Novembre 2021

CÉSECÉM

LE CONSEIL ÉCONOMIQUE, SOCIAL, ENVIRONNEMENTAL, DE LA CULTURE ET DE L'ÉDUCATION DE MARTINIQUE

CYBERSÉCURITÉ : UN ENJEU INCONTOURNABLE

Télécharger le document

SOMMAIRE

UN NOMBRE DE CYBER ATTAQUES EN AUGMENTATION

Les cybers attaques visent à :

- **accéder à des informations sensibles,**
- **modifier ou détruire des informations sensibles**
- **extorquer de l'argent aux utilisateurs**
- **interrompre les processus normaux de l'entreprise**

Chiffres-clés

- Hausse de **220 %** des incidents de phishing au plus fort de la pandémie par rapport à la moyenne annuelle (Source : F5 Labs).
- **32 %** des utilisateurs interrogés affirment avoir été la cible de fraude liée à la crise sanitaire (Source : Bitdefender)
- D'ici la fin 2021, **50 %** des salariés continueront à travailler à domicile pendant une partie du temps ou de manière permanente (Source : Versa)
- F5 Labs a analysé 14 millions de connexions mensuelles dans une organisation de services financiers et a enregistré un taux de fraude manuelle de **0,4 %**. Cela équivaut à 56 000 tentatives de connexion frauduleuses

Cyber attaques récentes

Ville de Marseille/Métropole de Marseille (92 communes) - Nuit du 13 au 14 mars 2020

Attaque informatique généralisée la veille du premier tour des élections municipales et un mois plus tard, les collectivités demeuraient encore largement affectées pendant la période de confinement où le télétravail était de rigueur.

« Nos serveurs ont été cryptés à hauteur de 90 % contre une demande de rançon », a indiqué la Métropole qui, vendredi 10 avril 2020, tablait sur un retour à la normale autour du 20 mai, expliquant devoir « reconstruire un système complet ».

Source : www.weka.fr

Groupe France Télévisions - Vendredi 26 juin 2020

Cyber attaque visant l'un de ses sites de diffusion qui n'a toutefois pas eu d'impact sur ses antennes. Le groupe a précisé dans un bref communiqué que « l'un de ses sites de diffusion a été infecté par un virus informatique ».

Sources :

- www.20minutes.fr
- France Télévisions victime d'une cyber attaque (20minutes.fr)

Mardi 02 février 2021

Près de 3,2 milliards de combinaisons d'identifiants et de mots de passe d'utilisateurs de Gmail, Hotmail, LinkedIn ou encore Netclic ont été diffusées sur un forum de hackers.

Source : www.maddyness.com

Logiciel CENTREON - Lundi 15 février 2021

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a alerté sur la découverte d'une intrusion informatique « touchant plusieurs entités françaises » via le logiciel français Centreon, qui compte parmi ses clients de grandes entreprises ainsi que le ministère de la Justice. « Les premières compromissions identifiées datent de fin 2017 et se sont poursuivies jusqu'en 2020 », écrit l'ANSSI dans un rapport présentant les informations techniques liées à cette campagne d'attaque.

Source : www.lefigaro.fr

Hôpitaux français - Mercredi 17 février 2021

Les hôpitaux français ont subi 27 cyber-attaques majeures en 2020.

La fréquence de ces attaques a augmenté depuis le début de l'année 2021.

Cédric O, secrétaire d'État à la transition numérique, indiqué que 110 hôpitaux français ont été « accompagnés dans des audits de sécurité » grâce au soutien de l'ANSSI, et « 11 d'entre eux sont accompagnés au jour le jour ».

Définition

- Pratique consistant à protéger les systèmes, les réseaux et les programmes contre les attaques numériques.
- Ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour **protéger les personnes et les actifs informatiques matériels et immatériels** (connectés directement ou indirectement à un réseau) des États et des organisations (avec un objectif de disponibilité, intégrité & authenticité, confidentialité, preuve & non-répudiation).
- Multiples niveaux de protection répartis sur les ordinateurs, les réseaux, les programmes ou les données que l'on a l'intention de sécuriser.

