MISSION ECOTER

Mission pour l'Économie numérique, la Conduite et l'Organisation des Territoires

Actes du Colloque en visioconférence

Cybersécurité : comment les collectivités peuvent-elles mieux appréhender ce risque ?

14 octobre 2020

BANQUE des TERRITOIRES | Caisse des Dépôts GROUPE

LES ÉMOTIONNEURS
concepteurs . créateurs . producteurs

La Mission Ecoter

- **Mission pour l'Economie Numérique, la Conduite et l'Organisation des Territoires**
- La Mission Ecoter, Association loi 1901, regroupe, depuis 1997, Collectivités Territoriales (villes, départements, régions, structures d'agglomération, agences publiques, syndicats de communes, organismes consulaires et de développement économique local) et Entreprises actrices dans le secteur des collectivités (Numérique, Santé, Education, Environnement, Transports, Finances locales….) pour :
- accompagner les collectivités dans leurs transformations,
- échanger sur les usages et les services numériques aux citoyens,
- mettre en place une veille adaptée et efficace aux projets de transformations,
- peser sur les décisions politiques et administratives pour les territoires,
- diffuser les informations les plus fiables dans un secteur innovant,
- former les élus, les cadres territoriaux et les acteurs d'entreprises à l'économie numérique, aux finances, aux ressources humaines…

LES PARTICIPANTS

Mauna TRAIKIA
Conseillère Territoriale Déléguée au développement numérique, Plaine Commune – Grand Paris

François CHARBONNIER
Investisseur Confiance Numérique, Caisse des Dépôts

Vincent RIOU
Directeur associé Avisa Partners

Alain MELKA
Modérateur
Directeur Général des Services
Mission Ecoter

Pierre GACIC
Chef de la division de la coordination territoriale Agence nationale de la sécurité des systèmes d'information (ANSSI)

Thierry VINCON
Haut fonctionnaire
Ancien Maire Saint-Amand-Montrond

Franklin BROUSSE
Avocat, expert en droit des nouvelles technologies d'information et de la communication (NTIC)

- **Alain Melka – Directeur Général des Services - Mission Ecoter – Modérateur :**

Ce colloque en visioconférence est une première pour la Mission Ecoter, première autour d'un sujet qui nous paraît essentiel « La cybersécurité : comment les collectivités peuvent-elles mieux appréhender ce risque ? ». Avec un développement accru du numérique et la multiplication des objets connectés dans la vie de tous les jours, les collectivités locales et territoriales sont de plus en plus la proie de cybermenaces. Alors que ce mois d'octobre 2020 est placé sous le signe de la cybersécurité, nous avons décidé de croiser les regards, d'échanger les bonnes pratiques et de mesurer les solutions majeures pour tout mettre en œuvre afin de protéger au mieux les collectivités locales et territoriales. Bien entendu, l'objectif de cette visioconférence est d'instaurer un débat qui va au-delà de cette heure de conférence. Ma première question concerne Thierry Vinçon, ancien maire de Saint-Amand-Montrond, située en cœur de France, Thierry Vinçon, vous avez une grande expérience en matière de cybersécurité, quel regard portez-vous sur cette recrudescence de cybermenaces ? En effet, nous constatons depuis plusieurs années un nombre considérable d'attaques aussi bien contre nos entreprises et que nos collectivités.

