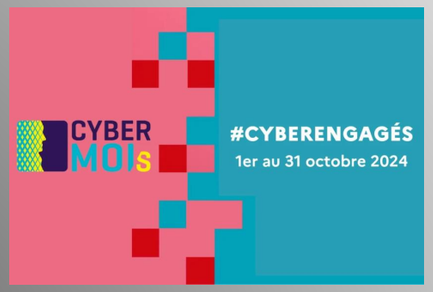
C'est dans l'échange permanent, le retour d'expérience, la transmission et l'accompagnement, que Mission Ecoter s'associe aux projets individuels et collectifs de nos territoires. Soutien et partenaire indéfectible des collectivités dans leur transition numérique et le développement de projets innovants, Mission Ecoter, c'est avant tout 25 années d'expertise au service des territoires

Et comme chaque année, il est naturel de s'associer au Cybermoi/s. En effet, fervent défenseur et partenaire des territoires, la Mission Ecoter donne ainsi la parole aux élus et aux entreprises autour des problématiques liées à la cybersécurité. Parce que, c'est bien au cœur des territoires qu'il nous faut agir !

L'Avant-propos de

Denis THURIOT

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



Les villes médianes cybervigilantes

Au-delà du sacre d'un grand nombre de nos sportifs tricolores et de l'engouement de nos compatriotes, les Jeux Olympiques de Paris 2024 ont également permis de largement médiatiser les enjeux de la cybersécurité et les conséquences potentielles des cyberattaques en nombre croissant. Une médiatisation bienvenue pour sensibiliser les élus locaux et faire prendre conscience des risques. A nos collectivités médianes à présent de décrocher la médaille d'or de la cybervigilance.

Les JO de Paris, événement hors normes (206 nations représentées, 878 épreuves sportives sur 40 sites de compétition dans 22 villes, 10 millions de spectateurs et 4 milliards de téléspectateurs), ont nécessité une attention particulière de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) qui s'est vu confier le pilotage de la stratégie de prévention des cyberattaques, avec l'accompagnement des experts d'Atos et de Cisco, partenaires des JO. Un dispositif efficace (formations, guides de sensibilisation, surveillance de l'ensemble des réseaux et systèmes informatiques 24h/24, chiffrement des données, collaboration avec des professionnels du milieu de la cyber-défense, etc.) a permis d'éviter le pire. Aucune cyberattaque n'a affecté la tenue des cérémonies et le bon déroulement des épreuves. Seulement 141 événements de cybersécurité affectant des entités en lien avec l'organisation des Jeux Olympiques de Paris 2024 ont été rapportés à l'ANSSI entre le 26 juillet et le 11 août derniers.

Évidemment, un tel dispositif d'ampleur et une telle efficacité ne peuvent s'envisager à l'échelle d'une commune, et encore moins à celle des particuliers. Ces derniers sont pourtant des cibles faciles : un Français sur quatre reçoit un message suspecté d'être une tentative d'arnaque au moins tous les jours. Les attaques sont de plus en plus sophistiquées et touchent aujourd'hui tous les acteurs de la société. Nos collectivités locales ne sont évidemment pas épargnées par ce fléau mondial. D'après l'ANSSI, 187 incidents cyber ont affecté les collectivités territoriales de janvier 2022 à juin 2023, soit 10 par mois.

La majorité des incidents concernaient des communes et/ou des EPCI à fiscalité propre. La prise de conscience des cyberrisques et des cyberdangers est forte au niveau national et européen (l'application élargie de la directive européenne NIS 2 Network and Information Security doit être mise en place prochainement afin d'équilibrer les pratiques cyber à l'échelle européenne en élargissant son champ d'application à plus de secteurs et d'organisations). Mais, au niveau infra-national, celui des villes médianes notamment, nos collectivités sont loin d'avoir le niveau requis de sécurité informatique, alors que 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 villes médianes, de plus en plus connectées (capteurs collectant des données, systèmes d'information pour optimiser les services, usage croissant du digital…) voient leurs risques de sécurité augmenter. Selon la formule désormais connue, il ne s'agit maintenant plus de savoir si une cyberattaque peut avoir lieu, mais plutôt quand elle aura lieu.

Pourquoi nos territoires médians, de plus en plus engagés dans la construction d'un territoire intelligent, sont-ils devenus des cyber-cibles de choix ? D'abord parce qu'ils détiennent des données sensibles qui ont une valeur dans le cadre d'une attaque à but lucratif (rançon, revente, usurpation d'identité, etc.). Les villes médianes, qui n'ont pas toujours les moyens de développer leur propre plate-forme, peuvent en outre être tentées d'accepter des propositions de partage des données avec des entreprises privées. Se posent alors les questions du consentement citoyen, de l'anonymisation des informations, de l'éthique des algorithmes ou encore de la souveraineté des données. Les cyber-pirates attaquent, il est vrai, au hasard mais d'abord ce qui est rentable… et surtout ce qui vulnérable. Ensuite, parce que nos territoires médians n'investissent pas assez dans la cybersécurité. La protection passe en effet par des ressources budgétaires suffisantes. Or, 75 % des élus et agents reconnaissent dépenser moins de 2000 € par an pour la cybersécurité de leur collectivité (source ANSSI). Cette dernière devrait plutôt représenter entre 5 et 10 % du budget informatique total. Mais, plus facile à dire qu'à faire dans certaines collectivités aux budgets contraints. Enfin, nos territoires médians sont des cibles de choix parce que leurs élus et leurs agents ne sont pas assez sensibilisés et préparés aux cyberattaques. Seules 14 % des collectivités se disent préparées en cas d'attaque, et seulement une sur cinq (19 %) dispose d'une procédure de réaction (source ANSSI). Si le risque cyber peut se maîtriser, il est particulièrement complexe pour la ville intelligente ; il est nécessaire qu'une gouvernance soit mise en place pour traiter le sujet. Les points faibles de nos villes médianes en matière de cybersécurité peuvent donc se résumer ainsi : manque de connaissance sur le sujet, absence de ressources humaines et d'élus dédiés, manque de temps et manque de budget.

Pourtant, les conséquences d'une cyberattaque sont nombreuses, catastrophiques dans certains cas et, pour certaines, méconnues. Une cyberattaque peut se transformer en bombe à fragmentation pour une ville médiane. La méconnaissance des risques et des conséquences n'affecte pas seulement le fonctionnement de la commune.

L'ANSSI rappelle que, lors de la compromission informatique, « de multiples services publics (aides sociales, état civil, urbanisme, administration des cimetières, gestion de l'eau et des déchets, etc.) et services internes à la collectivité (téléphonie, messagerie, finance, ressources humaines, etc.) ne sont plus opérationnels ».

Et il faut aussi prendre conscience du délai, souvent très long, pour reconstruire le système d'information piraté, avec un coût qui s'ajoute aux coûts déjà conséquents de l'indisponibilité éventuelle d'équipements publics. Le risque judiciaire doit être connu, car la fuite et la destruction de données peuvent être répréhensibles si les mesures de protection mises en place par la commune sont jugées insuffisantes. Nos collectivités locales sont tenues par obligations juridiques en matière de cyber sécurité. Le Guide des obligations et responsabilités des collectivités locales en matière de cybersécurité (disponible sur www.cybermalveillance.gouv.fr) les recensent.

La responsabilité administrative de la collectivité (sanctions administratives et pécuniaires de la CNIL en cas de manquements graves, indemnisation de préjudices subis par les usagers…), et la responsabilité civile et pénale des élus (violation des règles relatives à la protection des données personnelles, fautes d'imprudence ou de négligence…) peuvent être engagées. En outre, l'impact des conséquences d'une cyberattaque sur l'image et la crédibilité d'une ville peut être redoutable et conduire à l'affaiblissement du lien de confiance avec les administrés.

Une fois conscient des risques et des conséquences, comment agir ? Avec MonServiceSécurisé, l'ANSSI accompagne les administrations et tous les agents du service public en proposant un outil pédagogique pour simplifier les démarches de sécurisation et d'homologation. L'ANSSI a également contribué, en 2017, à la création du GIP ACYMA pour fédérer l'ensemble des institutions et des acteurs nationaux ou locaux, des secteurs publics ou privés, afin d'apporter la meilleure réponse aux élus pour construire une véritable « résilience cyber » des territoires. C'est également un des axes de travail de la Mission Ecoter France et Territoires Numériques que je préside et qui a remis, en 2023, à Jean-Noël Barrot, alors Ministre délégué chargé de la Transition numérique et des Télécommunications, le Livre Blanc « Cybersécurité & Territoires ».

Les villes médianes peuvent jouer un rôle central dans l'acquisition et la diffusion des bonnes pratiques nécessaires pour sécuriser leur territoire. En identifiant les risques et en évaluant le niveau d'exposition et de protection, en prenant en compte le risque cyber dans les dispositifs de prévention des risques majeurs (inondation, submersion marine, industriel, nucléaire, etc.), en désignant une ressource dédiée (pour garantir notamment le respect des exigences RGPD), en menant des actions de sensibilisation et de formation des agents, en maintenant à jour les systèmes d'information (y compris les logiciels, les applications et les systèmes d'exploitation sur les appareils et les serveurs), et en activant des logiciels de sécurité et des outils de défense.

A titre d'exemple, la Ville de Nevers a participé, en 2022, au parcours cybersécurité proposé par l'ANSSI dans le cadre du plan France Relance et j'ai pu constater qu'elle était dans la moyenne des villes françaises de même strate en termes d'indice de cybersécurité. Avec mes équipes, nous avons démarré un plan de sécurisation sur 3 ans, pour un budget global estimé à un peu plus de 250 000€. 50 actions ont été programmées qui touchent à la sensibilisation, à l'environnement utilisateur, aux applications, à la gestion des fournisseurs, à l'administration des infrastructures, au réseau, à la protection des données, à la gestion des identités, à la détection des attaques, à la gestion des incidents et à la résilience, à la sécurité des objets connectés, à la gouvernance…

Les premières actions ont été lancées : la formalisation d'une politique de sécurité de systèmes d'information, le renforcement des protections techniques internes (avec la mise en place d'outils de sécurisation des comptes et des accès aux serveurs, ou le déploiement automatisé des mises à jour de logiciels par exemple), la réalisation d'audits et d'évaluations régulières de nos fournisseurs de solutions numériques et de nos infrastructures internes, la sensibilisation des agents et des élus (notamment via une campagne test de phishing par mail). Il ne faut pas perdre de vue que 80 % des risques cyber sont liés à l'humain et que 90 % des menaces proviennent d'un mail frauduleux. Et une décision simple et non coûteuse : la délégation « cyber » confiée à un élu.

En matière de cybersécurité, comme en matière d'innovation, la mutualisation, la coopération et les échanges de bonnes pratiques s'imposent. Ensemble, les villes médianes sont capables de mieux faire face aux cyber-risques. En 2018 avec Michel Angers, le maire d'une ville du Québec, nous avons lancé la coopération économique stratégique entre villes médianes basée sur le digital et les nouvelles technologies. Nous avons créé le Sommet International de l'Innovation en Villes Médianes (SIIViM) qui promeut, chaque année en alternance à Nevers, sous le Haut Patronage du Président de la République française, et au Québec, l'innovation dans tous ses états, qu'elle soit de produits, de process, de modes de production ou d'organisation. Nous avons également lancé le Réseau des Villes Médianes Innovantes pour donner aux villes adhérentes les conseils et les moyens de construire un territoire intelligent, toujours au service de leurs habitants, au service de l'humain. Et la thématique cybersécurité tient une place de plus en plus importante dans les conférences et tables-rondes organisées dans le cadre du SIIViM.

Un des enjeux de la cybersécurité en France est d'ailleurs l'intégration de l'intelligence artificielle. Pour Pierre Barnabé, ex-vice-président exécutif en charge du Big Data et de la cybersécurité au sein du groupe Atos, il faut investir dans l'innovation, en particulier l'IA et la robotisation pour faire face à des cyberattaques toujours plus complexes.

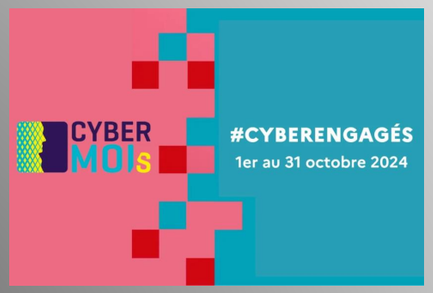
L'intelligence artificielle permet d'analyser des flux en temps réel pour détecter une attaque potentielle, impossible à détecter « physiquement ». Le SIIViM et le Réseau des Villes Médianes Innovantes participent donc pleinement à la connaissance des risques cyber et à la diffusion des bonnes pratiques pour y faire face, sans perdre de temps grâce aux retours d'expérience de ses membres avec des économies à la clé.

Un risque n'est pas une fatalité. Il faut organiser 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. 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 sensibilisation des élus à la cybersécurité progressant, la vigilance et la prévention pouvant empêcher de graves cyber-catastrophes, et les dispositifs et boucliers évoluant avec les menaces, nous pouvons donc réduire notre niveau d'anxiogénité face aux cyber-risques. Encore une fois, la peur n'évite pas le danger et les bonnes pratiques limitent les risques. Dans les villes médianes, l'heure est la cybervigilance, éclairée et convenablement dotée humainement, financièrement et techniquement.
Et, pour terminer sur une note d'humour, je rappelle que certaines menaces seront toujours difficiles à prévoir. A l'exemple de cette fouine qui a discrètement sectionné plusieurs fois les câbles de fibre optique dans la fan zone des Jeux Olympiques à Vincennes mais qui a finalement été démasquée lors de l'enquête ouverte par la section de lutte contre la cybercriminalité du parquet de Paris… Si même les animaux s'y mettent…

Bertrand RINGOT

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



La Ville de Gravelines a été la cible d'une cyberattaque le matin du 25 avril 2024. Un hacker a réussi à pénétrer notre système d'information et a mené plusieurs attaques pour le rendre inopérant. Grâce à l'intervention rapide des techniciens, qui ont détecté une surcharge de processeur sur plusieurs serveurs, les actions du pirate ont été considérablement limitées, évitant ainsi toute fuite de données et réduisant les dommages à quelques serveurs touchés. Par mesure de précaution, tous les serveurs, PC et accès internet des bâtiments de la mairie ont été coupés.