Cadre réglementaire

Union européenne

- **Premier traité de coopération internationale sur la cyber sécurité** : Convention de Budapest, 2001 - signé par les 45 États membres du Conseil de l'Europe, même si tous ne l'ont pas ratifié par la suite.
- Centre européen de lutte contre la cybercriminalité, 2013 - Inauguré par l'Union européenne (UE) au sein d'Europol, il vise à faciliter la coopération entre États européens dans la lutte contre le cyber crime.
- « Paquet cyber sécurité », septembre 2017 - Ensemble de mesures : certification de cyber sécurité à l'échelle de l'UE, consolidation de l'Agence permanente de l'UE pour la citoyenneté…

France : prise en compte de la cybercriminalité dans le droit

Loi informatique et libertés (1978)

Réglemente la liberté de ficher les personnes humaines.

Dispositif juridique prévoyant **des peines allant jusqu'à cinq ans d'emprisonnement et 75 000 euros d'amende** pour les attaques informatiques.

La loi prévoit en outre une aggravation des peines dans le cas de cyber attaques visant directement l'État.

Article L.1111-8-2 du code de la santé publique

Institue **l'obligation de signalement des incidents de sécurité des systèmes d'information**.

Décret d'application n°2016-1214 du 12 septembre 2016

Précise que les incidents graves de sécurité des systèmes d'information du secteur santé doivent être signalés sans délai à compter du 1er octobre 2017 pour :

- Les établissements de santé,
- Les hôpitaux des armées,
- Les centres de radiothérapie,
- Les laboratoires de biologie médicale.

Arrêté du 30 octobre 2017

Présente les modalités de signalement et de traitement des incidents graves de sécurité des systèmes d'information.

Les autres facteurs à prendre en compte

Les acteurs

- Les États et leurs forces armées ;
- Les acteurs économiques (de la PME à la multinationale)

www.sage.com

Les coûts

- 1.000 milliards de dollars par an à l'économie mondiale, soit 50% de plus qu'en 2018 - Source : https://www.capital.fr/
- Déploiement d'une enveloppe totale de **1 milliard d'euros dont 720 millions de fonds publics, pour renforcer la filière** et tripler son chiffre d'affaires à 25 milliards d'euros en 2025 au lieu de 7,3 milliards en 2019.
- Des moyens supplémentaires (136 millions d'euros) vont être alloués à l'ANSSI pour réaliser notamment des diagnostics de sécurité auprès des établissements de santé et des collectivités territoriales, en s'appuyant sur des acteurs locaux de confiance.
- Financements, issus du plan de relance et du « programme d'investissement d'avenir »

Sources :