- **Thierry Vinçon : Haut fonctionnaire, ancien Maire Saint-Amand-Montrond**

A Saint-Amand-Montrond, la ville que j'ai administrée pendant 12 ans, on a mis en place plus de 91 projets de Smart City depuis 2010. Nous sommes arrivés à une interaction de toutes les fonctions opérationnelles. Le rôle de l'élu et d'être en quelque sorte un pilote des données afin de continuer l'action publique au profit des services rendus à la population. Pour cela il faut tout d'abord une stratégie, elle répond à un objectif, de ne pas tout faire dans le désordre et surtout de protéger l'action et la sécurité des données. Le risque réside dans une mauvaise stratégie qui ne hiérarchise pas les actions, qui n'assure pas le souci et la conservation des données publics-privés ou personnelles. Aujourd'hui, le risque réside aussi à mon avis dans la création du territoire dont on a la responsabilité. Il faut créer (comme la Mission Ecoter le fait) des interconnexions entre l'ensemble des territoires qui sont engagés dans cette stratégie. Enfin, troisième risque, c'est l'absence de dialogue entre les collectivités territoriales et l'État. Bien sûr concernant les différents problèmes énoncés il faut des réponses adaptées. La première réponse est avant tout un vrai pilotage de ce qui se fait aujourd'hui sur un territoire. Pour cela il faut une image de l'ensemble des solutions. Il faut également dresser à partir de cette photographie, l'ensemble des orientations et des outils à disposition possible. C'est ce que la Banque des Territoires a lancé. La période de la Covid-19 nous invite plus encore, à régler ces problèmes, il faut les hiérarchiser. Sont concernées en premier lieu, les métropoles qui subissent de plein fouet les conséquences de cette crise de la Covid-19, les petites villes sont moins attaquées pour le moment, mais il faut tout de même mettre en place toute une stratégie dont l'ANSSI nous proposera des solutions. Ce que j'ai voulu créer à Saint-Amand-Montrond, ce sont les bases d'une Smart City innovante en lien avec la Mission Ecoter que je remercie pour son aide et son soutien indéfectible.

- **Alain Melka** : Thierry Vinçon, pouvons-nous dire qu'il y a actuellement davantage de cybermenaces et cyberattaques ?

- **Thierry Vinçon** : Oui j'ai l'impression! Parce que les hackers visent à la fois des grosses sommes et des petites sommes accumulées. C'est la conséquence à la fois d'une volatilité des données, d'un grand nombre de données et d'une protection plus ou moins efficace. En effet, il suffit d'une seule faille pour faire tomber l'ensemble du système, c'est pour cela qu'il faut adopter des réflexes sanitaires aussi en matière de Numérique.

- **Alain Melka** : François Charbonnier, la Banque des Territoires–Caisse des Dépôts, investit énormément dans le domaine du numérique, quand en est-il dans la lutte contre la cybercriminalité ?

- **François Charbonnier : Investisseur Confiance Numérique, Caisse des Dépôts**

C'est une très bonne question, en effet la Banque des Territoires investit beaucoup au profit des collectivités locales et territoriales, ça correspond aussi à sa création récente qui est l'un des cinq métiers de la Caisse des Dépôts. La Banque des Territoires a un axe très important, la transition numérique comme la Smart City, la ville numérique, où la ville qui doit tout simplement s'informatiser ou numériser sur un domaine ou un autre. Il n'y a pas non plus que des projets spectaculaires, cela correspond aux attentes et besoins mais également aux priorités de la collectivité. Pour nous il est important d'accompagner cette transition. Dans ce domaine, nous avons au niveau de nos projets, des projets d'investissements où nous pouvons investir dans des sociétés innovantes comme Cap Collectif pour la participation citoyenne. Nous pouvons également accompagner les collectivités en amont en examinant la possibilité de financement. Nous avons aussi des logiques d'accompagnement. Pour répondre plus précisément à votre question, concernant la cybersécurité, on a en ce moment un axe d'investissement, de confiance numérique qui répond à ce besoin, à ces projets qui peuvent aider les collectivités. Nous travaillons également sur un projet de guide sur la confiance numérique à destination des collectivités plus précisément à destination des élus des territoires. Aussi, nous travaillons de près avec certaines grandes fédérations, d'associations dont la Mission Ecoter mais également avec l'ANSSI et avec cybermalveillance.gouv.fr qui a un dispositif aussi important, qui se déploie dans les territoires.

- **Alain Melka** : Est-ce qu'avec ce guide, la Banque des Territoires va-t-elle prendre son bâton de pèlerin et aller au-devant des élus et des territoires ?