Pour assurer la continuité du service public, des réseaux indépendants ont été rapidement mis en place en mode dégradé, utilisant un ou deux nouveaux PC et des connexions sur smartphone pour les finances, les marchés publics, les élections, la médiathèque et le CCAS. Ces services ont fonctionné en mode SaaS (applications cloud accessibles directement en ligne). La téléphonie a également été impactée : une solution de contournement a été mise en œuvre pour les accueils, revenant aux téléphones physiques.

Nous avons immédiatement fait appel à l'une des huit sociétés agréées par l'ANSSI pour gérer ce type de crise. Leur collaboration avec notre équipe de la DSIN a permis une analyse approfondie de l'attaque à l'aide d'outils spécialisés.

Par la suite, le prestataire a travaillé en étroite collaboration avec la DSIN pour résoudre la situation, en reconstruisant une partie du système d'information, en corrigeant les failles de sécurité et en renforçant les mesures de protection. L'objectif était de consolider la structure du système d'information en partant sur une nouvelle base saine. Les sauvegardes ont été restaurées, garantissant l'absence de perte de données.

Le mardi 14 mai, toutes les conditions étaient réunies pour relancer progressivement l'ensemble du système d'information de la Ville de Gravelines. Les principaux coûts liés à cette cyberattaque ont concerné les services d'accompagnement, de supervision et d'expertise fournis par des structures externes, notamment le prestataire agréé en gestion de crise, s'élevant à plusieurs dizaines de milliers d'euros. De nouveaux outils de sécurité ont également été mis en place, entraînant des coûts annuels similaires.

Ce que nous retenons de cette cyberattaque :

- Les cyberpirates ont souvent une longueur d'avance et exploitent la moindre faille.

- Le contexte géopolitique (guerres, JO, etc.) a conduit à une augmentation des attaques, c'est une réalité.

- L'IA aide les cyberpirates à perfectionner leurs attaques, mais elle assiste aussi les éditeurs de solutions de sécurité avec des outils de détection avancés, que nous avons testés.

- Il est crucial de prévoir un stock de réserve de PC neufs, smartphones ou clés 4G pour établir rapidement des réseaux de secours.

- Une solution de téléphonie alternative pour les accueils, contournant le système informatique, est nécessaire.

- Des emails de secours hors de la messagerie classique doivent être prévus pour assurer la communication, vitale durant la crise.

- Le temps passé avec les organismes d'État (police, gendarmerie, ministère, ANSSI, CNIL, CIRT) est essentiel, surtout durant les deux premiers jours, et il est important de s'y préparer. Les sites de l'ANSSI et cyber.gouv sont des ressources précieuses.

- Il convient de limiter la communication avec les médias tant que la crise est en cours pour ne pas fournir d'informations aux pirates potentiellement à l'écoute.

- Il est prudent de sélectionner à l'avance un partenaire agréé pour gérer les situations de crise et de vérifier son niveau de recommandation sur le site de cyber.gouv.fr ainsi que sa disponibilité.

- Les attaques se produisent souvent le week-end (bien que cela ne soit pas notre cas), rendant préférable une solution de sécurité managée externe, avec malheureusement un coût conséquent.

- Le vieillissement du système d'information crée des vulnérabilités techniques et humaines, d'où la nécessité d'audits réguliers des différents composants du système et d'une politique de sécurité du système d'information (PSSI).

- Une sauvegarde à trois niveaux (disque dur avec une solution immuable, une réplication sur un site externe (PRA) et des bandes) est essentielle pour garantir la récupération des données. Nous nous étions préparés à cela.

- Lorsqu'une cyberattaque survient, vous vous isolez en interne par mesure de sécurité, mais vous vous retrouvez également isolé de l'extérieur. Même si vous avez toutes les conditions requises pour fonctionner, que ce soit en mode dégradé ou une fois la situation rétablie, vous devez prouver votre fiabilité aux autres pour rétablir les échanges de flux, qui sont nombreux avec la dématérialisation (paye, comptabilité...).

- La communication interne durant la crise est cruciale pour expliquer, rassurer et détecter les urgences, même si les outils se limitent souvent à des réunions et à des informations diffusées sur papier.

- Il est important d'écouter et de soutenir les équipes techniques, sans les épuiser, car la pression est forte et les nuits sont peu réparatrices.

- Le soutien de la direction et des responsables politiques est essentiel pour surmonter cette période difficile. Il permet de limiter les sollicitations envers la DSIN et de réorganiser le fonctionnement des services. Nous avons eu la chance de bénéficier de ce soutien dès le départ.

En conclusion, bien que nous ayons renforcé notre sécurité au cours des trois dernières années, il est évident que les cyberpirates nous ont rattrapés. Le nerf de la guerre demeure l'équation complexe entre le temps, le coût et les ressources allouées.

Alain MELKA
Directeur Général des Services
Mission Ecoter

#CYBERENGAGÉS
1er au 31 octobre 2024

Quentin MEULLEMIESTRE
Directeur Général des Services Adjoint
Mission Ecoter

Cybersécurité dans les territoires : enjeux et défis d'un monde connecté

Comme chaque année désormais le Cybermoi/s est une campagne de sensibilisation aux enjeux de la cybersécurité. 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. Une nouvelle fois, Mission Ecoter 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 exposées aux cyberattaques. Ces dernières peuvent entraîner des conséquences graves, tant sur le plan financier que sur le plan opérationnel.

Force est de constater : les JOP 2024 ont marqué un tournant en matière de cybersécurité pour les grands événements sportifs. Les leçons apprises lors de cet événement serviront de référence pour les futurs Jeux Olympiques et pour sécuriser d'autres événements d'envergure mondiale. Sans oublier les collectivités territoriales de notre pays.
Au-delà, et dans un contexte de digitalisation accélérée, les collectivités territoriales sont exposées aux risques cybernétiques. Des petites communes aux grandes métropoles, aucune entité n'est à l'abri.

Les cyberattaques, qu'il s'agisse de rançongiciels, de phishing ou d'intrusions, peuvent paralyser les services publics, compromettre la vie privée des citoyens et engendrer des pertes financières considérables.

Les enjeux de la cybersécurité pour les territoires

Protection des données personnelles :
- **Les collectivités gèrent une quantité importante de données sensibles (état civil, finances locales, etc.). Leur protection est un enjeu majeur pour préserver la confiance des citoyens.**

Continuité des services publics :
- **Une cyberattaque peut interrompre l'accès aux services en ligne, tels que les démarches administratives ou les paiements en ligne, avec des conséquences directes sur la qualité de vie des habitants.**

Réputation des collectivités :
- **Une attaque réussie peut ternir l'image d'une collectivité et fragiliser sa relation avec les citoyens.**

Coûts financiers :

- **Les coûts liés à une cyberattaque peuvent être très élevés, allant de la remise en état des systèmes à la prise en charge des rançons.**

Les défis à relever

Sensibilisation des élus et des agents :

- **Il est essentiel de former les acteurs locaux aux risques cybernétiques et aux bonnes pratiques en matière de sécurité informatique.**

Manque de ressources :

- **Les petites collectivités disposent souvent de moyens limités pour investir dans la cybersécurité.**

Évolution rapide des menaces :

- **Les cybercriminels innovent sans cesse, rendant la lutte contre la cybercriminalité complexe.**

Coordination entre les différents acteurs :

- **Une coopération efficace entre les collectivités, l'État et les acteurs privés est nécessaire pour faire face à ces menaces.**

Les solutions pour renforcer la cybersécurité des territoires

Renforcement des systèmes de protection :

- **Mise en place de solutions de sécurité robustes (antivirus, pare-feu, etc.), réalisation d'audits de sécurité réguliers, formation des équipes.**

Sensibilisation des citoyens :

- **Campagnes de communication pour informer les citoyens sur les risques liés à Internet et les bonnes pratiques à adopter.**

Coopération entre les collectivités :

- **Mise en place de réseaux de partage d'informations et de bonnes pratiques entre les collectivités.**

Soutien de l'État :

- **Développement de dispositifs d'aide financière et d'accompagnement technique pour les collectivités.**

Ce n'est un secret pour personne, 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.

La cybersécurité est donc devenue un enjeu stratégique croissant pour les territoires. En investissant dans la prévention et en adoptant les bonnes pratiques, les collectivités peuvent se prémunir contre les cyberattaques et préserver les intérêts de leurs citoyens.

Collectivités

Éric BERLIVET
Maire de Roche-La-Molière
Vice-Président de Mission Ecoter

Nicolas BARD
DSI Externe de la Mairie 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 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 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 d'honneur de Mission Ecoter, "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.

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.**

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.

Luc BOUARD
Maire de La Roche-sur-Yon
Président de La Roche-sur-Yon Agglomération
Conseiller départemental de la Vendée

L'ère des données face aux défis de la cybersécurité

À La Roche-sur-Yon, le numérique prend une place de plus en plus centrale. La gestion des services publics, la dématérialisation des démarches administratives et le déploiement de nouvelles infrastructures sont désormais étroitement liés aux technologies numériques. Avec l'essor de la ville intelligente et une gestion de plus en plus décentralisée, cette tendance ne fait que s'accélérer.

Si ces avancées sont synonymes de progrès, elles nous exposent aussi à de nouveaux risques. La dépendance accrue aux systèmes numériques rend des territoires comme le nôtre particulièrement vulnérables aux cyberattaques. En tant que collectivité, La Roche-sur-Yon et son agglomération mutualisent de nombreux services, ce qui implique la collecte et la gestion d'une grande quantité de données sensibles. Ces informations sont des cibles privilégiées pour les cybercriminels.

Les récentes attaques informatiques de collectivités ont démontré la gravité de ces menaces, qui ont terni l'image des administrations locales et perturbé durablement des services publics essentiels. Pourtant, les citoyens doivent pouvoir faire confiance à leur collectivité pour protéger leurs données.

Le respect du RGPD est désormais une norme pour les collectivités, mais il ne suffit pas. La protection des données personnelles ne garantit pas seulement la vie privée des citoyens, elle encourage également des pratiques responsables dans la gestion de ces informations. Assurer cette sécurité, c'est aussi s'engager à respecter des principes éthiques dans la gouvernance des données. La cybersécurité des données locales est donc un enjeu majeur pour maintenir la confiance des citoyens. Il est crucial que nos administrations adoptent une posture proactive et soient pleinement conscientes des défis techniques et éthiques que cela implique.

À La Roche-sur-Yon, nous sommes pleinement conscients de ces enjeux. Renforcer la cybersécurité au sein de nos structures est une priorité absolue, non seulement pour protéger nos infrastructures techniques, mais aussi pour garantir la sécurité de chaque citoyen.

Nicolas DESFACHELLE
Vice-Président de la Communauté Urbaine d'Arras,
Cohésion territoriale & mutualisation, tourisme & attractivité, numérique

CYBER MOIS #CYBERENGAGÉS 1er au 31 octobre 2024

Les 4 piliers de la cybersécurité dans la communauté urbaine d'Arras

Armer. La cybersécurité ? La communauté urbaine d'Arras n'a pas attendu d'être attaquée, ou ne serait-ce que la menace de l'être, pour se saisir du sujet. Comment ? En s'attachant d'abord l'expertise du meilleur des pare-feu qui soit : l'homme. Et quel homme ! Un tout petit plus petit que Wembanyama mais trois fois plus épais, longue barbe blanche, tatoué de partout : Eric est en quelque sorte le Hells Angels – Responsable Sécurité des Systèmes d'information (RSSI) en fait - de la direction mutualisée des services informatiques et technique (DMSIT) de la CUA, celui qui a la charge de mettre en fuite les chauffards du web, les terroristes du numérique, les vandales du digital. Un recrutement, donc. Voilà la première décision de la CUA pour gagner du temps et du terrain dans le domaine de la cybersécurité.

Mutualiser. Sans doute le mot « mutualisée » ne vous aura-t-il par ailleurs pas échappé ? Voilà en effet une autre idée cohérente de la communauté urbaine d'Arras. A vous qui gérez ou travaillez en collectivité, vous mesurez combien l'importance du travail en équipe est essentiel. Et pour qu'il soit le plus efficient possible, l'uniformisation des règles et des comportements est capitale. Cela s'applique aussi bien entendu aux outils informatiques et techniques déployés pour y parvenir. Se disperser dans les ustensiles comme dans les usages, c'est comme offrir une multitude de pièces d'un puzzle que les pirates, chercheurs de failles en or, se feront un plaisir de reconstituer.

D'où l'impérieuse nécessité d'une mutualisation, pour sécuriser le mieux possible les espaces et systèmes informatiques par lesquels transitent les informations échangées entre l'EPCI, ses communes membres et les usagers. Cet effort de mutualisation, c'est celui qu'accomplit aujourd'hui la CUA à l'échelle de ses 46 communes membres, mais aussi de ses services et de ses partenaires.

(In)Former. Mais le volet technique n'est pas le seul à prendre en considération. Ce serait trop simple, et voilà qui ne calmerait sans doute pas les ardeurs des délinquants. Et on en revient ainsi à l'humain, qui est à la fois la première faille et le premier bouclier. Pas question, bien entendu, de tatouer tous les élus, agents et usagers façon Éric - ce serait là trop brutal ! – mais il s'agit de ne jamais baisser la garde, et donc, in fine, de donner à toutes celles et tous ceux qui manipulent les outils et les données les clés d'un travail en toute (cyber)sécurité. Former, former encore, former toujours en quelque sorte. Parce que les techniques des hackeurs évoluent sans cesse, et qu'il faut évoluer avec elles, et contre elles. Les failles dites psychologiques sont sans nul doute plus dangereuses que les failles techniques ! Méfiance et vigilance doivent guider les pratiques. Et il importe donc à Éric et à ses pairs de la DMSIT de parfois se muer en flics (bienveillants) pour contrecarrer les voyous. Et ainsi éviter de devoir jouer aux pompiers…

Voilà comment la CUA entend à son échelle lutter contre la cybercriminalité. Sachant que le système n'est pas imparable, et qu'il ne faut pas non plus imaginer échapper à toutes les attaques. L'idée, c'est de faire en sorte, le jour où l'une d'elles sera déclenchée, d'en limiter au maximum l'impact, en étant capable d'y répondre le plus rapidement possible et surtout de préserver des « tirs » ennemis les données les plus critiques et sensibles.

