sictiam

NUMÉRIQUES TÉLÉCOMMUNICATIONS ÉNERGIES

L'exposition aux menaces cyber est indéniable. Cependant, un constat alarmant se dégage : une part non négligeable de collectivités indique que le risque cyber n'est pas une priorité pour elles ou qu'elles ne se sentent pas concernées.

Les exemples de cyberattaques ayant des répercussions directes sur les services publics ne manquent pas. Face à l'attaque subie par la collectivité départementale des Alpes-Maritimes en novembre 2022, j'ai décidé d'apporter les meilleures réponses possibles pour améliorer les process de repérage des cyberattaques et les process de réponse et de gestion de crise lors d'une attaque.

Avec le SICTIAM, nous sommes résolus à promouvoir une cybersécurité efficace et accessible pour tous, car nous sommes convaincus que cela est essentiel pour garantir un environnement numérique sûr et résilient pour toutes les collectivités territoriales.
Nous nous engageons à soutenir les efforts continus visant à renforcer la protection des infrastructures et des données tout en formant les agents de la fonction publique territoriale aux meilleures pratiques de sécurité informatique.

Charles Ange Ginésy
Président du Département des Alpes-Maritimes et du SICTIAM

Journée Cybersécurité avec nos Adhérents - 12 avril 2024

Cybersécurité : collectivités et établissements publics trop vulnérables ?


Kevin Heydon, délégué de l'ANSSI et Jessé Ammendola, Directeur Général du SICTIAM

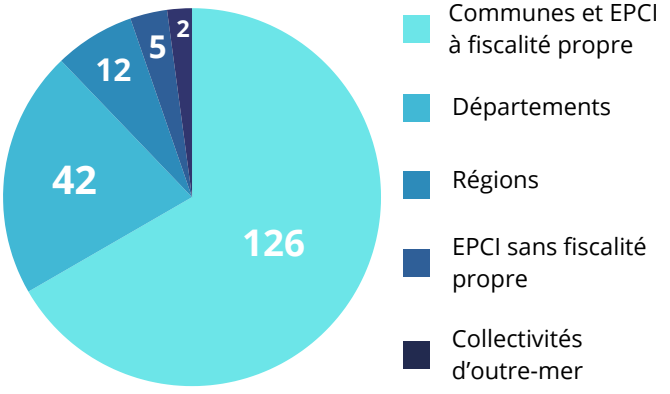
En avril, une journée consacrée à la cybersécurité a été organisée en partenariat avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Cette initiative a permis au SICTIAM de mettre en avant son engagement constant envers les collectivités et établissements publics dans la prévention des cyberattaques et d'intervenir en cas de besoin. Célia Nowak et Kevin Heydon, délégués de l'ANSSI, ont offert un aperçu de la cybermenace et des principales implications de la directive NIS2.

L'ANSSI, placée sous l'autorité du Premier ministre, est l'organisme de référence en matière de cybersécurité et de cyberdéfense en France. Elle identifie et analyse les menaces cyber, partage des informations pour sensibiliser et protéger contre ces menaces, et soutient les victimes d'attaques. L'ANSSI offre également des ressources aux collectivités territoriales, comme des formations et des outils.

Interview de Célia Nowak et Kevin Heydon

Pouvez-vous nous faire un état des lieux des cyberattaques dans les collectivités ?

L'appât du gain et la recherche de déstabilisation sont les principales motivations des attaquants qui peuvent frapper les collectivités (par ailleurs, l'espionnage est aussi une menace croissante au niveau national).
Ce qu'il faut garder à l'esprit, c'est que les **attaques opportunistes** sont bien plus nombreuses que les attaques ciblées : toutes les collectivités et tous les établissements publics peuvent être frappés à l'occasion d'un envoi massif et indifférencié de courriels malveillants, quelle que soit leur taille ou leur localisation. Pour s'en prémunir, il faut éviter d'être le « fruit facile à cueillir ». Un certain niveau de sécurité de base, d'**hygiène informatique**, permet de ralentir suffisamment les attaquants opportunistes, pour qu'ils décident d'aller chercher une victime plus facile à pirater.



