CONCOURS SUR ÉPREUVES D'ADMISSION
DANS LE CORPS DES OFFICIERS DE LA
GENDARMERIE NATIONALE

ouvert aux capitaines ou officiers de grade correspondant comptant au plus huit ans d'ancienneté dans ce grade et aux fonctionnaires civils de l'État, des collectivités territoriales, d'un établissement public ou d'un organisme international comptant au moins cinq ans de service dans un corps de catégorie A ou assimilé et âgés de trente-cinq ans au plus.

- OG OA -

SESSION 2023

ÉPREUVE DE SYNTHÈSE DE DOSSIER

(Durée : 04 heures – Coefficient : 05 - Note éliminatoire < 5/20)

La note de synthèse est construite selon un plan classique : introduction, développement, conclusion. Elle est entièrement rédigée. Seules les grandes parties peuvent éventuellement être précédées d'un titre. Elle doit être objective, dénuée d'appréciation personnelle.
Le candidat doit rédiger en 600 mots (tolérance + 10%) une note de synthèse claire, précise et concise.

Le non-respect du nombre de mots imposé pour la rédaction entraîne l'attribution d'une pénalité fixée dans le tableau ci-dessous :

NOMBRE DE MOTS ÉCRITS PAR LE CANDIDAT	PÉNALITÉ CORRESPONDANTE
Rédaction de 661 à 670 mots	Moins 1 point
Rédaction de 671 à 680 mots	Moins 2 points
Rédaction de 681 à 690 mots	Moins 3 points
Rédaction de 691 à 700 mots	Moins 4 points
Rédaction de plus de 700 mots	Moins 10 points

Où en est-on de notre cybersécurité ?

14	211022 – JDD - Jeux olympiques : comment Paris 2024 se prépare à la menace des cyberattaques	2	28
15	171022 – 01.net - Meta admet que son métavers est un « monde vide » et « triste »	2	30
16	191022 – 01.net - Piratage : combien coûte un compte TikTok, LinkedIn ou Facebook sur le Dark Web ?	3	32
17	231022 – Numerama - Il faut vraiment que vous arrêtiez d'aller sur les réseaux sociaux avec votre ordi pro	2	35
18	231022 – Ouest France - TÉMOIGNAGE. « Tout est parti d'un SMS » Kelly, victime d'une arnaque téléphonique qui explose	3	37
	TOTAL	39	

Pièce 1

Cyberharcèlement/jeux vidéo: le gouvernement veut "faire cesser cette haine en ligne inacceptable"

jeux | technologies | informatique | harcèlement | agression | sexisme

Paris, France | AFP | 01/11/2022 20:36 UTC+1

Le gouvernement va organiser "dans les prochains jours" une réunion entre les victimes de cyberharcèlement, responsables de l'industrie du jeu vidéo, plateformes de streaming et principaux réseaux sociaux, pour "faire cesser cette haine en ligne inacceptable", a annoncé mardi le ministre du numérique.
Avec la ministre déléguée à l'Égalité Femmes-Hommes Isabelle Rome, "je souhaite que nous réunissions tous les acteurs concernés (...) dans les prochains jours" pour identifier "quelles peuvent être les bonnes solutions (afin de) faire cesser cette haine en ligne inacceptable", a annoncé Jean-Noël Barrot, ministre délégué à la transition numérique, en ouverture de la Paris Games Week, le principal salon français du secteur.
Une multitude de témoignages glaçants ont secoué ces derniers jours le monde des streamers français, ces joueurs ou joueuses de jeux vidéo qui partagent et commentent leurs parties en direct. Plusieurs figures féminines ont dénoncé, preuves à l'appui, les cyberviolences sexistes et sexuelles qu'elles subissent depuis des années sur les réseaux.
Sur YouTube comme sur Twitch et les autres plateformes, ce sujet n'est pas nouveau et beaucoup trop récurrent, ont déploré les streameuses alors que la vague "MeToo" a déjà cinq ans d'existence. Début 2021, un pôle spécialisé pour lutter contre la haine en ligne a été créé au sein du parquet de Paris tandis que le grand public peut signaler les comportements et contenus illicites sur la plateforme Pharos depuis 2009.
Présents essentiellement sur Twitch, propriété du géant Amazon, les principaux streamers francophones sont des figures masculines comme Squeezie et ZeratoR, dont les chaînes ont connu des pics d'audience respectifs d'un million et 700.000 spectateurs.
Signataire en juin du code de conduite de l'Union européenne contre la haine en ligne, Twitch avait annoncé en décembre 2021 la mise en place d'un système pour détecter les utilisateurs malveillants, après une vague de harcèlement raciste et homophobe.
Le code de conduite de l'UE contre la haine en ligne, lancé en 2016, compte une dizaine de signataires, dont Facebook, Microsoft, Twitter, YouTube, Instagram, Snapchat, Dailymotion, Jeuxvideo.com, TikTok, et LinkedIn, ou encore l'application de messagerie Viber.

