COLLECTIVITE DE CORSE

RAPPORT
N° 2022/E6/391

ASSEMBLEE DE CORSE

6 EME SESSION EXTRAORDINAIRE DE 2022

REUNION DES 20 ET 21 DÉCEMBRE 2022

RAPPORT DE MONSIEUR
LE PRESIDENT DU CONSEIL EXECUTIF DE CORSE

DEFINIZIONE DI A STATEGIA SICUREZZA DIGITALE DI A CORSICA È ADESIONE A U CAMPUS CYBER NAZIUNALE

DÉFINITION DE LA STRATÉGIE CYBERSÉCURITÉ DE LA CORSE ET ADHÉSION AU CAMPUS CYBER NATIONAL

COMMISSION(S) COMPETENTE(S) : Commission du Développement Economique, du Numérique, de l'Aménagement du Territoire et de l'Environnement

Commission des Finances et de la Fiscalité

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

RAPPORT DU PRESIDENT DU CONSEIL EXECUTIF DE CORSE

En 2022, le nombre de cyberattaques contre les organisations, qu'elles soient publiques ou privées, a connu une hausse sans précédent.

Les sources de menaces se sont très largement étendues, avec notamment une forte augmentation des attaques par ransongiciels (ransomware).

Le contexte économique et géopolitique, favorable à la prolifération de groupes cybercriminels, et plus généralement, l'omniprésence du numérique dans tous les actes de la vie contemporaine, expliquent la hausse spectaculaire de cyberattaques.

La guerre en Ukraine et la cyberguerre qui en découle ont naturellement contribué à cette progression.

Selon les analystes spécialisés, le nombre de cyberattaques continuera d'augmenter en 2023.

Se préparer à faire face à des attaques de nature et de source différentes à mesure que les tensions géopolitiques s'intensifient et que le monde se numérise, devenant ainsi de plus en plus connecté, constitue un impératif de l'agenda politique.

La Corse n'est évidemment pas à l'abri de ces risques majeurs. Au cours des dernières années, elle a en effet connu trois attaques d'ampleur visant des institutions publiques :

- L'Università di Corsica a subi en 2019 une attaque paralysant son système informatique. Le cryptovirus, un rançongiciel de type Dharma, a encrypté l'ensemble des fichiers et notamment des fichiers système.
- L'hôpital de Castellucciu a été victime en mars 2022 d'une attaque par rançongiciel de type « Vice Society ». Son système informatique a également paralysé, impactant directement le traitement des patients en radiothérapie.
- Enfin, l'Office d'équipement hydraulique de la Corse a fait l'objet d'une attaque au début du mois de novembre 2022. Il s'agissait là aussi d'un rançongiciel, de type « Lockbit » cette fois. Cette attaque a fortement perturbé le fonctionnement de l'office pendant quelques jours.

Selon l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI), parmi les actes de cybercriminalité recensés, les rançongiciels représentent aujourd'hui la menace la plus sérieuse. Ils augmentent en nombre, en fréquence, en sophistication et peuvent être lourds de conséquences sur la continuité d'activité voire la survie de l'entité qui en est victime[1].

1 Un guide « Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d'incident ? »

Définition rançongiciel :
Les rançongiciels ou ransomwares sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. La machine peut être infectée après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou encore suite à une intrusion sur le système. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.
Le but principal recherché étant d'extorquer de l'argent à la victime en échange de la promesse (pas toujours tenue) de retrouver l'accès aux données corrompues.
Source Cybermalveillance.

Prise en compte des enjeux de la Cybersécurité en Corse

En l'espace de quelques années, le numérique est devenu, en Corse comme ailleurs, un moteur essentiel de transformation économique, sociale et culturelle des organisations humaines et des sociétés. A ce titre, il constitue un des leviers stratégiques du projet d'autonomie porté par le Conseil exécutif et la majorité territoriale.

La capacité du numérique à structurer et accompagner l'ambition d'une Corse plus dynamique et innovante, plus solidaire et plus démocratique, dépend de multiples facteurs. Elle exige également de répondre aux enjeux et défis de la sécurité de nos réseaux de télécommunication et de nos systèmes informatiques, de la protection de nos données d'intérêt général ou de nos entreprises mais aussi de nos données personnelles.

Lors de l'élaboration du son Schéma Directeur Territorial d'Aménagement Numérique de la Corse - Smart Isula, la Collectivité de Corse a clairement identifié ces enjeux de protection et de sécurisation comme prioritaires.

Elle avait toutefois anticipé cette orientation stratégique en engageant dès 2021 une première action, à travers sa candidature au dispositif du plan France Relance numérique relatif à la création d'un centre d'urgence Cyber territorial, dénommé CSIRT territorial[2].

La candidature a été retenue et la Corse est devenue la première Collectivité à signer avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) l'acte fondateur permettant la mise en œuvre opérationnelle d'un CSIRT en Corse[3].

Le CSIRT de Corse est en cours de constitution. Il sera opérationnel d'ici avril 2023 et aura vocation à soutenir les institutions publiques et privées face aux attaques dont elles pourraient être victimes.

