MISSION ECOTER
France et Territoires Numériques

Actes du Colloque en visioconférence

Cybersécurité, quelles solutions innovantes pour nos territoires ?

22 juin 2021

LES ÉMOTIONNEURS
concepteurs . créateurs . producteurs

Mission Ecoter-France et Territoires Numériques

Economie Numérique des Territoires

- La Mission Ecoter-France et Territoires Numériques, 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

Gwenaelle MARTINET
Conseillère auprès du directeur général de l'Agence nationale pour la sécurité des systèmes d'information (l'ANSSI)

François CHARBONNIER
Investisseur Confiance Numérique, Caisse des Dépôts

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

Amandine DEL-AMO
Chargée de missions partenariats-cybermalveillance.gouv.fr

Jean-Baptiste VORON
CTO Cybersécurité France – Atos

Eric GREFFIER
Directeur Technologie et Développement – Partenariat Paris 2024 – Cisco France

Pascal RABIER
Customer Engineering Team Lead pour le Secteur Public – Google Cloud France

➢ **Alain MELKA – Directeur Général des Services - Mission Ecoter-France et Territoires Numériques – Modérateur :**

Un grand merci d'être si nombreuses et nombreux à nous suivre et à vous êtes inscrits à cette nouvelles visioconférence consacrée aujourd'hui à la **Cybersécurité**, et plus précisément à : **quelles solutions innovantes pour nos territoires ?**

Un grand merci également à nos invités, experts, présents en duplex, et qui ont répondu à notre invitation, visioconférence rendue possible grâce à notre brillant partenaire chargé de la production technique Les Emotionneurs.

Parce que la Cybersécurité demeure un enjeu majeur, enjeu parfois abstrait pour de nombreuses collectivités territoriales, parce que 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… que notre visioconférence va s'articuler autour de 3 questions majeures : Comment sécuriser les collectivités dans leur transformation numérique et de ce fait protéger les services et nos concitoyennes et concitoyens ? Quels sont les dispositifs et les offres proposés par le secteur privé afin de faire face à ce fléau ? Dans le cadre du « Plan de relance », comment peut-on établir un diagnostic et proposer un plan de sécurisation pragmatique et adapté aux différentes menaces ?

Rappel : Pour la seule année 2020, l'Agence nationale pour la sécurité des systèmes d'information (l'ANSSI) a reçu 2287 signalements, soit environ 6 par jour, parmi lesquels 759 étaient de réels incidents. Ce qui représente 33% du total des signalements. Sept d'entre eux étaient des incidents majeurs et 20 ont donné lieu à des opérations de cyberdéfense.

J'évoquais le plan de relance, avec nous, en duplex, Gwenaëlle MARTINET, *Conseillère auprès du directeur général de l'Agence nationale pour la sécurité des systèmes d'information (l'ANSSI), Gwenaëlle pouvez-vous nous rappeler le rôle de l'Agence, notamment en direction des collectivités dans le cadre du plan de relance ?*

➢ **Gwénaëlle MARTINET - Conseillère auprès du directeur général de l'Agence nationale pour la sécurité des systèmes d'information (l'ANSSI) :**

Bonjour à tous ! Merci beaucoup, Alain. En effet, je confirme vos chiffres, et je vais essayer de vous éclairer un peu sur ce méandre qui peut vous paraître complexe, je veux parler du plan de relance que vous évoquiez !

Pour rappel, l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI) s'occupe de la sensibilisation et de l'information auprès du plus grand nombre via la publication de guides et des formations accessibles notamment aux agents de l'État.

L'ANSSI joue également un rôle de prévention essentielle pour élever le niveau de cybersécurité auprès du plus grand nombre, avec la publication de référentiels, la qualification de prestataires de sécurité, des visas de sécurité sur des produits, des certifications etc. Tout ça attesté par notre rôle, notre capacité, à avoir une activité de recherche au plus haut niveau, qui nous permet justement cette légitimité au niveau national et international.

Par ailleurs, nous avons également un rôle de défense qui nous permet d'intervenir lors d'une attaque chez les victimes, notamment dans les ministères. Quant au plan de relance, il est arrivé en fin d'année dernière, et il nous a permis de mettre en place des mesures particulières au profit notamment des collectivités territoriales, qui sont aujourd'hui, et vous l'avez rappelé avec les chiffres, une priorité essentielle ! Les attaques quotidiennes ou quasi quotidiennes sur les collectivités territoriales montrent qu'il est absolument primordial aujourd'hui de s'intéresser à elles et d'être une aide afin de leur faire comprendre ce qu'est la cybersécurité, mais également de les accompagner.

La cybersécurité, est quelque chose de complexe qui demande beaucoup de moyens, qui demande beaucoup d'énergie pour mettre en place des actions pérennes. L'idée du plan de relance dans son volet cyber est vraiment de mettre à disposition un accompagnement personnalisé auprès des bénéficiaires qui le souhaitent afin de les aider à faire un état des lieux. Également, pour les aider à comprendre l'état de la menace qui pèse sur ces systèmes et les enjeux qu'il y a autour de ces menaces, afin de savoir effectivement ou ils en sont et où ils doivent aller.

➢ **Alain MELKA :**

Quelles sont les mesures à mettre en place pour y arriver ?

➢ **Gwenaëlle MARTINET :**

Cela est mis en place dans le cadre du plan de relance via un dispositif qu'on appelle les parcours de cybersécurité. Ces parcours sont ouverts essentiellement aux collectivités territoriales. Sur les 136 millions d'euros du plan de relance, 60 millions d'euros sont dédiés aux collectivités territoriales. C'est vraiment pour nous une priorité majeure parce qu'on est conscient de l'enjeu, on est conscient du besoin d'être accompagné et du besoin de mettre en place des choses livrées, bien définies avec l'accompagnement de l'ANSSI, même si ce n'est pas toujours l'ANSSI qui interviendra auprès de chacun.

En effet, il y a différents prestataires, car nous n'avons pas les moyens d'aller auprès de chaque bénéficiaire, mais en tout cas, nous construisons avec ces prestataires, le cadre qui va permettre la mise en place de ces parcours de cybersécurité. L'idée est vraiment déjà de se déclarer candidat. A cet effet, on a une plateforme qui est accessible sur démarches simplifiées, le lien est disponible sur notre page internet. https://www.ssi.gouv.fr/

Le bon profil est d'avoir un système d'information, ça veut également dire avoir un responsable des systèmes d'information, qui est nommé, qui est identifié et qui sera notre interlocuteur au quotidien. C'est la personne avec laquelle nous pourrons discuter des mesures en place et qui pourra faire durer ces mesures. Donc l'accompagnement est pris intégralement en charge par l'ANSSI.