- **François Charbonnier :** Ce guide a l'ambition « de mettre les pieds dans le plat » : le but est de porter un vrai message, qui mérite d'être en lien directement avec les territoires. Le message principal est le suivant : la cybersécurité et la confiance numérique sont peut-être des sujets complexes qui peuvent faire peur et c'est tout à fait normal, cependant l'élu à la seule vraie responsabilité de s'emparer du sujet, de donner l'impulsion à ses équipes pour traiter cette problématique. L'objectif de notre guide est cette prise de conscience, prise de conscience qui est double. La première des choses est de reconnaître que la cybersécurité et la confiance numérique sont des sujets clés des collectivités, à l'heure où nous entamons des transitions numériques à divers degrés. Il est également indispensable d'agir! En effet, parfois, il se passe plusieurs années avant qu'on agisse. Agir ne veut pas forcément dire effectuer des choses compliquées. Nous avons travaillé avec l 'ANSSI, afin de faire passer quelques grands messages de très haut niveau sans rentrer dans le détail, qui relève plutôt du domaine des experts. Oui pour nous c'est une première étape en lien avec les Directions régionales, afin d'intervenir dans les territoires et de pousser ce message important d'autant plus que l'urgence est vraiment là.

- **Alain Melka** : Vincent Riou, vous êtes Directeur associé d'Avisa Partners, pouvez-vous nous en dire plus ?

- **Vincent Riou : Directeur associé Avisa Partners**

Le CEIS a fusionné avec une autre société d'intelligence économique en début d'année 2020 qui s'appelle Avisa Partners. Maintenant on s'appelle tous Avisa Partners, nous sommes la principale société française intelligence économique et de cybersécurité opérationnelle. Nous avons une filiale spécialisée en cybersécurité offensive, qui permet de répondre aux incidents qui interviennent assez régulièrement dans les collectivités territoriales et locales. Cette filiale, s'appelle Lexfo, qui est forte d'une soixantaine d'ingénieurs et qui est en passe d'être qualifiée par l'ANSSI, prestataire de réponse aux incidents de sécurité.

- **Alain Melka** : Vincent, je parlais de menaces grandissantes et de risque plus que réelle comment vous intervenez et de manières concrètes ?

- **Vincent Riou :** Nos champs d'actions sont assez larges, mais j'ai envie d'insister sur les fondamentaux. Nous sommes dans une logique de construction d'outils de défense, avant de réfléchir à ses outils de défense, il faut réfléchir au point de vue de l'attaquant, c'est important afin de ne pas se retrouver débordé ! Et en cybersécurité, c'est particulièrement vrai, les menaces sont extrêmement mobiles et agiles. Les raisons de s'attaquer à une collectivité territoriale et locale sont nombreuses, tout d'abord, il y a l'idéologie des motifs politiques, l'attaquant va chercher à atteindre l'image du politique à travers la diffusion de fausses informations, d'effacement de sites institutionnels voire du vol de données. En effet, nous avons déjà dû traiter du vol de mail d'un élu local, dont le but était de le dénigrer et chercher à le déstabiliser. Les vols de données plus graves peuvent également exister dans le cadre d'espionnage. Comme par exemple pour sécuriser le gain d'un marché public ou connaître la stratégie future de la collectivité sur des sujets sensibles comme l'urbanisme, la mise en chantier de grands projets, les collectivités peuvent subir ce genre d'attaque. Dans une logique de déstabilisation toujours, des cyberattaques peuvent-être conduite à l'encontre des personnes dans la ville, Nous pouvons citer la manipulation de feu rouge, la paralysie des moyens de communication des systèmes de secours, ou encore et plus gravement, on peut porter atteinte au système de distribution de l'eau et du traitement des déchets. L'accroissement de la numérisation de ce système accroît également la perméabilité de l'attaque informatique. Nous réalisons dans ma société plusieurs exercices avec des mises en situation réelle pour mesurer la perméabilité réelle des organisations. Ces attaques vont être sciemment visibles et vont permettre aux experts d'intervenir en cas d'agressions. Mais d'autres auront comme caractéristiques principales, la futilité, la discrétion totale, comme dans le cadre d'espionnage par exemple. Dans ce cas, je pense que l'ANSSI nous le confirmera, des infections peuvent rester actives pendant plusieurs années tout en exfiltrant des données. Néanmoins, la dernière motivation de l'attaquant est la plus connue, celle de l'appât du gain. Cette cybercriminalité est le fait de grandes organisations transfrontalières, parfois affiliées à des Etats, ces organisations sont dotées de structures et de moyens de plus en plus important. En effet, les gains sont importants, les risques sont faibles, avec une possibilité d'action depuis l'étranger et les peines prononcées sont assez décevantes au regard des faits commis avec violence. Avec la multiplication et la démocratisation du télétravail, nous avons remarqué davantage d'attaques, celles-ci ont explosées cette année. Ce phénomène ne risque pas de s'arranger si nous ne prenons pas le sujet à bras-le-corps et c'est triste car dans la plupart des cas dans lesquels nous sommes intervenus les attaques auraient pu être évitées par l'application de règles d'hygiène numérique de base. Il faut être clair les gestes barrière ça fonctionne également en informatique !