De janvier 2022 à juin 2023, l'ANSSI a traité 187 incidents cyber affectant les collectivités territoriales, soit une moyenne de 10 incidents par mois.

Jeux olympiques 2024. Quels sont les principaux défis auxquels les collectivités territoriales sont confrontées en matière de cybersécurité ?

Pour toutes les collectivités, hôtes ou non, le contexte des JOP2024 et aussi la situation internationale entraînent un **accroissement probable du volume d'attaques cyber** sur cette période. Ne serait-ce que par les faux courriels qui promettront des places gratuites ou toute autre tentation pour inciter au clic sur la pièce jointe ou le lien vérolés.

Dans ce contexte, l'**hygiène informatique** et la **sensibilisation des agents** demeurent les deux piliers de base. Il faudrait aussi ajouter la capacité à réagir en cas d'attaque (réflexions autour du PCS, contacts d'urgence, exercices de gestion de crise comme ceux déjà prêts à l'emploi fournis par l'ANSSI).

Comment l'ANSSI collabore-t-elle avec les différentes administrations locales, notamment le SICTIAM, pour renforcer la résilience face aux cyberattaques ?

Les Opérateurs Publics de Services Numériques, ainsi que des collectivités et intercommunalités déjà avancées dans leur propre action cyber, peuvent clairement aider à **mutualiser les compétences et les moyens** dans un contexte où la ressource humaine se fait rare en cyber… et où il y a forcément un coût d'entrée à se protéger ne serait-ce qu'au niveau minimum (pour justement faire face aux attaques opportunistes).

À titre d'illustration, nous testons avec plusieurs acteurs de la région (dont le SICTIAM et le centre de réponse à incident (CSIRT) régional, Urgence cyber Région Sud) le nouveau service **Mon Aide Cyber**, mis à disposition par l'ANSSI pour que des « Aidants » puissent réaliser un diagnostic cyber de moins de 2 heures, et recommander **6 actions à réaliser dans les 6 prochains mois.** Ce sont des actions concrètes, de priorité maximale et à fort impact en matière de sécurité.

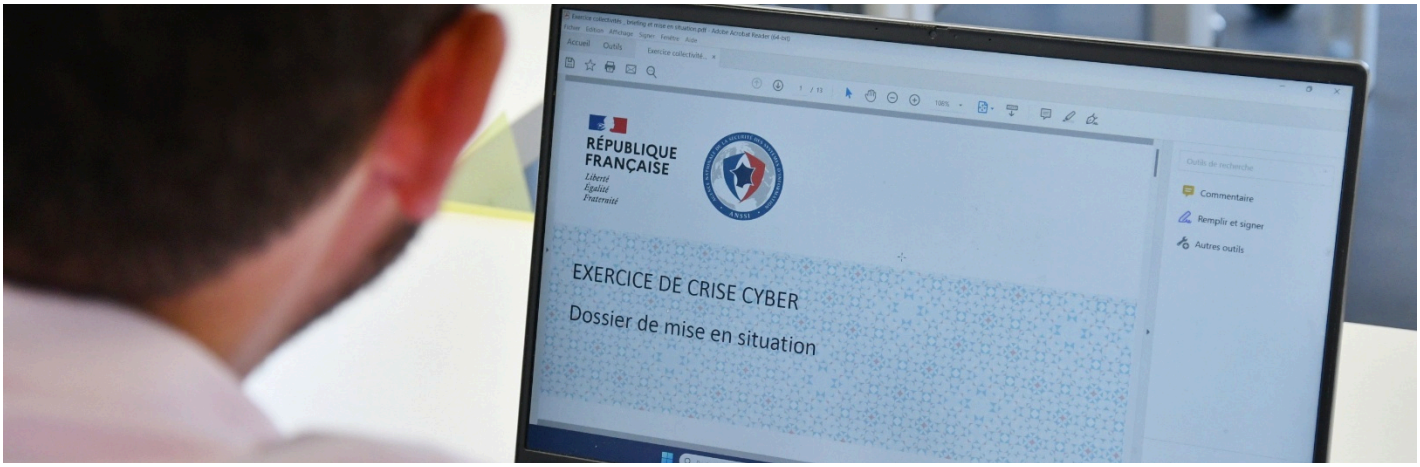
Plus largement, l'ANSSI propose aux entités publiques de la veille, des portails et des outils automatisés de haute valeur pour sécuriser leurs projets, évaluer la sécurité de leur infrastructure critique et mesurer leur exposition sur Internet. Le plus simple est de **nous contacter à paca@ssi.gouv.fr** pour en bénéficier gratuitement.