➢ **Alain MELKA :**

Les mesures techniques qui sont nécessaires pour cet accompagnement afin d'augmenter le niveau de cybersécurité, sont-elles subventionnées par l'ANSSI dans le cadre du plan de relance ?

➢ **Gwenaëlle MARTINET :**

En effet, on accorde une subvention aux bénéficiaires qui ensuite vont mettre en place tous les marchés nécessaires afin d'être capable de mettre en œuvre au final des actions de sécurité.

Cela peut consister en une mise en place d'activité, de déploiement d'un logiciel de sécurité, d'outils d'authentification, d'outils de gestion d'administration. Ainsi, beaucoup d'éléments vont dépendre du niveau initial de cybersécurité du bénéficiaire. Voilà, en sommes les principales mesures cadres du plan de relance, qui sont également accompagnés par deux autres mesures plus « petites », des appels à projets plutôt pour les collectivités très matures, qui ont déjà une politique de sécurité des systèmes d'informations et déjà une feuille de route cyber, dans laquelle ils s'inscrivent depuis quelques temps et qui ont besoin ponctuellement d'un soutien financier pour un projet. Donc là, nous étudions le projet et nous co-finançons avec eux la mise en place de ce projet, afin de donner un coup de pouce et d'être un catalyseur pour la suite.

Nous avons une dernière offre au profit des collectivités territoriales qui se matérialise par le soutien à la création de centres de réponse à incident. Au bout du spectre, on a cybermalveillance.gouv.fr, ils vous en parleront tout à l'heure car ils ont une action extraordinaire au profit des particuliers, mais aussi des petites entreprises, des PME. Ainsi, les victimes potentielles peuvent se retourner vers des centres locaux de proximité afin de les aider.

Ainsi ces centres de réponse aux incidents régionaux sont en train de voir le jour et cela en étroite discussion avec chacune des régions. En effet, ils deviendront demain des interlocuteurs essentiels pour les collectivités territoriales en cas d'incident.

Voilà donc le panorama, de ce qui est fait dans le cadre du plan de relance, avec les parcours, les appels à projets, les centres de réponse à incident. L'ensemble de ces actions visent à sécuriser l'État, les services publics et à faire en sorte d'augmenter de manière significative le niveau de cybersécurité de manière durable. L'idée est vraiment que les actions perdurent et restent en place, afin que derrière, chacun ait compris comment faire pour assurer sa cybersécurité.

➢ **Alain MELKA :**

Gwenaëlle, merci, vous restez avec nous, car nous reviendrons sur les changements d'habitudes, les méthodes de travail, lieu de travail. Je pense que là aussi, ça a une incidence essentielle et importante au regard des chiffres que j'ai donnés. L'accompagnement personnalisé, les parcours de cybersécurité, les appels à projets, le soutien financier, le soutien à la création on y reviendra ! J'ai encore une ou 2 questions à vous poser, mais c'est déjà très c'est clair, c'est précis, bravo au travail qui est effectué par l'Agence depuis déjà pas mal de temps ! Il y a également je le disais, cybermalveillance.gouv.fr. Mission Ecoter-France et Territoires Numériques est partenaire depuis déjà quelque temps. Pour représenter cybermalveillance.gouv.fr, j'ai le plaisir d'accueillir, Amandine Del-Amo. Amandine, vous êtes chargée de mission partenariats cybermalveillance.de.fr. Première question : cybermalveillance.gouv.fr existe depuis quand et quelle est sa mission ?

➢ **Amandine DEL-AMO – Chargée de missions partenariats cybermalveillance.gouv.fr :**

Bonjour à toutes et à tous. En quelques mots, le dispositif est la réponse voulue par l'État pour faire face à la croissance de la cybercriminalité et répondre ainsi aux besoins de la population dans le but de les aider à se prémunir et à y faire face.

La plateforme a été lancée en 2017 dans le prolongement des missions de l'ANSSI, à cet effet, Cybermalveillance.gouv.fr a donc été créé comme solution pour le reste de la population, qui était démuni contre les différentes cyberattaques. Ainsi le dispositif s'adresse aux particuliers, aux entreprises plutôt TPE, PME, aux collectivités, plutôt les petites collectivités et aux associations. Nous avons 3 missions essentielles :

- Nous a été confié en premier lieu l'assistance des victimes d'une cyberattaque, en leur permettant à travers notre plateforme d'obtenir en ligne un diagnostic de leur situation et des conseils adaptés afin de pouvoir y remédier. Cette assistance va jusqu'à la possibilité d'une mise en relation avec des prestataires référencés sur notre plateforme. On a un peu plus de 1100 prestataires référencés, qui vont pouvoir apporter leur aide aux victimes qui ne sont pas forcément en mesure d'appliquer seul nos conseils.

- Notre 2ème mission est la prévention, avec la diffusion de nombreux supports sur les bonnes pratiques notamment à adopter afin de pouvoir se protéger. Cette prévention passe aussi par la mise à disposition sur notre plateforme de différents contenus pédagogiques. En effet, vous allez avoir beaucoup de contenus divers et variés, des articles, des vidéos, des infographies, des alertes aussi en temps réels. Par ailleurs, nous organisons également des campagnes de sensibilisation à grande ampleur sur les chaînes du groupe France télévisions, menées avec nos membres et nos partenaires. Ces campagnes sont donc diffusées à l'attention du plus grand nombre.

- Enfin, la 3ème mission est l'observation de la menace. L'idée est d'avoir la vision la plus précise possible des phénomènes cyber criminels afin de pouvoir mieux adapter nos services aux besoins de nos différents publics, puis également d'alimenter en informations, en documentations, tous les acteurs étatiques qui luttent quotidiennement contre la cybercriminalité. Par ailleurs, voici quelques chiffres : aujourd'hui nous avons 50 membres au sein du dispositif qui participent à la vie du GIP. Nous avons un peu plus de 1100 prestataires référencées sur l'ensemble du territoire et qui viennent en aide auprès des victimes.

- A ce jour, nous avons totalisé plus de 270 000 victimes assistées depuis la création de la plateforme et nous avons 47 types d'incidents qui sont traités via notre plateforme. Le constat est le suivant nous observons une augmentation globale très significative de cyberattaques depuis 2020, quelle que soit leur forme et quelle que soit la méthodologie utilisée. Les « attaquants » sont arrivés à s'adapter à la conjoncture, à l'actualité et donc nous avons eu une nette augmentation des recherches d'assistance lors de cette période de confinement.