- **Alain Melka** : Quels sont les gestes barrières en informatique ?
- **Vincent Riou :** C'est de la mise à jour régulière, la règle de base. Nous constatons que la plupart des cas d'attaques, notamment les rançons, proviennent de l'exploitation de vulnérabilités, de problèmes de non mises à jour de certains systèmes qui sont publics. Par manque de conscience, la non mise à jour des systèmes d'informations représente 99% des cas d'attaques. Nous pouvons citer comme exemple, un mot de passe trop simple, une authentification « multifacteur » qui n'a pas été mise en place, des défauts de configuration qui proviennent de l'inconscience des services informatiques des entreprises ou des collectivités. Également, les clics malheureux sur des mails piégés. Nous avons également la surexposition des services sur internet, avec beaucoup de services cloud ouverts pendant le confinement pour permettre aux entreprises et aux collectivités de continuer à travailler malgré le télétravail sans que cela soit maîtrisé du point de vue de la sécurité.
- **Alain Melka :** Franklin Brousse, vous êtes Avocat, et en préparant cette émission, vous avez insisté sur le fait que nos collectivités sont assez mal préparées, qu'entendez-vous, par-là ?
- **Franklin Brousse : Avocat, expert en droit des nouvelles technologies d'information et de la communication (NTIC)**

Oui tout à fait ! Et j'en veux pour preuve tous les cas de cyberattaque que j'ai pu traiter, que ce soit dans la sphère des collectivités ou des entreprises. On voit souvent dans le cas d'une cyberattaque des victimes souvent pas ou mal préparées. En effet, face à une cyberattaque, les victimes sont souvent démunies. Que faire ? A qui s'adresser ? Or c'est très important d'être préparé aux cyberattaques, car la capacité à réagir rapidement est cruciale dans ces cas-là. Parce que si l'on réagit mal ou trop tard on peut aggraver les conséquences d'une cyberattaque et aggraver le préjudice pour la collectivité et le cas échéant les administrés. D'où la nécessité d'être préparé à ce type d'événement et de savoir quoi faire au bon moment, car le risque zéro n'existe pas même si l'on doit mettre en place tout ce qui doit être fait. La première étape est la formation, la sensibilisation des collaborateurs est également importante ; ensuite il faut mettre en place une procédure qui va permettre de réagir en cas de cyberattaque. C'est-à-dire poser les questions suivantes : que dois-je faire ? qui dois-je contacter ? qui d'autre est également concerné ? quelles sont les causes de cette cyberattaque ?... Cela pose également les questions concernant le prestataire. En effet, quel est le prestataire concerné qui héberge mes données ? Problématique importante également vers qui se retourner pour déposer une plainte ? En matière de cyberattaque, face à des problématiques pénales, on va pouvoir porter plainte en s'adressant au service de gendarmerie ou de police. En France, nous avons les services de lutte contre la cybercriminalité, vous avez la brigade régionale d'Île-de-France et de Paris, vous avez également un service de la gendarmerie nationale, vous avez aussi la possibilité de faire une déclaration en ligne sur le site du gouvernement cybermalveillance.gouv.fr. Aujourd'hui, il existe des outils pour porter plainte et aller chercher de l'aide. Encore faut-il le savoir ! L'autre point, sur lequel je voudrais attirer votre attention est la donnée personnelle. Cela peut créer d'autres préjudices et des problèmes de responsabilité pour les élus, les cyberattaques visant souvent des données personnelles. Concrètement, on est face à un vol de données personnelles ou une prise en otage des données personnelles. Si des données personnelles sont concernées, il est urgent de notifier une violation de données personnelles et également de prévenir les personnes concernées. Comme, cette notification doit intervenir dans un délai très court, maximale de 72 heures, vous vous doutez bien que si on n'est pas préparé on ne peut pas réagir à temps. On va subir l'événement et on ne va respecter ses obligations qui font parties de la réglementation en matière de données personnelles. Il y a une même nécessité sur tous ces sujets-là, la nécessité d'être préparée et de réagir rapidement.