Essaimer. Mais Éric et la DMSIT ne sont pas les seuls à se soucier de la cybersécurité. La direction du Rayonnement de la CUA, en charge de la stratégie et des usages du numérique, s'est-elle aussi intéressée à la question, qu'elle a d'ailleurs érigée en l'un des thèmes centraux de son rendez-vous professionnel bi annuel, le Numéricamp, en avril dernier. Au menu, notamment, une terrifiante simulation de cyber-attaque d'une collectivité, qui aura eu pour effet de convaincre les plus perplexes que le risque (et encore moins ses conséquences) n'est pas à prendre à la légère, suivie d'un plateau télé puis d'une table ronde au gré desquels journalistes, élus, techniciens, policiers et gendarmes experts en cybercriminalité auront confirmé que personne n'est à l'abri et qu'il n'y a rien de pire que d'imaginer qu'on l'est et qu'on le restera ad vitam aeternam. Parmi les intervenants conviés à en témoigner figurait Laurent Thellier, directeur du CESI, grande école d'ingénieurs implantée à Arras que la CUA accompagne financièrement pour structurer un Fab Lab Cybersécurité. Il s'agit là de former 200 jeunes par an en alternance dans des entreprises des Hauts-de-France aux compétences ad hoc dans le domaine industriel, et ainsi irriguer les PME du territoire, de les sensibiliser et de les aider à se protéger.

4 piliers… mais aussi 10 commandements (qui valent aussi dans la sphère privée !)

Des e-mails inhabituels et bizarres, tu te méfieras
De l'usage des clés USB, tu t'éloigneras
L'utilisation professionnelle de l'utilisation privée du matériel, tu sépareras
A la sauvegarde régulière des données, tu procèderas
De mettre tous tes documents dans un seul et même panier, tu éviteras
Aux mises à jour des logiciels, tu te plieras
Des téléchargements illicites, tu te garderas
Les outils installés et contrôlés par le service support, tu utiliseras
Un mot de passe fort, tu imagineras
La double authentification, tu favoriseras.

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

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**

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.

André FIGOUREUX
Maire 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.

Tony FLAHAUT
Directeur du Numérique, Communauté d'agglomération du Pays de Saint-Omer

Cybersécurité et Territoires : Protéger nos Collectivités locales face aux Cybermenaces

La transformation numérique de nos territoires apporte son lot d'opportunités, mais aussi de défis, parmi lesquels la cybersécurité se révèle être l'un des enjeux majeurs. A la Communauté d'agglomération du pays de Saint-Omer, il est de notre responsabilité de sensibiliser et d'accompagner nos communes et partenaires dans la mise en œuvre de mesures de cybersécurité robustes afin de protéger nos infrastructures, nos données et nos citoyens.

Comprendre la Menace : Un Enjeu pour Tous les Territoires

Les collectivités locales sont de plus en plus la cible de cyberattaques, qu'il s'agisse de rançongiciels (ransomware), de phishing, de vols de données ou de sabotages informatiques. Ces attaques ne concernent pas uniquement les grandes métropoles : nos territoires, quelle que soit leur taille, sont également visés. La vulnérabilité réside souvent dans des systèmes d'information moins bien protégés, des utilisateurs insuffisamment sensibilisés ou des ressources limitées pour faire face à ces menaces.

Conseils et Bonnes Pratiques pour les Collectivités

Pour garantir une sécurité optimale de nos systèmes et protéger les données sensibles des citoyens, voici quelques bonnes pratiques à adopter :

- **Sensibilisation et Formation : Les utilisateurs sont souvent le maillon faible de la chaîne de cybersécurité. Il est essentiel de sensibiliser et de former les élus, les agents territoriaux et les partenaires sur les risques et les comportements à adopter pour se protéger. A la CAPSO, c'est notre partenaire KAMAE, qui nous permet de mener cette campagne par le biais d'un espace ludique d'autoformation à la cybersécurité. Dans le cadre de ce cybermois, nous allons récompenser les meilleurs agents avec des goodies afin de maintenir une bonne appropriation de la solution et ainsi garantir la réussite de ce programme.**

- **Mise à Jour des Systèmes : Veiller à ce que tous les logiciels, systèmes d'exploitation et antivirus soient régulièrement mis à jour. Les correctifs de sécurité apportés par les éditeurs corrigent des vulnérabilités connues qui peuvent être exploitées par des cybercriminels. Ainsi, il peut être pertinent de s'abonner a des fils d'informations concernant ces découvertes de failles, et la publication des correctifs associés. La veille technologique reste un excellent rempart dans la lutte contre la cyber-malveillance.**

- **Sauvegardes Régulières : Effectuer des sauvegardes régulières et sécurisées de vos données. En cas d'attaque par ransomware, disposer de copies des données permet de rétablir le fonctionnement des services sans payer de rançon. Assurez-vous que ces sauvegardes soient également protégées contre les attaques. Un hébergement en dehors de votre SI peut être judicieux. Assurez-vous également qu'elles sont fonctionnelles en effectuant des tests de restauration réguliers.**

- **Sécurisation des Accès : Mettre en place une gestion rigoureuse des accès aux systèmes d'information. Utilisez l'authentification à deux facteurs (2FA) lorsque cela est possible, et veillez à ce que les mots de passe soient complexes et changés régulièrement. D'autre part, l'implémentation d'un bastion, permettra d'assurer la sécurité des connexions effectuées par des tiers ou partenaires sur vos infrastructures.**

- **Protection des Réseaux : Installer des pares-feux, des systèmes de détection et de prévention des intrusions (IDS/IPS) pour surveiller et contrôler le trafic réseau. Ces outils permettent de détecter des activités suspectes et de bloquer des tentatives d'intrusion. La mise en place d'un SOC managé peut également se révéler être une bonne option dans le cas d'équipes pas suffisamment dimensionnées pour assurer une surveillance constante sur la sécurité de votre infrastructure. Dans ce cas, une équipe de cyber analyste scrute les alertes de votre système et peut vous permettre de réagir très rapidement en cas d'attaque. Elle peut également vous assister dans « l'après » et favoriser un retour à la normale rapidement.**

- **Plan de Réponse aux Incidents : Préparez-vous à l'éventualité d'une cyberattaque en élaborant un plan de réponse aux incidents. Ce plan doit définir les actions à entreprendre en cas de cyberattaque, les personnes à contacter, et les procédures de reprise d'activité. Tester ce plan régulièrement est crucial pour s'assurer de sa pertinence.**

Solutions et Outils à Disposition des Territoires

Plusieurs solutions existent pour aider les collectivités à renforcer leur cybersécurité :

- **Les Centres de Veille et d'Alerte : Le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) proposent des alertes et des recommandations en cas de menaces émergentes. Dans notre cas, nous avons déjà pu juger des compétences du CSIRT Hauts de France, qui nous a accompagné lors de l'attaque d'une commune de notre territoire en juin 2023.**

- **Mutualisation des Ressources : Mutualiser les compétences et les outils entre collectivités permet de partager les coûts et de bénéficier de solutions plus robustes. La création de groupements de commande pour l'achat de solutions de cybersécurité peut s'avérer une approche gagnante.**
  A la CAPSO, notre service commun numérique nous permet, pour les communes qui souhaitent y adhérer, de proposer l'ensemble de ces outils et sécurisations des systèmes en s'appuyant sur notre équipe de techniciens et notre infrastructure.

- **Solutions Logicielles : Investissez dans des solutions logicielles adaptées aux besoins des collectivités, incluant des antivirus de nouvelle génération, des outils de gestion des accès (IAM), et des plateformes de surveillance des cybermenaces.**

- **Les sites Cybermalveillance.gouv.fr et ANSSI : Ces plateformes vous permettront de vous informer sur les menaces numériques et les moyens de s'en protéger. Vous y retrouverez des bonnes pratiques, des tutoriels, des guides complets afin de garantir un niveau de sécurité élevé sur votre système d'information.**

Un Engagement Collectif pour un Territoire Plus Sûr

La cybersécurité est l'affaire de tous. Au-delà des outils technologiques, c'est un engagement collectif qui doit animer nos territoires. Chaque acteur, qu'il soit élu, agent, partenaire ou citoyen, a un rôle à jouer dans la protection de nos systèmes. En adoptant des pratiques responsables et en restant vigilant, nous contribuerons ensemble à un espace numérique plus sûr pour notre territoire.
La Communauté d'agglomération du pays de Saint-Omer s'engage pleinement dans cette démarche en soutenant et en accompagnant ses communes pour relever ce défi.

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

De plus en plus de communes, grandes ou petites, sont victimes de cyberattaques avec de graves répercussions sur leur fonctionnement. On parle d'une attaque toutes les 30 à 40 secondes. Cette situation exige une prise de conscience collective ainsi qu'un solide dispositif de cybersécurité.

La Ville de Béthune est pleinement mobilisée dans la mise en œuvre de son plan d'actions visant à réduire les risques « cyber » qui pèsent sur la collectivité. Cette thématique a d'ailleurs été intégrée dans le projet d'administration qui est en vigueur depuis le début de l'année 2024. De ce fait, il ne s'agit plus d'un sujet investi seulement par notre Direction de la Transformation Numérique mais bien d'un sujet commun à l'ensemble des services. Des opérations d'alerte et de sensibilisation auprès de chaque agent sont d'ailleurs régulièrement menées, en lien avec les facilitateurs du numérique, un dispositif basé sur le volontariat.

Dans le même ordre d'idée, pour être bien accompagnée, la Ville a répondu au nouvel appel à projets France 2030 de l'ANSSI.
Notre objectif est de renforcer notre niveau de protection en élaborant une politique de sécurité numérique globale et en rédigeant un plan de continuité d'activité. Ce plan permettra de mettre en place une gestion de crise optimale mais aussi d'être mieux préparé en cas d'incident cyber.

Nous allons également renforcer les liaisons avec nos prestataires afin de sécuriser au maximum les interventions sur nos outils et infrastructures numériques par la mise en œuvre d'un « bastion » d'administration.

Dans cet esprit, nous augmentons la sécurisation du réseau wifi public afin de permettre une utilisation en toute sécurité des services par les usagers.

Nous sommes donc entrés dans une phase d'amélioration continue de la cybersécurité qui n'est pas une fin en soi. Il s'agit finalement d'une somme d'actions quotidiennes qui doivent avoir pour résultat une atténuation des menaces identifiées dans le plan d'actions.
Nous profiterons naturellement du cybermoi/s, pour communiquer et organiser des actions internes autour de cette thématique.

Afin de donner d'autres perspectives, nous engageons une réflexion avec notre intercommunalité - la Communauté d'Agglomération Béthune Bruay Artois Lys Romane – pour travailler sur un projet de mutualisation de nos ressources dans le domaine de la cybersécurité.

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

Nadège HORNBECK

Adjointe au Maire de Sélestat chargée de la Ville de Demain, de la Communication et du Numérique
Vice-Présidente de la Région Grand Est chargée de la Santé, de la Prévention et du Handicap
Vice-Présidente de Mission Ecoter

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.

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.

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.

Karine LAURO

Ingénieure chargée de transition numérique, Saint-Lô Agglo

Regards croisés, sécurité numérique et numérique responsable

En 2020, selon le CLUSIF, 30% des collectivités territoriales avaient été victimes d'une attaque au rançongiciel. Le caractère exponentiel des cyberattaques avait poussé l'ANSSI à se déclarer en 2021 "inquiet pour la cybersécurité des collectivités territoriales".

Face au risque grandissant, l'Etat a souhaité la mise en place d'un ensemble de dispositifs de lutte contre la cybercriminalité : en premier lieu les CSIRT, computer security incident response teams, centre de secours et d'assistance aux victimes de cyber-incident à l'échelle régionale. Puis, le service VIGINUM, administration de vigilance et de protection contre les ingérences numériques étrangères et les fausses informations.

Le législateur a ensuite transcrit dans le droit français les directives européennes du digital service act et du digital market act. La loi du 21 mai 2024 visant à sécuriser et réguler l'espace numérique, prévoit ainsi la mise en place d'un filtre anti-arnaque.

Par voie de conséquence, le numérique est au cœur des enjeux de sécurité nationale et européenne et pose un défi sociétal et d'autant plus à l'aune de l'émergence de l'intelligence artificielle : des crypto-arnaques, tentatives d'escroquerie via les cryptomonnaies sous une fausse identité simulée par intelligence artificielle générative, ont désormais fait leur apparition.

Des instances étatiques expertes en cybercriminalité, des textes législatifs et règlementaires, des pare-feu, anti-virus, annuaires de confiance, infrastructures sécurisées et la prise de conscience co-existent, pour autant, la menace d'origine cyber n'a jamais été aussi prégnante au sein des collectivités territoriales concernées à hauteur de 42% du total des cyberattaques.

Au regard de la montée en puissance de la cybercriminalité par-delà tous les moyens dissuasifs actuels, il convient de s'interroger sur :

- **Quelle stratégie territoriale explorer pour un environnement numérique de confiance ? (I) ;**
- **Quelle gouvernance pour asseoir la garantie de la cybersécurité et le respect des droits et libertés ? (II)**
- **Un cas d'école, la cybersécurité des territoires connectés et durables (III)**

(I) Le numérique responsable, pour engager concrètement les territoires à la cyber-vigilance

Selon l'étude 2023 du groupement d'intérêt public 'cybermalveillance.gouv.fr', les collectivités territoriales bien que conscientes des risques et des enjeux de la cybersécurité rencontrent souvent des difficultés à l'évaluation de leur degré de vulnérabilité.

