MISSION ECOTER
France et Territoires Numériques

BANQUE des TERRITOIRES | Caisse des Dépôts GROUPE

CYBERSÉCURITÉ & TERRITOIRES

LIVRE BLANC

Remis le 26 juillet 2023 à Jean-Noël BARROT, Ministre délégué chargé de la Transition numérique et des Télécommunications

Atos

2023

CISCO

L'Édito de Christian ESTROSI

Président de Mission Ecoter
France et Territoires Numériques

Maire de Nice et Président de la Métropole
Président délégué de la Région Sud PACA

Plusieurs sujets liés à l'innovation sont à forts enjeux pour les collectivités, la Cybersécurité en fait naturellement partie. C'est un enjeu majeur de la transformation numérique et de la transition énergétique. Les nombreuses attaques cyber perpétrées ces dernières années touchant nos administrations en font aujourd'hui un sujet incontournable. Néanmoins, cet enjeu reste encore trop souvent abstrait pour de nombreuses collectivités territoriales. Sécuriser les collectivités dans leur transformation numérique, c'est assurer la continuité du service public, protéger nos concitoyennes et concitoyens, notre souveraineté et surtout notre démocratie, parce qu'il existe entre autres des solutions innovantes pour nos territoires.

Dans le cadre de nos travaux au sein de Mission Ecoter-France et Territoires Numériques, nous sensibilisons, informons et formons les élus, cadres de collectivités et d'entreprises à ce sujet qui justifie à lui seul l'attention que doit être portée dans ce domaine par les collectivités territoriales et les entreprises. A cet effet, nous avons organisé ces derniers mois deux visioconférences qui ont regroupées acteurs public et privé, experts, afin de croiser les regards, d'échanger les bonnes pratiques, de mesurer les enjeux majeurs et de proposer des solutions innovantes pour nos territoires. C'est dans cet esprit, que nous avons voulu - avec l'un de nos membres fondateurs La Caisse des Dépôts et Consignations-Banque des Territoires et nos partenaires, Atos et Cisco - proposer ce Livre Blanc qui présente un état des lieux de la situation tout en déclinant des solutions concrètes et opérationnelles.

Plus de 50 milliards d'objets connectés seront en circulation cette année

À l'heure de l'essor de l'internet des objets, dopé par le déploiement des réseaux 5G et 6G… la question de la sécurisation des communications électroniques prend une dimension inégalée. En effet, plus de 50 milliards d'objets connectés seront en circulation cette année, ce qui rendra encore plus perméables les questions de cybersécurité (vols de données, détournements financiers…).

La Cybersécurité doit être au cœur de nos préoccupations

L'enjeu cyber est donc aujourd'hui incontournable. Organisations privées, administrations publiques, individus sont constamment menacés à différents niveaux et doivent se pencher sérieusement sur cet enjeu cyber. Par ailleurs, c'est aussi prendre conscience de la séquence très particulière vécue depuis 2020 avec la crise du COVID-19, qui a vu une multiplication de ces risques cybers avec là aussi des vulnérabilités qui touchent l'ensemble des acteurs de nos territoires avec des niveaux de dangerosité là aussi très divers.

Dès lors, la question de la sécurisation des communications électroniques est fondamentale et prend une dimension inégalée. Car la Cybersécurité doit être cœur de nos préoccupations à l'échelle locale, nationale mais également à l'internationale. En effet, la politique internationale s'articule désormais principalement autour du cyberespace, les événements de ces derniers temps ont placé les enjeux de cybersécurité au cœur des relations diplomatiques et stratégiques, car elles conditionnent non seulement la prospérité économique mais également le maintien de la paix mondiale.

L'Avant-propos de Denis THURIOT

Vice-Président de Mission Ecoter-France et Territoires numériques

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

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

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

Il est donc urgent d'accélérer l'accompagnement des élus, des agents des collectivités, de tous les acteurs publics et privés, institutionnels, économiques ou associatifs, afin qu'ils puissent comprendre, mesurer, anticiper les risques et réduire leur vulnérabilité. Même si le risque zéro n'existe pas, prévenir avant qu'il ne soit trop tard, en adoptant les bons réflexes pour nous assurer la meilleure sécurité numérique possible, n'est plus une option mais une exigence. Les cyberattaques préoccupent effectivement les usagers car elles mettent généralement en péril leurs données personnelles. Dans cette optique, la coopération entre les territoires apparaît indispensable ; elle est la condition *sine qua non* d'une gestion complète de la cybervulnérabilité des réseaux. Elle peut aussi se mener à un niveau régional.

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

Nous sommes cependant, dans l'immédiat, tous porteurs de questions : comment protéger efficacement l'accès aux données personnelles ? Comment empêcher le piratage des infrastructures stratégiques ? Comment se prémunir contre la professionnalisation des cybercriminels dans un contexte de développement des objets connectés ? Et bien d'autres questions encore. Des réponses se trouvent dans ce livre blanc. Il était une nécessité et sera, je le souhaite, le livre de chevet des élus locaux en charge des données et des infrastructures numériques qui trouveront, dans ses pages, les conseils et les partages d'expériences utiles à une politique de cybersécurité efficace et très attendue par les habitants de nos territoires. La cybersécurité est bel et bien un enjeu citoyen, et fait désormais partie des enjeux de sécurité plus globale.

Les cyberattaques préoccupent effectivement les usagers car elles mettent généralement en péril leurs données personnelles

SOMMAIRE

Mission Ecoter
France et Territoires Numériques

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

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

Mission Ecoter-France et Territoires Numériques est aujourd'hui présidée par Christian ESTROSI, Maire de Nice, Président de la Métropole Nice Côte d'Azur, Président délégué de la Région Provence-Alpes Côte d'Azur, 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.

États des lieux sur la situation et l'évolution de la menace cyber

Définition

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

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

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

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

Source : Sofaxis

88% des virus conçus par les hackers ne sont pas détectés par les antivirus

Enjeux

Nous le constatons quotidiennement la menace d'origine cyber est de plus en plus élevée et croissante. Ce propos peut paraître anodin, mais il ne l'est pas ! Il justifie à lui seul l'attention que doit être portée au sujet par les États, les pouvoirs publics, les organisations de tous les secteurs et les citoyens. Cette tendance générale est appuyée par différents constats plus spécifiques.

S'agissant de l'environnement tout d'abord, une tendance structurante sous-jacente est celle de la numérisation croissante de la société et de l'économie, et de leur dépendance grandissante aux systèmes numériques. Les systèmes d'information et les processus, qu'ils mettent en œuvre et qu'ils supportent, sont de plus en plus complexes.

Source : Sofaxis

42% des cyber attaques visent les collectivités

Il est difficile de prévoir l'évolution des tendances (technologies et usages numériques), et par extension de comprendre et d'anticiper la menace d'origine cyber. Le cyberespace est par ailleurs largement reconnu comme un nouvel espace d'affrontements militaires - cela a notamment fait l'objet d'une conclusion du sommet de l'OTAN de 2016. Il permet également l'effritement de la frontière entre des enjeux de défense nationale et des enjeux de criminalité.

Source : Sofaxis

30% des collectivités ont subi une cyberattaque en 2020

Les acteurs malveillants sont de plus en plus nombreux et variés. Ils peuvent mener des attaques à moindre frais. Ils sont également capables d'opérations particulièrement sophistiquées. Ils peuvent s'appuyer sur une véritable logique de marché : soit pour accéder à des compétences et des outils, soit pour monétiser des services d'attaque. En tout état de cause, le conflit cyber présente une nette asymétrie en faveur des attaquants.

Les compétences en matière d'opération dans le champ cyber prolifèrent. La diffusion de celles qui permettent des actions offensives est particulièrement inquiétante, a fortiori lorsqu'elles se situent à la rencontre d'acteurs animés d'intentions malveillantes et d'autres disposant de compétences techniques qu'ils sont prêts à monétiser.

La prolifération des outils d'attaque est également source d'inquiétude. De plus en plus simples d'utilisation, ils sont disponibles de façon croissante en sources ouvertes, ou vendus à des prix abordables.

Source : Sofaxis

Dans 9 cas sur 12 l’attaque est liée à la demande d’une rançon

Les finalités des attaques évoluent. Elles sont parfois complexes à appréhender. Les attaques à vocation de pré-positionnement ou de rebond - de type supply chain attack par exemple - sont de plus en plus courantes. Elles se produisent lorsqu'un pirate accède au réseau d'une collectivité ou d’une entreprise par le biais d'un fournisseur tiers ou de la chaine logistique.

On assiste par ailleurs à une recrudescence des actions de déstabilisation à grande échelle, utilisant les réseaux sociaux et s’appuyant sur des opérations d’exfiltration puis de divulgation de grandes quantités de données. De façon générale, les finalités des attaques sont de plus en plus multiples - une même attaque pouvant servir une combinaison de plusieurs finalités.

Les modes opératoires des attaques montrent une sophistication technique croissante - même si les manœuvres simples fonctionnent toujours. On observe une préparation et une planification conséquente de certaines attaques, illustrant les quantités importantes de ressources que certains acteurs sont prêts à engager.

Les parties défensives ont globalement mis du temps à prendre conscience des enjeux, encore trop souvent cantonnés à un domaine de techniciens. Un manque récurrent « d'hygiène cyber » est encore très régulièrement constaté, chez toutes sortes d'acteurs. De façon générale, les surfaces à défendre - qui constituent pour la partie adverse des surfaces d'attaque - sont de plus en plus importantes : davantage d'accès, d'utilisateurs, de raisons d'attaquer, de données à protéger, de vecteurs d'attaque. La complexité intrinsèque du sujet rend difficile la mesure objective de la menace et des coûts qu'elle est susceptible d'introduire.

Notons enfin que l'ensemble de ces tendances ne se succèdent pas : elles se cumulent

Les vulnérabilités informatiques sont à la source d'un dilemme complexe : lorsque la puissance publique a connaissance d'une vulnérabilité, doit-elle la publier, pour que l'éditeur puisse chercher à la corriger ; ou doit-elle la garder secrète, au profit de certaines fonctions régaliennes comme le renseignement ?

Un choix de politique publique, orienté vers la divulgation des vulnérabilités, sous-tend une approche consistant à faire augmenter le niveau général de sécurité des systèmes d'information en « bouchant les trous » au fur et à mesure qu'ils sont découverts. Cette démarche transfert, en quelque sorte, la responsabilité de la puissance publique vers les éditeurs dans un premier temps, qui doivent élaborer des correctifs, puis vers les utilisateurs, qui doivent les appliquer. En tout état de cause, cette démarche part du principe qu'il existe un correctif pour une vulnérabilité donnée avant qu'elle ne soit divulguée.