Aussi, un autre retour d'expérience que je souhaitais vous faire partager, c'est le fait que les cyberattaques impliquent souvent un prestataire informatique. En effet, une collectivité héberge rarement ses propres logiciels et ses propres données. Il y a donc la nécessité d'anticiper ce risque et de vérifier que ce prestataire dispose d'une sécurité en matière numérique, vérifier régulièrement que le système est testé contre les cyberattaques. Vérifier si lui-même est prêt à une cyberattaque potentiellement le contraindre à appliquer cette politique de sécurité, à réaliser des tests périodiques, du fait de la réglementation en matière de protection des données. Il est également nécessaire d'évaluer les mesures qu'il a prisent au niveau de son organisation et de la technique pour protéger les données personnelles. Ce qui correspond à une obligation très importante dans le RGPD. En cas de cyberattaque, il y a un double risque, d'une part l'atteinte à votre système d'information, de bloquer le service d'exploitation d'une collectivité mais on a également l'atteinte aux données personnelles et là on peut se retrouver face à une double peine. Face à une éventuelle sanction de la part de la CNIL, vous n'avez pas assez protéger les données personnelles de vos administrés par exemple, cette fonction peut-être aggravée dans l'hypothèse où la CNIL va constater que vous n'avez pas garantie la sécurité de vos prestataires en matière de données personnelles. Enfin, le sujet de la cybersécurité et des cyberattaques est aussi un sujet des relations entre les collectivités et leurs prestataires notamment sur la protection des données personnelles.

- **Alain Melka** : Vous évoquez le RGPD Check, vous pouvez nous en dire plus ?
- **Franklin Brousse :** Oui tout à fait ! J'allais faire cette transition. En effet, il faut être préparé en interne et ensuite contrôler ce qui se passe à l'extérieur. C'est-à-dire, vérifier que vos prestataires ont des garanties et qu'ils sont eux-mêmes préparés. Contrôler la conformité RGPD de ses prestataires et quelque chose qui est extrêmement chronophage et complexe, et donc il faut arriver à le dématérialiser pour pouvoir faire une évaluation efficace et réel du niveau de maturité de vos prestataires sur ce sujet-là. A cet effet, on a créé une plate-forme qui au travers d'un dossier de conformité permet d'avoir 180 points de contrôle avec un certain nombre de justificatifs à fournir de la part des prestataires, pour vérifier qu'ils ont bien dans leur service et dans la pratique les sujets de protection des données personnelles. La deuxième idée de cette plateforme est de se dire : cette plateforme est un tiers de confiance dont l'objectif va être de mutualiser cette évaluation de conformité auprès des prestataires, avec l'idée de se dire si vous prenez les collectivités à l'échelle régionale, il y a de très grandes chances qu'elles aient un nombre de fournisseurs en commun. L'idée étant de mutualiser, afin d'être plus efficace. Ainsi on propose à travers cette plateforme une mutualisation des fournisseurs. A cet effet je pense que de manière générale sur tout ce qui touche à la cybersécurité il y a un intérêt à mutualiser.

- **Alain Melka :** Mauna Traikia, vous êtes élue à Plaine Commune, en termes de lutte contre la cybercriminalité, qu'est-ce qui se passe sur votre territoire ?