- Concernant les collectivités, plus à proprement parler, elles ont été impactées majoritairement par les rançongiciels. C'est en fait, un petit programme, qui va s'installer sur votre système d'information, qui va chiffrer l'intégralité de vos données et qui va vous proposer en fait des chiffrements. Ainsi, voici la première menace très importante pour les collectivités. Ensuite vient le piratage informatique, qui est une menace assez prégnante et enfin, le piratage de compte, c'est à dire, le piratage de boîte mail, d'accès aux réseaux sociaux, de compte bancaire. Voilà, je me focalise sur ces 3 premières et 3 plus importantes menaces pour les collectivités, qui doivent vraiment en prendre conscience !

Ainsi, comment faire pour se prémunir contre ces risques ? Cybermalveillance.gouv.fr vous propose quelques solutions. Il y a 2 aspects à prendre en compte, il faut tenir compte du volet technique, puis on verra ensuite le volet humain.

Le volet technique, nous préconisons pour les collectivités, qui disposent d'un service technique, d'établir une politique de sécurité si ce n'est pas déjà fait, ou en tout cas de suivre les préconisations de l'ANSSI et notamment de leurs guides, qui sont très bien faits ! En revanche pour les collectivités qui ne disposent pas de service informatique, il ne faut surtout pas jouer « aux apprentis sorciers », il faut se faire accompagner par des professionnels, parce que les enjeux sont vraiment très importants. En effet, nous avons encore pu le constater récemment, les menaces sont vraiment très importantes et il y a de plus en plus de collectivités attaquées ! Ainsi, pour vous aider à trouver le bon prestataire pour vous accompagner, nous avons lancé un label qui s'appelle le label experts cyber, que nous avons conjointement réalisé avec les membres du dispositif et via l'Afnor. Ce label, va vous permettre en fait d'identifier, dans votre région, les prestataires informatiques compétents, qui vont pouvoir vous accompagner et dont l'expertise a été vérifiée. Ainsi, ils vont pouvoir vous accompagner en cas d'attaque mais surtout aussi en amont, dans la sécurisation de votre système informatique et de tous vos outils numériques, que ce soit la téléphonie ou votre site web. A ce jour, nous avons un peu plus de 80 labellisés sur tout le territoire français, qui s'adresse à tous les professionnels, collectivités, TPE, PME et associations.

Par ailleurs, un autre aspect à ne pas négliger, c'est le volet humain. En effet, il y a une acculturation à la cybersécurité qui est indispensable auprès de tous les agents des collectivités, quelle que soit la fonction, et j'allais dire cette acculturation doit être aussi bien les stagiaires que les élus ! Tous les niveaux de la collectivité doivent être concernés. Cette sensibilisation est nécessaire. On parlait tout à l'heure des campagnes d'hameçonnages et bien elles sont très courantes. Il suffit qu'une personne soit peu sensibilisée pour faire rentrer un code malveillant et compromettre les identifiants de session ou donner ainsi l'accès à l'attaquant du système informatique de la collectivité. Tout le monde doit être sensibilisé ! Tout le monde doit vraiment, comprendre qu'il a un rôle majeur à jouer dans la défense du système informatique de la collectivité. Ce facteur humain est stratégique dans la chaîne de sécurité, il est vraiment essentiel de les sensibiliser pour prendre conscience à chacun son rôle à jouer dans cette défense. Ainsi pour vous y aider, on a créé un kit de sensibilisation. Ce kit est une boîte à outils qui tourne autour de 2 axes, l'un face au risque et l'autre concernant le partage des bonnes pratiques. En effet, il est important de comprendre les risques pour savoir comment appliquer les bonnes pratiques. Nous avons 17 thématiques abordées et qui sont déclinés sous différents types de format. Ces éléments sont disponibles sur notre site gratuitement. http://www.cybermalveillance.gouv.fr/

Par ailleurs, je voudrais prendre quelques minutes pour vous parler d'une initiative que nous avons eu l'année dernière à destination des collectivités. En effet, nous avons lancé un programme de sensibilisation pour les élus, aux risques numériques afin de partager avec eux les bonnes pratiques, en essayant d'avoir une approche assez pragmatique par rapport à leurs problématiques d'élus.

Ainsi, nous avons essayé de les interpeller, de les mettre en mouvement sur ce sujet qui ne leur parle pas forcément à tous. De ce fait, nous avons créé ce programme en 3 volets.

Le premier, sur les principales menaces et les réflexes essentiels à avoir.

Le deuxième, concerne la vigilance, toutes les collectivités, quelle que soit leur taille, sont des cibles potentielles et nous avons des témoignages de collectivités qui furent victimes d'attaques, elles livrent ainsi leurs expériences.

Enfin, le troisième volet a vu le jour il y a quelques semaines, c'est un « best of » d'actions de sensibilisation, mis en avant par 6 collectivités qui témoignent de ce qu'elles ont pu mettre en place. Ce sont des collectivités de taille complètement différentes, afin de montrer que, quels que soient les moyens humains et financiers, il est possible de mettre en place des choses et de sensibiliser ses agents et élus autour de cette problématique. Dans le cadre de ce programme, on a également créé des vidéos de sensibilisation pour les élus avec la Banque des Territoires, vidéos lancées en fin d'année dernière.

➢ **Alain MELKA :**

Bien évidemment, le dispositif s'adresse à toutes et à tous, on l'a bien compris. Prévention, bonnes pratiques, campagne de sensibilisation, partenariat avec Mission Ecoter-France et Territoires Numériques et avec d'autres... le label, les solutions, l'acculturation, la sensibilisation… Il est temps de céder la parole à Jean Baptiste Voron, CTO Cybersécurité France chez Atos. Jean-Baptiste, chez Atos, vous êtes sur l'anticipation, c'est bien ça ?

➢ **Jean-Baptiste VORON – CTO Cybersécurité France – Atos :**

C'est exactement ça ! Merci beaucoup, Alain. Effectivement il y a une notion d'anticipation qui est essentielle. Avant de parler d'innovation et du traitement de tous les fondamentaux dont on vient d'évoquer, l'anticipation doit être au cœur de la préoccupation cyber. En effet, il est très important d'aller vers l'innovation ! On va le voir, il y a vraiment quelques belles avancées et beaux progrès qui devraient profiter à tout le monde. L'anticipation fait partie des meilleurs outils que nous avons dans l'arsenal de cyberdéfense.