Une autre approche cherche plutôt à augmenter le niveau général de sécurité des systèmes d'information en ne divulguant pas - ou pas systématiquement - les vulnérabilités pour les utiliser en faisant de « l'attaque à des fins de défense ». Concrètement, il s'agit d'utiliser ces vulnérabilités pour s'introduire dans des systèmes susceptibles d'être mobilisés à des fins qui iraient à l'encontre des intérêts d'une nation (par ex. : espionnage étatique, sabotage d'infrastructures critiques, terrorisme).

Cette posture ne met pas à l'abri certaines vulnérabilités, qui, découvertes, sont utilisées en secret par des acteurs malveillants. Elle laisse ainsi la porte ouverte, en ne permettant pas à de nombreux systèmes légitimes d'être complètement protégés, les exposant à des risques directs de compromission, et plus largement en exposant leurs éditeurs à des risques de perte de confiance des utilisateurs. Ce choix de politique publique emporte également d'importantes considérations de confiance vis-à-vis de l'action gouvernementale.

Sur le territoire national, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), qui est qualifiée en matière de sécurité et défense des systèmes d'information, n'a ainsi aucune prérogative de renseignement. Lorsqu'elle a connaissance d'une vulnérabilité, sa mission est sans ambiguïté : agir dans l'intérêt de la protection et de la défense des systèmes concernés.

En revanche, le débat s'est déporté sur une autre question essentielle : la protection juridique des découvreurs de vulnérabilités, appelés parfois « lanceurs d'alerte », dont l'activité était exposée à des sanctions pénales. En 2016, l'article 47 de la loi pour une République numérique a ainsi prévu que le code de la défense soit complété par un article L. 2321-4, disposant que « pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information (N.D.A. : l'ANSSI) une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.

« L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que les conditions dans lesquelles celle-ci a été effectuée.

« L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

Il est à noter que l'ANSSI lance une nouvelle solution pour sécuriser et homologuer les services publics en ligne : MonServiceSécurisé
« Avec MonServiceSécurisé, l'ANSSI accompagne les administrations et ainsi tous les agents du service public, quel que soit leur niveau de cybersécurité, en leur offrant un outil pédagogique pour simplifier leurs démarches de sécurisation et d'homologation. Cette solution est également un gage de confiance pour leurs partenaires et leurs usagers », a déclaré Emmanuel Naëgelen, Directeur général adjoint de l'ANSSI.

Ainsi, la cybersécurité **est devenue aujourd'hui un sujet majeur en** termes de politiques **publiques et les enjeux qui en découlent** sont devenus extrême**ment important**s**. En effet, la numérisation** de nos sociétés a **développé de nouvelles dépendances, de** nouvelles vulnérabilités qui impactent au quotidien tous les domaines de notre vie à l'instar de la santé, du commerce, des transports, etc.

Par ailleurs, avec la période de crise sanitaire, le télétravail s'est fortement développé lors des différentes périodes de confinements laissant entrevoir la mutation du travail de demain

De ce fait, le développement des nouvelles technologies et des usages du numérique a engendré des conséquences à l'échelle locale, nationale et internationale. Ces grandes mutations technologiques ont fait prendre conscience aux collectivités territoriales, entreprises et aux États qu'il était essentiel de ne pas négliger les investissements concernant le développement des infrastructures numériques.

Avec l'accès à Internet, devenu indispensable, la numérisation de nos sociétés génère des gains de productivité et des économies considérables. Le développement des « territoires intelligents » permet ces économies, notamment avec l'utilisation de capteurs qui réduisent les consommations énergétiques, ainsi que l'installation de la 5G et demain de la 6G. Mais cette dépendance au numérique n'est pas sans conséquence lorsqu'il existe une faille dans le réseau.

Témoignages

Le vrai sujet est le coût humain et les coûts cachés de la cybersécurité !

Plusieurs collectivités ont entrepris des initiatives en matière de sensibilisation, soit qu'elles aient participé à la table ronde au Sénat le 28 octobre 2021, soit qu'elles soient citées sur le site cybermalveillance.gouv.fr

« L'actualité récente a montré qu'une prise de conscience des collectivités locales face aux enjeux de la cybersécurité était nécessaire. Dans ce contexte, la mairie de Longueil-Sainte-Marie (60) a souhaité engager des actions pour connaître, dans un premier temps, son niveau de sécurité, puis dans un second temps, mettre en place les mesures correctives nécessaires.

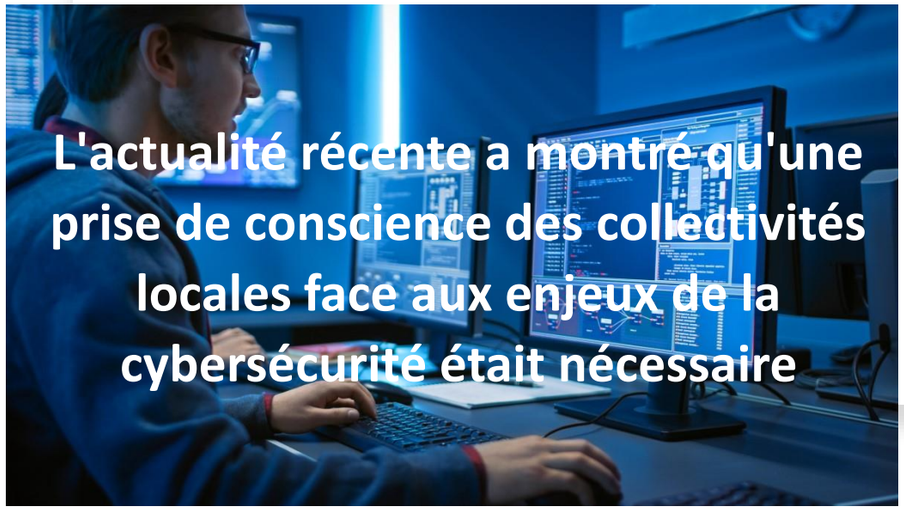
Accompagnés par l'Association pour le développement et l'innovation numérique des collectivités (Adico), nous avons préparé un dossier d'homologation au RGS (Référentiel Général de Sécurité). Cette étude a permis de cartographier notre système d'information et de procéder à une analyse de risques sur l'ensemble de son périmètre. En disposant de cette vision globale, nous avons pu définir un plan d'action qui permet de réduire les risques. Concrètement, cela se traduit essentiellement par de la sensibilisation et nous envisageons notamment de réaliser des campagnes de faux mails d'hameçonnage afin d'accroître la vigilance des agents et des élus.

Au terme de cette étude, un arrêté d'homologation a été pris. À l'instar des démarches menées dans le cadre de notre mise en conformité au RGPD, cette décision représente un engagement éthique auprès de nos administrés. À l'entrée de la mairie, un autocollant est même affiché pour que les usagers puissent facilement comprendre qu'ils entrent dans un environnement de confiance numérique. »

Longueil-Sainte-Marie (60)

« Lors de l'attaque des sites institutionnels de la ville de Toulouse en mai dernier, nous avons dû mettre en place en urgence une cellule de gestion de crise. Fin 2020, la vague d'attaques EMOTET ne nous a pas épargnés, cependant, nous étions davantage préparés. Notre partenaire, Orange CyberDefense (OCD) nous a accompagnés pendant une quinzaine de jours dans l'organisation, les prises de décisions et le management des opérations (techniques, communication, etc.). Ce retour d'expérience nous a permis de consolider notre dispositif et d'identifier les points à améliorer. En parallèle, nous avons poursuivi les actions de remédiation et d'amélioration de nos infrastructures, de nos outils de détection et d'analyse. Nous sommes actuellement en train de réaliser un guide sur la gestion de crise au sein de la collectivité et nous allons organiser prochainement un exercice de gestion de crise cyber pour entraîner nos agents et nous préparer. »

Toulouse Métropole (31)



L'agglomération de la Rochelle, dans le cadre de ses services mutualisés travaille depuis plusieurs années à l'amélioration continue de sa cybersécurité.

Ainsi, une charte à destination de la communauté d'agglomération et de la ville de La Rochelle est en cours de rédaction à destination de tous les acteurs utilisant les Systèmes d'Information (élus, agents, personnel non permanent...) pour protéger les valeurs de nos collectivités : la disponibilité et la qualité du service public, le respect des obligations légales, la confidentialité et l'intégrité des données sensibles, la protection des investissements, la valorisation de l'image et la préservation de l'environnement.

De plus, nous mènerons des campagnes de sensibilisation pour présenter la charte et ses bonnes pratiques à l'ensemble de nos collaborateurs.

Nous envisageons également de créer un parcours de sensibilisation pour les nouveaux arrivants d'une demi-journée autour de questions très pragmatiques : Où est-ce que je dois stocker mes données pour qu'elles soient sauvegardées ? Pourquoi est-il primordial d'éteindre ses équipements le soir ? Comment je peux déclarer un incident ? Et donner des conseils sur la gestion des mots de passe, les mails malveillants, les usages pro-perso, la protection de la vie privée, etc.

Enfin, il nous semble important de former spécifiquement les acteurs manipulant des données dites « sensibles » sur une journée complète avec des exercices et une évaluation finale. »

La Rochelle (17)

« 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, technique appelée hameçonnage (phishing en anglais). Face à ces constats, nous avons décidé de former en ligne tous nos agents et élus pour leur apprendre à déjouer les pièges des e-mails malveillants. Puis, notre responsable de la sécurité des systèmes d'information (RSSI) a lancé une campagne intensive de faux mails d'hameçonnage sans information préalable. Le résultat : 23 % des agents ont manqué de vigilance et cliqué. Nous avons décidé d'inscrire la campagne dans la durée. Et les résultats sont très encourageants ! Le taux de clics a considérablement baissé, de 23 % à 6 % en un an. C'est une très bonne nouvelle pour la collectivité. »

Vannes (56)

« Même nos petites communes peuvent être victimes de cybermalveillance, comme le vol de données, le piratage avec demande de rançon, etc. Faire connaître la plateforme de prévention et d'assistance Cybermalveillance.gouv.fr au plus grand nombre est indispensable afin que les agents des collectivités sachent vers qui se tourner en cas de cyberattaque. De plus, la sensibilisation aux bonnes pratiques en matière de sécurité numérique avec l'affichage de conseils a permis d'initier au sujet en interne et susciter des questionnements. »

Tillières-sur-Avre (27)

« Faisant suite au renouvellement de la flotte informatique (postes et serveurs) début 2016, l'Office a souhaité réaliser un audit de sécurité afin de renforcer le pilotage du Système d'Information (SI). Avec le soutien de SOLURIS, une analyse de risques a été réalisée pour déterminer la criticité des applications métiers et identifier les vulnérabilités du système d'information pour pouvoir apprécier les risques et les traiter si nécessaire. Dans ce cadre, le Référentiel Général de Sécurité (RGS) a été mis en oeuvre afin d'appliquer les bonnes pratiques de gestion de la sécurité pour le Système d'Information.