- **Mauna Traikia : Conseillère Territoriale Déléguée au développement numérique, Plaine Commune – Grand Paris**

Plaine Commune regroupe 9 villes de Seine-Saint-Denis, soit 430 000 habitants et des véritables enjeux au niveau de développement économique et numérique avec un périmètre assez vaste. Nous allons être terre d'accueil des Jeux Olympiques de 2024, ce qui est un véritable défi au niveau de la cybersécurité, des enjeux sociaux et des enjeux économiques. Notre transformation numérique a démarré en 2014 au travers deux grands axes. Le premier : les systèmes d'informations qui concerne les infrastructures, l'acculturation, la sensibilisation, la formation et permettre la montée en compétence de l'ensemble des services. Une collectivité est un tiers de confiance concernant la gestion de la donnée personnelle de la protection et de son usage. La donnée est centrale, elle est la cible des cybercriminels. De ce fait, nous sommes un acteur de confiance afin de construire le service public de demain. Concrètement, nous sommes passés par une phase d'audit au départ très technique, l'aspect sécurité est arrivé très vite dans le cadre de notre projet. Je me permets de donner quelques conseils aux collectivités qui sont parmi nous aujourd'hui. En effet, je préconise de cartographier et de faire en sorte que la transformation numérique en termes de systèmes d'informations soit protégée et pérenne dans le temps. Un deuxième axe toujours technique, mais aussi important, ce sont les relations avec les fournisseurs. Un conseil que je donne souvent aux autres collectivités, c'est de regarder les contrats sur la propriété de la donnée et son usage. Ainsi, les aspects juridiques sont cruciaux. Cela nous permet de revenir sur la gouvernance de la donnée et je crois que nous partageons tous cet enjeu de la gouvernance et de la souveraineté numérique autour de la donnée. En effet, la collectivité gère le cycle de vie de la donnée, vos données sont précieuses, protéger-les et faites-en sorte de réfléchir avec vos services juridiques sur la propriété. Et si elle n'est pas inscrite, inscrivez-là pour qu'elle vous revienne. La cybersécurité et l'imperméabilité des systèmes sont deux enjeux pour les collectivités. Aujourd'hui, il est nécessaire de se réapproprier ses données et d'en être les garants. Sensibiliser et former sont très importants pour sensibiliser les collègues élus. A Plaine Commune, j'ai souhaité sensibiliser les élus et agents aux enjeux du numérique, dont la cybersécurité qui est un enjeu majeur ! Au-delà de la sensibilisation, c'est comment dans mon quotidien, je suis un acteur de la protection du système d'information, c'est un élément essentiel. Je tiens à saluer à ce titre, le travail de l'ANSSI auprès des collectivités en termes de sensibilisation et de mise à disposition d'outils qui permettent de faire avancer le sujet. Cette transformation numérique nous permet de reprendre le contrôle de nos systèmes d'informations. Néanmoins, nous sommes de plus en plus les cibles car nous avons ouverts nos systèmes d'informations avec le télétravail, l'accès à distance à son mail. Nous avons un devoir d'anticipation sur ce sujet-là, et de monter en compétence les agents. Aujourd'hui, la cybersécurité est un acte majeur des collectivités mais également de leur développement. Nous avons la chance en France d'avoir le savoir-faire pour anticiper et mieux appréhender ce risque.

- **Alain Melka :** Pierre Gacic, vous êtes le Chef de la division de la coordination territoriale au sein de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Pouvez-vous nous dire quelques mots sur l'ANSSI et ses activités ? J'aimerai également qu'on évoque la mutualisation.

- **Pierre Gacic : Chef de la Division de la coordination territoriale, Agence nationale de la sécurité des systèmes d'information (ANSSI)**