Avant cela, quelques mots sur Atos, Atos qui est une grosse société, dont Atos cybersécurité, une division qui compte 450 experts en cybersécurité, avec beaucoup de retours d'expériences, des opérateurs, des architectes, des consultants, des auditeurs. Par ailleurs, c'est également 8 sites physiques en France, à partir desquels nous rayonnons sur l'ensemble du territoire national afin d'aider nos clients du secteur privé ou public. Mais pour en revenir à l'anticipation, la première chose est de bien évaluer et de comprendre la menace, qu'est ce qui est vraiment critique et vitale pour moi ? Est-ce que c'est le site web de la collectivité ? Est-ce certaines applications ? est-ce que ce sont certaines données des archives ? Est-ce que c'est ma messagerie qui est critique?

Ainsi, il faut déjà en amont se poser ces questions-là, cela va permettre de définir quels sont les risques auxquels je ne souhaite pas m'exposer, quels sont les risques que je tolère et quels sont les risques auxquels je ne souhaite pas m'exposer afin de pouvoir ainsi concentrer mes efforts sur des actifs vitaux pour la collectivité. Donc ça, c'est la première chose, évaluer les risques, comprendre la menace et puis sensibiliser.

Je ne vais pas refaire le discours de cybermalveillance, mais il est très important de communiquer sur la cybersécurité, sensibiliser les élus, sensibiliser les décideurs pour que ce message soit partagé aussi bien par les personnes qui font de la technique, les services, mais aussi par l'ensemble de ceux qui portent la responsabilité auprès des citoyens.

La sensibilisation, existe absolument partout au niveau de cybermalveillance.gouv.fr, le contenu est vraiment super avec les kits, etc. Si ça ne suffit pas, il y a encore des approches sur lesquels on peut très facilement faire des évaluations en passant quelques heures dans la peau d'un hacker, se convaincre que la collectivité est exposée. Ainsi, il faut agir, c'est un bon moyen de communiquer en disant voilà tout ce qu'on peut observer sur internet concernant ma collectivité et voilà quels sont les risques auxquels je m'expose. Si ça ne suffit pas, on peut aussi aller vers des tests d'intrusions et donc à travers quelques campagnes simples, aller vers des personnes qui seraient moins sensibiliser aux risques.

Eh bien oui ! c'est possible de s'introduire dans un système d'information et de causer des dommages. Après l'anticipation, il y a l'innovation qui est essentiel, avant de parler de technique, il est important de se dire, je vais changer ma façon de faire de la cybersécurité. En effet, il y a un vrai défi aujourd'hui de la part des collectivités territoriales, des TPE, des PME, de se dire, j'ai un problème de charge, j'ai un problème pour me conformer à l'ensemble des règles, de pouvoir visualiser l'ensemble des formations.

En effet, toutes les exigences me demandent beaucoup de temps et ce temps je ne l'ai pas ! Et nous le constatons sur le terrain tous les jours. Le temps manque, les compétences manquent et donc là aussi il faut innover dans sa façon de faire la cybersécurité. Nous, ce que nous proposons, c'est d'envisager le service manager en confiant certaines missions. Par exemple la mise à jour de mes antivirus, par exemple, le patch et la correction de mes postes de travail de mes serveurs, ainsi, je délègue la protection de ma messagerie à quelqu'un d'autre, à un expert qui va s'en charger et ça c'est une façon de faire qui n'est pas encore très ancrée en France, mais c'est très important.

En effet, il faut savoir s'appuyer sur ceux qui savent afin de se protéger efficacement et se recentrer sur d'autres activités qui sont tout aussi importantes. Ce sont des petites révolutions, dans la façon de faire, mais ça amène énormément de très bons résultats financiers, mais également d'un point de vue humain. Par ailleurs, il y a une autre façon de déléguer vers des services complets. En effet, des services complets externalisés, je suis sûr que Pascal et Éric les évoqueront dans leur intervention !

Ainsi, quand je parle de services externalisés, on va parler de cloud, évidemment, c'est au cœur des préoccupations et des questions. La sécurité du cloud est excellente et elle progresse aujourd'hui, bien plus vite que la plupart des autres périmètres de nos clients que nous accompagnons quotidiennement.

Le problème n'est plus la sécurité. Le problème, ça va être la confiance, la confiance que j'accorde auprès de mes fournisseurs, la confiance que j'accorde à mes équipes qui utilisent les services externalisés. Ainsi, on est en train de changer de paradigme. En effet, c'est une innovation de se dire comment je construis cette confiance, entre moi, la collectivité et le fournisseur de services. Est-ce que je peux m'appuyer sur un tiers de confiance qui va venir m'aider à créer ce triangle vertueux, du fournisseur, du tiers de confiance et de la collectivité territoriale ? Je pense que là, c'est vraiment là-dessus qu'il faut travailler et tous les grands acteurs, tous les fournisseurs de services sont vraiment engagés dans cette démarche, de dire comment on amène la confiance aussi bien d'un point de vue contractuel que d'un point de vue technique et de se dire comment je délègue une partie de cette confiance à des tiers dont c'est le métier, aussi bien pour faire de la gestion des identités que pour faire de la gestion des données.

Enfin, la gestion de mes traces d'activité pour pouvoir détecter toute malveillance qui serait opérée par ou via les fournisseurs de services donne des résultats très concrets. Vous pouvez insister là-dessus, ce sont des choses très concrètes qui existent et qui sont à mettre en place dès aujourd'hui, très rapidement afin de protéger les environnements.

Par exemple, Office 365 fourni par Microsoft, protège les environnements Google Workplace fourni par Google. Le savoir-faire de ces acteurs-là, amène ce petit niveau de confiance supplémentaire qui permet d'améliorer, on va dire les relations entre la collectivité territoriale et en tout cas la confiance qu'on peut accorder à ses acteurs qui fournissent encore une fois un service d'un très haut niveau de qualité.

Enfin, ça peut être également l'utilisation des authentifications France Connect pour pouvoir se connecter à des environnements Microsoft Google. Voilà, c'est une façon de dire, je délègue une partie de l'authentification de mes environnements.