Pièce 2

Opinion | L'IA, un atout pour la sécurité des JO 2024

Les Échos, par William Eldin (fondateur de XXII)
Publié le 1 juin 2022 à 19:01Mis à jour le 2 juin 2022 à 09:05

Avec une coupe du monde de rugby dans un an et des Jeux olympiques et paralympiques l'année suivante, notre pays est pleinement mobilisé pour faire de ces rendez-vous sportifs mondiaux une vitrine du savoir-faire et un outil de rayonnement de la France. Cependant, les récents événements de la finale de la Ligue des Champions de football nous forcent à l'humilité et confirment la nécessité d'accroître les efforts d'anticipation et de pilotage des enjeux sécuritaires. Le moindre incident ou accident aurait une résonance médiatique et politique proportionnelle à l'engouement suscité. Face à ce défi, l'intelligence artificielle peut être une assistance précieuse aux opérateurs qui assureront la sécurité de ces deux rendez-vous.
Les chiffres sont impressionnants : 48 matches et 450.000 visiteurs étrangers pour la Coupe du Monde de Rugby 2023 en guise de 'répétition grandeur nature' ; les Jeux Olympiques et paralympiques seront quant à eux un événement hors normes avec 15.000 athlètes, 13,5 millions de spectateurs et plus de 25.000 journalistes. Un des défis des autorités, ministère de l'Intérieur en tête, sera l'intégration des nouvelles technologies pour assurer la sécurité des personnes et des infrastructures. Dans ce cadre, l'analyse vidéo en temps réel via l'intelligence artificielle est aujourd'hui opérationnelle et mature. Et des solutions 100 % françaises et souveraines existent déjà.

Limite de nos capacités de vision
La police et la gendarmerie nationales seront en première ligne. A leurs côtés, ce sont plus de 20.000 agents de sécurité privée qui compléteront les ressources humaines pour accueillir, orienter et protéger les spectateurs, sportifs, autorités et journalistes dans de bonnes conditions. Pour réaliser leurs missions de manière optimale, ces opérateurs auront nécessairement besoin d'une assistance technologique, complémentaire permettant de les aider à anticiper et prendre les bonnes décisions. L'intelligence artificielle et la vision par ordinateur peut être ce partenaire technologique. Pourquoi ? Parce que l'humain est aujourd'hui arrivé au maximum de ses capacités de vision : il est impossible pour une équipe - aussi nombreuse soit-elle - d'analyser des dizaines de milliers de vidéos au sein d'un centre de sécurité, qui plus est en gestion de crise quand la prise de décision doit être quasi immédiate : 70 % de l'information perçue par l'humain passe par nos yeux et la charge cognitive associée au traitement de l'information sature naturellement notre capacité à réfléchir et agir.
Les opérateurs ont besoin d'être « augmentés » par la technologie, tout en conservant la décision finale, notamment pour fluidifier les déplacements de véhicules et de personnes et les accès aux sites, identifier des comportements inhabituels, faire respecter les jauges grâce au comptage de personnes dans les files d'attente, ou encore identifier des actes suspects.

Savoir-faire français
Il est toutefois indispensable de clarifier et de légiférer rapidement sur le cadre légal dans lequel les
expérimentations et la mise en oeuvre de l'IA pourront se réaliser lors de la coupe du monde de rugby 2023 et les JO 2024. L'idée n'est aucunement de donner une carte

blanche à une technologie qui prendrait le pas sur l'humain. L'approche doit être pragmatique et éthique.
Sur le terrain de la compétition technologique internationale, la France a une réelle carte à jouer à cette occasion pour faire valoir son avance en matière d'IA et de technologies compatibles avec le respect des libertés publiques et individuelles. Tout comme notre capacité à encadrer la sécurité des événements est scrutée aujourd'hui, notre capacité à incarner un Etat modèle en matière d'IA éthique le sera aussi.
Les deux prochaines années doivent être une vitrine des savoir-faire français en matière de nouvelles technologies. Notre pays bénéficie de fleurons nationaux et de pépites capables de répondre aux enjeux qui se dressent devant nous. Il est désormais de notre responsabilité collective (politiques, industriels,
régulateurs, etc.) d'avancer dans le même sens pour réussir ces Jeux. L'équipe de France ne doit pas
uniquement être sur les terrains le jour J mais dès aujourd'hui dans les coulisses de l'organisation.