---

a été publié par l'ANSSI, en partenariat avec la Direction des Affaires criminelles et des grâces (DACG) du ministère de la Justice. Il est téléchargeable à l'adresse https://www.ssi.gouv.fr/guide/attaques-parrancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/

2 Délibération n° 21/083 AC du 30 avril 2021.

3 Dans le cadre de cette convention une subvention de 1 M€ a été versée à la Collectivité de Corse afin d'assurer le financement de la structure pendant ses 3 premières années de fonctionnement (délibération n° 21/154 CP du 28 juillet 2021).

Dans le même temps, les travaux menés au titre du Schéma Directeur Territorial d'aménagement numérique de la Corse - Smart Isula et présentés en juin 2022 à l'Assemblée de Corse ont permis de définir 4 pistes d'actions consacrées à la Cybersécurité :

- Élaborer la feuille de route de la politique cybersécurité de la Corse (Action 119),
- Encourager l'émergence d'un « CyberCampus » en Corse (Action 70),
- Soutenir les initiatives dans les secteurs Cyber, IA, datacentre, robotique (Action 88),
- Offrir un soutien opérationnel aux territoires en matière de Cybersécurité (Action 162).

Par ailleurs, la Collectivité de Corse s'attèle depuis de nombreuses années à sécuriser ses propres systèmes et infrastructures informatiques à travers une stratégie de sécurité interne portée par sa Direction du Digital et des Systèmes d'information. Si la Collectivité de Corse n'a pas subi d'attaque, celle dont a été victime l'OEHC a immédiatement donné lieu à une réaction concertée. Les équipes ont été mobilisées pour mettre en place les mesures appropriées de protection et définir une démarche de sécurité réactive, globale et structurée autour d'une vision d'ensemble intégrant la Collectivité de Corse, ses agences et offices.

Le présent rapport a donc pour objectif la mise en œuvre de deux des actions du SDTAN Smart Isula évoqué ci-dessus. Elles concernent l'élaboration d'une stratégie cybersécurité pour la Corse (Action 119) et l'émergence d'un « CyberCampus » en Corse (Action 70).

Ces actions visent à renforcer l'implication de la Collectivité de Corse dans la mise en œuvre d'une stratégie territoriale de cybersécurité et la création d'un écosystème d'acteurs susceptible de partager les méthodes, techniques, outils et les savoir-faire de la cybersécurité au profit de l'ensemble de la société insulaire.

La mise en œuvre de ces deux initiatives structurantes du SDTAN de Corse en matière de cybersécurité se déclinerait comme suit :

- La première consiste à élaborer la stratégie cybersécurité de la Corse. Il s'agit d'engager une démarche d'intelligence collective autour du partage et de la diffusion des enjeux cybersécurité en Corse pour définir les actions à entreprendre, les moyens à mobiliser et le cadre de gouvernance d'une politique de cybersécurité en Corse (ceci en associant des acteurs comme l'ANSSI ou le Campus Cyber National). Cette stratégie étudiera notamment les conditions d'émergence d'une structure dédiée à la Cybersécurité en Corse (CyberCampus). Elle abordera aussi les questions relatives à la souveraineté des données, en résonance avec les enjeux politiques liés à l'autonomie de la Corse.
- La deuxième initiative consiste à adhérer au réseau des acteurs de la cybersécurité incarné par le Campus Cyber national et ainsi de pouvoir exprimer la voix de la Corse auprès de cette instance au regard de la réflexion stratégique qui y sera menée.

Elaboration de la stratégie cybersécurité de la Corse

Forte de son initiative en faveur de la création du CSIRT de Corse et des orientations du SDTAN de Corse - Smart Isula, la Collectivité de Corse souhaite doter la Corse d'une véritable stratégie en matière de cybersécurité[4].

Pour cela, elle proposer d'initier une concertation élargie à l'ensemble des acteurs de la société insulaire qu'ils soient publics ou privés, qu'il s'agisse de prestataires de services ou de cibles potentielles d'attaque, afin d'identifier les besoins, les risques, les objectifs à s'assigner dans le cadre d'une stratégie cybersécurité territoriale.

En effet, en matière de cybersécurité, la synergie entre les différents acteurs est indispensable. Si, en Corse, des initiatives existent, elles doivent s'assembler pour offrir une réponse réactive, collective, à la hauteur des enjeux liés à la souveraineté numérique de notre île.

La définition de cette stratégie nécessite une assistance à la maîtrise d'ouvrage mobilisée aux côtés des équipes de la Collectivité de Corse. Elle permettra de mettre en place les outils d'intelligence collective, d'animation, de restitution et de synthèse des contributions.