Or, l'un des leviers à la mesure de l'exposition au risque s'inscrit potentiellement dans les démarches de labellisation. En effet, suivre les principes d'action d'un label qualité orienté numérique revient à mettre en œuvre les cadres règlementaires et législatifs. L'élaboration du référentiel numérique responsable s'est ainsi foncièrement inspirée du cadre européen sur la protection des données à caractère personnel. Le label numérique responsable impose de “collecter uniquement les données nécessaires lors de la création d'un nouveau service numérique” puis, “d'informer les utilisateurs de l'usage qu'il sera fait de leurs données” et “de sécuriser le stockage, l’archivage et la suppression des données selon des conditions fixées en interne ». Pareillement, l'on peut penser que les prochains référentiels sur la régulation de l'intelligence artificielle (IA) pour une IA éthique et frugale s'inspireront aussi des règles européennes émergentes du digital service, market et IA act.

Ainsi, les labels, ‘numérique responsable’, les certifications, ‘SecNumCloud’ sont autant d'atouts pour évaluer le risque cyber et construire un environnement de sécurité numérique.

En fait, le label pose un cadre, le périmètre pour agir. Il clarifie la mise en situation. Car, c'est le référentiel sur lequel repose le label qui fournit ainsi les clés pour agir en précisant là où des mesures sont à prendre, là où il convient de regarder et faire preuve de vigilance. Alors, le label est un outil que l'on peut comme tous les outils, exploiter à tort de manière inconsciente et irresponsable et l’on parlera de greenwashing ou bien que l'on puisse exploiter à raison et c'est le numérique responsable éthique au sens de la loi de réduction de l'empreinte environnementale du numérique. L'environnement numérique se bâtira alors dans l'esprit des trois piliers du développement durable écologiques, économiques et sociétaux et des principes démocratiques de l'attention aux droits et libertés.

L'acculturation pas-à-pas à la sécurité étant pourvue par l'engagement concret dans la démarche de labellisation numérique responsable, le référentiel encourage à organiser la gouvernance de la stratégie de sécurité numérique.

(II) La gouvernance collégiale, pour mettre en place une stratégie de cybersécurité territoriale responsable

La stratégie numérique tend à définir de nouveaux paradigmes fonctionnels. Le défi est de réussir à trouver un équilibre entre des stratégies divergentes du ‘tout numérique’ au ‘tout papier’.
La gouvernance de la sécurité numérique s'entend donc de manière raisonnée et responsable. Pour ce faire, il est possible d'appliquer des méthodologies telles celles issues de la pensée créative et d'établir de manière précise la cartographie des processus fonctionnels et des parties-prenantes pour pouvoir concevoir des services et systèmes adaptés et maîtrisés. Car, le facteur humain est l’un des éléments clé de la sécurisation et de la résilience des systèmes. D'où l'intérêt d'envisager la conduite des projets de sécurisation sous une vision centrée utilisateur. Toutefois, il ne s'agit pas de basculer dans le travers inverse du secret et finalement par trop de restriction annihiler la fluidité de circulation de l'information agissant à l'encontre des collaborations, coopérations et transversalités. De plus, souplesse et agilité sont nécessaires par le caractère très organisé et expert des réseaux de cybercriminalité obligeant à une révision régulière des plans de prévention, de continuité et de reprise d’activité.

Par conséquent, sécurité et insécurité numérique sont tout autant impactantes pour le fonctionnement des organisations. Et la gouvernance du numérique doit se construire dans un esprit responsable et de responsabilité.

Car, si l'enjeu sociologique et comportemental au travers des démarches qualité et de labellisation peut s'affirmer comme un vecteur structurant de la stratégie de cybersécurité responsable, le succès d'une bonne défense dépend aussi de la capacité à engager l'ensemble de ses parties-prenantes notamment externes à l’image du syndicat mixte Manche numérique où lors de la rencontre cloud, datacenter, territoires et données souveraines 2024, Jérôme Lamache, directeur des services numériques précisait l’aspect de la cybersécurité lié à “la certification iso 27001 et du SecNumCloud”. Le numérique est ainsi à considérer nécessairement de manière collégiale en association à la comitologie des exécutifs et de la direction générale des organisations et au plus haut niveau de responsabilité.

(III) L'hybridation des solutions, pour faire face aux vulnérabilités humaines et techniques
La cybersécurité sous le prisme des territoires connectés et durables,

La cybersécurité relève d'une matérialité tangible. Car il existe des systèmes physiques, des matériaux, composants d'infrastructure technique que l'on peut exploiter à des fins délictueuses alors, la cybersécurité est nécessaire. L'humain et plus globalement la responsabilisation des individus, notamment sous l'impulsion des démarches de labellisation numérique responsable, n'est qu'un élément de l'ensemble des stratégies pour parer aux vulnérabilités des systèmes informatiques.

La cybersécurité des réseaux d'objet connecté présente quatre points de vulnérabilité :
D'abord l'objet communiquant en soi et le transport du signal, qui tous deux se font en environnement hertzien et constituent autant de potentialité de détournement. Sur le flux de communication, le chiffrement et la cryptographie des trames du signal en sortie d'objet connecté reviennent à la mise en place d'un premier niveau de sécurité pour freiner les tentatives de détournement du signal. Le chiffrement est ainsi un facteur de dissuasion.
Puis, l'autre pan de la sécurisation est la détection des intrusions et pourrait revenir à la mise en place de système d'émulation des différentes interfaces homme-machine pour en observer une activité potentiellement anormale et pallier aussi toutes les failles de sécurité liées à l'erreur humaine et la négligence.

Ensuite, l'objet dès sa conception peut lui-même comporter des failles de sécurité.

Enfin, il y a le stockage et l'hébergement où parfois, plutôt que le choix vers le décloisonnement par l'infonuagique, il est préféré le centralisme d'un hébergement sur site. En effet, du point de vue de Jérôme Lamache, sur l'hébergement, il s'agit "de réfléchir à des datacenters de proximité avec la vraie question de réfléchir à quelle échelle…départementale, régionale. On voit bien qu'un datacenter unique n'a pas d'intérêt en tout cas, n'est pas suffisant, on est vraiment sur du réplicable, on est déjà répliqué avec des datacenters du département de la Manche mais il serait plutôt de bon aloi de commencer à regarder des datacenters sur trois sites d'où l'intérêt de travailler au niveau régional. Et la difficulté pour les collectivités, c'est aussi de comprendre la nécessité de stocker ses données sur des lieux mutualisés, nous avons 450 collectivités, 400 serveurs potentiellement sous des escaliers, dans des greniers, dans des sous-sols donc il y a un vrai enjeu de mutualisation avec les technologies actuelles de virtualisation et d'efficacité également. "

En vérité, la robustesse des systèmes pourrait relever de choix techniques mixtes et hybrides. Ainsi, sur l'hébergement, la cybersécurité est intimement liée à la capacité d'isolement des briques architecturales et découle du dosage entre internalisation et externalisation. Toutefois, l'externalisation interroge sur le cadre règlementaire, potentiellement souverain et protecteur de l'usage des informations et des données essentielles.

Et pour conclure, s'il convient de définir les clés de réussite d'une stratégie de cybersécurité responsable, en trois mots : écoresponsabilité, collégialité, hybridation.

Émile Roger LOMBERTIE

Maire de Limoges
Vice-président de Limoges Métropole en charge du développement économique et de la protection des données
Président d'Ester technopole

Limoges, l'autre grande ville numérique !

L'accès au numérique et la ville intelligente sont initiés au sein de la Ville de Limoges. La ville numérique est une ambition dont l'objectif est d'améliorer la qualité de vie des habitants. Grâce aux nouvelles technologies, la gestion et l'organisation de la plupart des services et dispositifs qui participent au cadre de vie (infrastructures publiques, énergie, gestion des réseaux, circulation, e-services) sont pensés pour gagner en efficience.

Aujourd'hui, nous poursuivons la réflexion pour rendre la ville plus écologique, plus intelligente, plus autonome et respectueuse de la nature à travers le numérique. Tous nos services et directions internes sont impliqués dans cette démarche proactive. Le concept de ville numérique intègre divers dispositifs physiques connectés au réseau. Il contribue à optimiser l'efficacité des services urbains et à se connecter aux citoyens.

« Limoges : la grande ville à la campagne » jouit aussi d'un contexte local favorable au développement des usages du numérique : elle détient son propre réseau fibre, elle est lauréate du prix de la meilleure transformation de zone urbaine et enfin elle est porteuse d'une culture sur le territoire intégrant une politique volontariste d'aménagement numérique. La Ville de Limoges est aussi un moteur régional avec le lancement de la smart city dans un contexte économique du numérique dynamique.

Et puis Limoges a une réelle réputation internationale en cryptologie grâce à des laboratoires universitaires de rang mondial dans ce domaine comme X-LIM, en relation étroite avec 150 entreprises spécialisées en cybersécurité. Cela permet de proposer une offre de formation importante et de fédérer une communauté French Tech Limousin parmi les plus actives.

Le mercredi 13 décembre 2023, pour faire face à la cybermenace et accompagner l'écosystème économique local, nous avons lancé, au nom de la Communauté urbaine Limoges métropole, la création d'un Centre de Ressources en Cybersécurité (CRC), avec l'appui de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). L'enjeu d'acculturation collective est grand et les cyberattaques concernent aujourd'hui indifféremment des organisations de toutes tailles et de toutes natures : les TPE-PME (40 %), les collectivités territoriales (23 %), les établissements de santé (10 %), les établissements d'enseignement supérieur (8 %) et les entreprises stratégiques (6 %). Une de nos grandes entreprises et un centre hospitalier local en ont fait les frais il y a peu de temps.

Autre chantier dans lequel Limoges est partie prenante : la sécurisation des données de santé. Nous participons à la création de la chaire d'excellence en cybersécurité, vie privée et trust pour la santé (CV-Santé) créée au sein de l'université de Limoges. Cette dernière est la seule à faire partie du Centre international en cybersécurité et fédère une équipe pluridisciplinaire autour de la protection des données médicales du patient et au-delà, de toutes les informations échangées au quotidien via nos outils connectés. Limoges dispose d'un CHU lui aussi impliqué dans cette réflexion incontournable à travers le dossier patient.

Comme beaucoup d'autres territoires, il nous faut anticiper pour ne pas subir. Entre modernisation et accessibilité de nos services, protection des concitoyens et continuité de l'action publique, nous sommes à la croisée des chemins. Sans piloter un pied sur l'accélérateur et un autre sur le frein au risque de rester sur place, bâtir des systèmes interconnectés qui génèrent une amélioration de l'activité économique autant que facilitent la vie quotidienne, nécessite autant la confiance partagée des acteurs locaux que leur envie de faire ensemble. Et c'est bien là que réside le rôle du politique, permettre que ce petit miracle s'accomplisse jour après jour.

Daniel MARECHAL
Directeur des systèmes d'information
Redon Agglomération

Cybersécurité et Territoires

De plus en plus connectés, nos territoires doivent faire face au défi toujours plus grand de la cybersécurité. Les cyberattaques ne cessent de croître, accentuées par le contexte géopolitique que nous connaissons.
Conscients des risques, leurs moyens restent toutefois limités. C'est d'autant plus vrai pour les plus petites entités.

C'est le constat que nous dressons, après avoir engagé des audits auprès de nos communes membres, réalisés par notre direction des systèmes d'information.

Il en est ressorti un niveau de maturité Cyber évalué à 25%, beaucoup trop juste pour faire face aux menaces, avec une réelle difficulté sur le manque de moyens, partagée par la majorité de nos communes. REDON Agglomération, 68 000 habitants, est un territoire rural, regroupant 31 communes, dont 24 ont moins de 3 000 habitants.

Il nous parait essentiel que l'EPCI soit le bon échelon pour répondre à cette situation. Notre collectivité a donc décidé de créer en 2022 un service commun informatique pour accompagner les mairies sur la mutualisation du numérique et l'élévation de leur niveau de cybersécurité. Dix-huit d'entre elles ont rejoints notre service.

Nous leur avons proposé une stratégie Cyber basée sur les sept fondamentaux suivants :

- **La cybersécurité est une dépense vitale. Se défendre a un coût**
- **Importance de sensibiliser les agents, les élus, les fournisseurs,**
- **Principe de tout fermer par défaut, notamment les ports du pare-feu, principale porte d'entrée à l'internet**
- **Bien identifier les surfaces d'attaques, les portes d'entrée, les différents accès autorisés,**
- **Principe d'une défense en profondeur, en segmentant le réseau (l'objectif est de limiter**
- **L'impact de l'attaque si celle-ci a réussi à pénétrer le système d'information),**
- **Importance d'un plan de sauvegarde et d'une durée de rétention suffisante (allant jusqu'à 12 mois). Les attaques contiennent bien souvent un agent "dormeur", généralement déposé sur un ordinateur, qui n'est pas détecté par l'antivirus et qui peut s'activer plusieurs mois après**
- **Être préparé à gérer une crise**

Techniquement, pour limiter la surface d'attaque, nous avons déployé un cloud privé, reliant directement les communes adhérentes à notre salle Datacenter. Celle-ci dispose d'outils avancés, comme une sonde de détection des intrusions (renifleur).
La cybersécurité étant un chantier permanent, notre direction des systèmes d'information supervise quotidiennement les actifs sécurité déployés au sein des mairies, comme les pares-feux périmétriques.

La mutualisation, l'expertise et le partage financier permis par le service commun informatique nous semble être une réponse particulièrement appropriée, soulageant le niveau de responsabilité des petites mairies et confortant une relation gagnante – gagnante entre notre intercommunalité et les communes de notre territoire.

Nathalie POIGNON
Directrice du service communication
Ville de Marseillan

Création de vidéos humoristiques pour sensibiliser les agents communaux aux cyberattaques

Face à l'augmentation des cyberattaques ciblant les administrations publiques, il est devenu essentiel de sensibiliser les agents communaux aux risques numériques et aux bonnes pratiques de cybersécurité. Plutôt que de miser sur des formations classiques, souvent perçues comme fastidieuses, la mairie de Marseillan a fait preuve de créativité en développant des vidéos humoristiques scénarisées et jouées par les agents eux-mêmes.

Un projet innovant piloté par le service communication

L'initiative de créer ces vidéos a été insufflée par le service communication qui a identifié un double enjeu : sensibiliser tout en captivant l'attention des agents, souvent réticents face à des contenus trop techniques. En choisissant de traiter le sujet des cyberattaques sur un ton humoristique, le service communication a voulu désamorcer la gravité apparente du sujet, tout en rendant l'apprentissage des bonnes pratiques plus accessible et agréable.