William Eldin, CEO et co-fondateur de XXII

Pièce 3

La gendarmerie fait face à la cybercriminalité

lefigaro.fr/secteur/high-tech/
02 septembre 2021
Par Emma Confrere

Un technicien extrait des données d'un smarthone, au centre de lutte contre les criminalités numériques de la gendarmerie nationale, à Pontoise. Florian GARCIA

Devant l'explosion du nombre de cyberattaques en France, 7 000 gendarmes réunissent leurs forces.
«Aujourd'hui, tout porte à croire que la prochaine crise sera cyber. Les élections présidentielles en 2022, la présidence française de l'Union européenne au premier semestre 2022, la Coupe du monde de rugby en 2023 et les JO de Paris en 2024 sont autant de grands événements où il est certain que nous serons soumis à une menace cyber importante», explique le général de division Marc Boget, qui a officiellement pris la tête du ComCyberGend le 1 er août dernier.
Ce commandement de la gendarmerie dans le cyberespace a été créé le 25 février 2021 afin de rassembler les forces cyber de la gendarmerie sous un étendard unique. Basé à Cergy-Pontoise, au pôle judiciaire de la gendarmerie nationale, cet organisme comporte plus de 7 000 cyberenquêteurs répartis dans toute la France, et bientôt 10 000.

Des unités partout en France
Si autant d'effectifs sont mobilisés, c'est notamment à cause de l'explosion du nombre de faits liés à la cybercriminalité. En 2020, ils ont augmenté de 22 % par rapport à l'année précédente, pour un total de plus de 100 000 infractions en France. Les trois quarts sont des escroqueries, pour la plupart sous forme de rançongiciels. Il s'agit d'attaques informatiques perpétrées par des pirates dans le but de récupérer des milliers, voire des millions d'euros. Particuliers, entreprises, institutions et collectivités sont ciblés par ces criminels. Ce sont principalement les des petites et moyennes entreprises qui sont visées, dans 46 % des cas. Les très petites entreprises, qui emploient moins de dix salariés,

représentent ensuite 21 % des attaques de rançongiciels en France.«Très souvent, les employés sont affolés et désemparés face à cette situation. Les services informatiques ne dorment plus, c'est une véritable pagaille», souligne une membre du ComCyberGend.
Afin de lutter contre ces cyberattaques, plusieurs unités sont regroupées au sein du commandement. Au niveau central, c'est le Centre de lutte contre les criminalités numériques (C3N) qui dirige les opérations nationales. Onze antennes sont réparties sur le territoire français jusqu'en outre-mer. Cette entité lutte principalement contre la diffusion de contenus illicites, les ventes illégales et l'apologie du terrorisme sur le web. Concernant la pédopornographie, c'est le Centre d'analyse des images qui s'en charge, lui-même rattaché au C3N. En 2020, un demi-million de contenus ont été découverts par ces équipes.
Lorsque les enquêtes nécessitent de trouver des preuves numériques, le Centre national d'expertise
numérique apporte son savoir-faire. Des militaires, experts de haut niveau travaillent en lien avec le
ComCyberGend. Leur rôle: extraire des données numériques contenues dans des GPS ou des disques durs, par exemple. Les smartphones, ordinateurs, composants et puces électroniques sont également analysés. Un travail minutieux mais qui est en constante évolution. Les ingénieurs et techniciens effectuent des remises à niveau permanentes afin de suivre les avancées technologiques.

Prévenir et accompagner les victimes
Lors des attaques, il faut aussi accompagner les victimes, l'un des fers de lance du ComCyberGend. Plusieurs plateformes sont disponibles, comme Perceval, qui permet de lutter contre la fraude à la carte bancaire sur internet. En 2020, 320 000 signalements ont été enregistrés, soit une hausse de 86 % par rapport à 2019. Au total, les préjudices sont estimés à plus de 136 millions d'euros.
«La prévention est également essentielle, notamment du côté des communes, souvent ciblées par les
pirates», mentionne un cybergendarme. En partenariat avec l'Association des maires de France, plus de 12 000 collectivités territoriales et établissements publics ont été sensibilisés aux cybermenaces en 2020. Avec la pandémie de Covid-19 et l'explosion du vol de données, le ComCyberGend a aussi sensibilisé 452 hôpitaux français et 776 industries de santé.

INTELLIGENCE ONLINE
Au cœur du renseignement

Sur qui s'appuiera le ministère de l'intérieur pour cybersécuriser les Jeux olympiques de Paris ?

05 juillet 2022

Décidé à faire des Jeux olympiques de Paris de 2024 un laboratoire de la sécurité, le ministère de l'intérieur étudie les solutions d'une myriade de jeunes pousses, principalement dans les domaines de l'analyse de données de masse et du renseignement en source ouverte (OSINT).