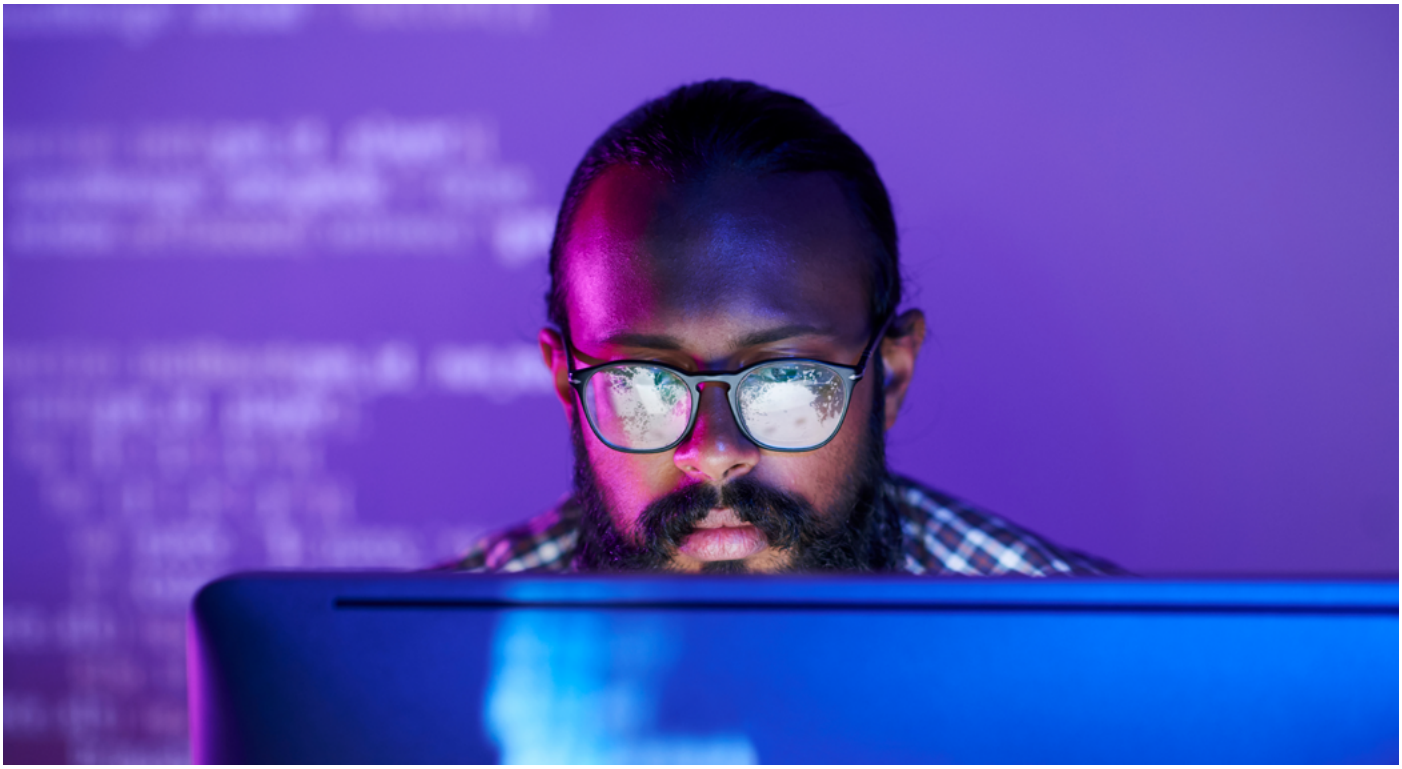
www.20minutes.fr

www.capital.fr

> **Les dirigeants d'entreprises sont responsables de l'intégrité et de la confidentialité des données. En tant qu'employeur, il s'agit également de protéger les salariés en ce qui concerne leurs informations personnelles.**

Les entreprises peuvent internaliser les compétences dans le domaine de la cyber sécurité grâce à une Direction des Systèmes d'Information (DSI).

- www.france24.com
- www.courrierdesmaires.fr



STRATÉGIE DE DÉVELOPPMENT DE LA CYBERSÉCURITÉ

2009 - Création de L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

- Surveiller les réseaux afin de détecter les attaques et permettre de réagir au plus vite ;
- Développer des produits et services de cyber sécurité à destination des usagers ;
- Apporter son expertise et son assistance aux administrations et aux entreprises ;
- Sensibiliser le public sur les cyber menaces www.ssi.gouv.fr
- Renforcement des effectifs de l'Anssi : 600 personnes en fin 2021 contre 400 en 2017.