Ainsi l'humour devient ici un vecteur de sensibilisation : en tournant en dérision des situations du quotidien où la vigilance numérique est nécessaire (ou souvent oubliée), ces vidéos permettent de faire passer des messages clés sur les comportements à adopter sans paraître moralisatrices.

Les agents communaux, acteurs de leur propre sécurité numérique

La particularité de ce projet réside également dans le fait que les agents communaux eux-mêmes se mettent en scène dans les vidéos. Ce choix a plusieurs avantages :
Proximité et identification : en voyant leurs collègues ou eux-mêmes dans les situations représentées, les agents se reconnaissent plus facilement et se sentent directement concernés par le message. L'effet miroir est amplifié, ce qui renforce l'impact de la vidéo.
Humour authentique : les situations vécues par les agents au quotidien sont réinterprétées de manière légère et comique, ce qui permet de dédramatiser les erreurs ou les failles humaines tout en montrant l'importance de ne pas les reproduire.

Engagement des équipes : faire participer les agents à la réalisation des vidéos stimule leur implication dans la démarche de cybersécurité. Ils deviennent non seulement spectateurs, mais aussi acteurs de leur propre protection numérique.

Un contenu scénarisé autour de scénarios quotidiens

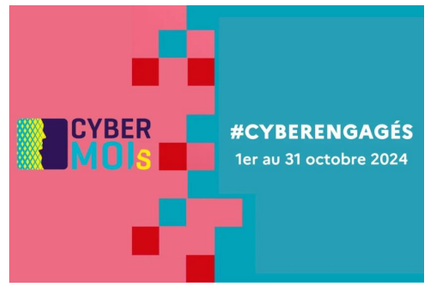
Les vidéos, bien qu'humoristiques, reposent sur un travail scénaristique minutieux. Chaque vidéo présente une situation commune au sein des services municipaux, où des erreurs de cybersécurité peuvent survenir, souvent sans que les agents ne s'en rendent compte. Parmi les scénarios développés :
Le partage involontaire d'informations sensibles : Un agent communique ses mots de passe, illustré de manière exagérée pour marquer l'absurdité du geste.
Le téléchargement par clef USB : Un autre agent ouvre un fichier joint provenant d'une clef USB anonyme, entraînant la compromission du réseau interne de la mairie, avec une mise en scène humoristique où tout le système semble s'effondrer.
L'utilisation de mots de passe faibles : Ce classique est traité de façon comique avec une mise en scène émanant d'un jeu connu.
Ces scénarios illustrent, de manière caricaturale mais percutante, les risques de comportements négligents en matière de cybersécurité.

Un projet fédérateur et engageant

Au-delà de la sensibilisation, ces vidéos ont permis de renforcer l'esprit d'équipe entre les différents services communaux. En participant à l'élaboration et au tournage des vidéos, les agents ont découvert un autre aspect de leur environnement de travail, tout en prenant conscience de la responsabilité partagée en matière de cybersécurité.

La création de ces vidéos humoristiques mettant en scène les agents eux-mêmes pour sensibiliser aux cyberattaques est une approche innovante et efficace. En rendant l'apprentissage amusant et participatif, Le service communication de la mairie de Marseillan démontre qu'il est possible de traiter un sujet sérieux tout en suscitant l'adhésion des équipes. Ce type de démarche prouve que la sensibilisation à la cybersécurité peut se faire de manière créative, tout en renforçant la cohésion des équipes autour d'un enjeu sensible et commun.

Lionel MONTILLAUD
Maire de Sainte-Hélène



Cybersécurité et Territoires
« 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. 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 !

Emmanuel QUERE
Directeur adjoint du Syndicat Départemental d'Energie et d'Équipement du Finistère

Souveraineté et sécurité des données dans le projet Finistère Smart Connect

Principes de gestion et d'utilisation des données collectées
Les données sont collectées, stockées et gérées dans les systèmes de gestion de bases de données du SDEF. Elles sont mises à disposition des partenaires pour les données qui les concernent. Les partenaires demeurent propriétaires de leurs données et peuvent en disposer librement. Le SDEF ne peut donc diffuser ou exploiter ces données sans leur accord. La diffusion des données en open data relève, naturellement, d'une décision du propriétaire de la donnée.

Les données actualisées sont mises à disposition des partenaires pour leurs besoins propres, sur une plateforme et des applications dédiées ou via des API. Les partenaires disposent d'un compte utilisateur afin d'avoir un accès à la plateforme et aux applications « métiers ». Pour ce faire, le SDEF gère un système d'identification des utilisateurs, protégé par login et mot de passe.

Connexion sécurisée du serveur SDEF dans le datacenter
Les serveurs du SDEF, sont hébergés chez Bretagne Telecom à Chateaubourg (35). Ils sont connectés au réseau de transit via deux liens opérateurs, protégé par deux équipements SDWAN connectés simultanément à deux liens opérateurs via un réseau d'interconnexion. Des liens de 2x100 Mbps sont activés et peuvent augmenter jusqu'à 10Gbps sur commande.

Les matériels proposés permettent cette évolution de débit des accès opérateurs. Ils supportent jusqu'à 1000 liens VPN simultanément (soit 1000 passerelles).

Les fonctions qui sont déployées sont les suivantes : Stateful firewall, Auto VPN self-configuring Site-to-site VPN, Intrusion detection & prevention (IDS/IPS), Advanced Malware Protection, (AMP), Layer 7 applications visibility &Traffic Shaping, Application priorization. Les fonctions Auto VPN sont utilisées pour connecter les équipements de sécurité placés au niveau des passerelles, au cœur de réseau.

Deux commutateurs sont utilisés pour connecter les serveurs, les équipements de stockage et de calcul et les équipements SDWAN du datacenter du réseau du SDEF.
Un second datacenter (Cogent) est mobilisé à Rennes. Des équipements, dédiés au projet (sécurité, serveur PRA, sauvegarde) sont installés dans ce 2ème datacenter. L'ensemble des données et images du serveur situé sur le site de production sont sauvegardés sur les équipements hébergés dans le 2ème datacenter. En cas de perte des services du datacenter principal, un plan de reprise d'activité des services critiques sous 48 heures et la reprise des services métiers sous 96 heures.

Connexion sécurisée des passerelles LoRaWAN au réseau de collecte

Un très fort niveau de sécurisation du réseau est en place, depuis les passerelles LoRaWAN, jusqu'au datacenter : les capteurs cryptent les données AES 128 bits jusqu'à la passerelle et au réseau LoRaWAN, les passerelles LoRaWAN sont connectées sur des boitiers de sécurité disposant de fonctionnalités de firewall, détection et prévention d'intrusion, anti malware et filtrage applicatif de niveau 3 et 7. Ces fonctions protègent les passerelles d'attaques venant des réseaux opérateurs ou des accès Internet.

Deux tunnels VPN connectent les équipements de sécurité associés aux passerelles LoRaWAN vers les équipements et serveurs du SDEF. Des fonctions Auto-VPN calculent les tunnels en cas de perte du lien opérateur ou de défaut d'un équipement central.

Évolution de connexion sécurisée des passerelles LoRaWAN au réseau de collecte

Les données entre les passerelles et le LNS étant déjà sécurisées et cryptées, le boitier firewall sera dans le futur remplacé par une connexion APN privée, cela afin de réduire les coûts et le matériel sur site. Le niveau de sécurité restera, pour autant, adapté au besoin.

Supervision et cybersécurité

La supervision est constituée d'un ensemble de serveurs et de postes de travail qui réalisent la centralisation et le stockage des flux. Ils permettent leur analyse et l'administration du parc de capteurs.

Modalités de stockage des données

Le datacenter où sont stockées les données bénéficie d'un niveau de sécurité Tier 3+ - ISO 27001 et fournit des baies 42U, une alimentation électrique secourue, une climatisation secourue et des liens opérateurs de 50Mb/s à 10Gb/s.

Le datacenter est connecté au réseau de transit via deux liens opérateurs protégés par deux équipements SDWAN connectés simultanément aux deux liens opérateurs via un réseau d'interconnexion. Ils supportent jusqu'à 1000 liens VPN simultanés.

Entreprises

Thierry ELKAIM
Directeur du Développement
Partenariat Paris 2024
Cisco France

Cybersécurité : quels enseignements tirer des Jeux de Paris 2024 ?

Le constat est simple et unique : absolument aucune cyberattaque n'a eu d'impact sur le bon déroulement des Jeux.

Pourtant, comme l'a dit l'ANSSI, les attaques ont bien existé, de manière intense. Elles avaient déjà visé le COJOP avant les Jeux, et se sont poursuivies dès le jour de la cérémonie d'ouverture, jusqu'à la clôture. Rien de très nouveau : des attaques en masse de déni de service (DDOS), du phishing (hameçonnage), des tentatives d'intrusion sur le réseau des JO, mais aussi des tentatives d'intrusion physique sur des sites informatiques… De manière indirecte, de nombreuses escroqueries ont visé aussi le grand public via des sites de ventes de faux billets ou de fausses boutiques de merchandising Paris 2024.

Alors pourquoi une telle réussite ? 4 raisons majeures se dégagent :

1) La prise de conscience du danger en amont

Le constat des Jeux de Tokyo en 2021 était alarmant : 450 millions d'incidents cyber, et par extension 4 Milliards d'évènements au total.
Ces chiffres ont réveillé très tôt les esprits et fait prendre conscience du grand danger cyber qui pesait sur Paris 2024, le plaçant au même niveau que la menace terroriste.
(On s'apercevra par la suite que le nombre d'incidents et d'évènements cyber ne sont pas forcément significatifs, sachant qu'une seule attaque organisée correspond à des milliers d'incidents et des milliards d'évènements).

Dès 2021, certains professionnels de la sécurité estimaient que ces nombres fulgurants de Tokyo pourraient être multipliés par huit à l'occasion de Paris 2024, en tenant compte des avancées technologiques, de l'automatisation et la multiplication générale des attaques à venir, mais aussi de l'extension de la surface d'exposition (plus d'objets connectés grâce au progrès de la technologie dans les stades, et donc plus d'incidents et d'évènements cyber…).

2) La sensibilisation et la responsabilisation de tous

Des juillet 2022, la responsabilité du pilotage de la stratégie de prévention des cyberattaques, en vue des Jeux, est confiée à l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

S'en suivront de nombreuses actions de sensibilisation menées auprès de tous les acteurs de l'écosystème, qu'ils soient publics ou privés, en partant du principe que c'est toute la chaine de fourniture des Jeux, la Supply Chain, qui serait visée. (Et donc pas seulement le système d'information du COJOP étendu aux stades).
Dès lors, au sein de l'Etat, des entreprises de l'écosystème, et des villes hôtes, a été mise en place une gouvernance cyber en vue des JOP.

3) La préparation

Coté COJOP, la très compétente équipe interne a conçu un solide système opérationnel de défense et de résilience, en s'appuyant sur des professionnels :

- **Atos/ Eviden, pour gérer le Cyber Centre d'Opérations de Sécurité (CSOC)**
- **Cisco, pour alimenter le CSOC avec ses technologies les plus éprouvées (XDR, gestion des vulnérabilités, protection internet, firewalls, double authentification, contrôle d'accès au réseau, etc. etc.) entrainées à détecter et à répondre à tous types d'incidents de manière réactive. Talos son service de connaissance de la menace mondiale a également participé aux opérations.**

Pendant plusieurs mois, le dispositif a été maintes fois rodé à travers des exercices de préparation, des simulations d'attaques de tous types, de gestion de crise et de reprise d'activité ou des audits de stade, permettant d'arriver le jour J en totale confiance.

4) La coordination

La qualité des renseignements recueillis, mais surtout la capacité à les partager, les comprendre et à les traiter rapidement de manière collective et immédiate, grâce à une coordination exemplaire, ont été certainement clé dans cette réussite.
On pourra noter au passage que Franz Regul, le RSSI du COJOP, a su mobiliser autour de lui toutes les énergies, de manière transverse, au-delà de sa propre organisation. Il a notamment réuni l'ensemble des RSSI des partenaires de Paris 2024 et des collectivités hôtes, au sein d'un club, qui s'est réuni mensuellement des janvier 2024, et quotidiennement pendant les JOP.

Enfin une autre explication plausible de cette performance, est que les cyber bandes organisées ne souhaitent pas perdre de temps à lancer des attaques super sophistiquées, quand ils comprennent que la cible est à ce niveau de préparation et de protection, comme ce fut le cas pour Paris 2024.

Pour ce qui est des attaques de moindre sophistication, souvent lancées au hasard et de manière aléatoire et qui viennent alimenter les millions d'incidents, elles n'impactent que les entreprises ou collectivités les plus vulnérables, car moins concernées par le sujet.

Aussi, si vous suivez les 4 principes ci-dessus, prise de conscience, responsabilisation, préparation et coordination, vous êtes normalement bien armés pour faire face….

Pour mémoire, Cisco était partenaire officiel de Paris 2024 sur les équipements réseaux, les infrastructures de cybersécurité et les logiciels de visioconférence.

Maxime GEFFRAY
Responsable communication - Oodrive

Sécurité numérique : enjeux et solutions pour les territoires et les collectivités en 2024

Les cyberattaques dans les territoires et collectivités ne cessent de croître, alors même que ces institutions sont au cœur de leur transition numérique.
De janvier 2022 à juin 2023, l'ANSSI a traité 187 incidents concernant des collectivités, 89% d'entre elles disent avoir été la cible de cyberattaques.

Objectifs lucratifs, déstabilisation, compromissions en lien avec des opérations d'espionnage étatique, les motivations sont grandes pour les attaquants visant ces acteurs de premier plan, qui apparaissent parfois comme des proies faciles.
De plus en plus connectées, les collectivités territoriales françaises doivent faire face au défi toujours plus grand de la cybersécurité. Quelle importance revêt la menace du piratage informatique au sein des administrations locales à ce jour ? Et quels moyens peuvent-elles mettre en œuvre afin de s'en prémunir ?