Les Jeux olympiques (JO) de Paris de 2024 approchant à grands pas, le ministère de l'intérieur accentue ses efforts pour en faire un laboratoire de la sécurité intérieure, avec un double objectif : sécuriser l'événement et prospecter à la recherche de technologies qui pourraient équiper ses services. Plusieurs solutions développées par de jeunes pousses ont ainsi été testées en avril, sous l'égide de la Délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité (DPSIS), en lien avec les services du ministère - Direction générale de la sécurité intérieure (DGSI), Direction générale de la gendarmerie nationale (DGGN), Direction générale de la police nationale (DGPN) -, dont les besoins sont différents.
Le tout, encadré par un programme général de sécurité (PGS), sera orchestré par l'entreprise française d'informatique Atos, déjà à la manœuvre en 2018 pour les JO d'hiver de PyeongChang.

Les spécialistes du big data examinés
Alors que la préoccupation capacitaire de la DGSI demeure la préparation de l'après-Palantir, la DPSIS s'est penchée sur les technologies de plusieurs spécialistes du big data, à l'image de celle du français Temno (IO du 02/05/22). Dirigée par Guilhem Giraud, un ancien de la société française de cyber-renseignement Amesys (devenue Avantix), Temno développe une plateforme immersive en exploitant la technologie du metaverse.
Les solutions de Sahar, dirigé par Erwan Le Gall, ancien du spécialiste français du cyber-renseignement Suneris (IO du 11/05/21), sont également étudiées. L'entreprise, qui s'est développée
grâce à la Cyberdéfense factory - l'incubateur de start-ups piloté par la Direction générale de l'armement (DGA) -, reste particulièrement proche du ministère des armées. L'Agence de l'innovation de défense (AID) l'a d'ailleurs mise en avant, en juin, lors de la grand-messe de la cybersécurité française, le Forum international de la cybersécurité (FIC). Sahar est spécialisé dans l'analyse de données principalement issues des réseaux sociaux.

Le Club de l'OSINT très impliqué
Au travers de ce programme, le ministère a eu l'opportunité d'analyser les systèmes de renseignement en source ouverte (OSINT) proposés par l'écosystème français. D'où, selon nos informations, la forte implication du groupe informel du ministère de l'intérieur dénommé Club de l'OSINT. Ce dernier rassemble les praticiens de l'OSINT de plusieurs services du ministère et vise à mutualiser les tests et la définition des besoins.

Dans ce domaine, la DPSIS s'est intéressée aux technologies du spécialiste de l'investigation sur le dark web Aleph Networks, également convoitées par le renseignement sud-coréen (IO du 27/06/22), ainsi que celles de la jeune pousse Owlint.

Cybersécurité : la gendarmerie, l'AMF et cybermalveillance.gouv.fr lancent un outil d'autodiagnostic destiné aux élus