2017 - Lancement d'un dispositif national d'assistance aux victimes d'actes de cyber malveillance

Incubé par l'ANSSI et copiloté avec le ministère de l'Intérieur, la plateforme cybermalveillance.gouv.fr permet de mettre en relation des victimes de cyber attaques - particuliers, entreprises ou collectivités territoriales - et des prestataires de services susceptibles de les aider dans leurs démarches.

www.cybermalveillance.gouv.fr

Septembre 2021 - Lancement du «Campus Cyber»

- Réunir sur 20.000 m2 à La Défense une soixantaine d'acteurs-clés du secteur - grands groupes, start-up, acteurs publics, organismes de formation, acteurs de la recherche et associations.
- Renforcer à la fois les capacités de veille, de détection et de réponse aux menaces partagées, en développant par exemple une base de données commune.

2021 - Création des CERT (Computer Emergency Response Team) régionaux

Structures capables de réagir efficacement en cas d'urgence et d'assister les victimes.

Source : www.lefigaro.fr

LES DIFFICULTÉS POUR AGIR

L'interconnexion croissante des réseaux et les besoins de dématérialisation exposent les systèmes d'information à des incidents de sécurité. Dans le secteur santé, ces systèmes apparaissent comme critiques, que ce soit au regard de leur disponibilité ou vis-à-vis de l'intégrité et la confidentialité des données qu'ils manipulent. La mise en défaut de ces systèmes pourrait impacter fortement l'activité de l'ensemble des acteurs du secteur et la prise en charge des patients.

Aujourd'hui, les pirates informatiques sont de plus en plus expérimentés, leurs capacités sont bien souvent plus puissantes que celles des services informatiques qui peinent à exécuter leurs missions. Face à la recrudescence des menaces et à ce sentiment d'impuissance, les Responsables de la Sécurité des Systèmes d'Information (RSSI) sont de plus en plus inquiets. Selon l'enquête Forbes Insigths, réalisée par Fortinet, ils seraient 84% à penser que les cybers attaques augmenteront dans les prochaines années.