L'ANSSI, l'autorité nationale en termes de cyberdéfense, est un service du Premier Ministre, elle regroupe environ 500 agents implantés pour l'essentiel à Paris et bientôt à Rennes, eh oui, nous allons nous délocaliser un petit peu ! Nous disposons d'un réseau de délégués dans toutes les préfectures de région. Le cœur de nos missions se sont évidemment les systèmes d'informations de l'Etat, des administrations de l'Etat, mais également des opérateurs d'importance vitale et des opérateurs de service essentiel. Mais en raison de cette mission, de ce rôle de sécurité nationale, nous avons une mission beaucoup plus générale d'élévation du niveau de maturité de l'ensemble des acteurs, les acteurs économiques non régulés, des entreprises notamment les plus petites et des collectivités territoriales quelle qu'elle soit leur taille. Je ne reviendrai pas sur la menace, elle a été très bien décrite par les autres intervenants. Ce sont donc les élus qu'ils faut convaincre, sensibiliser et acculturer. C'est pour nous quelque chose de fondamental. Autre principe, c'est celui de la libre administration des collectivités territoriales, l'ANSSI ne peut s'immiscer à l'intérieur d'une collectivité territoriale sans en avertir les élus en amont, ils risqueraient de mal le prendre. Vous parliez de mutualisation, il existe deux sortes de collectivités territoriales, les plus grandes que nous nous traitons à l'ANSSI, les acteurs économiques régulés, nous les connaissons, les régions, les départements, les plus grosses intercommunalités, nous les fréquentons au quotidien, nos délégués les connaissent, on peut leur proposer un certain nombre de services. Pour le reste des collectivités, c'est une action plus indirecte, ça passe par cybermalveillance.gouv. fr, qui se charge de la réponse aux incidents et de la sensibilisation. Mais le maître mot derrière tout cela c'est la mutualisation. Elle peut se faire de deux façons, une façon qui existe déjà, c'est tout le réseau de l'intercommunalité, des opérateurs publics numérique, ce sont des syndicats mixtes, des associations etc...Ils sont regroupés au sein d'une fédération, un réseau qui s'appelle *Declic*, qui fonctionne très bien et sur lequel nous nous appuyons. Nous voudrions que cette mutualisation se renforce et couvre l'ensemble du territoire national. Ce que nous poussons également, et que nous avons fait inscrire dans la stratégie cyber de 2018, c'est la création de centre de ressources, un certain nombre d'acteurs notamment de collectivités territoriales, dans beaucoup de cas sous l'égide des régions, (comme en Occitanie et en Nouvelle Aquitaine) afin qu'elles puissent regrouper, mutualiser, leur capacité. Récemment un centre de ressources fut inauguré à Toulon afin de servir comme centre de réponse aux attaques pour les collectivités territoriales de la région PACA.

Alain Melka : Pour expliquer les gestes barrières informatiques, il faut entre autres augmenter le niveau des outils de sécurité, notamment les antivirus, les antispam etc… Bien souvent ces outils ont un coût élevé en fonctionnement, la mutualisation et l'externalisation sont-elles vraiment des solutions ?

Vincent Riou :

Les gestes barrières que je mentionnais précédemment ne représente seulement qu'un « cout humain », mais je ne parlais pas d'acquisition de solutions de cybersécurité. Bien sûr, il faut s'équiper, la mutualisation est une voie pour diminuer le coût unitaire et faire l'acquisition de solution de logiciels. Il existe également l'UGAP, dans le cadre de service cyber, pour mutualiser ses coûts d'acquisition de logiciels. Mais les gestes barrières sont avant tout de mettre une politique de mot de passe, d'avoir une charte informatique, de mettre à jour son système d'information, cela ne coûte pas grand-chose et c'est l'essentiel des barrières pour se protéger contre la plupart des attaques informatiques. Il y a effectivement un travail de fond sur les systèmes, sans oublier de s'équiper d'un bon antivirus… Mais avant de s'en équiper, à mon sens, il faut déjà effectuer les gestes de base.

Pierre Gacic :

Bien entendu dans la mutualisation il y a des enjeux politiques, on ne voit pas pourquoi sur des aspects techniques de ce type, on aurait davantage de charge au sens électrique du terme que d'autres services mutualisés et qui sont pris en charge par des syndicats intercommunaux. En ce qui concerne l'intercommunalité, cela ne pose pas de problème majeur. Ensuite effectivement lorsqu'un Président de région ou Vice-président de région décide de mettre en place un centre de mutualisation de ce type là et d'étendre ses services on peut le lui reprocher.

Alain Melka : Comment la mutualisation peut-elle fonctionner ? Qui veut répondre ?

Franklin Brousse :

Je voulais revenir sur ce point, car dans mutualisation, il y a quelque chose que j'appellerai le partage. C'est-à-dire le partage de bonnes pratiques. En effet, c'est quelque chose qui ne coûte pas cher. Le partage des bonnes pratiques et des outils au niveau local est important ! Plutôt que d'agir seul dans son coin. En effet, il est important d'aller voir ses collègues DSI dans d'autres collectivités de son territoire et de partager ces bonnes pratiques. Ça me paraît essentiel. La mutualisation c'est également le partage !