La sensibilisation du personnel est apparue comme un axe essentiel afin que chaque utilisateur prenne conscience des enjeux en matière de sécurité et de vie privée. Plusieurs actions sont menées en ce sens.

Afin d'accompagner la mise en place d'une charte informatique opposable, un travail impliquant les collaborateurs a été engagé en 2018/2019 sur les pratiques essentielles de sécurité à mettre en oeuvre au quotidien. Ce travail a permis d'élaborer une affiche distribuée et expliquée au personnel lors d'un petit déjeuner de travail. Ce document est diffusé à chaque nouvel arrivant lors de sa prise de poste.

Chaque année, des actions de sensibilisation sont menées.

Chaque trimestre, une newsletter est diffusée pour rappeler une bonne pratique ou attirer l'attention sur un risque informatique. Par exemple en septembre 2020, la newsletter « Les mots de passe, c'est un peu comme les brosses à dents » a permis de faire un rappel des règles relatives à la gestion des mots de passe.

Annuellement, une réunion de sensibilisation est organisée avec le soutien de SOLURIS. En 2020, les agents de proximité et les responsables d'immeubles qui venaient d'être dotés de téléphones portables ont pu être sensibilisés aux cybermenaces et prendre connaissance des pratiques de sécurité à mettre en œuvre sur les smartphones.

Un groupe de travail « sécurité informatique » composé de 4 collaborateurs et du référent sécurité de l'Office a été créé en 2017. Ce groupe de travail suit les plans d'actions annuels portant sur la sécurité informatique et la protection des données, rédige les newsletters et s'assure de l'acceptabilité et de la mise en œuvre des règles de sécurité auprès du personnel. »

Rochefort Habitat Océan (17)

« En janvier 2021, la Ville et l'agglomération d'Angers ont été la cible d'une cyberattaque avec rançongiciel, qui a immédiatement et durablement impacté les services de la Ville. Les connexions ont été réalisées depuis une adresse IP hors de France. L'attaque s'est déroulée dans la nuit du vendredi 15 au samedi 16 janvier. Ainsi, les 3000 postes informatiques et plus de 500 serveurs du Centre communal d'action sociale (CCAS), de la ville d'Angers et de la communauté urbaine ont été totalement immobilisés suite à une attaque informatique criminelle. Pendant plusieurs semaines les agents se sont retrouvés privés de leurs outils de travail : mails, applications métier, logiciels… Si les messageries et la bureautique ont pu être réinstallés sous dix jours et le travail reprendre progressivement, les services en ligne à destination des usagers – démarches administratives, inscription en crèche et en bibliothèque ont mis davantage de temps à être rétablis. Suite à cette attaque le Maire-Président, Christophe Béchu a voulu la plus grande transparence en termes de communication.

En effet, c'est d'abord, le compte personnel du Maire-Président qui a été piraté et ensuite, une attaque d'une plus grande ampleur a visé les services informatiques et numériques de la mairie.

La mairie a même dû ressortir le fax, rangé depuis de nombreuses années. "Je ne pensais pas que l'on en aurait cet usage en 2021. Il sert typiquement, comme hier, à envoyer le dépôt de plainte au procureur, de manière à ce qu'il arrive en temps réel au lieu d'envoyer quelqu'un pour le porter", explique Christophe Béchu. L'impact de la cyberattaque dépasse le simple cadre de la mairie. Par exemple, la bibliothèque a dû être fermée puisque la base de données n'était plus accessible à cause de la cyberattaque. En France, c'est l'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information qui lutte contre ces attaques. Donc dès le samedi matin, la mairie d'Angers s'est rapprochée d'eux.

"Le poids de l'informatique dans la vie quotidienne des services publics n'a cessé d'augmenter. Avec le Covid, avec toutes les procédures à distance, avec le télétravail, on a continué à mettre dans nos serveurs des fonctionnalités qui autrefois n'existaient pas. On s'est beaucoup plus concentrés sur le fait d'augmenter les services qu'on offrait à la population via le numérique qu'au fait de protéger l'architecture de ces systèmes", conclut le maire d'Angers.

Angers (49)

Propositions

Ainsi, à travers nos actions et démarches, nous sensibilisons, informons et formons depuis des années les élus et les agents sur les questions liées à la cybersécurité via nos colloques, rencontres et formations en intra ou en visioconférence en mettant l'accent plus particulièrement sur les enjeux et usages du numérique, de la protection des données et surtout de la cybersécurité et de ses innombrables questionnements. Des sujets incontournables à l'heure du fort développement du télétravail.

Ainsi plusieurs propositions sont à décliner :

Les recommandations de la Fédération Française de la Cybersécurité en partenariat avec le Commandement de la Gendarmerie dans le Cyberespace ComCyberGend et Mission Ecoter-France et Territoires Numériques.

- **Organisationnel**

- Identifier les référents institutionnels en cas de crise (ANSSI, Police Nationale, Gendarmerie...) Définir un plan de gestion de crise (opérationnelle et communication) :

→ Définir le rôle de chacun en cas de cyberattaques

→ Suivre une liste de priorités en cas de cyberattaques

- Définir et mettre en place une politique de protection des systèmes d'information et des données personnelles

- Prévoir un guide cyber à destination des élus avec une étude d'impact adaptée à l'institution

- Avoir un arbre de décision pour les élus (DSI ou non) des collectivités territoriales

- Qualifier ses prestataires (Plan Assurance Sécurité) et les auditer.

- **Sensibilisation**

- Sensibiliser des utilisateurs des outils informatiques (cybermalveillance.gouv.fr) Sensibiliser le département informatique vis-à-vis des risques encourus (une cyberattaque n'est pas que de la technique (il existe également les aspects humain et opérationnel) Séparer utilisation personnelle et professionnelle

- Développer un guide d'hygiène informatique à transmettre à tous les membres de la collectivité (une charte du bon usage d'Internet et des réseaux sociaux)

- Encourager la formation du personnel sur les risques de cybersécurité (MOOC ANSSI, etc) Prévoir une vigilance informatique

- Prévoir les comportements post-attaques (notamment les réactions psychologiques).

- **Technique**

- Effectuer un bilan de maturité

- Sécuriser les messageries et les mots de passe

- Séparer les réseaux d'utilisation quotidienne et les réseaux de stockage des données Mapping de tous les appareils existants (matériels, utilisateurs, etc.) et faire remonter l'apparition de nouveaux appareils

- Effectuer des sauvegardes régulières

- Ne pas connecter un support amovible personnel à vos équipements professionnels Activer les mises à jour pour les services de pare-feu, antivirus, DNS, AD, etc.

En complément, d’autres conclusions furent tirées lors de la table ronde du 28 octobre 2021 au Sénat sur le thème : « Les collectivités territoriales face au défi de la cybersécurité »

« **1. Sensibiliser les élus communaux et intercommunaux ainsi que leurs services aux enjeux de la cybersécurité.**

Un travail d'information doit être mené en particulier, sur :

- L’ampleur des menaces numériques, lesquelles sont accentuées par trois facteurs :

a)Le développement des services publics numériques et des territoires connectés ;
b)Le recours grandissant au télétravail dans la fonction publique territoriale;
c)La formation insuffisante des élus et des agents.

- L’existence de lourdes conséquences en cas d'attaques :

a)Dysfonctionnement des services publics locaux (mise à l'arrêt de parkings, de piscines, de musées, de stations d'épuration, graves perturbations de l'état civil empêchant, par exemple, la délivrance de permis d'inhumer pendant une semaine...) ;
b)Perte irrémédiable de données informatiques, de ressources humaines et financières ;
c)Conséquences financières : mise au chômage technique d'employés de mairie, pertes de ressources liées à la mise à l'arrêt de certains services payants, éventuel paiement de rançons...
d)Conséquences humaines : altération du lien de confiance avec les citoyens et impact psychologique sur les agents territoriaux.

2. Appliquer le principe de subsidiarité en matière de politique de sécurité numérique.

Deux critères doivent être pris en compte pour apprécier le niveau pertinent d'intervention : la soutenabilité financière et la technicité requise. Ce principe permettrait aux petites collectivités, identifiées comme des « maillons faibles », de bénéficier, par l'effet de la mutualisation, d'une protection numérique renforcée. L'échelle de pertinence doit être appréciée in concreto selon les réalités territoriales. Il peut s'agir du niveau soit intercommunal soit départemental. Cette recommandation suppose toutefois de lever les freins psychologiques tenant à la sensibilité des données des communes et à la crainte corrélative du transfert de ces dernières.

3. Mettre en place des plans ou des procédures de continuité et de reprise d'activité en cas de survenance d'une crise d'origine numérique (mesures d'urgence à prendre, prestataires à contacter, notification aux autorités publiques telles que la CNIL et l'ANSSI...).

4. Revaloriser les fonctions de RSSI (responsable de la sécurité des systèmes d'information) dans les collectivités d'une certaine taille.

Il est nécessaire d'en faire un véritable « directeur de la Sécurité numérique » dont les fonctions ne doivent pas perçues comme uniquement techniques. Le caractère stratégique de cette fonction doit se traduire dans la rémunération proposée ainsi que dans l'organigramme des services (rattachement à la Direction générale par exemple). »

Banque des Territoires
Caisse des Dépôts

La Banque des Territoires est une Direction de la Caisse des Dépôts qui rassemble des expertises de conseil et de financement à destination des acteurs territoriaux pour faciliter la réalisation de leurs projets. Au service de l'intérêt général, elle propose des solutions de financement et d'accompagnement aux collectivités locales, entreprises publiques locales, aux organismes de logement social et aux professions juridiques. La Banque des Territoires se donne pour mission d'accompagner la transformation et la modernisation des territoires de France. Dans cette perspective, le thème de la confiance numérique s'impose naturellement comme une problématique stratégique pour la Banque des Territoires.

L'actualité quotidienne illustre la nécessité absolue pour les acteurs territoriaux de bien « maîtriser » le numérique, plus particulièrement sous l'angle de la cybersécurité. On ne compte malheureusement plus les exemples de villes dans le monde que des cyberattaques ont momentanément paralysées. En France, l'autorité nationale en matière de cybersécurité, l'ANSSI, a constaté une explosion des cyberattaques en 2020, avec des attaquants qui se professionnalisent de plus en plus, tendance confirmée en 2021 avec un nombre d'attaques par rançongiciel multiplié par quatre. La crise sanitaire, qui a favorisé le développement du télétravail et fragilisé ainsi les périmètres de sécurité numérique des entreprises, n'est pas le facteur principal de cette hausse en réalité structurelle.

Cette question de maîtrise numérique et de protection va être de plus en plus prégnante

Grandes, médianes ou petites, toutes les villes et intercommunalités sont concernées par cette problématique de « confiance numérique », ainsi que les départements et les régions. C'est notamment vrai au travers de services déjà largement ***digitalisés*** comme le sont ceux d'état civil, d'urbanisme ou encore de gestion administrative. De plus en plus de services se ***digitalisent***, et cela concernera bientôt la plupart de ceux proposés par toutes ces collectivités au fur et à mesure que s'informatiseront leurs infrastructures de transport, d'énergie, d'eau, leur signalisation routière, leur éclairage, leurs systèmes de vidéoprotection, etc.