Quels sont les principaux enseignements tirés des incidents de cybersécurité survenus dans les collectivités territoriales ?

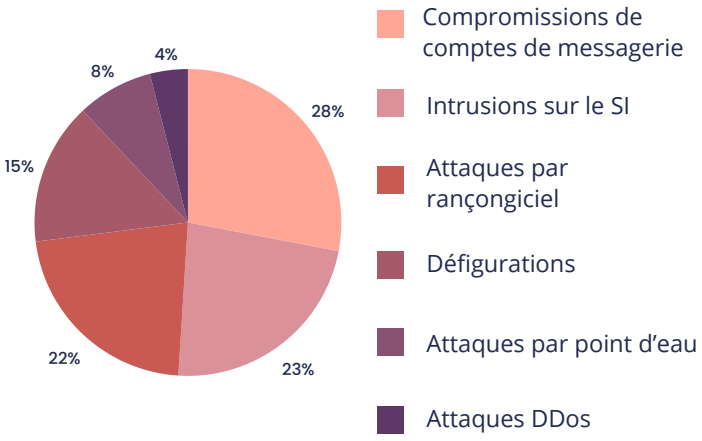
Sur un plan très concret, déjà disposer de **sauvegardes régulières, stockées hors ligne**, et dont la restauration a été testée, au moins pour ses données les plus critiques. Toutes les victimes à qui ces sauvegardes hors ligne manquaient, ou chez qui la restauration n'a pas fonctionné, ont vu l'impact financier et opérationnel de l'attaque exploser.

Ensuite, il faut garder à l'esprit que les impacts de la crise ne seront pas informatiques, même si la source est cyber. C'est donc bien toute l'**organisation de gestion de crise de la collectivité** qui doit se mobiliser… et se préparer en amont (nous travaillons d'ailleurs avec plusieurs interlocuteurs de la région à une proposition de fiche réflexe type, qui pourrait enrichir un PCS). Prévoir **qui contacter en cas d'urgence** est déjà un pas important.

Célia Nowak, déléguée de l'ANSSI



Incidents par catégorie d'attaques



Comment percevez-vous le constat selon lequel de nombreuses collectivités ne parviennent pas à assurer une protection adéquate en raison de contraintes budgétaires ? Quelles aides sont disponibles pour renforcer leur sécurité ?

Si la cybersécurité nécessite des efforts parfois difficiles à valoriser auprès des administrés, **le coût et la visibilité** d'une attaque sont toujours (beaucoup) plus élevés. Les ordres de grandeur partagés par des collectivités victimes, y compris de taille modeste, le démontrent à chaque fois.

Dans le cadre de France Relance, l'État a permis à plus de soixante collectivités et établissements publics de la région de mettre le pied à l'étrier, ou de progresser, sur leur sécurité numérique, avec un appui méthodologique et financier direct. Plus largement, plusieurs opérateurs publics de services numériques (dont le SICTIAM) ont bénéficié du financement de **« licences mutualisées »** pour permettre aux entités les plus modestes d'accéder à des services et produits de sécurité à des prix bien plus abordables.

