N°7
LE MENSUEL
OCTOBRE 2023

sictiam

NUMÉRO SPÉCIAL CYBERMOI/S

#ChersAdhérents

Au SICTIAM, nous considérons la sécurité des systèmes d'information comme un pilier essentiel de nos missions. C'est pourquoi en ce mois d'octobre, nous invitons toutes les collectivités et les établissements publics à suivre la grande campagne de sensibilisation aux enjeux de la cybersécurité, le Cybermoi/s.

Créé en 2012 par l'Agence de l'Union européenne pour la cybersécurité, ce mois de sensibilisation a été adapté en « Cybermoi/s » en 2022 par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et Cybermalveillance.gouv.fr. Il constitue une opportunité précieuse pour mettre en lumière les engagements du SICTIAM envers la protection numérique de nos Adhérents. Nous sommes là pour vous accompagner, vous conseiller et vous aider à renforcer votre posture de sécurité numérique.

Il est important de rappeler que depuis 2021, les efforts constants de nos équipes dans le domaine de la cybersécurité, illustrés par notre participation au programme « Licences Mutualisées » dans le cadre de France Relance et notre collaboration avec l'ANSSI, démontrent l'engagement du SICTIAM envers l'optimisation opérationnelle et la protection des infrastructures numériques essentielles.
Cependant en tant qu'opérateur public de services numériques et énergétiques, notre rôle va bien au-delà de la simple fourniture de services. Nous sommes résolument déterminés à être le partenaire de confiance de nos territoires en matière de cybersécurité en promouvant les directives de l'ANSSI. C'est la raison pour laquelle le SICTIAM propose aux Adhérents des programmes de sensibilisation visant à renforcer leur résilience face aux menaces numériques.

Je vous invite donc à profiter de cette édition spéciale du Mensuel pour vous cyber-responsabiliser grâce aux conseils de Kevin Heydon et Célia Nowak, Délégués à la sécurité numérique PACA de l'ANSSI, et à découvrir nos services cybersécurité.

Ensemble, nous pouvons renforcer la sécurité de nos collectivités et assurer un avenir numérique prospère.

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

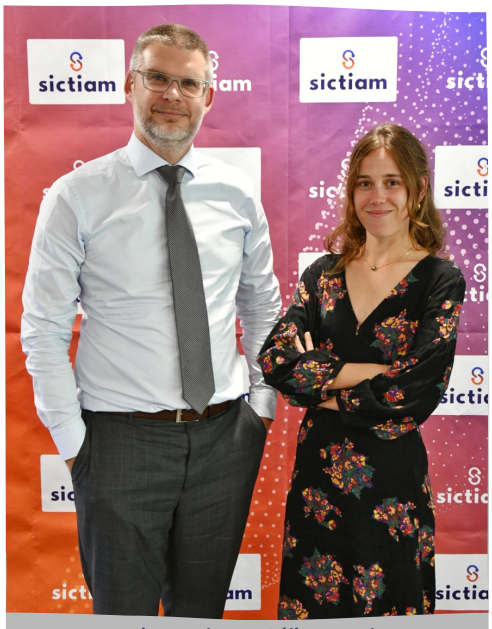
#Interview

L'ANSSI et le SICTIAM, ensemble pour protéger votre sécurité numérique !

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité et de cyberdéfense. En Provence-Alpes-Côte d'Azur, l'ANSSI a déployé deux délégués à la sécurité numérique pour représenter et porter ainsi l'action de l'autorité nationale cyber auprès de toutes les forces vives du territoire. En ce Cybermoi/s c'est un honneur d'avoir pu interviewer Kevin Heydon et Célia Nowak, délégués à la sécurité numérique de l'ANSSI en région PACA.

Quelles sont les relations entre l'ANSSI et le SICTIAM ?

Le SICTIAM bénéficie d'un parcours de cybersécurité au titre du plan France Relance, pour améliorer sa propre sécurité numérique. Le SICTIAM a également été retenu en 2022 pour proposer aux collectivités de la région des produits et services cyber à un prix réduit sur plusieurs années.
Ces deux projets initiés par l'ANSSI ont constitué pour nous l'opportunité de mieux connaître les équipes du SICTIAM, que nous appuyons désormais parfois sur leur action cyber au profit du territoire. Nous avons aussi une forte envie commune d'agir ensemble auprès des acteurs publics de la région. Plusieurs belles idées sont en cours de concrétisation !