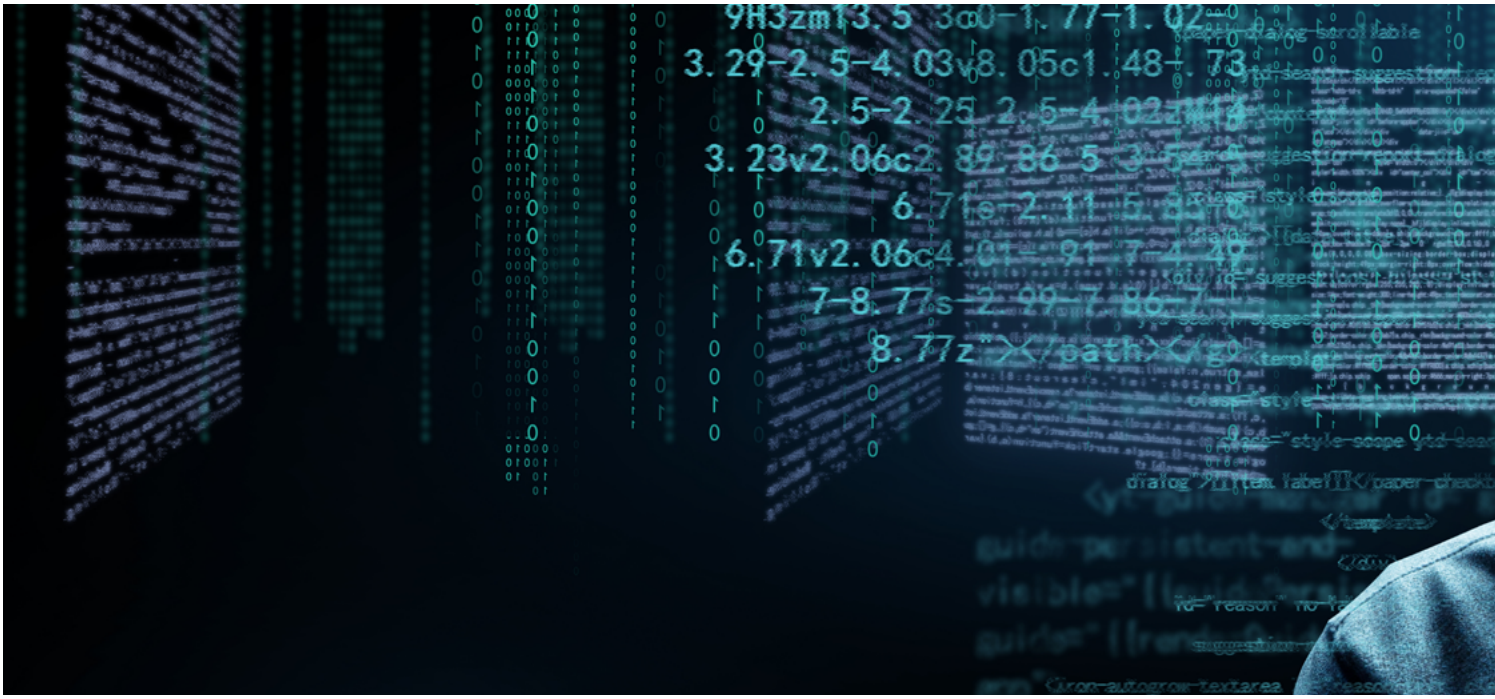
Source : www.upper-link.com

Les hackers ne cessent de développer de nouvelles méthodes pour parvenir à atteindre les données ou pour empêcher une entreprise de fonctionner correctement. Source : www.cmim.fr

La cybercriminalité est un sujet complexe, les cyber-menaces évoluent plus rapidement que toute barrière défensive, car elles capitalisent sur les technologies émergentes (comme le big data, l'intelligence artificielle…) ou profitent du développement du cloud. Sans compter qu'il faut en moyenne au moins 200 jours pour repérer la présence de pirates sur les réseaux et les périphériques.

De plus, l'ampleur et la portée des activités malveillantes perpétrées par le crime organisé, les terroristes, les pirates informatiques, les hacktivistes, les concurrents et les gouvernements sont suffisantes pour que les chefs d'entreprise se sentent désemparés.

Pourtant, les attaques criminelles n'interviennent pas par hasard. La probabilité de subir les conséquences d'une cyber-attaque est déterminée par la manière dont l'entreprise se protège et par les choix qu'elle opère au quotidien. Il incombe donc aux entreprises de ne pas faciliter la tâche des pirates. Les organisations doivent tout d'abord comprendre la nature et la valeur de ce qu'elles protègent, connaître ensuite le type de menaces auxquelles elles sont confrontées et enfin mettre en place une véritable stratégie de protection, qui inclut également les salariés.