Cette question de maîtrise numérique et de protection va être de plus en plus prégnante. Et ceci concerne également d'autres acteurs territoriaux que sont les établissements de santé et les ports, de plus en plus numériques, qui voient leurs missions cruciales régulièrement mises en péril par des cyberattaques.

Dans ce contexte d'urgence, un constat doit cependant être partagé aujourd'hui : les acteurs des territoires manquent de solutions de cybersécurité adaptées à leur profil :

- Des solutions maniables par des équipes non expertes ;
- Des solutions accessibles aux budgets de tous les acteurs territoriaux ;
- Des solutions mutualisables avec simplicité et souplesse entre différents acteurs territoriaux.

Positionnement de la Banque des Territoires

Au sein de la Caisse des Dépôts, la Banque des Territoires porte notamment les activités du groupe au profit des acteurs territoriaux. Tiers de confiance historique, elle a vocation à accompagner les transitions de tout type qu'ils traversent, et en particulier la transition numérique : dans cette perspective, le thème de la confiance numérique s'impose naturellement comme une problématique stratégique.

La Banque des Territoires s’est ainsi positionnée sur le sujet de la confiance numérique, à travers trois axes principaux :

- L’investissement dans l’innovation technologique au service des territoires : cybersécurité, identité et signature numériques, souveraineté numérique, legaltech ;
- La sensibilisation des acteurs territoriaux, avec la réalisation en 2020 d’un guide et de plusieurs vidéos conçues sur mesure pour les élus des collectivités locales ;
- Dans le cadre du Programme d’Investissements d’Avenir – devenu « France 2030 » – de l’Etat, participation en tant qu’expert à des jury d’attribution et opération d’un mandat d’appel à manifestation d’intérêt « Sécuriser les territoires ».

L’investissement dans la confiance numérique et la cybersécurité

Afin d’aider au déploiement de solutions de confiance numérique et de cybersécurité adaptées aux territoires, la Banque des Territoires peut :

- Soit investir dans une startup proposant déjà une telle offre, afin de l’aider à renforcer son innovation et son déploiement sur les territoires ;
- Soit investir dans une startup dont l’offre technologique, adaptée à une typologie de clients plus proche des grands comptes, est susceptible d’être déclinée à court ou moyen terme dans une version moins experte et accessible aux acteurs des territoires. Le financement apporté par la Banque des Territoires est alors fléché vers cet axe stratégique.

La Banque des Territoires a ainsi investi en 2021 dans la start-up rouennaise Yes We Hack, qui automatise et optimise le recours de ses clients aux services de « hackers éthiques » afin que ceux-ci détectent et signalent des failles de sécurité inconnues, véritables chemins d’accès pour des cyberattaquants hostiles.

Elle a également investi en 2022 dans la start-up lyonnaise Hackuity, qui part du constat que plus des trois quarts des cyberattaques exploitent une vulnérabilité système ou logicielle connue mais non corrigée par l'entité attaquée. Hackuity propose une vision à 360° des vulnérabilités de ses clients, et les aide à optimiser le défi sans fin de leur remédiation – l'application des fameux patches et mises à jour de sécurité aux systèmes les plus critiques.

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

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

A travers six objectifs clés, l'ambition est de permettre une très forte croissance de la filière française de cybersécurité, qui permettra de faire rayonner la France dans une concurrence internationale accrue et de permettre le doublement des emplois de la filière. Prérequis évident au renforcement de la filière, la stratégie nationale vise à stimuler la recherche et l'innovation industrielle françaises en matière de cybersécurité, à travers des liens stratégiques entre recherche publique et privée qui mèneront à une augmentation des thèses et des brevets.

Les collectivités et acteurs des territoires ne sont pas délaissés. Un budget de 136 millions d'euros a été confié à l'ANSSI afin de renforcer la cybersécurité de l'Etat et des territoires sur la période 2021-2022. Un dispositif et des aides financières permettent d'améliorer la sécurisation de chacun des acteurs concernés (collectivités, hôpitaux, administrations), tandis qu'un accompagnement est dispensé pour favoriser l'émergence de CSIRTs (*Computer Security Incident Response Team*) régionaux, afin de mieux fédérer au niveau régional la réponse aux crises d'origine cyber qui frappent les collectivités territoriales et administrations locales.

La Banque des Territoires est pleinement impliquée dans la stratégie et dans le Programme d'Investissement d'Avenir / France 2030

- **En tant qu'expert invité à certains jurys d'audition d'octroi de financement ;**

- **En tant qu'opérateur d'un appel à manifestation d'intérêt (AMI) « Sécuriser les territoires » pour le compte de l'Etat afin d'aider à faire émerger les innovations de cybersécurité de demain adaptées aux besoins des collectivités, hôpitaux et ports.**

Atos

Atos est un leader international de la transformation digitale avec 112 000 collaborateurs et un chiffre d'affaires annuel d'environ 11 milliards d'euros. Numéro un européen du cloud, de la cybersécurité et des supercalculateurs, le Groupe fournit des solutions intégrées pour tous les secteurs, dans 71 pays. Pionnier des services et produits de décarbonation, Atos s'engage à fournir des solutions numériques sécurisées et décarbonées à ses clients. Atos est une SE (Société Européenne) cotée sur Euronext Paris.

La raison d'être d'Atos est de contribuer à façonner l'espace informationnel. Avec ses compétences et ses services, le Groupe supporte le développement de la connaissance, de l'éducation et de la recherche dans une approche pluriculturelle et contribue au développement de l'excellence scientifique et technologique. Partout dans le monde, Atos permet à ses clients et à ses collaborateurs, et plus généralement au plus grand nombre, de vivre, travailler et progresser durablement et en toute confiance dans l'espace informationnel.

La cybersécurité, un enjeu de service public pour les collectivités

Entre 2019 et 2020, l'ANSSI a recensé une hausse de 255 % des attaques par rançongiciels. À lui seul, ce chiffre traduit l'insécurité numérique à laquelle sont désormais confrontées les collectivités et les administrations. Insuffisamment préparées, vulnérables, elles ont été parmi les principales victimes de ces actes de malveillance, qu'elles ont souvent payé au prix fort. Les nécessaires et bénéfiques transformations digitales amènent le numérique à prendre de plus ne plus d'importance dans l'action et le fonctionnement des collectivités. Et en parallèle, les dommages peuvent être potentiellement élevés. Dommages opérationnels, d'abord, car les services sont durablement perturbés, avec parfois des conséquences humaines et matérielles dramatiques. Dommages financiers, ensuite, car il faut réparer ce qui a été endommagé, quand c'est possible. Dommages psychologiques, enfin, car la confiance des agents et des administrés en ressort profondément ébranlée, de même que l'image et l'attractivité du territoire.

La cybersécurité est une affaire d'organisation, de méthode et d'attentions au quotidien

Malheureusement, les dommages comme les menaces ne vont aller qu'en s'amplifiant. D'une part, parce que les collectivités accélèrent leur nécessaire transformation numérique, voire jouent un rôle central dans celle de leur territoire, et possèdent donc des données toujours plus abondantes et plus sensibles. D'autre part, parce que le cyberespace apparaît désormais comme le terrain privilégié des confrontations géopolitiques, du crime organisé et de la délinquance crapuleuse, autant de dangers dont la collectivité peut être la victime intentionnelle ou collatérale.

Dans ce contexte, les élus ne peuvent plus ignorer la cybersécurité, ou la déléguer entièrement à leur service informatique au prétexte que ce serait une question purement technique. Ils doivent s'emparer du sujet car, désormais, l'enjeu est politique : la qualité et la continuité du service public, la réalisation des projets du territoire, et la confiance de la population dans ses représentants et son administration dépendent du bon fonctionnement des systèmes numériques et de la protection des données qu'ils renferment. La cybersécurité est clairement une préoccupation que doit partager l'ensemble de la structure et des agents et qui, de ce fait, relève du champ d'intervention et de responsabilité des élus.

Certes, il ne s'agit pas de demander à ces derniers de choisir tel ou tel antivirus, mais ils doivent impérativement prendre conscience qu'avant d'être une question d'outils, la cybersécurité est une affaire d'organisation, de méthode et d'attentions au quotidien. Et que, de ce point de vue, ils peuvent donner l'impulsion et appuyer de leur détermination des actions qui ne coûtent pas forcément très cher mais qui peuvent avoir un impact déterminant. Dans leur commune, leur métropole, leur département ou leur région, ils peuvent être les moteurs d'un plan de mise à niveau en quatre temps.

1. Connaître et réduire la surface d'exposition

Dans la très grande majorité des cas, les collectivités touchées par une attaque ne sont pas spécifiquement visées, mais prises dans de larges filets jetés à l'aveuglette par des hackers. Or, pour passer entre leurs mailles, il suffit de se faire petit. Dans le jargon de la cybersécurité, on parle de réduire sa surface d'exposition (ou surface d'attaque), c'est-à-dire de limiter au maximum les points d'entrée par lesquels peuvent s'infiltrer les pirates et leurs logiciels malveillants. La première chose est donc de passer au crible le système d'information pour connaître cette surface d'exposition et prendre quelques mesures de précaution immédiates pour la minimiser. Des outils existent et sont librement accessibles pour opérer ces premières démarches d'inventaire ; quelques jours, au plus, suffisent pour obtenir une idée assez claire de son niveau d'« exposition ».

La très vaste majorité des cyberincidents peut ainsi être évitée

2. Évaluer et améliorer son hygiène numérique

Après avoir recensé les « portes et fenêtres » du système d'information, et condamné celles qui ne servent à rien, on s'assure ensuite que les autres, celles qui sont indispensables à la communication, à la collaboration et à l'échange de données, sont correctement protégées. Les hackers préfèrent les proies faciles et, s'ils ne trouvent pas une ouverture laissée entrouverte par négligence, méconnaissance ou imprudence, ils passent généralement leur chemin. La très vaste majorité des cyberincidents peut ainsi être évitée si l'on améliore ce qu'on appelle l'« **hygiène numérique** », c'est-à-dire un ensemble de réflexes élémentaires de précaution.

Cette prophylaxie digitale concerne au premier chef les équipes informatiques, à travers, par exemple, la mise à jour consciencieuse des logiciels, le débranchement des machines inutilisées, l'actualisation régulière des droits d'accès, ou encore le respect des bonnes pratiques de conception (Security by Design) et de développement. Cependant, le gros de l'effort doit porter sur le reste du personnel car la plupart des attaques commence par un clic sur un lien douteux, le téléchargement d'un logiciel d'apparence anodine, le choix d'un mot de passe trivial ou une utilisation mal maîtrisée des outils connectés. Involontaires maillons faibles de la cybersécurité, les agents peuvent en devenir les fers de lance en adoptant quelques bonnes pratiques au quotidien.