➢ **Alain MELKA :**

Merci Jean Baptiste ! Sensibiliser les élus et les décideurs, innovation, déléguer, confiance, il faut bien se dire une chose, c'est que la cybersécurité, ce n'est pas comme une maladie grave ou un accident de la route, avec le fameux cela n'arrive qu'aux autres. Non, non, non, ça peut nous arriver ! Ça peut nous arriver à tout moment et à tout instant. Il existe des possibilités. Il faut vous faire accompagner. Pour cela, nous avons le plaisir d'accueillir également Éric Greffier, Directeur Technologie et Développement - Partenariat Paris 2024 chez Cisco France. Éric, Cisco France est partenaire de Paris, 2024 quelques mots sur votre entreprise, la veille technologique, le mécanisme de protection. Vous proposez également des solutions aux collectivités locales et territoriales.

➢ **Eric GREFFIER – Directeur Technologie et Développement – Partenariat Paris 2024 – Cisco France :**

Quelques mots sur Cisco, née avec internet à la fin des années 80. Je me permets de préciser que 80% du trafic internet aujourd'hui passe par un équipement réseau Cisco. Mais dans le Grand Cisco, vous avez une partie qui est entièrement dédiée au sujet de sécurité.

En effet, le marché de la cyber résilience est extrêmement florissant et je pense que la COVID (Jean-Baptiste aurais pu le dire aussi) a probablement en plus accéléré tout cela. Donc imaginer, que du côté des « méchants », vous avez des structures qui sont extrêmement bien organisées, avec recherche et développement afin de réaliser des attaques très sophistiqués, malheureusement c'est aussi une course à l'échalote !

En termes d'armement, il faut entre guillemets que les « gentils », dont on fait partie, se dotent de moyens et de la capacité à faire progresser la compréhension de toutes ces menaces.

Ainsi, je vais mettre quelques chiffres en avant, mais ceux qui sont importants, c'est essentiellement le fait que chez Cisco, on a 400 ingénieurs dédiés à la recherche, ce sont des malwares de la malveillance. Alors, on a la chance, grâce à notre part de marché réseau, de voir énormément de trafic réseau passé et donc de pouvoir détecter un peu plus que la moyenne les choses qui ne se passent pas normalement.

Par ailleurs, l'autre chiffre très important, au-delà de l'investissement qui a été réalisé chez Cisco en termes d'acquisition d'intelligence chez les start-ups, c'est aussi en parallèle le fait qu'on dépense entre 1 et 2 milliards en recherche développement interne autour des sujets de cyber. Je suis vraiment désolé de parler d'argent, mais on est obligé.

Bien entendu, Cisco est un parmi énormément d'acteurs à être obligée d'investir pour être capable de proposer des solutions qui soient pertinentes par la sophistication des attaques.

Ainsi, je voulais vous donner ces quelques chiffres. Après Alain, vous indiquez, oui, nous avons une démarche très importante au niveau de cette veille. Ce que je disais sur la partie Talos, qui est cette entité de recherche, encore une fois, l'idée est de pouvoir détecter le plus rapidement ce qui se passe quelque part dans le monde et de pouvoir mettre dans nos solutions matérielles et logicielles l'information pour que ces outils de protection puissent détecter ces nouveaux virus. Voilà donc une petite présentation qui vous donne un petit peu de perspective.

➢ **Alain MELKA :**

Nous allons très vite donner la parole à Pascal, parce que le temps tourne aussi. Pascal Rabier, vous êtes Customer Engineering Team Lead pour le Secteur Public chez Google Cloud France et vous me disiez en préparant cette visioconférence le cloud n'est pas l'ennemi de la cybersécurité bien au contraire. C'est ce que disait également tout à l'heure Jean-Baptiste. Alors expliquez-nous pourquoi vous êtes aussi sûr de vous-même en ce qui concerne le cloud.

➢ **Pascal RABIER – Customer Engineering Team Lead pour le Secteur Public – Google Cloud France :**

Tout d'abord, merci d'avoir invité Google à participer à cette table ronde. Auparavant, j'aimerais juste préciser qu'on partage chez Google cloud les constats qui ont été fait jusqu'à présent !

En effet, on est convaincu que nous allons pouvoir y répondre efficacement tous ensemble au niveau de l'écosystème de la technologie. C'est pour ça que je suis ravi d'être à côté de nos partenaires, Atos, qui est un grand partenaire service en France, mais également, Cisco, avec qui nous déployons des solutions de cloud hybride et enfin, cybermalveillance.gouv.fr avec qui nous sommes très fiers de faire partie des « supporters ».

Effectivement, ce qu'on constate, et je rejoins complètement Jean-Baptiste, c'est qu'aujourd'hui la cybersécurité est un maillon essentiel et même le premier pour réussir un projet de transformation numérique incontournable. Et on ne peut pas laisser la cybersécurité menacer ça parce que l'environnement est de plus en plus complexe, en particulier avec le télétravail.

Ainsi, pour vraiment réussir cette transformation numérique en toute sécurité, il faut des solutions qui soient innovantes. Ces solutions doivent être vraiment utilisables par le plus grand nombre et en particulier par les collectivités locales, elles doivent être abordables parce que souvent, les collectivités locales n'ont pas les moyens des grandes entreprises privées ou des organisations étatiques plus centrales. Par ailleurs, elles doivent être simple parce qu'on a vu qu'il y a un vrai enjeu de certifications, de compétences et même de compétences disponibles sur le marché.

Ainsi, on doit pouvoir utiliser ces outils le plus simplement, de manière plus intégrée. Non pas avoir des outils disparates ou c'est l'utilisateur de l'équipe technique qui recolle les informations entre ces outils. Enfin, cette démarche de sécurisation des solutions doit favoriser l'expérience utilisateur. Chez Google cloud, nous sommes connus pour nos solutions dans le cloud, Google cloud Platform est l'infrastructure à ce service et donne des solutions un petit peu plus évoluées ou des solutions de collaboration.

Par ailleurs, nous sommes un peu moins connus pour nos solutions qui permettent de sécuriser vos applications, vos données ou qu'elles soient en fait dans vos datas centers ou dans les datas centers de vos hébergeurs ou d'autres classes. Effectivement, c'est là où, je veux en venir à ce qu'on propose pour aider nos clients.