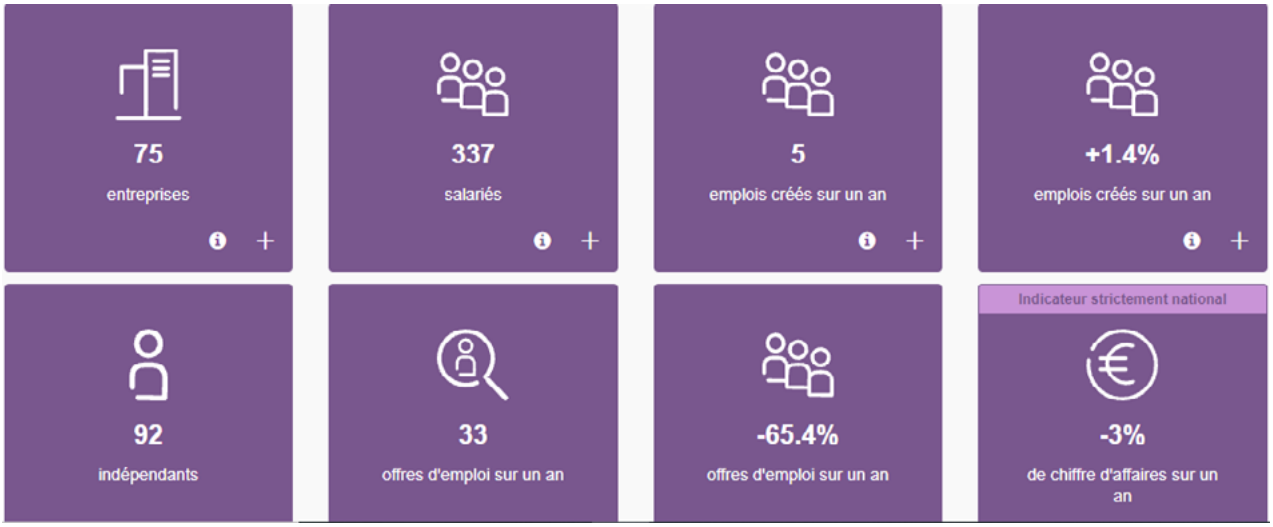
Les principales difficultés

- Pénurie de profils
- Manque certain d'attractivité, notamment auprès des filles
- une pénurie de candidats ;
- des carrières dans la cybersécurité encore peu connues vis-à-vis du grand public ;
- des métiers méconnus et réduits à la dimension technique ;
- un taux de remplissage des formations initiales qui questionne le niveau d'attractivité de la filière ;
- des canaux de recrutement divers ;
- des initiatives remarquables sur lesquelles capitaliser ;
- l'évolution des compétences demandées par les entreprises ;
- une offre de formations en cybersécurité large mais peu lisible ;
- des difficultés de recrutement externes qui conduisent à renforcer les mobilités internes ;
- une sensibilisation encore insuffisante des dirigeants d'entreprises et des DRH.
- Source : étude Source : Observatoire des métiers du numérique, de l'ingénierie, du conseil et de l'évènement (OPIIEC)

Source : numeum.fr | www.hbrfrance.fr

La mise en œuvre de mesures efficaces de cyber sécurité est particulièrement difficile aujourd'hui, car il y a plus d'équipements que de personnes, et les hackers sont de plus en plus innovants.

Chiffres-clés du secteur



Source : Observatoire des métiers du numérique, de l'ingénierie, du conseil et de l'évènement (OPIIEC) www.opiiec.fr