Grâce à des ressources prêtes à l'emploi comme les préconisations de l'ANSSI ou le site cybermalveillance.gouv.fr, qui propose, par exemple, « IMMUNITÉ cyber », un questionnaire d'auto-évaluation établie par la gendarmerie nationale et l'Association des maires de France, les collectivités peuvent évaluer leur hygiène numérique, identifier leurs principales lacunes, et mettre en œuvre des actions de remédiation, de sensibilisation et de formation. Là encore, ce sont des chantiers rapides, peu coûteux, et tout autant adaptés aux métropoles qu'aux mairies rurales. Une bonne hygiène numérique est même plus cruciale encore pour les petites structures, qui disposent de moins de moyens alors que leurs services et leurs données n'ont pas moins de valeur pour leurs administrés.

3. Analyser les risques

Les deux premières étapes permettent de parer à l'essentiel. Dans la suivante, on va s'interroger sur la probabilité d'être malgré tout victime d'une attaque et sur les dégâts qui en résulteraient. Cette approche par le risque et le prisme de scénarios redoutés permet de faire émerger des actions prioritaires et d'élaborer une feuille de route. Celle-ci débute souvent par quelques mesures simples mais capitales, comme clarifier la marche à suivre en cas de comportement suspect du système d'information.

Une bonne hygiène numérique est même plus cruciale encore pour les petites structures, qui disposent de moins de moyens alors que leurs services et leurs données n'ont pas moins de valeur pour leurs administrés.

Alors qu'en cas d'attaque, la vitesse de réaction est cruciale pour limiter les dégâts, trop peu de collectivités ont mis en place de telles procédures. Auparavant réservées à un public expert, les analyses de risques se généralisent et les méthodes sont aujourd'hui librement accessibles sur le site de l'ANSSI. L'objectif est bel et bien de faire en sorte qu'elles soient intégrées aux pratiques IT de la collectivité et que les SI les plus critiques soit clairement identifiés, documentés et protégés (inventaire fiable, authentification renforcée, sauvegardes, mise à jour, …). Pour une première approche, une dizaine de jours d'effort sont nécessaire pour identifier les SI les plus critiques et élaborer les plans d'actions et la stratégie, en incluant la collecte des informations essentielles.

4. Déployer des solutions de défense et mobiliser l'organisation

Enfin, ce n'est qu'en dernier lieu que l'on s'intéresse aux dispositifs technologiques de défense active. On l'a dit, les collectivités sont le plus souvent les victimes malchanceuses d'attaques aveugles, que le déploiement rigoureux de mesures de protection élémentaires suffit en général à endiguer. Cependant, il leur arrive aussi d'être la cible d'attaques délibérées, et elles le seront probablement de plus en plus. En effet, du fait de leur rôle croissant dans la gestion d'infrastructures et de services essentiels (eau, énergie, mobilité…), dans le domaine de la santé et de l'aide sociale, dans le développement économique des territoires et comme tiers de confiance du partage des données à l'échelle locale, leurs systèmes et leurs données sont davantage exposés à la convoitise et à la malveillance des pirates. L'analyse de risques aura permis d'identifier ces menaces, d'en évaluer les impacts potentiels et de déterminer les dispositifs organisationnels et techniques à même de les contenir.

Simple, rapide et peu coûteuse en comparaison des enjeux, cette démarche en quatre temps, dont il est essentiel de respecter la chronologie, peut progressivement mais rapidement élever le niveau de la sécurité numérique de la collectivité face à des attaques inéluctables. Elle nécessite l'appui sans faille des élus pour en faire une priorité et mobiliser toute l'organisation, mais aussi l'accompagnement d'un spécialiste de la cybersécurité, qui apportera méthode, expertise et renforts aux équipes informatiques, par ailleurs très sollicitées sur le front de la transformation numérique.

Cisco

Cisco est le leader mondial des technologies permettant à l'Internet d’exister depuis plus de 35 ans. Sa mission est de connecter de manière sécurisée les personnes, les applications et les objets.
Cisco a été choisi comme partenaire officiel des Jeux Olympiques et Paralympiques de Paris 2024 sur les infrastructures de cybersécurité, les équipements réseaux et les logiciels de visioconférence. Ce choix s’est fait notamment pour son expérience internationale et sa large gamme de solutions de cybersécurité. Cisco travaille donc au quotidien avec les équipes du comité d’organisation (COJOP) et avec Atos pour se préparer à la protection, à la détection et à la réponse face à d’éventuelles cyber attaques.

1) Tendances et constats observés récemment :

a) Une menace toujours plus grande, toujours plus coûteuse et insaisissable :

- **Hausse du nombre d'attaques**
  - La période Covid a vu l'accélération de la digitalisation des entreprises et des collectivités, et du développement du travail hybride. En parallèle, le nombre de cyberattaques a constamment augmenté, avec une sophistication toujours plus grande, que ce soit dans l'accès aux réseaux, la pénétration des systèmes d'information, voire la fourniture de logiciels malveillants à travers sa chaîne logistique.
    - Ainsi en France 54% des entreprise en 2021 ont subi une attaque, (OpinionWay Cesin 2022)
      https://www.infoprotection.fr/le-cesin-livre-ses-derniers-enseignements-sur-la-cybersecurite/#:~:text=Selon%20le%20dernier%20Barom%C3%A8tre%20de,des%20collaborateurs%20semblent%20s'%C3%A9mousser.

- Dans son Panorama de la menace informatique "L'Agence Nationale de la Sécurité des Systèmes d'Information" (ANSSI) reporte une augmentation de 37% des intrusions avérées dans des systèmes d'information en 2021.
  (https://www.ssi.gouv.fr/actualite/une-annee-2021-marquee-par-la-professionnalisation-des-acteurs-malveillants/)

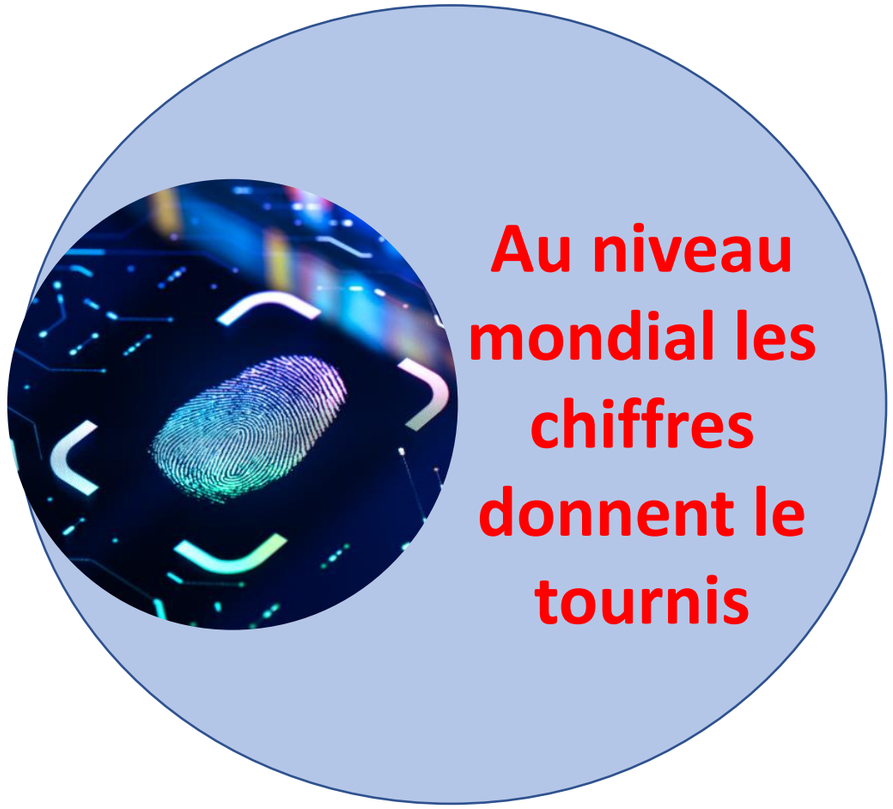
- Le nombre de cyberattaques augmente en volume, car on peut distinguer :
  - Des attaques organisées et préparées sur des cibles qui peuvent rapporter gros en termes d'impact financier ou de déstabilisation
  - Mais aussi des attaques aléatoires automatisées, où des robots ratissent le plus large possible, quelle que soit la cible, sa localisation et sa taille.

D’après le centre de réponse à incident mondial de Cisco Talos Group, les ransomwares restent la principale menace au 2e trimestre 2022, (18% de toutes les menaces observées) au même niveau que les pré ransomwares (attaque de ransomware sur le point de se produire, mais le cryptage des fichiers n’a pas encore eu lieu) et devant les chevaux de Troie. Parmi les autres menaces de ce 2e - trimestre, citons les voleurs d’informations (infostealers) qui peuvent être utilisés pour accéder à une variété d’informations sensibles, telles que les coordonnées, les détails financiers et même la propriété intellectuelle en vue de les revendre ou de menacer de les publier. Enfin les malveillances internes sont en progression constante (Ex : des employés sur le départ et bénéficiant encore de droits).

- **Coût croissant des attaques :**
  - Au niveau mondial les chiffres donnent le tournis. Le coût mondial de la cybercriminalité devrait atteindre 10 500 Milliards de dollars d’ici 2025, selon une projection de « Cybersecurity Ventures » reprise à l’AG d’Interpol en Octobre 2022, avec une augmentation de 15% par an au cours des cinq prochaines années. Au congrès Cybertech de Rome les chiffres de l'Association Italienne pour la Sécurité Informatique (Clusit), cités par le Figaro/AFP du 5/05/22, évoquent un coût de la cybercriminalité de 5700 Milliards d’Euros pour l’année 2021 avec un cinquième des attaques en Europe.
    https://www.lefigaro.fr/secteur/high-tech/la-cybercriminalite-a-coute-plus-de-6000-milliards-de-dollars-en-2021-20220510

• Longtemps sous-estimées, les menaces sur les réseaux opérationnels OT (Operational Technology) s'imposent aujourd'hui comme un enjeu majeur. Les réseaux opérationnels (OT) regroupent des objets connectés, des objets industriels comme des automates, des caméras, dans des usines ou dans des villes, là où les réseaux IT (Information Technology), connectent au sein des entreprises des datacenters, des PC, des imprimantes…

De Stuxnet à log4J en passant par Pipedream, les attaques ciblant les environnements OT se sont multipliées en 2021.



- Le baromètre de la start-up française Anozrway confirme en septembre 2022, que le niveau de la menace cyber n'a jamais été aussi critique. Selon l'étude, la perte de chiffres d'affaires cumulés pour les entreprises françaises victimes de rançongiciel s'élevaient à 1,06 milliard d'euros pour la période janvier-août 2022.