État des lieux de la cybersécurité au sein des territoires français

Des collectivités conscientes des risques mais aux moyens limités

Selon une étude menée en 2023 par OpinionWay pour le compte de Cybermalveillance.gouv.fr, près d'une collectivité sur deux s'estime exposée aux menaces informatiques.
Toutefois, 65 % d'entre elles allouent moins de 5 000 € par an à leur budget IT. Par ailleurs, 75 % des élus dépensent moins de 2 000 € par an pour la protection numérique.

Ces chiffres sont à mettre en regard du coût estimé des cyberattaques sur les collectivités territoriales. D'après le centre régional de cybersécurité de Bourgogne-Franche-Comté (CSIRT), les piratages informatiques ont coûté près d'un million d'euros à la région au cours du dernier trimestre 2023.

Les enjeux multiples de la protection numérique
Le contraste entre l'impact potentiel des attaques informatiques sur les collectivités et le niveau de sécurité employé pour les contrer s'explique par différentes raisons.
À ce titre, la décentralisation des services de l'État et la multiplication des flux d'informations ont un impact considérable.

On estime en effet que 20 à 25 % des données détenues par les territoires sont de nature sensible ou critique.
La manipulation de ces données par les élus implique un accompagnement budgétaire et des compétences IT qui leur font souvent défaut.

20 % des collectivités déclarent ne pas être en mesure d'estimer leur exposition aux risques informatiques. (Enquête OpinionWay)

Il est aussi à noter que les petites entités sont de plus en plus touchées par les piratages. En effet, les villes moyennes sont généralement moins protégées et donc plus vulnérables face aux hackers.

De nombreuses réglementations entourent le sujet de la cybersécurité afin de permettre aux collectivités d'asseoir leur souveraineté numérique.

Dernière en date, la directive NIS 2, adoptée au Parlement européen, devra s'appliquer aux communes de plus de 30 000 habitants. Cette nouvelle réglementation entrera en vigueur en France au plus tard au deuxième semestre 2024.
Denis Thuriot, président de l'association Mission Ecoter, œuvre notamment dans le but d'accompagner les collectivités dans leurs transformations numériques.

Particulièrement engagé dans les thématiques de l'innovation et de la cybersécurité, il reconnaît les challenges auxquels font face les collectivités en matière de sécurité informatique tout en mettant en avant la responsabilité des élus dans ce domaine. Également maire de Nevers, Denis Thuriot a ainsi investi 250 000 € dans un plan de sécurisation sur trois ans, affichant clairement la protection numérique comme une priorité.

Bonnes pratiques et solutions en matière de sécurité informatique

La vigilance de l'utilisateur : un point déterminant
La grande majorité des brèches de cybersécurité (68 à 70 % des cas) est causée par une erreur humaine : en général l'ouverture d'un mail frauduleux.

Webinar : sécurité numérique pour les territoires et collectivités

Découvrez comment renforcer la sécurité informatique au sein des territoires et collectivités locales.

Voir le replay

À ce titre, la formation et l'acculturation des personnes sont de toute première importance. Parmi les actions à mettre en place au sein des institutions, nous pouvons noter :

- **Élaborer une procédure écrite et acculturer les partenaires :**

Les collectivités se doivent de sensibiliser leurs collaborateurs et partenaires aux risques. Par exemple, l'organisation de fausses campagnes de phishing au sein des administrations locales et des organisations prestataires est un moyen d'avertir sur l'une des pratiques frauduleuses les plus courantes sur Internet.

- **Limiter les usages pro/perso des équipements informatiques :**

Selon le rapport OpinionWay, 62 % des élus et des agents déclarent utiliser des équipements personnels dans le cadre du travail, multipliant ainsi les risques de piratage. Cet aspect est particulièrement critique depuis la pandémie du Covid-19 et la généralisation du télétravail.

- **Inciter les agents à modifier leurs mots de passe régulièrement :**

Trop souvent négligée, cette pratique est pourtant cruciale pour la sécurité des données. Le site cybermalveillance.gouv.fr a publié un article sur la manière de bien gérer ses mots de passe.

- **Automatiser les mises à jour :**

L'opération de mise à jour est souvent ressentie comme une contrainte, elle est pourtant essentielle pour corriger les failles de sécurité des logiciels et des appareils numériques. Pour éviter qu'elles ne soient constamment repoussées, certains logiciels peuvent être configurés de manière à les automatiser ou les programmer lors de périodes d'inactivité.

- **Éteindre les ordinateurs la nuit :**

C'est un geste simple qui permet de limiter la vulnérabilité des postes de travail face aux attaques. Par ailleurs, la mise hors tension permet de préserver les composants électroniques des ordinateurs et de diminuer les factures d'électricité.

La création d'un espace de travail sécurisé

Outre la formation des collaborateurs et la mise en place de bonnes pratiques au sein des collectivités, des solutions techniques existent afin de sécuriser les espaces de travail.
Oodrive est le seul acteur européen à avoir reçu la qualification SecNumCloud pour son offre SaaS. Ce label désigne le plus haut niveau de sécurité délivré par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

.

La suite collaborative proposée par Oodrive comprend quatre solutions hébergées sur un cloud sécurisé :

- **Oodrive work : permet de centraliser, éditer et partager des données sensibles, en interne et avec des partenaires.**
- **Oodrive meet : assure la numérisation des réunions de gouvernance et des documents associés en toute confidentialité.**
- **Oodrive sign : en conformité avec la réglementation eIDAS, cet outil permet la signature à valeur probante de documents en face-à-face ou à distance.**
- **Oodrive save : sécurise la gestion des sauvegardes ainsi que la récupération de données perdues.**

À ce jour, la cybersécurité nécessite encore des efforts et des investissements pour les collectivités, notamment en termes de formation et d'acculturation. De nature à impacter le fonctionnement des administrations à tous les niveaux, elle présente un aspect transversal dans la politique publique. Pour Denis Thuriot, maire de Nevers, la protection numérique ne doit cependant pas être vue sous le seul aspect sécuritaire. À l'image du projet de territoire intelligent actuellement en cours de développement sur l'agglomération neversoise, elle est aussi une véritable opportunité dans le cadre de la stratégie d'attractivité des collectivités.

Yoann KLEIN
Senior Cyber Security Advisor - Huawei

Sept éléments clés pour répondre aux défis cyber des acteurs territoriaux

En mars dernier, un rapport du commandement du ministère de l'Intérieur dans le cyberespace dressait un état des lieux des défis cyber en France. Près de 300.000 infractions liées au numérique ont été enregistrées en 2023, en augmentation de 9% par rapport à 2022. Ce rapport fait écho à un autre rapport rendu public en juin 2021 par la délégation sénatoriale aux entreprises, soulignant l'ampleur du risque cyber pour les entreprises mais aussi pour toutes les organisations publiques, en particulier les collectivités territoriales.

Le rapport urgeait de sensibiliser davantage les élus et les fonctionnaires territoriaux à l'existence de lourdes conséquences en cas de cyber-attaques : dysfonctionnement des services publics locaux, perte de données, conséquences humaines et financières… Il soulignait également que le dispositif de cyber protection publique était développé mais peu accessible aux petites collectivités territoriales.

Si tout le monde est témoin de l'augmentation des attaques et la visibilité croissante de ces dernières contre les villes et les entreprises, les collectivités territoriales ne savent pas toutes comment s'y prendre. Et de surcroît, elles ne sont certainement pas toutes équipées uniformément pour faire face au défi numérique. Trop souvent accablées par des budgets de sécurité limités, des technologies vieillissantes et des services informatiques de petite taille, un nombre important de collectivités territoriales sont devenues des cibles de choix pour les cyberattaques.

Et pourtant, les enjeux de la protection et la maîtrise numérique pour les acteurs territoriaux sont cruciaux et multifacettes :

1. Protection des Données Sensibles.

La protection des données est non seulement une obligation légale, mais aussi un élément clé pour maintenir la confiance des citoyens dans les services publics. Les acteurs territoriaux sont responsables de la gestion et de la protection de vastes quantités de données sensibles (informations personnelles sur les citoyens, dossiers médicaux, données fiscales, plans d'urgence, etc.). Une violation de ces données peut avoir des conséquences graves, comme le vol d'identité, la fraude ou l'atteinte à la vie privée. Pour s'en protéger, les administrations doivent mettre en place des mécanismes de protection robustes, y compris le chiffrement des données, des contrôles d'accès stricts et des audits réguliers de sécurité. En outre, il est essentiel de sensibiliser les employés et les former aux meilleures pratiques pour éviter les erreurs humaines qui peuvent compromettre la sécurité des informations.

Pour assurer la mise en œuvre efficace des exigences en matière de protection de la vie privée, Huawei adopte, pour le développement de ses produits et solutions, une approche exhaustive de la sécurité, depuis la conception du produit en phase de R&D jusqu'à sa commercialisation. D'autre part, nous avons effectuons des PIA (Privacy Impact Assessment) pour évaluer chacun de nos produits et services.

2. Continuité des Services Publics
En cas de cyberattaque, les systèmes informatiques des collectivités territoriales peuvent être compromis, entraînant l'arrêt des services essentiels tels que la délivrance de documents administratifs, les soins de santé ou la gestion des infrastructures critiques comme l'eau ou l'électricité. Il est donc essentiel d'établir des plans de continuité d'activité, incluant des systèmes de sauvegarde, des protocoles de reprise après sinistre et une capacité de réponse rapide aux incidents. Les tests réguliers de ces plans permettent de s'assurer que les services peuvent être rétablis rapidement, limitant ainsi les conséquences des cyberattaques.

Huawei propose à ses clients des solutions de reprise après sinistre, conçues pour minimiser les pertes de données dans les systèmes de production et prévenir les interruptions d'activité en cas de catastrophe. De plus, outre la qualité de nos produits, nous renforçons continuellement la résilience de notre chaîne d'approvisionnement, en collaboration avec nos partenaires et fournisseurs. Dans le cadre de programmes dédiés, nous les formons notamment sur la façon d'optimiser leurs processus internes pour en améliorer qualité et efficacité.

3. Réputation et Confiance :
Le bon fonctionnement des relations entre administrations locales et citoyens repose sur la confiance. Un incident de cybersécurité, comme une fuite de données ou une interruption de service prolongée, peut avoir des effets dévastateurs sur la réputation des acteurs territoriaux, incitant les citoyens à se méfier de la capacité des autorités à protéger leurs informations personnelles ou à maintenir la continuité des services. Cela peut aussi décourager les partenaires commerciaux ou institutionnels de collaborer avec une administration perçue comme vulnérable. Pour maintenir cette confiance, il est crucial de mettre en œuvre des politiques de cybersécurité robustes, d'assurer une transparence dans la gestion des incidents et de communiquer efficacement avec les citoyens en cas de problème.

La confiance est une question à multiples facettes, dont les définitions et la portée varient. La confiance s'applique à des niveaux individuel, organisationnel et international, mais n'en reste pas moins centrée sur l'humain, et basée sur notre besoin d'équilibrer la coopération et la compétition. Bien qu'il y ait évidemment des limites à ce qui peut être réalisé compte tenu du climat géopolitique et la tendance actuelle vers la souveraineté numérique, il existe néanmoins des opportunités réelles et substantielles d'améliorer la confiance. Chez Huawei, nous avons fait le choix de la transparence. Par exemple, au sein de notre centre de transparence de la cybersécurité européen à Bruxelles, nous mettons à la disposition de l'écosystème des informations techniques sur nos solutions, jusqu'au code source.

4. Conformité Réglementaire :
Les administrations territoriales sont tenues de respecter des réglementations strictes en matière de protection des données. En Europe, outre le Règlement Général sur la Protection des Données (RGPD) connu de tous, la directive européenne NIS2 (Network and Information Security Directive 2) leur impose de nouvelles obligations strictes en matière de cybersécurité. En intégrant les exigences de la NIS2 dans leurs pratiques de sécurité, les administrations locales non seulement réduisent leur exposition aux risques, mais renforcent aussi la confiance des citoyens et des partenaires envers leur capacité à sécuriser les infrastructures critiques. L'adoption proactive de ces mesures permet aux collectivités de se conformer aux nouvelles normes européennes et d'éviter des sanctions, tout en améliorant globalement la cybersécurité à un niveau systémique.

L'établissement de normes de cybersécurité reconnues et acceptées à l'échelle mondiale, mais utilisables à un niveau local et territorial est essentiel. L'arrivée du Cyber Resilience Act (CRA), réglementation de l'Union européenne visant à renforcer la sécurité des produits numériques en imposant des normes de cybersécurité tout au long de leur cycle de vie, est un signe positif, qui doit permettre de renforcer la confiance entre tous les acteurs de la chaîne cyber en l'appuyant sur des critères vérifiables, basés sur des normes communes.

Il est essentiel de pouvoir tirer profit des pratiques et de l'expertise de l'industrie, via par exemple l'utilisation de produits certifiés. C'est un moyen efficace de s'assurer d'utiliser les bons outils face aux problèmes de sécurité pour les collectivités territoriales.

5. Gestion des Risques :
Les acteurs territoriaux doivent anticiper et évaluer les menaces potentielles, telles que les ransomwares, le phishing ou les violations de données. Une approche proactive consiste à identifier les vulnérabilités et à les corriger avant qu'elles ne soient exploitées. Cela inclut une gestion des risques efficace et pragmatique pour les acteurs territoriaux, qui doivent anticiper, évaluer et mitiger les menaces potentielles. En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) propose un cadre méthodologique clair, notamment à travers l'EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), qui aide les collectivités à évaluer les risques liés à la sécurité de leurs systèmes d'information.

À mesure que la transformation numérique s'approfondit, la présence de vulnérabilités et d'incidents de sécurité a donné lieu à davantage de législations dans de nombreux pays, y compris la France. Pour tous, la gestion des vulnérabilités nécessite une collaboration en amont et en aval afin de s'assurer que toutes les parties concernées s'acquittent de leurs responsabilités. Il s'agit d'établir une relation continue de confiance et de coopération tout au long de la chaîne d'approvisionnement, de manière ouverte et coopérative. Huawei propose cinq principes de base pour la gestion des vulnérabilités : réduction des dommages et des risques, réduction et atténuation des vulnérabilités, gestion proactive, amélioration continue, ouverture et collaboration.