D'abord, j'aimerais revenir, et je rejoins complètement Jean-Baptiste en répondant à une question d'Alain, qu'effectivement le cloud a des propriétés fondamentales qui font que c'est un atout pour la cybersécurité. Alors bien sûr, il ne faut pas y aller n'importe comment, il faut le gérer. Mais dans le cloud, il y a toutes les capacités natives de stockage, de tous les événements qui peuvent se passer et qui vont nous permettre d'avoir la visibilité, y compris sur les actions de maintenance. En tout cas, chez nous faites confiance à nos équipes de maintenance, il y a tous les mécanismes fondamentaux de sécurité qui vont permettre d'automatiser les déploiements pour éliminer mêmes les erreurs humaines, ou alors pour mettre à jour plus rapidement en cas de faille détectée. Et puis, il y a aussi tous les outils qui vont équiper les DSI ou leurs prestataires.

En effet, la responsabilité doit être partagée et peut être potentiellement déléguée sur certaines activités, donc donner des outils qui soient vraiment compréhensibles mais conçus pour la sécurité afin de repérer facilement toute activité suspecte. En effet, on a tendance à parler dans le cloud de modèle de responsabilité partagée au niveau de l'administration de ce type de solution, mais en termes de sécurité chez Google, on a plutôt tendance à parler de destinée commune.

Ainsi, c'est ce que nous mettons en pratique à la fois chez nous et que nous permettons de mettre sur les systèmes et applications de nos clients. Il existe 2 grands principes, le premier, tout détecter et le second, ne faire confiance à rien. Ainsi depuis une dizaine d'années, on utilise ces 2 grands principes sur nos infrastructures. C'est le travail qui vient de la division cybersécurité de Google, qui va vraiment permettre de stocker tous les évènements et le temps afin de repérer les attaques, de les comprendre parce que certaines ont commencé il y a bien longtemps. On l'a vu avec l'éventail des menaces présentées par cybermalveillance.gouv.fr, il faut vraiment « historiser » un grand nombre de métriques, cela fait beaucoup de données mais il faut des outils qui vont permettre d'analyser et de mettre en valeur les informations pertinentes aux opérateurs ou aux personnes de l'équipe qui vont surveiller tout ça.

L'avantage de cette solution est qu'elle est disponible en mode abonnement, donc vous n'avez pas à vous soucier de la durée de l'historisation des données et de la durée de de la quantité de données à stocker, le coût est fixe, il est au nombre d'agents et c'est tout. Ainsi, ça permet d'avoir des budgets prévisibles.

Par ailleurs, l'autre stratégie est de ne faire confiance à rien, et là, effectivement c'est d'aller au-delà du système, du modèle, de sécurité traditionnelle ! Voilà aucune confiance.

L'idée, est vraiment de protéger, d'analyser, d'autoriser les accès de tous les utilisateurs de manière beaucoup plus fine que dans le modèle de sécurité traditionnelle. Donc le nouveau modèle de sécurité est fourni à nouveau sous forme d'abonnement et qui va permettre de valider chaque accès en fonction du contexte et qui va permettre de détecter en temps réel les malwares, les chiffres, avertir l'utilisateur parce qu'on tient absolument à faire en sorte que l'utilisateur, et on l'a dit, c'est important, c'est lui la première ligne de défense de l'organisation, c'est le premier allié, il faut lui donner les outils ! Comme déjà évoqué, commencer par le former, le sensibiliser et lui donner les outils pour qu'il comprenne ce qui se passe. Enfin, il faut protéger l'accès aux applications en fonction de la criticité réelle de ces applications, donc, tout ça à nouveau disponible sous forme de d'abonnement.

➢ **Alain MELKA :**

Très intéressant ce que ce que vous évoquez, il y a des outils. Les collectivités locales, territoriales, les élus, les décideurs, vous n'avez pas le droit, je dis bien, vous n'avez pas le droit de passer à travers, ce n'est pas possible. Il y a des outils, Pascal Rabier vient de nous en parler avec des solutions abordables. Par ailleurs, il y a 2 mots que j'aime beaucoup, c'est destinée commune, destinée commune les uns les autres vous travaillez ensemble, je le vois, vous vous connaissez. Et bien évidemment, on en arrive à François Charbonnier que l'on connaît bien, François, investisseur confiance numérique à la Banque des Territoires, la Banque des Territoires partenaire de la première heure de Mission Ecoter-France et Territoires Numériques. François merci d'être une nouvelle fois présent parmi nous. La Banque des Territoires investit énormément dans le domaine du numérique, mais qu'en est-il dans la lutte contre la cybercriminalité ?

➢ **François CHARBONNIER – Investisseur Confiance Numérique – Banque des territoires :**

Merci, Alain, de me recevoir et de me donner la parole sur ce sujet très intéressant. Effectivement, la Banque des Territoires, et donc le groupe Caisse des dépôts, participe évidemment à beaucoup d'actions énumérées, mais travaille essentiellement à l'accompagnement des collectivités, notamment dans des logiques d'infrastructures et de transition numérique.

Des nouveaux enjeux existent, on s'est penché davantage sur les sujets de confiance numérique et de cybersécurité qui sont pour nous d'autant plus important que nous avons aussi cet ADN de tiers de confiance historique.

En effet, du côté de la Caisse des dépôts, nous avons un positionnement sur cette matière riche qu'est la confiance numérique et la diversité des territoires. Ainsi, on investit déjà dans des solutions de cybersécurité et de confiance numérique innovante, donc ça peut être typiquement des start-ups. Par ailleurs, il est important de proposer des outils qui puissent encourager l'émergence d'outils, la structuration d'un écosystème qui soit à la fois compréhensible par les territoires, par les plus petites structures que soient les collectivités ou même les petites entreprises. Nous nous inscrivons aussi dans le cadre de la stratégie nationale de cybersécurité dont a parlé Madame Martinet, en début d'intervention.

En effet, nous somme pilote sur le sujet de l'innovation, avec un appel à manifestation d'intérêt cyber, en sécurisant les territoires dans le but de faire émerger à moyen terme les outils de cybersécurité qui seront spécialement adaptés aux acteurs des territoires. C'est quelque chose d'important, parce que nous sommes tous conscients des limites qu'il peut y avoir, des limites de budget, d'expertises. Et c'est justement ce constat que je viens de citer qui a fait qu'au-delà de cette logique de financement et d'innovation, on a cherché à profiter de notre proximité auprès des élus, y compris sur les logiques de transition numérique, pour faire un guide, justement pas du tout technique. Ainsi, je vais un peu présenter en quelques mots de guide, sachant que c'est une publicité loyale et que le guide est gratuit et disponible sur notre site internet : www.banquedesterritoires.fr/

En effet, ce guide répond à un besoin qu'on a cerné. Quand on est un élu, on va être assez dépourvu sur ce sujet. On a l'impression de ne pas connaître grand-chose, que c'est compliqué et qu'il faut surtout se presser de « refourguer » le sujet à un directeur technique, DSI ou à quelqu'un qui s'y connaît un peu plus. Ainsi, l'objet de ce guide est de se dire qu'il y a étape intermédiaire qui est donnée par l'impulsion. En quoi ce guide peut- être utile pour un élu ?