- Ce coût supplémentaire inédit, vient s'ajouter aux coûts du changement climatique, de la transition énergétique et de l'inflation que devront supporter les collectivités.

- **Territorialité : la cybersécurité est devenue un fléau mondial sans frontières.**

  Contrairement à la sécurité physique, la cybersécurité n'a pas de périmètre établi.

Le nombre de vulnérabilités continue d'augmenter, entretenant la menace

- Au niveau macro, les attaques peuvent provenir soit :
  - Au niveau international, d'Etats, de groupes criminels, de terroristes, ou encore d'officines spécialisées. Leurs moyens financiers sont énormes et leurs attaques hypersophistiquées provoquent des dommages importants, notamment financiers.
  - D'amateurs aguerris, au niveau national ou international, pouvant se fournir des rançongiciels sur le darknet à des prix tout à fait abordables. Ils peuvent s'attaquer à des cibles réputées plus faibles et se contentent de gains plus modérés.

- S'il atteint les chiffres évoqués plus haut, le commerce des cyberattaques pourrait s'avérer plus rentable que le commerce mondial de toutes les grandes drogues illicites réunies.

- Au niveau micro, là où la cybersécurité se résumait à défendre le périmètre clos du système d'information d'une entreprise ou d'une collectivité, cette notion a tendance à voler en éclat avec l'adoption du Cloud et l'externalisation du stockage des données, des applications, de la puissance de calcul…supprimant la notion de cybersécurité périmétrique.

- **Le nombre de vulnérabilités continue d'augmenter, entretenant la menace :**

  Pour rappel une vulnérabilité, est une faille dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système. Elles sont la conséquence de faiblesses dans la conception, la mise en œuvre ou l'utilisation d'un composant matériel ou logiciel, qui sont en général corrigées à mesure de leurs découvertes, l'utilisateur restant exposé à une éventuelle exploitation tant que le correctif n'est pas publié et installé. C'est pourquoi il est important de maintenir les logiciels à jour avec les correctifs fournis par les éditeurs de logiciels.

  - Avec la constante croissance et diversité de l'offre IT à travers le monde, et son adoption à grande échelle, le nombre de vulnérabilités reste très grand (près de 19 000). Même si le nombre de celles qui affichent une sévérité élevée est en recul significatif en 2021 par rapport à 2020 (source NIST américain) à 3784, la menace n'est donc pas prête de s'éloigner.

- Les objets connectés dont le nombre augmente très rapidement dans la ville, embarquent eux aussi des vulnérabilités et viennent amplifier cette menace. Face à une estimation de 75 milliards d'objets connectés attendus dans le monde d'ici 2025, la communauté européenne s'est emparée d'ailleurs du sujet en septembre 2022. Elle entend ainsi poser des « exigences essentielles » aux producteurs et distributeurs en matière de cybersécurité pour tout objet connecté ou logiciel, en les priant de mettre sur le marché des objets qui ne comportent pas de vulnérabilités connues et de limiter les surfaces d'attaque. Sont concernés le hardware, mais aussi les logiciels embarqués dans tous types de capteurs : les téléphones portables, les équipements réseaux ou encore les puces. En revanche, les logiciels open source en sont exclus.

  Se pose la question de savoir quand ce règlement sera-t-il appliqué et s'il sera efficace ?

Le manque flagrant de compétences sur le marché actuel et à venir

b) La prise de conscience de l'État

- A travers le ministère délégué chargé de la transition numérique et des télécommunications, l'ANSSI, ComCybergend, Cybermalveillance.gouv.fr, la Sous-direction de lutte contre la cybercriminalité, les actions se sont multipliées montrant que l'Etat avait perçu les enjeux autour de la cybersécurité, en sensibilisant et en aidant les entreprises, les collectivités et les particuliers. Il a ainsi créé, dans le cadre de France Relance, un réseau de centres régionaux de réponse aux incidents cyber (CSIRT : Computer Security Incident Response Team), en vue de soutenir le tissu économique et social de chaque territoire face aux cybermenaces.
- Il s'est aussi attaché à développer une filière souveraine de haut niveau sur le sujet.

c) Le manque flagrant de compétences sur le marché actuel et à venir

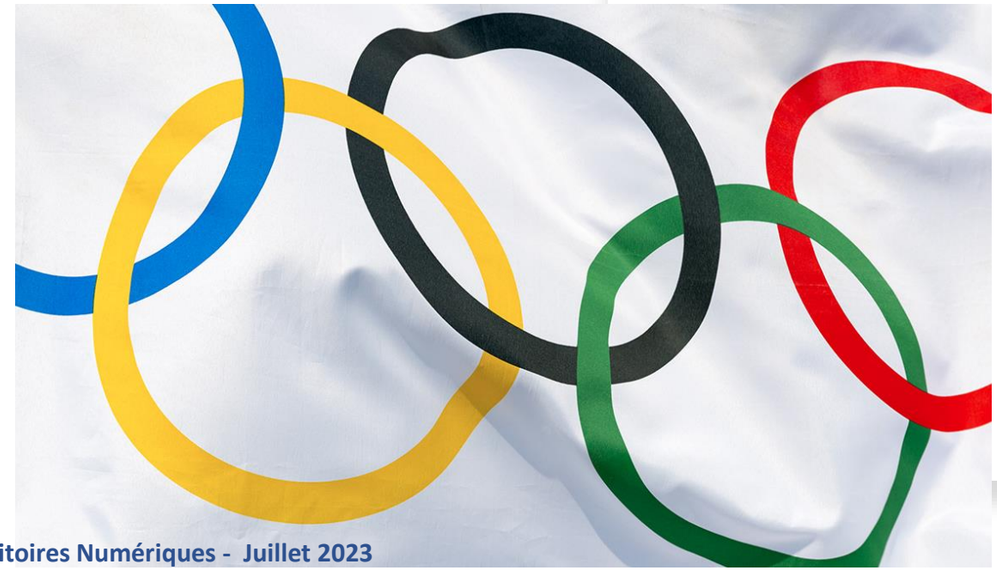
- Les chiffres varient d'une étude à l'autre mais s'accordent sur le manque de compétences cyber nécessaires, tous niveaux confondus. (Et il existe des postes accessibles sans de longues études)
- Il est question d'une pénurie de 317 000 personnes en Europe (étude 2022 de l'International Information System Security Certification Consortium (ISC)².
- Et de 15 000 en France (étude Wavestone 2022).
- Si les formations se développent, elles sont loin d'être suffisantes pour absorber la demande et combler le nombre de postes vacants.

2) Tendances et constats spécifiques aux Collectivités Territoriales :

Les RSSI des collectivités territoriales doivent se préparer à affronter de nouvelles menaces numériques dans les années qui viennent :

- **Avec Les Jeux olympiques et paralympiques de Paris 2024 et la Coupe du Monde de Rugby en 2023 la menace cyber va monter sur l'hexagone**.
  - Au-delà des risques sur l'organisation des épreuves, les collectivités hôtes et toutes leurs régions pourraient être la cible d'attaques plus ciblées à cette occasion.
- Sans faire de généralités, d'autant que les profils des collectivités sont très différents, la **cybersécurité dans les collectivités a souvent fait l'objet de compromis**, étant négligée au niveau budgétaire et humain, voire pour faciliter le confort des utilisateurs.

Avec Les Jeux olympiques et paralympiques de Paris 2024 et la Coupe du Monde de Rugby en 2023 la menace cyber va monter sur l'hexagone



- En dépit des nombreuses actions menées par l'Etat à travers l'ANSSI, ComCyberGend, Cybermalveillance.gouv.fr pour sensibiliser les collectivités locales au risque Cyber, beaucoup d'élus et d'administrations ne réalisent pas encore suffisamment les conséquences désastreuses d'une cyberattaque pour leur collectivité et ont donc du mal à les mesurer.
- Les collectivités locales ont longtemps pensé pouvoir échapper aux cyberattaques, s'imaginant ne représenter aucun intérêt pour les hackeurs, et que **« cela n'arrive qu'aux autres »**.
- Ce temps est révolu et l'actualité montre que **la question n'est plus de savoir si elles seront attaquées mais quand le seront-elles ?**

Aujourd'hui, les cyberattaques impactent davantage les administrés

- **Aucune collectivité n'est à l'abri.** Les villes étant de plus en plus regroupées en agglomérations, intercommunalités, **les hackeurs recherchent le maillon faible** à travers les plus petites, ou les moins bien protégées, pour remonter jusqu'à la tête.

- **Les villes intelligentes sont de plus en plus connectées**, leurs volumes de données augmentent, et leur sécurité n'est pas toujours garantie. Par ailleurs, dans le passé les failles de sécurité n'avaient que peu d'incidences directes sur les citoyens. **Aujourd'hui, les cyberattaques impactent davantage les administrés** (hôpitaux à l'arrêt, impossibilité d'émettre des permis d'inhumer…).

- L'adoption et l'intégration des appareils de **l'Internet des objets (IoT) et de l'Internet industriel des objets (IIoT) ont conduit à un maillage de plus en plus interconnecté des systèmes cyber-physiques (CPS)**, ce qui élargit la surface d'attaque et brouille les fonctions autrefois claires de la cybersécurité et de la sécurité physique. Désormais, les réseaux de capteurs urbains ou les caméras de surveillance, deviennent des sources potentielles d'intrusion. Une cyberattaque ou une attaque physique réussie sur les systèmes et réseaux de contrôle industriels de la ville peut ainsi perturber les opérations ou même priver la ville de services essentiels comme la santé, les transports ou l'énergie. La convergence entre systèmes d'information (IT) et systèmes opérationnels (industriels/OT) profitant des progrès de la cybersécurité, devient incontournable dans une optique de meilleure administration de ces réseaux permettant d'avoir une vision globale de la menace. À ce sujet, l'argument de réseaux qui seraient totalement isolés ne tient plus. En effet, les opérations de maintenance les concernant les obligent à s'interconnecter avec l'extérieur.

- **Le monde de l'éducation n'est plus en reste** : on estime à + de 60% le nombre d'établissements victimes de tentatives de phishing.

- **Facteur Humain :** il reste la première vulnérabilité d'une entreprise comme d'une administration face aux cyberattaques. Les collectivités adoptent de nouvelles technologies, mais ont du mal à trouver des talents pour utiliser efficacement ces solutions.

    - Tout d'abord, et malgré les efforts en cours, les agents ont encore besoin d'être sensibilisés aux menaces, en tant qu'utilisateurs du numérique dans leur environnement de travail.

- Le point commun de beaucoup de piratages est d'avoir réussi à convaincre un agent de communiquer des informations d'accès au réseau ou d'autres informations critiques à travers des faux courriels ou des sms, émanant de prestataires ou de partenaires.
- Force est de constater aussi que les ressources humaines en cybersécurité manquent et que les compétences sont difficiles à attirer pour le secteur public, qui ne peut s'aligner sur les salaires du privé.