6. Adaptation aux Évolutions Technologiques :
L'essor des objets connectés (IoT), des systèmes intelligents et du cloud computing élargit la surface d'attaque potentielle. Pour les administrations locales, il est essentiel de rester à la pointe des évolutions technologiques afin de sécuriser efficacement leurs systèmes. Cela nécessite une veille constante sur les nouvelles menaces et une adaptation des infrastructures en conséquence. Investir dans des technologies de sécurité avancées, comme l'intelligence artificielle pour la détection des anomalies, peut aider à prévenir les cyberattaques.

Cependant, si l'IA offre des opportunités et des avantages substantiels, elle est également confrontée à des défis en matière de sécurité et de protection de la vie privée, et c'est pourquoi Huawei a proposé un modèle de responsabilité partagée pour la sécurité de l'IA et la gouvernance de la protection de la vie privée. L'idée est de surmonter les cinq défis de sécurité de l'IA : sécurité logicielle et matérielle, intégrité des données, confidentialité des modèles, robustesse des modèles, confidentialité des données.

7. Partenariats et Collaboration :
La cybersécurité ne peut être assurée de manière isolée. Les administrations locales doivent collaborer avec une multitude d'acteurs pour renforcer leurs défenses. Cela inclut les agences nationales de cybersécurité, le secteur privé et les autres collectivités territoriales. La collaboration permet de partager des informations sur les menaces émergentes, de bénéficier de ressources et de compétences supplémentaires, et de coordonner les réponses en cas d'incident majeur.
Les partenariats et les collaborations sont les clés du succès pour Huawei. En 2021, nous avions tenu un forum sur le thème « Collaboration et confiance dans une cyberespace partagé », durant lequel l'un des panélistes a fait remarquer : « *Toutes les parties prenantes responsables devraient travailler ensemble pour assurer la collaboration, la confiance mutuelle et le partage dans le cyberespace. Nous devrions nous efforcer de réduire, et non d'augmenter, le déficit de confiance ; renforcer, et non affaiblir la coopération ; et faciliter, et non restreindre le partage. La cyber sécurité doit être guidée par une stratégie 4P : Public, Private, Professionnal et People* ».

Devant l'importance des enjeux de confiance numérique, il revient aux acteurs territoriaux, et principalement aux élus, de lancer la dynamique qui permettra à la collectivité de développer un projet cohérent, contrôlé et sécurisé. Il n'est pas nécessaire pour les élus de posséder une compréhension approfondie des aspects techniques du sujet ou d'en être un spécialiste. Cependant, il est primordial de définir une stratégie claire et de rassembler, cadres, agents territoriaux, mais aussi tout un écosystème de partenaires, autour de cet objectif.

Chez Huawei, nous pensons également que le développement d'un monde numérique et intelligent nécessite une collaboration forte. Nous croyons au pouvoir de dissoudre les frontières et de travailler ensemble pour construire un écosystème prospérant sur la base d'une réussite conjointe. C'est pourquoi, nous mettons tout en œuvre pour répondre aux exigences et défis des acteurs territoriaux.

Philippe LALOUM
Responsable IT & Cybersécurité - Isogeo

Panorama des cybermenaces entre avril et juin 2024 sous le prisme du cadre MITRE ATT&CK

Établir la priorité des efforts de cybersécurité dans le contexte de ressources contraintes des collectivités territoriales

Introduction

Les collectivités territoriales sont notoirement victimes de cybermenaces plus ou moins sophistiquées (voir à ce sujet la synthèse des cybermenaces qui les visent établie par l'ANSSI fin 2023 : Rapport menaces et incidents - CERT-FR (ssi.gouv.fr)). Elles sont en effet perçues par les cybercriminels qui les ciblent soit par opportunisme lucratif comme c'est majoritairement le cas, ou encore à des fins de déstabilisation, voire d'espionnage, comme des proies de choix, requérant de leur part un effort minimum pour un impact garanti et visible sur les multiples champs de compétence mis au service de leurs administrés dont elles sont par ailleurs dépositaires des données personnelles, et qui en subissent souvent les conséquences directes, allant de l'affectation des services de transports et hospitaliers à la compromission de l'identité numérique des concitoyens.

Particulièrement, entre avril et juin 2024, une recrudescence notable d'attaques a été observée (en voir la synthèse établie par les services d'intelligence de la menace de Microsoft : Intel Article - Microsoft Defender), nécessitant une évaluation rigoureuse des menaces pour prioriser les efforts de cybersécurité visant à s'en prémunir.

Dans cette perspective, le cadre "MITRE ATT&CK" offre une méthodologie structurée pour analyser les tactiques, techniques et procédures (TTP) utilisées par les attaquants.

Phases d'une cyberattaque selon MITRE ATT&CK

Pour comprendre les mécanismes d'attaque et renforcer les défenses, il est crucial de décortiquer les différentes phases d'attaques déployées par les cybercriminels. Ces phases sont illustrées dans le cadre MITRE ATT&CK, qui fournit une vue d'ensemble des méthodes employées par ces derniers, pour pénétrer les réseaux de leurs victimes, y faire persister des programmes malveillants, et compromettre ou exfiltrer les informations sensibles qu'ils recèlent.

Nous explorerons les principales tactiques récemment observées, en commençant par les étapes initiales de l'accès aux réseaux, en poursuivant par les techniques de contournement des mécanismes de défense en place, pour arriver au contrôle à distance de l'exfiltration ou la compromission des données.
Pour faciliter la compréhension du jargon du domaine de la cybersécurité utilisé au sein de ce document, il est recommandé de faire référence au CyberDico de l'ANSSI.

Accès initial aux réseaux

L'infiltration des réseaux commence souvent par des campagnes de phishing ciblées et des attaques par force brute sur des systèmes exposés sur Internet. Les courriels de phishing à destination des employés sont particulièrement efficaces pour obtenir des informations d'identification et installer des logiciels malveillants. Les systèmes exposés sur Internet et dont la sécurité d'accès n'a pas été renforcée à de multiples niveaux ne le sont pas moins.
En juin 2024, par exemple, l'Agence Française Nationale de la Sécurité des Systèmes d'Information (ANSSI) et ses partenaires ont détecté plusieurs cyberattaques contre des entités diplomatiques françaises, attribuées au groupe Nobelium (suivi par Microsoft sous le nom de Midnight Blizzard). Ces attaques incluaient du phishing ciblant des entités publiques et diplomatiques françaises pour exfiltrer des informations stratégiques.

Contournement des mesures de défense

Pour éviter la détection, les attaquants utilisent fréquemment des techniques de contournement des mesures de défense. Cela inclut l'utilisation de logiciels malveillants déguisés en applications légitimes, l'exploitation de vulnérabilités non corrigées et l'obfuscation des codes malveillants, technique par laquelle le code source d'un script malveillant est modifié pour rendre difficile ou impossible l'analyse d'innocuité.

Par exemple, en mai 2024, les chercheurs de Forcepoint ont découvert une campagne de logiciels malveillants nommée DarkGate par laquelle les victimes recevaient des fichiers PDF frauduleux déguisés en factures, envoyés depuis un e-mail compromis. Cela conduisait finalement à l'exécution d'un script AutoIt qui utilisait des techniques de camouflage pour dissimuler ses activités.

Commande et contrôle

Une fois à l'intérieur des systèmes, les cybercriminels établissent des canaux de commande et contrôle (C2) pour gérer leurs opérations à distance, en y faisant transiter des communications chiffrées pour échapper à la surveillance des systèmes de sécurité.
L'infrastructure de ces canaux est parfois déjà légitimement en place, ce qui facilite d'autant la tâche aux cybercriminels, comme ce fut le cas en juin dernier dans le cadre de la campagne NetSupport rapportée par l'institut technologique de cybersécurité SANS : les cybercriminels abusaient du mécanisme App Installer de Microsoft, depuis désactivé par défaut sur les poste Windows récemment mis à jour, permettant la distribution via Internet de programmes d'installation, pour installer sur les postes de leurs victimes un client de communication de configuration illégitime à leur avantage pour prendre le contrôle de ces postes via la solution de support et de contrôle à distance légitime NetSupport Manager.

Exécution

Avec l'accès et le contrôle établis, les attaquants déploient des scripts malveillants et des logiciels de type ransomware pour exécuter des charges utiles nuisibles. Ces actions visent à perturber les services publics critiques et à exiger des rançons pour restaurer les systèmes affectés.
Les cybercriminels abusent très fréquemment pour ce faire de l'interface de commande PowerShell de Microsoft, présente notamment sur les systèmes Windows.

Ainsi, en avril 2024, eSentire a observé que le groupe FIN7, basé en Russie, utilisait des scripts PowerShell malveillants pour distribuer l'outil d'accès à distance NetSupport via un site Web malveillant sponsorisé par des publicités Google : l'exécution d'attaques via le poste utilisateur compromis consécutivement à une campagne de phishing est en effet une technique d'attaque éprouvée.
Cet incident souligne l'importance de sensibiliser les utilisateurs, d'avoir des solutions de protection des terminaux efficaces et de limiter les privilèges administratifs locaux : Microsoft a noté que dans presque toutes les attaques réussies au ransomware, les attaquants disposaient d'un compte administrateur et de mots de passe d'administrateur local sur les postes compromis.

Exfiltration

Les cybercriminels procèdent ensuite à l'exfiltration des données sensibles, telles que les informations personnelles des citoyens, les données financières et les documents confidentiels, majoritairement au travers des canaux C2 de commande et contrôle préétablis, après collecte par des logiciels espions. Ces informations sont alors transférées vers des serveurs contrôlés par les attaquants ou encore vendues sur le dark web.
Les logiciels espions sont des programmes malveillants destinés à voler des informations sur un appareil ciblé et à les transférer à l'attaquant. La popularité de ces logiciels a engendré la création d'un écosystème dédié aux voleurs de données et l'émergence d'une nouvelle catégorie d'attaquants exploitant ces capacités pour leurs attaques. Cet écosystème a permis à de nouveaux acteurs malveillants d'utiliser ces outils pour extraire des données et détériorer des ressources.

Impact

Enfin, l'impact des attaques se matérialise à travers des perturbations dans les services, des pertes financières, et des atteintes à la réputation des collectivités. Les attaquants peuvent également utiliser des ransomwares pour chiffrer les données et exiger une rançon, laissant les organisations paralysées jusqu'à ce que des mesures de recouvrement soient mises en œuvre.

En juillet 2024, l'équipe de chasseurs de menaces de Symantec a signalé que LockBit restait la principale menace de ransomware, suivi par Play, 8Base (filiale de Phobos), et le ransomware émergent Qilin.

L'exploitation des vulnérabilités connues dans les applications publiques demeurerait ainsi le vecteur d'attaque principal, avec par exemple des campagnes visant les serveurs Web via une vulnérabilité du framework de développement Web PHP récemment découverte (CVE-2024-4577).
De plus, le retour du ransomware Clop, dirigé par le groupe Snakefly, indique un recours aux attaques classiques de double extorsion par lesquelles les données sont à la fois exfiltrées et chiffrées.
En dépit des actions coordonnées au niveau international des forces de l'ordre pour lutter contre cette menace, les ransomwares devraient rester une menace significative pour les entreprises dans un avenir prévisible.

Techniques et contre-mesures pour chaque phase

Accès initial

Techniques :
- Phishing ciblé : envoi de courriels frauduleux pour tromper les utilisateurs et obtenir leurs informations d'identification.

- Attaques par force brute : tentatives répétées de deviner les mots de passe pour accéder aux systèmes.

Contre-mesures :
- Authentification multifactorielle (MFA) : ajout d'une couche de sécurité supplémentaire pour vérifier l'identité des utilisateurs.

- Sensibilisation et formation des employés : programmes réguliers pour éduquer les employés sur les dangers du phishing.

- **Filtrage des courriels : utilisation de solutions de sécurité des courriels pour détecter et bloquer les courriels de phishing, comme les solutions françaises Mailo Collectivités et Mairiestem le proposent ou encore la solution Microsoft Defender pour Office 365.**

Contournement des mesures de défense

Techniques :
- **Malwares déguisés : logiciels malveillants camouflés en applications légitimes.**
- **Exploitation de vulnérabilités : utilisation de failles non corrigées dans les logiciels et systèmes.**
- **Obfuscation de code : techniques pour cacher le code malveillant et éviter la détection.**

Contre-mesures :
- **Mise à jour régulière des logiciels : application des correctifs de sécurité pour combler les vulnérabilités au travers, par exemple, de la solution Intune de Microsoft pour automatiser la gestion des points de terminaison.**
- **Solutions anti-malware : utilisation de logiciels de sécurité pour détecter et éliminer les malwares, comme la solution EDR européenne proposée par HarfangLab.**
- **Audit de sécurité et tests de pénétration : évaluation régulière des systèmes pour identifier et corriger les failles. Voir sur ce sujet le parcours cybersécurité proposé par l'ANSSI et le retour d'expérience de la ville de Charenton-le-Pont sur son application.**

Commande et contrôle alias C2

Techniques :
- **Serveurs C2 externes : utilisation de serveurs distants pour contrôler les systèmes compromis.**
- **Communications chiffrées : chiffrement des données de commande pour éviter la détection.**

Contre-mesures :
- **Détection et blocage des communications suspectes : surveillance du trafic réseau pour identifier et bloquer les communications C2.**
- **Isolation des systèmes compromis : mise en quarantaine des systèmes infectés pour empêcher la propagation.**
- **Utilisation de solutions de détection des intrusions (IDS) et de prévention des intrusions (IPS) : outils pour identifier et bloquer les activités malveillantes.**

Exécution

Techniques :
- **Scripts malveillants : exécution de scripts pour déployer des charges utiles nuisibles.**
- **Ransomwares : logiciels de rançon qui chiffrent les données et exigent un paiement pour les déchiffrer.**

Contre-mesures :
- **Segmentation du réseau : division du réseau en segments pour limiter la propagation des malwares.**
- **Sauvegardes régulières : réalisation de sauvegardes fréquentes et tests de restauration réguliers pour restaurer les données en cas d'attaque de ransomware.**
- **Blocage de l'exécution de scripts non autorisés : utilisation de politiques de sécurité pour empêcher l'exécution de scripts non approuvés.**

Exfiltration

Techniques :
- **Transfert de données sensibles : envoi de données volées vers des serveurs contrôlés par les attaquants.**
- **Vente sur le dark web : mise en vente des données exfiltrées sur des marchés illégaux.**

Contre-mesures :

- **Chiffrement des données : utilisation de techniques de chiffrement pour protéger les données sensibles.**
- **Surveillance du trafic réseau : analyse du trafic sortant pour détecter et bloquer les exfiltrations de données.**
- **Gestion des droits d'accès : limitation des accès aux données sensibles uniquement aux utilisateurs autorisés.**

Impact

Techniques :

- **Ransomwares : chiffrement des données et demande de rançon pour les restaurer.**
- **Sabotage : perturbation des services publics et destruction des données.**

Contre-mesures :

- **Plan de continuité des activités : établissement de procédures pour maintenir les opérations en cas d'attaque.**
- **Recouvrement des systèmes : utilisation de sauvegardes et de stratégies de recouvrement pour restaurer les systèmes affectés.**
- **Renforcement des mesures de sécurité : amélioration continue des politiques et des outils de sécurité pour parer aux nouvelles menaces.**

Les témoignages officiels de collectivités impactées par une cyberattaque concluante peuvent être consultées sur ce site de référence : Témoignages de collectivités victimes de cyberattaques - assistance aux victimes de cybermalveillance.