Avec **France 2030** enfin, l'ANSSI a lancé un appel à projets pour soutenir notamment des projets de renforcement de la sécurité numérique portés par des collectivités territoriales et des opérateurs publics de services numériques. En particulier, les projets dits **« mutualisants »** ou d'**initiative locale** pour impacter un pan collectif du territoire seront regardés avec beaucoup d'attention !

Le Département des Alpes-Maritimes met en place des subventions pour soutenir la mise en œuvre de solutions techniques de cybersécurité visant à réduire les risques de cyberattaques, telles que les solutions antivirus, les pare-feu et les systèmes de réplication (Guide des Aides – Fiche 15).

Comment convaincre les décideurs publics d'investir dans la protection des systèmes d'information de leur collectivité ou établissement public ?

Beaucoup l'ont déjà décidé ! Nous observons, notamment dans la région, de nombreuses collectivités qui ont sauté le pas, que ce soit d'initiative, suite à France Relance, à cause d'une attaque ou grâce au témoignage d'un pair.

La clé est de **prendre conscience du risque financier**, opérationnel, humain et réputationnel que fait courir une sécurité numérique absente ou trop faible à la collectivité, à ses agents et à ses administrés. Ensuite, il s'agit d'une **gestion des risques et de la prise de décisions associées**, que nombre d'élus et cadres territoriaux exercent déjà au quotidien dans de nombreux autres domaines.

En cas de cyberattaque, si une collectivité n'a pas mis en œuvre les moyens nécessaires, les élus/décideurs publics peuvent-ils avoir une responsabilité pénale ou civile engagée ?

Plusieurs réglementations s'appliquent aux collectivités territoriales et établissements publics en matière de sécurité des données : le référentiel général de sécurité (RGS), le règlement général de protection des données (RGPD), voire la loi de programmation militaire (LPM) ou la première version de la directive Network Information Security (NIS) dans le cas d'activités sensibles. Peut-être demain la seconde version de cette directive (NIS2) également.

Nous commençons aussi à voir en France des victimes se constituer partie civile pour **demander réparation** lorsque leurs données ont été divulguées ou lorsque l'attaque d'un tiers les a impactés.
Ainsi, au-delà des sanctions stricto sensu, on voit que cette notion de **responsabilité des décideurs** est en train d'évoluer dans notre société, sans compter l'impact social, voire politique, plus immatériel mais parfois déjà nettement présent.

À noter d'ailleurs le guide que l'association des maires de France a publié dès 2020 : « Cybersécurité : toutes les communes et intercommunalités sont concernées ».

Exercice crise cyber organisé par Célia Nowak et Kevin Heydon pour les Adhérents du SICTIAM

La directive NIS 2 : qu'est-ce que c'est ?

La directive NIS2 (pour Network and Information Security, seconde version) a été publiée au Journal Officiel de l'Union européenne en décembre 2022. Il est prévu qu'elle soit transposée en droit français d'ici **octobre 2024**.

Plusieurs milliers d'entités publiques et privées sur le territoire seront alors qualifiées « entités essentielles » ou « entités importantes », directement sur la base des critères fixés dans le texte, et se mobiliseront pour **mieux se protéger face à des acteurs malveillants** toujours plus performants et mieux outillés, touchant de plus en plus de victimes trop souvent mal protégées.

Est-ce que NIS 2 va s'appliquer à toutes les collectivités ? Et quand ?

La transposition de la directive européenne fera l'objet d'un vote au Parlement, qui fixera alors la lettre des critères et des exigences que portera NIS2. D'ici là, le plus simple est de se renseigner sur le portail **Mon Espace NIS2** mis en ligne par l'ANSSI. En constante évolution à mesure que les consultations et le projet avancent, il apporte déjà de nombreuses réponses sur le périmètre, les exigences et les modalités d'application, notamment au travers d'une FAQ.

Est-ce que cette réglementation a des impacts uniquement sur les équipes IT ?

La cybersécurité n'est jamais un sujet purement IT, puisqu'elle vise à protéger la confidentialité, l'intégrité et la disponibilité des données et métiers les plus sensibles ou critiques de son entité ! Les réflexions et les travaux impliqueront forcément des cadres et des élus non-informaticiens, ne serait-ce que pour **consacrer l'effort sur les bonnes priorités** et s'organiser au bon niveau.