Création de formation

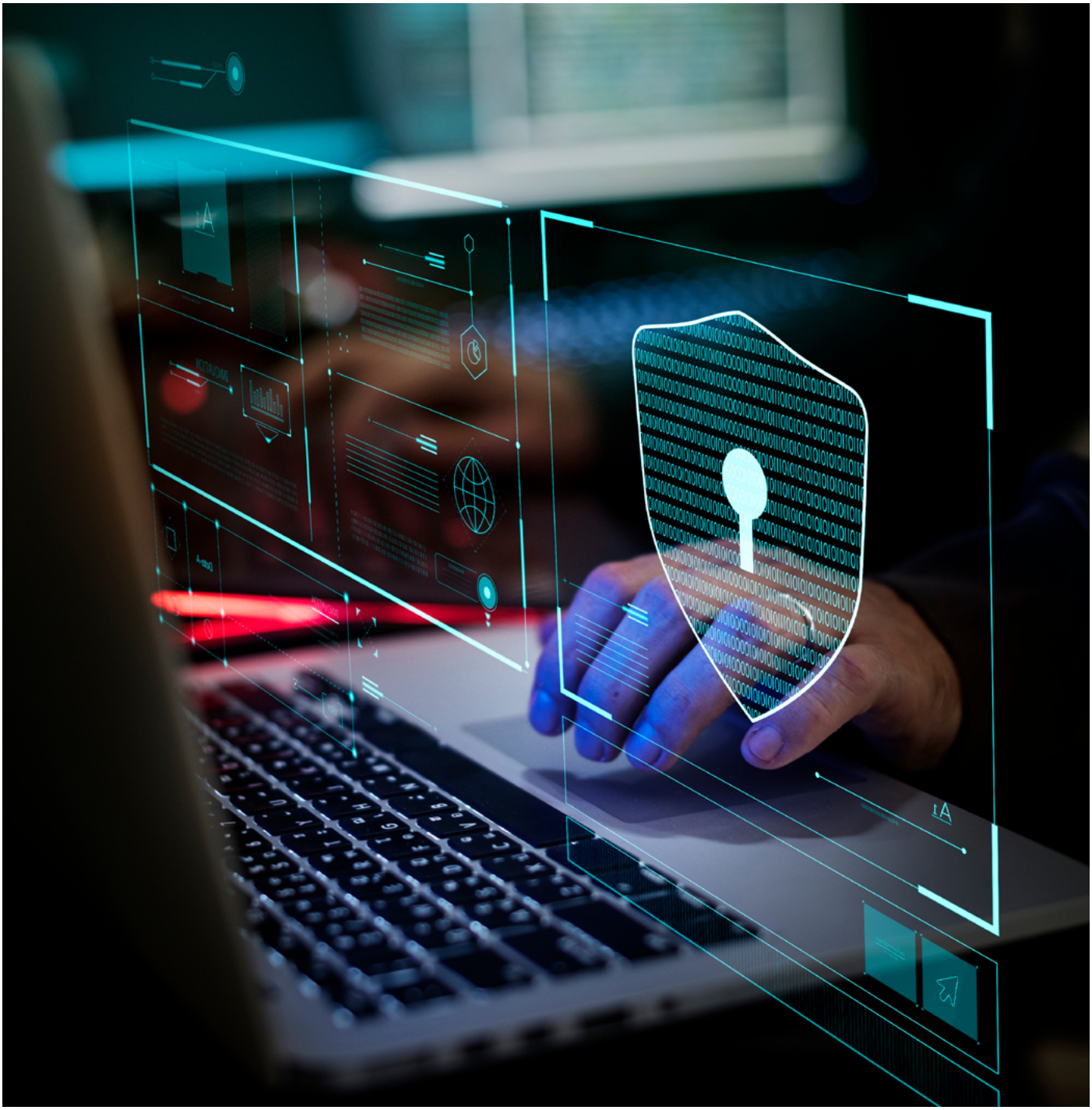
Ainsi Orange Antilles-Guyane confirme sa volonté de travailler sur un projet de formation ouverte à toutes les entreprises sur un modèle déjà mis en œuvre par Orange Campus et le Conservatoire National des Arts et Métiers depuis 2019 (Convention nationale cadre signée en avril 2019 entre Orange, le CNAM), avec pour ambition de développer une expertise locale et créer une filière métiers pour former et qualifier.

Ce projet totalement innovant, lancé dans le cadre du chantier « Rebond économique » de la CCIM, s'ouvre à toute entreprise désireuse de renforcer les compétences en cybersécurité de sa ressource informatique déjà présente et ce, quel que soient sa taille et son secteur d'activité.

Cette formation innovante allie des regroupements en présentiel et du e-learning.

Source : mobile.outremers360.coml

Au regard de la croissance des risques, le constat est clair : il y a un déficit de compétences locales en cybersécurité. Il est donc nécessaire de mettre en place un dispositif permettant d'accompagner la sécurisation de l'information, à travers la formation d'experts en cyber sécurité aux Antilles-Guyane.



CONCLUSION

Dans un contexte où tout le monde s'accorde à dire que le télétravail va devenir la nouvelle norme, le développement du secteur de la sécurité numérique est devenu un enjeu majeur.

CÉSECÉM

LE CONSEIL ÉCONOMIQUE, SOCIAL,
ENVIRONNEMENTAL, DE LA CULTURE
ET DE L'ÉDUCATION DE MARTINIQUE

www.cesecem.mq