Kevin Heydon et Célia Nowak
Délégués à la sécurité numérique de l'ANSSI
en région PACA

Quels sont les avantages pour l'ANSSI de passer par une structure de mutualisation comme le SICTIAM pour diffuser les bonnes pratiques auprès des acteurs publics ?

Les plus grands établissements publics ou collectivités territoriales disposent d'équipes informatiques en interne, et commencent à se doter de compétences cyber. Si le pari pour ces acteurs est important, le défi s'avère aussi complexe pour les entités plus modestes, qui ont du mal à assumer seules le ticket d'entrée d'une sécurité numérique de base. Or cette sécurité de base, cette « hygiène informatique », est pourtant nécessaire à tous les échelons lorsqu'on observe l'état de la menace et les victimes d'attaques cyber de ces dernières années. Dans ce contexte, les structures de mutualisation sont probablement l'un des aspects de la solution, que ce soit dans le partage préalable de bonnes pratiques comme dans la mise en commun et l'optimisation de moyens techniques et de compétences humaines en matière de cybersécurité.

L'actualité nous montre que le secteur public est de plus en plus attaqué (source ANSSI). Quelles sont les types de données recherchées ou à forte valeur pour les attaquants ?

Sur les signalements reçus par l'ANSSI en 2022, en matière d'attaques par « rançongiciels » :

23%
de ces cyberattaques ont frappé des collectivités territoriales ou établissements publics

Les attaques sont souvent opportunistes.
➠ L'entité n'est pas forcément ciblée en tant que telle, mais son faible niveau d'hygiène informatique en a fait une proie facile alors que le pirate ratissait large.
Tout est alors bon à prendre :

- paralysie des services,
- menace de divulgation des données,
- demande de rançon

Et cela peut entraîner des impacts sociaux, économiques ou politiques majeurs pour les élus, les agents et les usagers !

Comment défendre un budget sur la cybersécurité auprès des décideurs dans une collectivité ?

Lorsqu'une attaque – opportuniste ou ciblée – frappe une collectivité, celle-ci ne doit pas gérer une crise cyber ou virtuelle, mais une crise bien réelle dont l'origine est cyber ! Concrètement, la cyberattaque peut bloquer tout ou partie des applications que la collectivité utilise pour fournir des services parfois essentiels à la population : gestion de l'état civil, de la cantine, des déchets, de l'eau, de la sécurité, du cimetière, etc. Ainsi, décider de maîtriser le risque cyber relève bien de la direction de chaque collectivité et de ses élus.

La bonne nouvelle, c'est que l' «hygiène informatique» offre déjà un premier niveau de protection face aux attaques opportunistes, et peut s'avérer raisonnable en matière de coûts de mise en œuvre et de maintenance. En tout cas bien moins coûteuse que les impacts financiers d'une attaque réussie, comme en ont récemment témoigné publiquement plusieurs collectivités de la région !

Quelles actions une collectivité doit-elle mettre en place immédiatement, si ce n'est pas fait, pour se prémunir contre une potentielle cyberattaque ?

Les priorités sont cette fameuse « hygiène informatique » et la sensibilisation des agents (qui seront bien souvent l'ultime rempart une fois correctement formés). À cet effet, le portail www.cybermalveillance.gouv.fr, principalement destiné aux entités dont les systèmes informatiques sont plutôt simples, contient de nombreuses fiches utiles en matière de prévention comme de réaction.

La gendarmerie nationale propose aussi un diagnostic cyber et formule des recommandations prioritaires suite à un bref entretien. Plus largement, les guides de l'ANSSI comme celui relatif aux rançongiciels fournissent des référentiels concrets et applicables. La page ci-dessous en offre une synthèse appréciable : https://www.ssi.gouv.fr/entreprise/precautions-elementaires/dix-regles-de-base/. Par ailleurs, tous les établissements publics et collectivités territoriales peuvent bénéficier de services automatisés mis gratuitement à disposition par l'ANSSI, en contactant les délégués à l'adresse paca@ssi.gouv.fr. Enfin, l'appui d'une structure de mutualisation déjà compétente en cyber peut bien sûr s'avérer précieux !