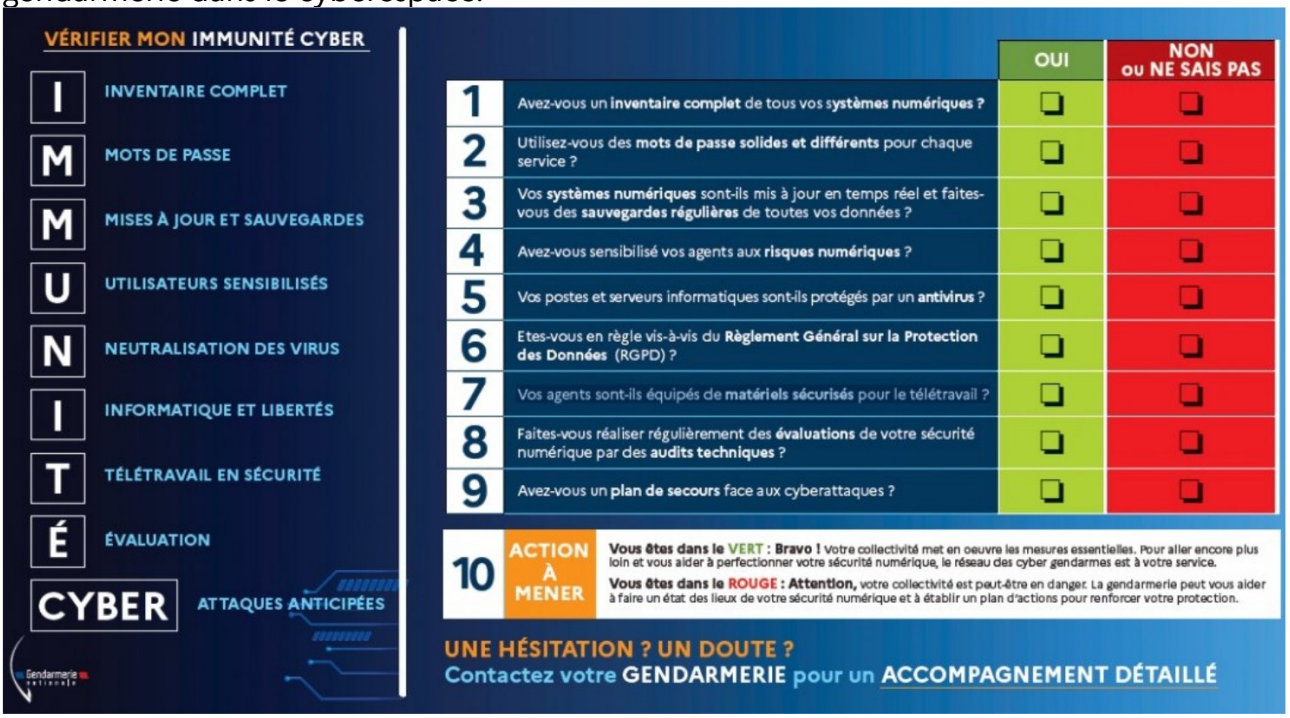
aefinfo.fr

Dépêche n° 657893
3 min de lecture
Par Marie Desrumaux Publiée le 09/09/2021 à 10h13

Le ministère de l'Intérieur, l'Association des maires de France et la plateforme cybermalveillance.gouv.fr lancent un dispositif d'autoévaluation de la sécurité numérique des collectivités. Ils ont adressé un courrier aux édiles, lundi 6 septembre 2021, à la veille du Forum international de la cybersécurité de Lille (1), pour les inciter à utiliser ce nouvel outil. Appelé "Immunité cyber", le dispositif vise à sensibiliser les élus à la cybersécurité et les incite à prendre contact avec la gendarmerie, qui leur fournira des conseils et les orientera, si nécessaire, vers des professionnels.
Développé par la gendarmerie en lien avec l'AMF (Association des maires de France) et la plateforme cybermalveillance.gouv.fr, le dispositif d'autodiagnostic "Immunité cyber" se présente sous la forme d'un questionnaire à neuf entrées. "Avez-vous un inventaire complet de tous vos systèmes numériques ?
Avez-vous sensibilisé vos agents aux risques numériques ? Vos agents sont-ils équipés de matériels sécurisés pour le télétravail ?" À l'issue des questions, un diagnostic est établi avec un classement par couleurs : vert pour les collectivités dont les systèmes sont bien sécurisés et rouge pour celles qui sont peut-être en danger. Dans le second cas, les élus sont invités à contacter une brigade locale de gendarmerie ou la brigade numérique sur magendarmerie.fr.
"Nous leur fournirons les premiers conseils et messages de prévention puis, en fonction de la situation, ils pourront être redirigés vers les spécialistes en technologies numériques départementaux au sein des sections opérationnelles de lutte contre la cybercriminalité qui se chargeront de prendre contact pour établir avec eux un audit de la situation", détaille le général Marc Boget, commandant de la gendarmerie dans le cyberespace, à AEF info (lire sur AEF info). "Là encore, en fonction des résultats, il pourra leur être conseillé de s'adresser à un prestataire privé de leur choix pour les actes de remédiation nécessaires. Cybermalveillance.gouv.fr fournit dans ce cadre, une liste d'intermédiaires reconnus pour leur sérieux qui sera particulièrement utile."

Des collectivités particulièrement touchées
Ce nouveau dispositif, présenté lors du FIC (Forum international de la cybersécurité) , est inspiré d'une autre initiative de la gendarmerie : la formation des maires à la gestion des incivilités (lire sur AEF info). "Cela a si bien fonctionné qu'il a été décidé de faire une déclinaison sur le cyber", indique à AEF info Jérôme Notin, directeur général du GIP Acyma, qui pilote cybermalveillance.gouv.fr. L'objectif est de sensibiliser les élus à l'importance de la sécurité numérique des collectivités, vulnérables aux cyberattaques. "Pour un particulier que nous avons assisté en 2020, nous avons aidé dix entreprises et 40 collectivités territoriales", souligne Jérôme Notin. Angers, la région Grand Est, des communes comme Mitry-Mory (Seine-et-Marne) ou Douai (Nord)
Des collectivités de toutes tailles ont été touchées par des rançongiciels, entraînant parfois une paralysie des services pendant plusieurs jours ou semaines (lire sur AEF info).
Cybermalveillance.gouv.fr fournira le contenu des modules de sensibilisation dispensés aux élus par des gendarmes dans le cadre du dispositif "Immunité cyber". Pour les collectivités qui s'aperçoivent, à cette occasion, qu'elles ont déjà subi des attaques ou des tentatives d'intrusions, il sera possible d'entamer immédiatement les actes d'investigation judiciaire

"grâce aux capacités d'investigation des sections opérationnelles de lutte contre la cybercriminalité des groupements", indique le général Marc Boget. Ces sections pourront d'ailleurs, le cas échéant, "bénéficier de l'appui de la section de recherche et de son groupe cyber de rattachement, voire l'échelon national". "Ce partenariat fort avec l'AMF n'est que le premier et d'autres partenariats sont en préparation avec l'ensemble des associations d'élus ou les régions de France par exemple", souligne le commandant de la gendarmerie dans le cyberespace.