Premièrement, on peut appréhender les enjeux juridiques. On peut voir ça aussi comme guide de survie qui donne quelques bons réflexes pour les élus. En effet, j'insiste vraiment là-dessus ce guide donne des informations sur mesure et permet aussi de se mettre en situation. C'est très important. On entend souvent dire ce sujet est abstrait.

Ainsi, il faut s'inspirer de ce qui s'est passé et se dire qu'est-ce qu'on ferait à la place ? Par ailleurs, quand on mène des travaux de confiance numérique au bénéfice des citoyens, c'est justement à leur bénéfice ! Et il faut savoir en parler et le valoriser. Il faut accepter des choses qui peuvent correspondre à des peurs mais quand on est en situation de décider, on n'est pas un expert, on n'a pas tout à comprendre mais pour autant, on doit donner l'impulsion.

C'est pareil en matière de sécurité publique, c'est pareil dans d'autres domaines de gestion de la pollution, etc. C'est exactement la même chose et ce n'est même pas une question de complexité qu'il peut y avoir derrière, mais il faut vraiment accepter ça et une fois qu'on accepte cette idée, ce qu'on pousse dans ce guide, c'est l'impulsion, c'est n'est pas juste de dire allez, on y va sur la cybersécurité.

En tant qu'élu il existe des actions sur la formation, la sensibilisation des agents, des élus et parfois des prestataires. Je veux qu'on sache ou on en est, c'est tout bête, mais si on ne sait pas ce qu'on a sous la main en termes de numérique, d'informatique ou parfois de très important chez les prestataires en délégation de service ou des partenaires, on ne peut pas avancer.

Ainsi, il faut donc savoir ce dont on dispose et de façon à mener des projets numériques qui soient fiables et pérennes, c'est de la cybersécurité ! Mais c'est aussi de la bonne conception. Par ailleurs, maîtriser la ville numérique au quotidien, ça veut dire quoi ? Tout d'abord, de savoir réagir si jamais on s'est fait attaquer. L'idée est de tout simplement se poser la question, vous avez un scénario avec une logique de rançon ? Qu'est-ce qu'on fait ? Dans ce cas-là, vous êtes en position de décider, est-ce qu'on paye la rançon, est-ce qu'on dépose plainte ? Est ce qu'on cherche à avoir les services d'un expert et puis peut être en amont, il y a peut-être des actions qu'on aurait aimé prendre et la cybersécurité c'est pile essayer de prendre en amont des actions au lieu de se dire j'aurais bien aimé les prendre. Enfin, nous avons réalisé avec cybermalveillance.gouv.fr 4 vidéos qui correspondent elles aussi à des situations dédiées aux élus des collectivités locales.

➢ **Alain MELKA :**

Merci François. Nous retenons, bien évidemment, les outils en direction des territoires les plus modestes aux plus importants. Un numérique de confiance aussi, ça me paraît essentiel. Et puis enfin, des mesures très simples pour savoir comment réagir. Hélas le temps vraiment en court beaucoup trop vite. Beaucoup de questions de notre public sont tombées, malheureusement nous arrivons au terme de notre visioconférence. Toutefois, il y en a 1 qui me parait en tout cas essentiel. Donc je vais vous demander de répondre très rapidement avant qu'on puisse faire un tour de table rapide pour conclure. La question, elle est destinée à Gwenaëlle : comment connaître les prestataires labellisés par l'ANSSI dans sa région ou son département ?

➢ **Gwenaelle MARTINET :**

Alors aujourd'hui, il n'y a pas de prestataires labellisés dans les régions et les départements, c'est une action qui est plutôt du côté de cybermalveillance.gouv.fr. Dans le cadre des parcours de cybersécurité, on a recensé des prestataires terrains dont les coordonnées sont partagées avec les bénéficiaires des parcours par les prestataires accompagnateurs. Donc ça, c'est quelque chose qui est disponible sur demande dans le cadre d'un parcours de cybersécurité.

➢ **Alain MELKA :**

Je le disais, nous arrivons au terme de notre visioconférence, à cet effet, quelques mots de conclusion. On va commencer par François, est ce que vous trouvez que nos collectivités, nos élus, nos cadres des collectivités, vous qui êtes en prise direct avec les collectivités locales et territoriales, trouvez-vous qu'ils prennent de plus en plus conscience de l'importance de la cybersécurité ?

➢ **François CHARBONNIER :**

Je pense qu'il y a de plus en plus de prise de conscience. Après il y a l'étape suivante qui est d'avoir conscience et de mettre en œuvre. Il y a parfois des petites réticences qui sont tout à fait normales à passer à l'action, parce que cela demande justement de s'emparer du clavier, de vaincre ses peurs.

➢ **Alain MELKA :**

Merci à vous, François ! Jean Baptiste, quelques mots de conclusion.

➢ **Jean-Baptiste VORON :**

Je pense que le leitmotiv, celui que j'essaie de faire passer, est qu'il y a des choses très simples à mettre en œuvre, très rapidement, très facilement. Bien sûr, il s'agit d'être bien accompagné pour se rapprocher des acteurs qui sont autour de cette table, aussi bien de leurs représentants d'agences étatiques ou bien vos correspondants techniques, vos fournisseurs sur le terrain, ils ont les compétences cybersécurité ! Ils sauront engager avec vous le fameux parcours cybersécurité, faire des choses simples, identifier vos risques, identifier la menace et conduire les premières actions les plus essentiels. Il y a énormément d'attaques et ça, je pense que c'est quelque chose qu'il faut partager. Il y a énormément d'attaques, les fameux bruits cyber qui peuvent être évités à partir de solutions et à partir de moyens de protection très simples, donc ça vaut le coup de les mettre en œuvre, surtout que maintenant c'est très accessible.

➢ **Alain MELKA :**

Au tour de Pascal. Le cloud, on l'a compris, ce n'est pas l'ennemi du tout, de la cybersécurité !