Le SICTIAM remercie Kevin Heydon et Célia Nowak pour leur précieuse contribution.

CONSIGNES EN CAS DE CYBERATTAQUE

Retrouvez l'ensemble des réflexes en matière de prévention comme de réaction à adopter sur cybermalveillance.gouv.fr

Je déconnecte les équipements informatiques (Wifi, réseau filaire) sans les éteindre et je ne touche plus les appareils

Si je suis Adhérent du SICTIAM j'alerte immédiatement le Syndicat au 04.92.96.92.92, sinon mon support informatique pour contenir, voire réduire les conséquences de la cyberattaque

Je tiens un registre des actions réalisées et je préserve les preuves

Je porte plainte au plus tôt (max. 48h) auprès du commissariat ou de la brigade de mon secteur

Je signale l'incident à l'ANSSI en écrivant à cert-fr@ssi.gouv.fr

Je notifie l'incident à la CNIL dans les 72h si des données personnelles ont pu être consultées, modifiées ou détruites par les cybercriminels

#OffreCybersécurité

Des solutions cyber adaptées aux territoires

Nous devons prendre les mesures nécessaires pour protéger vos données et la continuité de vos services. Pour vous accompagner, le SICTIAM vous propose plusieurs offres cybersécurité :

SENSIBILISATION

Les attaquants utilisent diverses méthodes pour compromettre les systèmes informatiques et voler des informations sensibles. En connaissant ces techniques, les agents sensibilisés peuvent apprendre à les repérer et à s'en protéger, renforçant ainsi la sécurité de l'ensemble de l'écosystème numérique de l'infrastructure.

Le SICTIAM propose des sessions de sensibilisation ciblées ou collectives.

AUDIT ET PLAN D'ACTION

Le SICTIAM a développé une solution complète et personnalisée pour renforcer la sécurité des systèmes d'information des territoires.

Inclus :

- Recensement des principaux risques de cyberattaques auxquels la collectivité peut faire face en déterminant pour chacun le niveau de criticité
- Audit du niveau de sécurité actuel pour construire une politique de sécurité pertinente et adaptée à la situation
- Mise en place d'un plan d'action au regard des risques principaux auxquels la structure publique doit faire face et des mesures de sécurité déjà mises en œuvre (PSSI)

Références : Saint-Martin-du-Var, Villefranche-sur-Mer, Beaulieu-sur-Mer

SIMULATION DE HAMEÇONNAGE

Appelé aussi phishing, le hameçonnage est l'une des méthodes les plus couramment utilisées par les cybercriminels pour infiltrer les réseaux des structures via des courriels piégés et accéder à des informations confidentielles. Le SICTIAM vous propose des tests vous permettant de mesurer la préparation de votre personnel et la résistance de vos systèmes contre de telles menaces.

Inclus :

- Abonnement au logiciel
- 4 campagnes par an
- Elaboration de la campagne
- Programmation de la campagne
- Envoi des résultats et accompagnement de la collectivité

Références : Cap-d'Ail, Vence

PARE-FEU

Dit firewall, ce système de sécurité de réseau informatique limite le trafic Internet entrant, sortant ou à l'intérieur d'un réseau privé et aide à prévenir les activités malveillantes. Le SICTIAM met à votre disposition son expertise pour installer, configurer et maintenir un pare-feu Stormshield conforme aux recommandations de l'ANSSI.

Inclus :

- Récupération de la configuration de l'ancien firewall
- Installation physique sur site et configuration du pare feu
- Sauvegarde des fichiers de log si une ressource de stockage dédiée est disponible
- Limitation de l'accès géographique au système d'information du bénéficiaire
- Filtrage URL
- Ajout du pare-feu dans la console de gestion du SICTIAM (SMC)
- Mise en place du SSO à la demande sous réserve d'un active directory

Business Pôle 2, 1047 Rte des Dolines, 06560 Valbonne
04 92 96 92 92 - contact@sictiam.fr - www.sictiam.fr

sictiam