Conclusion

La période d'avril à juin 2024 a mis en lumière une sophistication accrue des cybermenaces auxquelles sont exposées les collectivités territoriales depuis plusieurs années.

En utilisant le cadre MITRE ATT&CK pour analyser les menaces et prioriser les efforts de sécurité, les collectivités peuvent mieux protéger leurs systèmes et services critiques, même avec des ressources limitées.

Une approche proactive et bien informée est essentielle pour faire face aux menaces cybernétiques croissantes et assurer la résilience des infrastructures publiques.

Isogeo, en tant qu'éditeur d'une solution de gestion des données géographiques hébergée aussi bien en mode SaaS qu'en mode dit on-premises dans l'environnement de ses clients, doit également s'armer pour faire face à ces menaces et accompagner ses clients dans le respect des bonnes pratiques.

Vivian PELISSOU
RSSI - MGDIS

Cybersécurité : un enjeu stratégique pour MGDIS et toutes les organisations publiques

Entreprise responsable, en tant qu'éditeur de progiciels pour le secteur public, MGDIS positionne la cybersécurité comme un enjeu stratégique pour ses clients, pour son développement et pour sa pérennité.

Si le sujet n'est pas nouveau pour MGDIS, force est de constater, depuis plusieurs années et au niveau mondial, une recrudescence de tous types de cyberattaques. Tout récemment, l'évènement des JO 2024 à Paris n'a fait que confirmer cette tendance. Ces attaques visent aussi bien les structures publiques que privées, et ce, quel que soit le secteur d'activité ou la taille. Les TPE et PME sont encore en 2024 positionnées en premières victimes mais les organisations publiques, de toute taille sont également fortement impactées, petites ou grandes collectivités, ministères et établissements de santé, personne n'est épargné.

Les impacts liés à ces attaques sont nombreux : interruption prolongée de services, inaccessibilité de dossiers ou documents, fuites de données à caractère personnel, atteinte à la réputation, risques juridiques, financiers… La mise en danger de la vie de patients, le blocage complet de services publics essentiels à des populations fragiles ne sont pas un frein, bien au contraire…

Comme bon nombre de ses clients, MGDIS s'est fortement renforcée en investissement sur le sujet cyber. La cybersécurité a longtemps été traitée par les équipes de R&D dans leurs process de développement et de test ou par le service informatique, pour la protection du système informatique interne. En 2021, elle est passée sous la responsabilité d'un RSSI avec une équipe dédiée qui pilote cet enjeu et coordonne l'ensemble des actions à l'échelle de l'entreprise avec la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) et le lancement d'un projet de certification ISO 27001.

De nombreuses organisations publiques mènent des démarches équivalentes, d'autres s'interrogent encore sur le bon niveau d'investissements à mobiliser sur ce sujet au détriment de la mobilisation entière de leurs moyens au service des bénéficiaires de leurs missions de service public.

Cette tribune est une occasion de se réinterroger sur la pertinence des moyens mobilisés pour faire face aux enjeux de la cybersécurité et de mieux mesurer le retour sur investissement au service des agents publics et des bénéficiaires des services publics.

En effet, au-delà du bénéfice immédiat d'une meilleure protection contre les cyber-attaques, la mise en œuvre d'un SMSI ou, plus généralement, tout investissement orienté cybersécurité, génère de nombreux effets positifs à prendre en compte lors des arbitrages stratégiques.

Cybersécurité : une opportunité pour repenser la gestion des risques et renforcer la sensibilisation des équipes

L'analyse des risques cyber, étape incontournable pour tout Responsable Sécurité des Systèmes d'Informations (RSSI), permet d'identifier et d'évaluer les risques inhérents au système d'information étudié. Le risque étant avéré, la menace cyber devient un levier puissant pour renforcer la culture du risque dans l'organisation et un vecteur puissant de sensibilisation de l'Equipe de Direction puis de l'ensemble des équipes.

Par exemple, on entend beaucoup parler de ransomware, de déni de service et encore plus de fuite de données, effet du RGPD (Règlement Général sur la Protection des Données) depuis 2018.

Dans les faits, selon la méthode EBIOS RM promue par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), outre la vision formalisée des valeurs métiers de l'organisation, l'identification des menaces et de leurs objectifs concrétise, à partir d'attaques passées sur des structures équivalentes ou acteurs du marché, les activités potentiellement malveillantes susceptibles de compromettre la sécurité de notre SI.

La réflexion engagée et la méthode appliquée impose d'élargir sa vision des menaces et d'élargir son champ de connaissance. En travaillant sur la maîtrise des risques cyber, on s'approprie des outils et méthodes adaptés à la gestion des risques en général et à la résilience de l'organisation face aux menaces, accidents… pertinent par exemple dans une réflexion sur les impacts du changement climatique, encore plus complexe à aborder que la menace cyber.

En poursuivant le raisonnement, l'analyse de risque amène à élaborer la liste des parties prenantes impliquées dans le système d'information. Cette étape réactive le focus, et à défaut fait prendre conscience, de l'importance des interactions de l'organisation avec ses fournisseurs, ses bénéficiaires, ses partenaires… Cela met en avant la complexité de l'écosystème et les dépendances envers les uns et les autres. C'est à ce moment-là que l'on distingue souvent le manque de connaissance de ses fournisseurs, et l'ANSSI nous rappelle souvent combien la "supply chain" est souvent utilisée comme canal d'attaque, justement parce qu'elle est souvent négligée.

Cet exercice mené pour la cybersécurité sera également fort utile dans le cadre de la mise en place d'une démarche RSE (Responsabilité Sociétale des Entreprises) et d'une manière générale pour améliorer la sécurité de fonctionnement de l'organisation.

Au-delà de la découverte et du partage de la méthode et de son champ lexical, l'établissement de la cartographie des risques et du plan de traitement associé démontre la nécessité de l'implication de l'ensemble de l'organisation en vue de la mise sous contrôle et sera un outil pédagogique puissant.

La connaissance de la menace cyber : un sujet fédérateur pour renforcer la vigilance et l'engagement collectif

Depuis au moins 5 ans, toute personne intégrant l'effectif de MGDIS en tant que collaborateur et/ou sous-traitant a l'obligation de suivre le Mooc de l'ANSSI (https://secnumacademie.gouv.fr/). La sensibilisation de l'ensemble des parties prenantes aux risques cybers est l'occasion de rappeler que face à toute menace, quelle qu'elle soit, (attaque cyber, incendie, accident climatique…) le bon comportement humain et le développement des compétences de chacun sont des atouts majeurs.

Au-delà d'améliorer la sécurité de l'entreprise, le fait d'imposer le même Mooc à tout le monde place l'ensemble des équipes sur un même pied d'égalité et d'importance dans sa mission. Cela rappelle que chacune et chacun est essentiel au bon fonctionnement du collectif.

En pratique, en tant que RSSI, j'ai pu constater l'émergence d'un esprit de solidarité au sein des différentes "communautés" de collaborateurs métiers techniques ou non techniques de MGDIS face à des exercices de phishing. La communication très rapide d'une suspicion d'attaque via les réseaux internes de discussion démontre une réelle prise de conscience des menaces cyber et une maturité collective qui n'est pas si évidente à faire émerger dans le fonctionnement quotidien de l'organisation ou chacune et chacun n'a pas forcément conscience de l'impact de son travail dans la qualité du service rendu par l'organisation tout entière.

Cette dimension fédératrice face à la menace cyber est un levier de cohésion d'équipe et concours à donner du sens. Cette expérience partagée et ses effets positifs constatés, la réflexion sur d'autres domaines de mise en pratique, sont autant d'opportunité de créer du lien entre équipes au sein de l'organisation. Elle sera utile bien sûr dans la mise en œuvre d'une démarche RSE mais plus généralement dans le fonctionnement de l'organisation.

Contrôle d'accès physique : un levier global pour la sécurité des biens, des personnes et du système d'information

La revue complète des installations et des process de contrôle d'accès physique à des locaux n'est pas qu'un thème de cyber protection de son système d'information. Il est d'autant plus important qu'il protège également l'ensemble des biens d'une organisation même si ceux-ci ne sont pas catégorisés comme ressources informationnelles.

Le contrôle d'accès physique est aussi un moyen d'améliorer la protection des personnes sur leur lieu de travail face aux agressions extérieures de tout genre. Et la mise en place de systèmes d'alerte permet une réactivité des actions de secours et/ou des autorités en cas d'intrusion.

Sur ce point l'enjeu cyber est également un moyen simple de faire comprendre et de partager les objectifs auprès de l'ensemble des parties prenantes avec un effet bénéfique induit au-delà du seul sujet de la cybersécurité. Le retour sur investissement de la démarche cyber est renforcé et mutualisé avec d'autres enjeux tout aussi importants.

Préparation à la gestion de crise : se doter de moyens pour minimiser les impacts et assurer la continuité

Les évènements des années passées : COVID-19, confinement, … et ceux actuels de plus en plus prégnants comme les événements climatiques : tempêtes, inondations, … pour certains ou encore les pannes subites dues à un matériel défectueux ou un coup de tractopelle malencontreux dans une fibre optique, … nous amènent à réfléchir à notre capacité de réaction face à ces aléas. La crise cyber est particulière dans le sens où en général elle est concrétisée par une indisponibilité du système d'information associée à d'autres menaces connexes (vol de données…). En bref, une cyberattaque est une attaque organisée subie à laquelle on y associe un sentiment ou une recherche de faute.

Après avoir posé les principes généraux de la gestion de crise en 4 phases (références aux guides de l'ANSSI : https://cyber.gouv.fr/anticiper-et-gerer-une-crise-cyber), nous avons constitué nos scénarios redoutés à partir des analyses de risques déjà réalisées. Nous travaillons également sur nos process et outils de gestion de crise de cybersécurité et avons déjà déclenché des exercices d'alerte. C'est dans ce cadre qu'un exercice de gestion de crise est planifié prochainement en vue de valider et améliorer nos procédures et outils en mettant à l'épreuve notamment les comportements humains. Un DSI victime d'une cyber attaque me confiait récemment "*On a beau prévoir des scénarios catastrophes, la réalité est souvent bien pire. Imaginez cette situation sans préparation !*".

La préparation à la gestion de crise n'a pas l'objectif de se préparer à tous les évènements redoutés imaginables mais bien de se doter de moyens et d'un savoir-faire à l'épreuve des évènements de type cyber afin de minimiser leurs impacts et de garantir la continuité et la pérennité des activités de l'organisation.

Les bonnes pratiques de réaction seront une fois de plus bien utiles pour faire face à d'autres types de crise et permettront de développer, au-delà des outils et méthodes de réaction, une culture du sang-froid et de l'action coordonnée face à une menace.

Les bénéfices d'un SMSI : au-delà de la sécurité, une opportunité d'amélioration globale
Par ces quelques exemples, nous avons pu identifier bien des bénéfices connexes à la démarche de mise en place d'un SMSI.

Il apparait ainsi qu'une telle démarche est utile au-delà de la simple organisation de la sécurité. Elle permet de se poser ou de se reposer des questions simples autours de son activité et évaluer sa fragilité ou sa robustesse.
Ce type de démarche se doit d'être fédératrice et d'impliquer toute l'organisation avec le soutien et l'implication forte de la direction générale, sponsor essentiel.

J'espère que cette tribune contribuera à aider à aborder la lutte contre la menace cyber non seulement comme un mal nécessaire mais également comme une opportunité d'améliorer la performance globale de l'organisation et aidera à rendre les arbitrages de mobilisation de moyens humains et financiers plus positifs et enthousiasmants !

CONTRIBUTEURS

Mission Ecoter

Denis THURIOT
Bertrand RINGOT
Alain MELKA
Quentin MEULLEMIESTRE

Collectivités

Nicolas BARD
Éric BERLIVET
Luc BOUARD
Nicolas DESFACHELLE
Fatima EL OUASDI
André FIGOUREUX
Tony FLAHAUT
Olivier GACQUERRE
Nadège HORNBECK
Frédéric LAFFORGUE
Karine LAURO
Émile Roger LOMBERTIE
Daniel MARECHAL
Lionel MONTILLAUD
Nathalie POIGNON
Emmanuel QUERE

Entreprises

Thierry ELKAIM
Maxime GEFFRAY
Yoann KLEIN
Philippe LALOUM
Vivian PELISSOU

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

Maquette : M.E.

MISSION ECOTER

NOUS SOMMES #CYBERENGAGÉS

DU 1ER AU 31 OCTOBRE 2024

CYBER MOIS

Parlons Territoires

Livret CYBERMOI/S

Octobre 2024