➢ **Pascal RABIER :**

En effet ! Si nous chez Google Cloud nous pouvons aider les collectivités territoriales à réussir leur transformation numérique, en plaçant la sécurité au centre, c'est à dire ce qui est un des enjeux, les bonnes pratiques recommandées, l'essentiel est de prendre en considération la cybersécurité comme un pilier essentiel de la transformation numérique. Donc dans ce cas-là, si le message est bien passé, j'ai réussi ma prestation !

➢ **Alain MELKA :**

Éric, quelques mots, peut-être sur la formation ?

➢ **Éric GREFFIER :**

Justement, je souhaitais terminer sur ce sujet-là : rappeler à tous les élus que dans le cadre de notre responsabilité sociétale et environnementale d'entreprise nous proposons depuis 2001 des formations « certifiantes » et diplômantes. Ça s'appelle la Cisco Network Academy, c'est absolument agnostique. Les solutions Cisco, ce sont vraiment de l'éducation fondamentale, et il y a à peu près 35 000 personnes chaque année qui reçoivent des diplômes dont la grande majorité sont des étudiants, mais une minorité sont aussi déjà en reconversion professionnelle. On a parlé beaucoup de cybersécurité, s'il est bien un domaine où il existe une pénurie de compétences, c'est bien ce domaine-là et nous apportons notre modeste pierre à l'édifice et n'hésitez pas à nous contacter si vous êtes mis en relation avec des écoles pour pouvoir recruter des jeunes talents français.

➢ **Alain MELKA :**

Amandine, alors un site superbement bien fait, accessible, et à tous cybermalveillance.gouv.fr, quelques mots, avant de céder la parole à Gwenaëlle.

➢ **Amandine DEL-AMO :**

Moi, je voudrais juste dire, tous ensemble ! Notamment par rapport aux collectivités entre elles, sur ce qu'elles peuvent vivre en cas d'attaque mais aussi sur les outils qu'elles peuvent utiliser pour se sécuriser. Toutes les bonnes pratiques qu'elles ont mises en œuvre. Voilà, il faut absolument qu'elles partagent et qu'elles osent parler de ce qui leur est arrivées ou des actions qu'elles mettent en œuvre. Je pense que c'est vraiment important de de libérer la parole à ce niveau-là et que tout le monde partage ensemble, afin de pouvoir avancer et de pouvoir mieux se sécuriser encore.

➢ **Alain MELKA :**

Pour en terminer, Gwenaëlle, pour l'Agence Nationale pour la Sécurité des Systèmes d'Information l'ANSSI, le mot de la fin pour vous.

➢ **Gwenaëlle MARTINET :**

Merci beaucoup, Alain. Je voulais juste dire que la cause et urgente et l'enjeu est là, les moyens sont sur la table, les acteurs sont mobilisés, tous les prestataires de services, les fournisseurs de produits, on a ce qu'il faut en France pour sécuriser les systèmes d'information. Ainsi, il est urgent d'y aller, et aujourd'hui on est prêts à vous accompagner ! Alors l'ANSSI, évidemment, mais aussi cybermalveillance.gouv.fr, c'est tous les acteurs étatiques qui sont prêts à assurer, donc allez-y demander de l'aide. On est prêt à vous accompagner et ça, ça vaut le coup parce que, en cas d'attaque, c'est vraiment désastreux. Il faut donc absolument penser à la cybersécurité et les moyens qui sont aujourd'hui disponibles pour y arriver.

➢ **Alain Melka :**

Mesdames, Messieurs, merci infiniment d'avoir répondu à notre invitation, merci également au nombreux public qui nous suivi. Toutes ces informations évoquées aujourd'hui, vous les retrouverez aussi sur le site www.ecoter.org/. Cibles potentielles nous le sommes toutes et tous, surtout ne pas jouer à l'apprenti sorcier. De la confiance et puis les échanges de bonnes pratiques, nous les évoquions bien évidemment.

Un grand merci donc à vous toutes, un grand merci aux Émotionneurs, notre production technique, je ne le répéterai jamais assez, ils sont professionnels, brillants ! Aujourd'hui nous venons d'inaugurer des studios magnifiques au cœur même de Paris, j'en suis très fier !

Un grand merci également à Quentin Meullemiestre, qui m'a aidé à préparer cette visioconférence. Et puis si vous suivez l'actualité de Mission Ecoter-France et Territoires Numériques, sachez que nous sommes, vous le savez, extrêmement sensible à la transition environnementale des territoires qui est d'une importance capitale pour nos collectivités. Nous sommes actuellement au Low Carbon World, Parc des Expos à Paris, Porte de Versailles, demain et après-demain. J'aurai le plaisir d'animer une table ronde le 24, jeudi à 12h, pavillon 6 et ce sera, en direct sur les réseaux sociaux et le site du Low Carbon World, vous trouverez le lien de diffusion est sur le site www.ecoter.org.

Merci à tout le monde. Bien évidemment il y a encore beaucoup, beaucoup, de choses à dire et à partager sur la cybersécurité, nous y reviendrons ! Prenez soin de vous et à bientôt.

Informations utiles

- **Google cloud**

https://cloud.google.com/security

https://cloud.google.com/products#security-and-identity

- **Cisco**

https://www.cisco.com/c/fr_fr/products/security/index.html#~produits

- **Banque des Territoires**

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

- **cybermalveillance.gouv.fr**

❖ kit de sensibilisation : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/liste-des-ressources-mises-a-disposition

❖ Programme de sensibilisation des élus :

✓ 1er volet (avec les vidéos « collectivités »)

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/programme-sensibilisation-risques-numeriques-collectivites-territoriales

✓ 2ème volet : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/vigilance-cyberattaques-collectivites-toutes-concernees

✓ 3ème volet : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/sensibilisation-risques-numeriques-collectivites

❖ Mise en relation avec des prestataires labellisés pour la sécurisation en amont de ses infrastructures numériques (SI, téléphonie, site …) pour les collectivités ou TPE/PME https://www.cybermalveillance.gouv.fr/accompagnement/accuei

- **ANSSI**

https://www.ssi.gouv.fr/agence/cybersecurite/france-relance/

- **Atos**

❖ Des territoires citoyens

https://atos.net/fr/industrie/collectivites-territoriales

❖ « Soyez prêts à toutes les éventualités »

https://atos.net/fr/solutions/cybersecurite

Production technique

LES ÉMOTIONNEURS

concepteurs . créateurs . producteurs

Regardez la vidéo ici

Suivez l'actualité de Mission Ecoter-France et Territoires Numériques

FRANCE & TERRITOIRES
ÉCOnomie numérique des TERritoires