    - Les collectivités locales peinent donc à embaucher des compétences de type RSSI et doivent souvent les mutualiser.

L'État doit continuer à s'impliquer comme il le fait…

3) Recommandations :

Notre quotidien nous le rappelle, en quelques années la cybercriminalité a changé de visage. C'est un univers désormais très structuré, innovant, qui redouble d'artifices des plus sophistiqués et qui alimente une économie du cybercrime sans cesse grandissante.
Au même titre que la crise de l'énergie, que l'inflation, que le changement climatique, c'est un enjeu majeur à venir pour les collectivités qu'il ne faudra surtout pas minimiser.

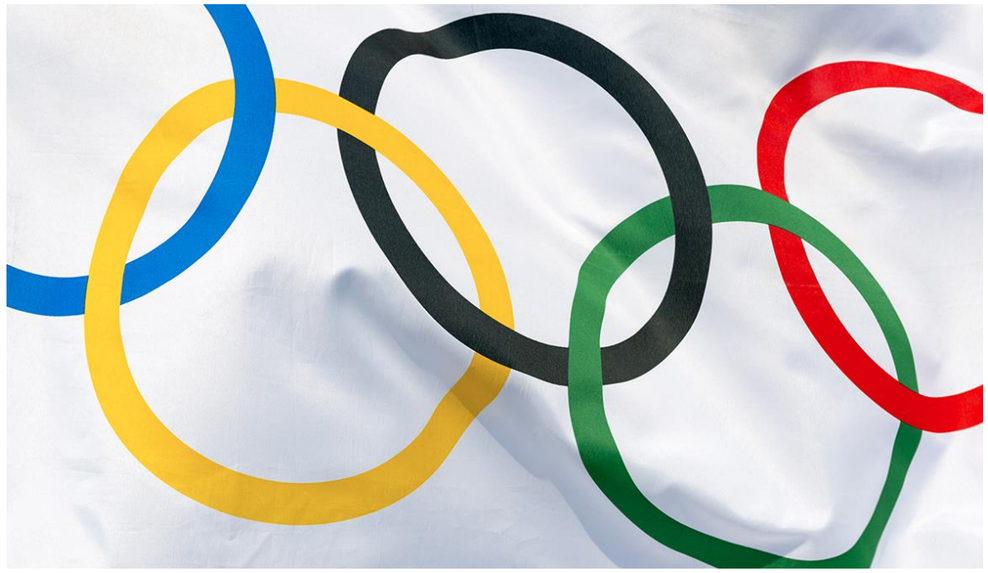
Se fixer un objectif de temps : l'année 2024

Pour être efficace, il est toujours mieux de se fixer un cap.

Pourquoi ne pas se fixer 2024, en l'occurrence l'année des Jeux Olympiques et Paralympiques, comme enjeu national pour la modernisation des infrastructures numériques des collectivités territoriales.

Comme évoqué plus haut, des systèmes vieillissants, reflet de la dette cyber, et ne bénéficiant pas des mises à jour nécessaires, facilitent le travail des hackeurs et de ce fait menacent les finances de la collectivité.

Dans la lignée de Terres de Jeux, cet investissement des collectivités, se révèlera être alors un héritage bénéfique des Jeux



Vision : la cybersécurité doit être considérée comme un sujet mondial pour être plus efficace au niveau local

L'État doit continuer à s'impliquer comme il le fait, que ce soit pour aider les collectivités ou les entreprises. Cependant, même s'il ne faut surtout pas rater l'opportunité de développer une filière nationale de haut niveau en cybersécurité, se limiter à une approche trop centrée sur la France serait contreproductif.

Pour faire face à ce fléau mondial, Il faudrait en effet favoriser une démarche ouverte aux échanges, aux partenariats et coopérations publics et privés à l'international, y compris au-delà de l'Europe.

Il s'agit en effet de pouvoir bénéficier du meilleur, en s'appuyant aussi sur des acteurs aux expériences des menaces de cybersécurité acquises au niveau mondial, et aux budgets de recherches conséquents, que n'auraient pas forcément des acteurs français, aussi bons soient-ils.

Jusqu'où les collectivités doivent aller en matière de cybersécurité ?

Au vu de la complexité de la cybersécurité et de la rapidité des évolutions, il n'est cependant pas envisageable de demander aux collectivités de devenir de vrais experts de la cybersécurité. Pour autant, elles doivent prendre les mesures pour se protéger et réagir efficacement**,** bien plus que par le passé.

Il s'agit d'éviter un effet ciseaux où le savoir-faire des attaquants progresserait plus vite que celui des collectivités territoriales déjà handicapées par leur manque de ressources en matière de cyberdéfense.

a) Processus :

○ Une approche collaborative de type 360° au niveau de la collectivité

- **Il est important de ne pas réduire la cybersécurité à des questions techniques** : il faut que chacun s'en empare et mutualise les bonnes pratiques. La majorité des élus et des directeurs ne sont pas des spécialistes de la cybersécurité et n'ont pas à l'être. Il faut cependant encore les encourager à mettre le sujet au bon niveau de priorité de la collectivité, et faire en sorte qu'ils favorisent une approche collaborative de la cybersécurité et non pas en silo. Leur impulsion est clé.

  - **La cybersécurité ne doit donc plus être uniquement le problème du DSI et du RSSI** mais être la préoccupation transversale de tous, en commençant par le Directeur Général des Services.

  - **Favoriser la convergence des fonctions de cybersécurité et de sécurité physique** pour mieux se préparer à identifier, prévenir, atténuer et répondre aux menaces.

  - La Convergence encourage également **le partage d'informations** et le développement de politiques de sécurité unifiées dans l'ensemble de la collectivité.

○ Analyse des risques : avant tout investissement dans des systèmes de protection et détection, nous recommandons aux collectivités de conduire des analyses permettant de comprendre et d'identifier leurs faiblesses connues, et leur exposition aux divers risques (technologiques, organisationnels et de mise en conformité). Une fois que cette analyse pointue est faite, les choix pour protéger les applications et les collaborateurs où qu'ils soient, à tout moment et sur tout type de terminal sont plus aisés. Il s'agira notamment de hiérarchiser les vulnérabilités qui présentent le plus de risques pour l'organisation.

○ Security by design :

Il est impératif que chaque service intègre en amont la cybersécurité à l'ensemble de son périmètre et ce, notamment, dès le lancement d'un nouveau projet.

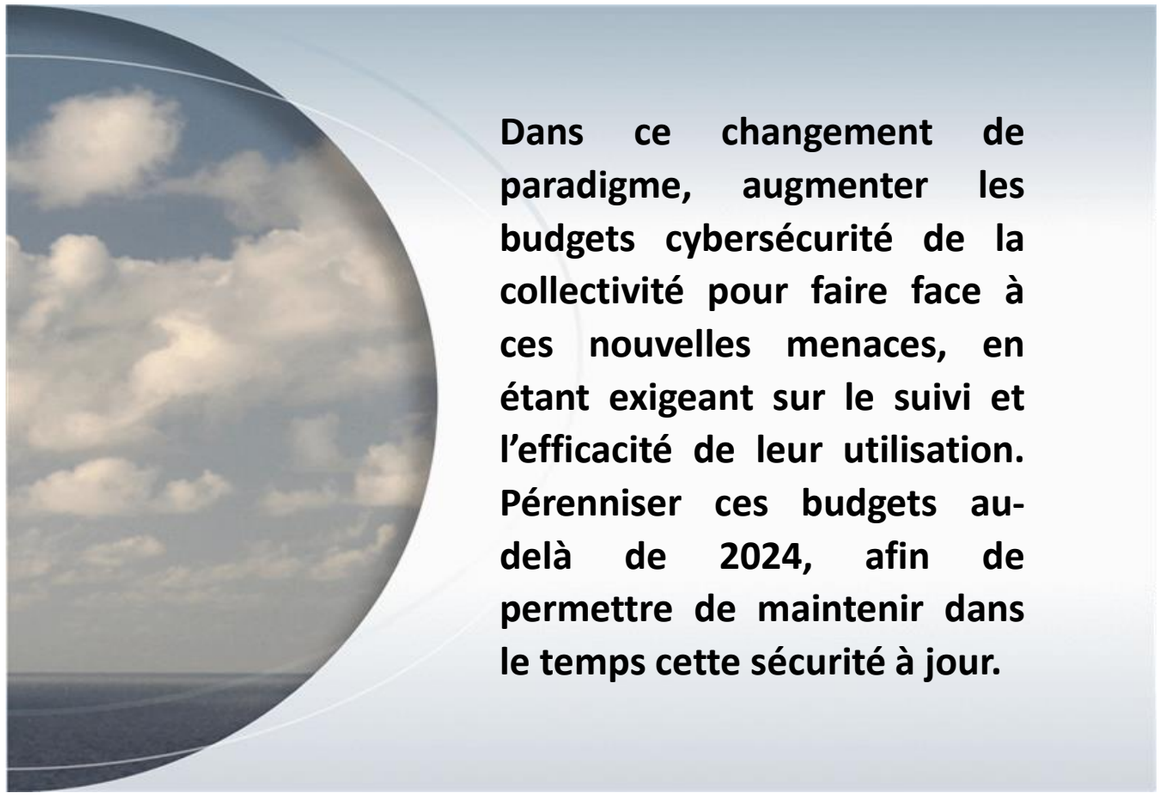
○ La résilience: pierre angulaire de la cybersécurité

Valider un plan de résilience, qui permette à la Collectivité de maintenir son activité en cas d'attaque avérée est primordial.

Face à un paysage actuel de menaces incroyablement diversifiées, avec la prolifération des cartels criminels de ransomware et l'activité des États-nations comme on le voit en Ukraine, c'est une période aussi chaotique que jamais pour les cybermenaces. La prévention, bien qu'elle soit un investissement noble et nécessaire, a une valeur limitée, car aucun système n'est parfait.

La résilience est donc l'objectif que nous encourageons en développant une défense en profondeur et des systèmes qui améliorent le temps de détection, une mesure essentielle pour contrecarrer les attaquants.

- La capacité de pivoter rapidement tout en maintenant la continuité des activités, est de plus en plus importante dans le monde d'aujourd'hui. Le fondement d'une résilience réussie vient de la compréhension des menaces et de vos propres faiblesses. Armé de ces connaissances, vous pouvez mettre en œuvre des protections pour réduire la probabilité que les menaces vous affectent et vous assurer que si une menace se réalise, les effets seront minimisés.



Dans ce changement de paradigme, augmenter les budgets cybersécurité de la collectivité pour faire face à ces nouvelles menaces, en étant exigeant sur le suivi et l'efficacité de leur utilisation. Pérenniser ces budgets au-delà de 2024, afin de permettre de maintenir dans le temps cette sécurité à jour.