Quels seront les impacts pour ces collectivités, notamment sur la partie budgétaire ?

L'investissement financier dépendra de la **maturité actuelle** de chaque collectivité en matière de sécurité numérique, comme de sa volonté à avancer seule ou à **mutualiser les talents et moyens** lorsque cela s'avère pertinent. Il sera là aussi à mettre en relation avec le coût évité d'une cyberattaque (en gardant à l'esprit que tout progrès de sécurité numérique réduit la probabilité et l'impact des attaques, sans rendre le risque nul). Par ailleurs, le texte européen prévoit **une proportionnalité des mesures** exigées, au travers de la distinction entre « entités importantes » et « entités essentielles ». Les critères amenant à l'une ou l'autre de ces catégories ont notamment fait l'objet de concertations avec de nombreuses fédérations et associations concernées (y compris dans la sphère territoriale) depuis le début de l'année 2024.

Comment les collectivités vont devoir répercuter ces exigences sur les fournisseurs ?

De la même manière que lors de l'entrée en vigueur du RGPD, l'entité donneuse d'ordre aura probablement à traduire ses enjeux de sécurité, réaffirmés par la directive NIS2, avec ses fournisseurs, historiques ou à venir.

Au-delà des conseils et recommandations que produira l'ANSSI à ce sujet, peut-être sera-t-il intéressant pour chaque collectivité de se rapprocher de celles partageant un contexte analogue, pour échanger expériences, bonnes pratiques et outils déjà développés à ce sujet. Cette **discussion régulière entre pairs** qui partagent le même contexte est d'ailleurs une bonne idée pour tout ce qui concerne la cyber !

Célia Nowak et Kevin Heydon sont disponibles à l'adresse e-mail suivante : paca@ssi.gouv.fr

Déploiement de la Fibre optique

72% des prises construites !

100 communes

80 000 adresses

2 400km de desserte

Lundi 18 mars 2024 - Inauguration du NRO de Saint-Auban par le Président Charles Ange Ginésy, entouré des Maires, des élus locaux et des acteurs de la transformation numérique.

La fermeture du réseau cuivre : c'est pour bientôt !

L'arrêt du réseau cuivre ne concerne pas seulement les particuliers. Les entreprises seront également concernées par cette transition. Il est donc important pour tous de se préparer à ce changement majeur dans le paysage des télécommunications. Il a été annoncé par Orange qu'aucune nouvelle offre sur support cuivre ne serait commercialisée après le 31 janvier 2026 et que tous les services actuellement disponibles sur le réseau cuivre, tels que la téléphonie voix, l'internet, et d'autres services, seront définitivement arrêtés au 31 janvier 2027.

Stela

Module ACTES de STELA !
Nouvelle homologation décrochée

Règlementairement, tout dispositif de télétransmission doit être homologué afin de garantir sa conformité au cahier des charges établi par le Ministère. Cette homologation ayant une durée de validité de 5 ans, l'échéance pour le SICTIAM était prévue pour début 2024.

Le module destiné à la dématérialisation du contrôle de légalité a ainsi fait l'objet d'un audit poussé, réalisé par un organisme agréé par la Direction Générale des Collectivités Locales (DGCL) qui a en dernier ressort procédé à divers tests afin de valider la viabilité du module.

Le SICTIAM a par conséquent eu la satisfaction de recevoir fin février 2024, la nouvelle décision portant homologation du dispositif STELA, valable jusqu'en 2029.

À noter : cette nouvelle date n'a aucune répercussion sur les conventions déjà établies avec l'Etat et mentionnant le dispositif STELA, elle fait en revanche office de nouvelle date de référence pour les futures conventions

SICTIAM, 125 rue des Amandiers, 06410 Biot
04 92 96 92 92 - contact@sictiam.fr - www.sictiam.fr

sictiam