Le dispositif d'autodiagnostic se présente sous la forme d'un court questionnaire.
| Droits réservés - DR
(1) AEF info est partenaire média du FIC

Le "porte-avions" de la cybersécurité française opérationnel début 2022

technologies | informatique | cybersécurité | gouvernement | télécoms | mobiles
Lille, France | AFP | 09/09/2021 13:21 UTC+2

Le campus cyber, une tour de 26.000 mètres carrés à la Défense qui doit devenir le "porte-avions" de la cybersécurité française en réunissant sur un même lieu des spécialistes privés et publics du domaine, commencera à fonctionner début 2022, selon son président.
"On devrait inaugurer le site avec le gouvernement au mois de janvier", a indiqué jeudi au Forum international de la cybersécurité de Lille le président du campus, Michel Vand Den Berghe.
Les premiers des 1.500 à 2.000 occupants prévus du site commenceront à s'installer à ce moment-là, a-t-il précisé.

Le campus cyber réunira des représentants d'entreprises de cybersécurité de toute taille, de la start-up aux géants comme Thales ou Airbus, de services de l'Etat comme la police, la gendarmerie ou les
renseignements, et d'instituts de recherche comme l'Inria mais aussi d'écoles spécialisées.
"On voudrait en faire le porte-avions de la cybersécurité française", capable de "faire émerger des champions français" dans ce domaine stratégique en pleine explosion, a déclaré Michel Van Den Berghe, ancien patron d'Orange Cyberdéfense.

Les acteurs privés de la cybersécurité détiennent environ 55% du capital de la société gérant le site, la participation de l'Etat s'élevant à 45%.
En rassemblant des acteurs très divers sur un même endroit, le campus cyber doit notamment permettre l'accélération de la circulation de l'information entre les professionnels du secteur.
"On voit qu'il y a une course de vitesse" entre la sensibilisation à la menace cyber et le développement de celle-ci, a indiqué de son côté Cédric O, le secrétaire d'État au numérique.
"Nous travaillons sur des projets de campus cyber régionaux, à Lille, Rennes, dans les Pays de la Loire" et dans d'autres régions, a-t-il ajouté.
lby/mdz/spi

L'Anssi dévoile les sept premières régions qui accueilleront un centre d'aide en cas de cyberattaque

aefinfo.fr/depeche/665547
Marie Desrumaux, Publiée le 11/01/2022 à 12h02

L'Anssi dévoile, mardi 11 janvier 2022, le nom des sept premières régions qui accueilleront un centre de réponse à incident cyber. Destinés à accompagner localement les victimes de cyberattaques, ces centres régionaux bénéficieront du soutien financier et méthodologique de l'agence, à travers le plan de relance, pour un lancement dans le courant de l'année. L'objectif est que ces structures, portées par les conseils régionaux, soient pleinement opérationnelles en 2024.
L'Anssi (Agence nationale de la sécurité des systèmes d'information) annonce, mardi 11 janvier 2022, la signature avec sept régions d'une convention pour la création de centres régionaux de réponse aux incidents cyber : Bourgogne-Franche-Comté, Centre-Val de Loire (lire sur AEF info), Corse, Grand-Est, Normandie, Nouvelle-
Aquitaine et Sud-Provence-Alpes-Côte d'Azur. Annoncée par le président de la République en février dernier (lire sur AEF info), la mise en place de ces centres doit permettre aux régions de proposer un service d'assistance et de conseil "de proximité" pour "toutes les entités du territoire touchées par la menace cyber".

Un programme d'incubation de quatre mois
Les Csirt (Computer Security Incident Response Team) régionaux devront réceptionner les "signalements d'incident", les "qualifier", et mettre en relation les victimes avec les structures "adaptées pour les accompagner dans la résolution de l'incident" : prestataire local qualifié par l'Anssi (Agence nationale de la sécurité des systèmes d'information) ou labellisé "ExpertCyber" par cybermalveillance.gouv.fr (lire sur AEF info), centre national de réponse à incidents de l'Anssi, services de police ou de gendarmerie, "auprès desquels les dépôts de plainte seront encouragés" (lire sur AEF info). Les centres régionaux travailleront en outre avec les entreprises, les collectivités
et les associations "pour les sensibiliser et les former aux bonnes pratiques cyber".