- Selon le cabinet d'études Gartner, les dépenses en solutions de cybersécurité devraient continuer à augmenter à 2023, pour atteindre alors 188,3 Md$ (+11,3%). En cause, l'accroissement du travail hybride, la transition des réseaux privés virtuels (VPN) vers l'accès réseau Zéro Trust et leur passage au cloud.

Il s'agira d'adopter des solutions évolutives et durables

- **Investir dans l'automatisation de la cybersécurité**, qui s'appuie sur l'intelligence artificielle pour pallier les manques de ressources humaines qualifiées, face à la complexité et l'étendue des tâches. C'est le moyen de passer d'une posture réactive à une posture d'anticipation afin d'anticiper au mieux les risques. Au passage l'automatisation permet aux attaquants d'être plus efficaces pour attaquer simultanément plusieurs cibles. Elle peut permettre au défenseur de réagir très vite et d'éviter des réactions en chaîne sur plusieurs sites contrôlés par différentes parties prenantes.

- L'automatisation permet de surveiller toutes les activités de la collectivité sur ses systèmes et dans le cloud, afin d'analyser ces données pour fournir des informations exploitables, utiles pour déceler des comportements suspects et décider si elles doivent réagir.

- **Data Privacy/Confidentialité des données** : en conformité avec le RGPD, accorder une importance particulière au processus liés aux données personnelles, que ce soit au niveau de la captation, de leur stockage, leur analyse et leur distribution à travers le réseau. Il est notamment recommandé de mettre en place des segmentations des réseaux autorisant l'accès aux données personnelles en fonction des accréditations.

b) Technologie

- **Revenir aux fondamentaux pour combler la dette cyber** :

  Se mettre en conformité avec l'état de l'Art en commençant par mettre à niveau leurs infrastructures numériques (réseaux, systèmes IT….) parfois dépassées, pour répondre aux besoins des nouvelles technologies. Il s'agira d'adopter des solutions évolutives et durables. La modernisation des infrastructures est en effet l'étape la plus sûre vers une meilleure protection.

  - **Ne pas laisser ses infrastructures vieillir et s'assurer de leurs mises à jour.** C'est ainsi le meilleur moyen d'éviter de créer des « passoires » facilitant le travail des attaquants.

Il s'agira d'adopter des solutions évolutives et durables

- **Un programme de sécurité doit désormais, impérativement combiner « quoi » (les terminaux) et « qui » (l'identité).**
  - Instituer l'ère de la Confiance Zéro : ne faire confiance à personne.
    - Selon Gartner, le segment ZTNA (Zero Trust Network Access) est celui qui connaîtra la plus forte croissance dans le domaine de la sécurité réseau avec une prévision de progression de 36% en 2022 et de 31% en 2023.
  - Vérifier l'identité des utilisateurs : sont-ils vraiment qui ils prétendent être ?
    - Implémenter impérativement des systèmes d'authentification multi facteurs (MFA).
    - Souvent, les vols d'informations sont dus à un manque de MFA ou à leur mauvaise utilisation.

- Sécuriser tout type de périphérique, quel que soit le type de connexion, en commençant par les terminaux des collaborateurs, qu'ils se connectent sur site ou à distance.

- Sécuriser l'accès aux applications et données de l'entreprise nécessite la mise en place de solutions VPN afin de garantir la confidentialité des échanges, et l'intégrité de ces derniers, ainsi qu'une segmentation des accès régulièrement mise à jour.

- **Maitriser sa surface d'exposition** : en réalisant un inventaire strict de tous les éléments présents sur un réseau, y compris les objets connectés et de déterminer leur niveau de protection.

c) Facteur humain :

- Face à l'évolution du type d'attaques, continuer à sensibiliser les agents aux bonnes pratiques concernant les mots de passe, la protection des comptes de type réseaux sociaux, la détection des pièges qui leurs sont tendus (hameçonnage), via la messagerie. Exemple : monter des opérations anti-phishing.

- Pour pouvoir embaucher les ressources nécessaires, être attentifs aux différents programmes de formation notamment ceux qui permettent de multiplier les sources, d'ouvrir les horizons et de changer de posture par rapport aux profils recherchés en sortant des stéréotypes.

CISCO, positionnement et investissement en France

- Cisco a été choisi comme **partenaire officiel des Jeux Olympiques et Paralympiques de Paris 2024 sur les infrastructures de cybersécurité, les équipements réseaux et les logiciels de visioconférence**. Ce choix s'est fait notamment pour son expérience internationale et sa large gamme de solutions de cybersécurité. Cisco travaille donc au quotidien avec les équipes du comité d'organisation (COJOP) et avec Atos pour se préparer à la protection, à la détection et à la réponse face à d'éventuelles cyber attaques.

- Cisco est le **leader mondial des technologies qui permet à l'Internet d'exister depuis plus de 35 ans.** Sa mission est de connecter de manière sécurisée les personnes, les applications et les objets. Cisco place l'innovation au cœur de sa stratégie et a notamment investi 7 milliards de dollars en 2021 en recherche et développement.

- **En s'appuyant sur son écosystème de partenaires français, Cisco accompagne ainsi ses clients du secteur public dans la numérisation de leur métier**. De l'administration centrale, aux collectivités territoriales, aux établissements scolaires mais aussi dans les hôpitaux. Ses solutions permettent aux agents publics de mener à bien leurs tâches au service des citoyens.

- ## Détection de menaces :

Cisco a créé « **Talos Intelligence Group** », l'une des plus grandes équipes de renseignement sur les cybermenaces au monde, composée de chercheurs, d'analystes et d'ingénieurs de classe mondiale. Son but est d'alerter les clients et le public des nouvelles menaces et tactiques d'attaques, de nous permettre d'intégrer rapidement une protection dans nos produits et intervenir pour aider les organisations à répondre aux incidents, à rechercher les menaces, à évaluer les compromis. Talos recherche et bloque les attaques malveillantes, qu'il s'agisse d'attaquants d'Etats Nations ou de cartels criminels de ransomware. Les renseignements recueillis et analysés par Talos sont rapidement distribués à travers des mécanismes de protection pour empêcher ces activités.

Ces renseignements peuvent notamment empêcher les collectivités d'être victimes de compromission de leur réseau informatique ou industriel, soit dans un schéma de protection automatisé via les produits Cisco, soit par le biais d'une relation de partage de renseignements par un triage des renseignements en temps réel au niveau mondial.

Talos est aussi sollicité par exemple dans la sécurisation d'organisation de grands événements comme le Superbowl aux USA

- ## Gestion des Vulnérabilités :

Cisco a investi massivement afin de fournir des informations exploitables à ses clients sur les priorités de mises à jour sur lesquelles se concentrer, afin de prendre les meilleures décisions en vue d'obtenir le plus grand effet, notamment pour des clients en état de cyber dettes. Ceci est possible grâce à la compréhension des techniques des adversaires, basée sur notre recherche sur les menaces et les renseignements générés par Talos, ainsi qu'à notre outil de management des vulnérabilités Kenna. Ce qui permet aux clients de faire des choix entre ce qui doit être corrigé immédiatement et ce qui peut être fait sur un délai plus long.

- **Investissement en France dans la cybersécurité :**
  - **IOT (Internet of Things)** : Cisco a récemment inauguré à Villeurbanne, en septembre 2022, son centre R&D mondial dédié à la cybersécurité des équipements industriels montrant la confiance accordée aux compétences lyonnaises héritées du rachat de la startup Sentryo en 2019. La cybersécurité de l'IOT est un domaine stratégique sur lequel le groupe compte investir 50 millions en France d'ici les trois prochaines années en concentrant ses ressources sur la région Lyonnaise. Le nouveau pôle Cybervision a vocation à accompagner les entreprises et collectivités dans la cybersécurité des réseaux opérationnels.

Cisco est aussi partenaire du Campus Cyber, lieu totem de la cybersécurité française qui rassemble les principaux acteurs nationaux et internationaux du domaine

- **Facteur humain : NetAcad**

  Historiquement Cisco a toujours œuvré pour la possibilité de former des profils hors de la filière traditionnelle informatique et télécoms. L'idée est d'aider les collectivités à identifier les talents non traditionnels, mais qui ont des qualités requises pour les métiers de la cybersécurité de la manière la plus inclusive.

- Cisco a annoncé le 18 octobre 2022, son nouveau plan de formation aux compétences informatiques et télécoms recherchées au cours des 10 prochaines années pour 25 millions de personnes, à travers le monde. En France, Cisco a investi plus de 110 Millions de $ et a contribué à la formation de plus de 275 618 apprenants depuis son lancement en 2001.

- Elle va notamment étendre le périmètre de son programme Cisco Networking Academy.

L’effort vise à s’assurer que le pipeline de talents technologiques suive le rythme des progrès technologiques et de l’automatisation, en proposant un programme de développement équitable et inclusif.

- Cisco Networking Academy a également lancé 2 nouveaux programmes d'accréditation. Le tout premier est un parcours de connaissance de la cybersécurité, développé pour fournir aux candidats une certification et les compétences nécessaires pour les placer dans des rôles de sécurité de niveau d'entrée.

  - En outre, l'académie lance le tout nouveau programme entièrement gratuit et mobile « Skills for All » qui fournit aux stagiaires des cours d'auto-formation, des outils interactifs et des ressources de carrière, tous conçus par des professionnels du marché.

- Toutes les offres de Cisco Networking Academy sont disponibles gratuitement au public, tandis que d’autres sont offertes dans les établissements d’enseignement secondaire et supérieur ou de formation professionnelle.

- Depuis la création de Net Academy, plus de 17 millions de personnes ont suivi un cours au sein de l’académie, et 95% de celles qui ont suivi des cours certifiants » ont eu une opportunité d’emploi ou d’éducation ultérieure à l’académie.

Remise du Livre Blanc : « Cybersécurité et Territoires » à Jean-Noël Barrot, Ministre délégué chargé de la Transition numérique et des Télécommunications

De gauche à droite : Jérôme Moreau (Eviden-Atos), Éric Greffier (Cisco) Quentin Meullemiestre (Mission Ecoter-France et Territoires Numériques), Denis Thuriot (Mission Ecoter-France et Territoires Numériques), Jean-Noël Barrot, Alain Melka (France et Territoires Numériques), François Charbonnier (La Banque des Territoires), Alain Bourcier (Nevers Agglo)

Directeur de la publication : **Alain MELKA**, Directeur Général des Services – Mission Ecoter-France et Territoires Numériques
Assisté de : **Quentin MEULLEMIESTRE**, Directeur Général des Services Adjoint – Mission Ecoter-France et Territoires Numériques

Maquette et graphisme :
Mission Ecoter-France et Territoires Numériques

LIVRE BLANC

2023

CYBERSÉCURITÉ & TERRITOIRES

MISSION ECOTER
France et Territoires Numériques

BANQUE des TERRITOIRES
Caisse des Dépôts GROUPE

Atos

CISCO