Alain Melka : le sujet est passionnant, on vous écouterait, madame, messieurs, des heures, mais hélas le temps tourne. Une petite minute, en mot de conclusion. Honneur à la dame.

Mauna Traikia :

La cybersécurité est un enjeu majeur, un enjeu qui dépasse notre territoire. Les cyberattaques ne cessant d'augmenter, il faut être tous mobilisés, les acteurs du numérique, les acteurs territoriaux, les services… et ne pas oublier nos concitoyens, concitoyennes, qu'il est impératif de sensibiliser et de faire participer à ce qui nous semble être un sujet majeur.

Thierry Vinçon :

Les élus sont les responsables de leur territoire. Aussi il faut d'abord, les convaincre, en mettant en place quelque chose qui est au cœur du dispositif, sinon tout va à la catastrophe. Si on prend en compte cet objectif, on met en place une stratégie et ensuite on la déroule.

François Charbonnier :

La Banque des Territoires a de vraies ambitions sur le sujet. La première ambition étant d'accompagner le message en essayant de se mettre dans la peau d'un élu. Ou qu'est-ce qu'on peut faire sur ce sujet quand on est DGS, DGA ? Est-ce qu'on doit juste transmettre le bébé au DSI ? Ou alors porter un vrai message ? Le Maire a bien entendu un mot à dire dans la manœuvre et c'est important qu'il tienne les rênes.

Vincent Riou :

La plupart des attaques informatiques ne sont pas forcément ciblées, dans la plupart des cas les attaquants sont un peu comme les cambrioleurs, ils utilisent des techniques de reconnaissance passive ou active, ils vont dénicher les cibles les plus faciles, en gros la maison la moins sécurisé du quartier. En effet, ils exploitent des outils d'attaque automatiser pour utiliser telle ou telle vulnérabilité. La question que doivent se poser tous les élus, c'est : est ce que nous sommes une cible facile ? C'est cette question que doivent se poser en permanence nos élus, et je dois l'avouer il n'est pas toujours facile d'y répondre.

Franklin Brousse :

Je voulais revenir sur le sujet des données personnelles avec le fait de rappeler aux élus que le respect des règles de protection des données personnelles s'impose à eux. C'est un facteur de transparence et de confiance à l'égard de leur administrés, c'est aussi un gage de sécurité juridique pour eux. Car si demain, ils ont un problème ils seront responsables. Il y a quand même un sujet de responsabilité aussi pour les élus, derrière ce sujet de cybersécurité. L'autre point très important est de partager un maximum les bonnes pratiques, sensibiliser les collaborateurs et contrôler ses prestataires. En effet à un moment donné les prestataires peuvent-être défaillant. Il faut donc vérifier s'ils ont pris des mesures et s'ils ont mis en place des outils.

Pierre Gacic :

L'élu est au centre de tout cela, c'est lui, c'est elle, qui prend la décision stratégique ! La décision stratégique par exemple d'augmenter son budget Informatique de 15% parce que c'est suffisant pour faire face à 95% des problèmes, c'est lui qui l'a prendra ce n'est certainement pas un DSI ou un RSSI. Les élus c'est eux qu'il faut convaincre !

Alain Melka :

Nous sommes arrivés au terme de cette visioconférence. Bien évidement le sujet de la cybersécurité étant d'une importance quasi première pour nos territoires, nous reviendrons tout au long de l'année à venir sur cette problématique. Vous avez nombreuses et nombreux à nous suivre, et je vous en remercie. Dans quelques heures, vous retrouverez sur notre site le replay de cette visioconférence grâce à notre partenaire et producteur technique Les Emotionneurs, que je remercie vivement, ainsi que Natalie Herrouin et Quentin Meullemiestre qui m'ont aidé à préparer ce passionnant échange.

On se retrouve le mardi 10 novembre, toujours avec la Banque des Territoires et Les Emotionneurs autour d'un sujet tout aussi problématique pour nos territoires, la 5G, enjeux et perspectives. Elus et experts nous accompagneront ainsi que Cédric O, Secrétaire d'Etat chargé de la Transition numérique et des Communications électroniques. N'oubliez pas de vous inscrire par mail : mission.ecoter@ecoter.org

Regardez la vidéo ici