Dans le cadre du plan de relance, l'Anssi apportera un soutien financier à la création de ces Csirt "via l'octroi d'une subvention à hauteur d'un million d'euros à chaque région volontaire". Les centres des sept premières régions participeront, à partir de février 2021, à un programme d'incubation de quatre mois mis en place par l'agence qui doit leur permettre "d'être rapidement opérationnels pour répondre de manière pertinente et efficace aux besoins identifiés, tout en s'intégrant pleinement à l'écosystème territorial et national". Une mise en réseau des Csirt régionaux est en effet prévue au sein du réseau français des équipes de réponse à incident, l'InterCert France, afin de créer "un groupe de coopération et de partage dédié à leurs enjeux territoriaux".

Une synthèse régionale de la menace
Une autre session de formation aura lieu de septembre à décembre 2022 pour les autres régions métropolitaines candidates. "L'objectif est que toutes les régions volontaires puissent disposer dès 2022 d'un tel centre, dont les capacités opérationnelles seront pleinement atteintes à l'horizon 2024", indique l'Anssi. La création de ces CSIRT est "une opportunité" pour l'ensemble des acteurs régionaux", souligne-t-elle, en évoquant la dynamisation locale du secteur de la cybersécurité et la limitation des pertes financières pour les victimes de cyberattaques. Par ce biais, les services de l'État en région auront aussi accès "à une synthèse de la menace cyber consolidée à l'échelle de leur territoire".

Hôpital de Corbeil-Essonnes : le groupe russophone Lockbit 3.0 revendique la cyberattaque et lance le chantage aux données

leparisien.fr/high-tec, par Damien Licata Caruso
Le 12 septembre 2022 à 11h03

Touché par une violente attaque informatique, le Centre hospitalier Sud francilien est aussi victime d'une tentative d'extorsion de la part de cybercriminels. Ils ont diffusé une partie de leur butin pour accentuer la pression.

Le Centre Hospitalier Sud-Francilien (CHSF) de Corbeil-Essonnes a été la cible d'une cyberattaque fin août.

Tous les indices pointaient vers eux et il ne manquait que leur sinistre tentative de chantage officielle. Le groupe Lockbit, un collectif de hackers russophones, a revendiqué ce lundi sur son site du Darknet la cyberattaque par rançongiciel et surtout le vol de données contre le Centre hospitalier Sud francilien (CHSF), situé à Corbeil-Essonnes.

Un rançongiciel ou « ransomware » en anglais correspond à un logiciel malveillant qui vient chiffrer, rendre totalement illisibles, les données d'un ordinateur, d'un serveur ou d'un réseau d'une entreprise ou d'une collectivité locale. Les pirates informatiques vont d'abord vendre à la victime leur clé de déchiffrement des données, le sésame pour y accéder de nouveau. Mais si la cible refuse de payer, ils actionnent un deuxième levier : la menace de publier les données siphonnées ou de les revendre au plus offrant. Ils l'ont activé lors de cette revendication et demandent 1 million de dollars pour détruire les bases de données siphonnées ou les racheter.

Un échantillon de données publié

Malgré des négociations engagées par les autorités pour desserrer l'étau autour de l'hôpital public, les cybercriminels continuent de penser qu'ils pourront obtenir une rançon… « d'une clinique au revenu annuel de 650 millions d'euros » d'après eux. Les institutions publiques ont pour consigne de ne jamais payer une rançon. « Cette entreprise ne veut pas remplir sa part de la transaction et racheter la clé de déchiffrement et les données de ses clients, patients et partenaires » explique le groupe, suivi de près par les cybergendarmes. « Cette entreprise ne soucie pas de la diffusion des cartes de soin, de l'historique médical ou des diagnostics de ses patients ». « Nous lui avons offert un prix très raisonnable car nous respectons les établissements de santé » concluent-ils. Avant de préciser qu'ils possèdent plus « d'un million de dossiers informatiques de cette entreprise ».

Les hackers ont mis en ligne quelques exemples pour prouver leurs méfaits. L'échantillon de documents publiés comprend des documents internes et des échanges avec l'administration mais aussi des factures de prestataires. Les archives les plus anciennes remontent à une dizaine d'années, selon les fichiers que nous avons pu consulter.