Au-delà des aspects stratégiques, le document attendu fournira un volet opérationnel qui comprendra notamment :

1) La cartographie des acteurs cyber agissant en Corse (leur nature, leur localisation, leur retour d'expérience, leur vision/ambition, leur capacité à collaborer),
2) Les conditions d'émergence d'une offre cybersécurité adaptée aux besoins de chaque catégorie d'acteurs (entreprises, institutions publiques, particuliers), les complémentarités des offres territoriales et nationales, les synergies public/privé,
3) Les conditions d'émergence du Cyber Campus territorial, dans ses objectifs, ses champs d'action, ses moyens, sa gouvernance, sa structure juridique. Le transfert de compétences de l'Etat en matière de cybersécurité y sera évoqué dans le cadre du processus d'autonomie de la Corse.

Il est proposé de mobiliser à cet effet la somme de 70 000 € HT (soit 84 000 € TTC).

Adhésion de la Collectivité de Corse au Campus Cyber

Le Campus Cyber national est incarné par une institution (SAS) nommée Campus Cyber.

Campus Cyber « *permet d'accueillir sur un même site (Paris -La Défense) des entreprises (grands groupes, PME), des services de l'État, des organismes de formation, des acteurs de la recherche et des associations. À ce jour, plus de 160 acteurs, issus d'une pluralité de secteurs d'activité, ont confirmé leur engagement. Le Campus Cyber met en place des actions visant à fédérer la communauté de la cybersécurité et à développer des synergies entre ces différents acteurs. Des partenariats entre le Campus national et des Campus territoriaux de cybersécurité seront développés dans les prochains mois.*

4 Cette action est identifiée dans le SDTAN de Corse SMART ISULA au titre de l'objectif « La cybersécurité un enjeu central de l'action publique » et de l'action 119 « Elaborer la feuille de route de la politique cybersécurité de la Corse ».

Ce rassemblement d'expertises stimule de nouvelles formes de coopération entre les entités présentes, dans le domaine de l'identification de la menace, la réponse à des incidents, l'élaboration de cursus de formations et toute autre forme d'innovation technologique. »[5]

Le Campus Cyber active 4 leviers :

1- Un lieu vivant et ouvert dédié à la programmation d'événements innovants propices aux échanges et à la découverte des évolutions de la société numérique de confiance.
2- Le rassemblement d'experts de l'analyse cyber afin de renforcer les capacités de veille, de détection et de réponse à la menace. Ceci inclut la création d'un observatoire de la cybermenace et d'une base commune composée des indices de compromission assemblés par les différents partenaires publics et privés.
3- Un support à la formation initiale et continue des différents publics (agents publics, salarié(e)s, étudiante(s), personnels en reconversion…) pour une montée en compétence globale de l'écosystème. Des programmes communs d'entraînement et de formation dispensés par des écoles ou des centres de formation. Le partage de ressources matérielles et académiques. La sensibilisation et création de nouvelles vocations.
4- L'innovation par le développement des synergies entre les acteurs publics et privés pour orienter l'innovation technologique et renforcer son intégration dans le tissu économique.

Afin d'assurer ses missions, le Campus Cyber propose aux régions et collectivités de participer à ses travaux au titre de « Membre Non Associé », prévu par les articles 5 et 6 des statuts de la SAS Campus Cyber (cf. statuts en annexe 1 du présent rapport).

Pour cela le « Membre Non Associé » devra s'acquitter d'une cotisation unique de 10 000 € (dix mille euros) HT valable pour une durée de neuf ans.

Cette adhésion en qualité de « Membre Non Associé » permettra à la Collectivité de Corse de :

- Participer à la gouvernance du Campus Cyber en étant électeur et éligible au sein du Collège des « Campus Territoriaux » ;
- Participer aux travaux de l'institution autour de l'élaboration des « Communs » et de bénéficier de ces derniers. Les « Communs » désignent les ressources et projets communs (données, produits, services, etc.) mutualisés, ouverts, élaborés, construits par et/ou mis à disposition des associés du Campus Cyber ;
- Faire appel aux infrastructures du Campus Cyber (auditorium, salle de conférence, espaces de démonstration, salles de réunion, etc.) aux conditions privilégiées réservées aux membres du Campus Cyber.
- Faire valoir le point de vue de la Corse au sein de l'institution.

5 Source site officiel du Campus Cyber https://campuscyber.fr/

Cette adhésion est formalisée autour du protocole d'accord « Membre Non Associé » du Campus Cyber figurant en **Annexe 2** du présent rapport.

En adhérant ainsi au Campus Cyber, la Collectivité de Corse se donne les moyens de rejoindre un réseau d'acteurs au fort potentiel mais également de faire valoir ses spécificités au sein d'une communauté plurielle aux compétences de haut niveau.

Il est ainsi proposé à l'Assemblée de Corse :

- D'approuver le présent rapport et ses annexes,
- D'autoriser le Président du Conseil exécutif de Corse à signer et honorer le Protocole d'accord « Membre Non Associé » du Campus Cyber,
- D'engager un montant de 84 000 € sur le programme 1212 opération 1212N011 au titre de l'accompagnement pour l'élaboration de stratégie Cybersécurité de la Corse.
- D'engager un montant de 10 000 € sur le programme 1212 opération 1212N002 au titre du Protocole d'accord « Membre Non Associé » du Campus Cyber,

Je vous prie de bien vouloir en délibérer.