Pièce 9

Reconnaissance faciale, caméras: la Quadrature du Net veut déposer plainte contre l'Intérieur

internet | lois | technologies | informatique | gouvernement | police
Paris, France | AFP | 24/05/2022 12:20 UTC+2

L'association la Quadrature du Net a engagé mardi une campagne de signatures en vue du dépôt d'une plainte collective contre le ministère de l'Intérieur, en dénonçant l'utilisation de la reconnaissance faciale, le fichage de visages et la vidéosurveillance.
L'association de défense des libertés numérique a lancé un site (plainte.technopolice.fr) où les personnes peuvent remplir un formulaire lui donnant mandat pour déposer plainte devant la Commission nationale de l'informatique et des libertés (CNIL).
La Quadrature s'inspire des plaintes collectives qu'elle avait déposées en 2018 contre les Gafam, en s'appuyant sur le Règlement général sur la protection des données (RGPD). Ces procédures, déposées au nom de 12.000 signataires, ont abouti à de lourdes amendes contre Google et Amazon de respectivement 50 et 746 millions d'euros. Cette fois, l'association s'attaque à ce qu'elle présente comme les "quatre piliers" d'un "système de surveillance de masse": la "vidéosurveillance", la "détection automatisée de comportement", le "fichage" et la "reconnaissance faciale".
Au-delà de la plainte et du nombre de signatures qui seront recueillies, l'objectif est aussi de "visibiliser ces technologies" et de "mettre le sujet dans le débat public", dans le contexte notamment d'éventuelles évolutions législatives dans le domaine de la sécurité pour les Jeux olympiques de 2024 en France, explique à l'AFP Noémie Levain, juriste à la Quadrature.
"Que ce soit la reconnaissance faciale ou la vidéosurveillance algorithmique qui sont en passe d'être légalisées, personne ne sait que ça existe. On n'en parle pas, à part quelques spécialistes", ajoute-t-elle.
Dans le détail, l'association prévoit d'attaquer dans sa plainte la vidéosurveillance, en assurant que le nombre de caméras "a explosé", "alors que leur effet sur la criminalité est infime". Une "absence de nécessité" qui "les rend illégales juridiquement", argumente la Quadrature, en réclamant le retrait de l'ensemble des caméras ("plus d'un million") déployées dans l'espace public.
Elle attaque aussi les fichiers de police TAJ (traitement des antécédents judiciaires), qui comprend "huit millions" de photos de visages et TES (titres électroniques sécurisés) où se trouve "le visage de toute personne demandant une carte d'identité ou un passeport". Dénonçant, la "démesure" de ces fichiers, elle demande la "suppression" des photos qu'ils contiennent.
L'association va également demander à la CNIL de "mettre fin" à l'utilisation par la police de logiciels de reconnaissance faciale. Elle dénonce enfin la "vidéosurveillance algorithmique", qui "se déploie dans les villes de manière hyper opaque", mais ne l'attaquera pas directement dans la plainte, des actions juridiques ayant déjà lieu au niveau local.

Traqueuses de cybercriminels

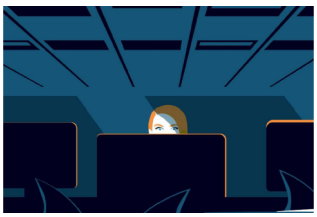
Elles sont une poignée à infiltrer les réseaux cryptés et à s'attaquer au darkweb. Les trentenaires, rompues aux technologies du numérique, arrivent en renfort et investissent sans complexe cet univers fascinant.

Madame Figaro, par Anne Vidalie (illustrations, Arnaud Tracol)

26/08/22

La commissaire divisionnaire Anne Souvira, 66 ans dont quatre décennies de police judiciaire, le reconnait sans ambages : elle a failli se faire avoir comme une bleue. En quelques clics distraits sur Internet, la voilà sur le site de sa banque, prête à régler son loyer après avoir tapé machinalement son identifiant et son mot de passe. Mais son sixième sens, alerté par un détail, retient sa main au dernier moment. « J'étais sur un faux site, raconte la cheffe de la mission cyber auprès de la Préfecture de police de Paris. Mon manque de vigilance aurait pu me coûter cher car je doute fort, étant donné ma connaissance de ces arnaques, que ma banque ait accepté de me rembourser… » Pendant sept ans, jusqu'en 2015, cette policière pugnace et enjouée a dirigé l'unité parisienne spécialisée, la Brigade d'enquêtes sur les fraudes aux technologies de l'information (Befti), avant de conseiller le préfet de police de la capitale sur ces questions.

Comme Anne Souvira, une poignée de femmes ont décortiqué, très tôt, les menaces venues du numérique, quand leurs collègues masculins préféraient traquer les braqueurs et les trafiquants de drogue. Parmi ces pionnières : la contrôleuse générale Catherine Chambon, première patronne de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), le service national né au tournant du siècle, puis première cheffe de la Sous-direction de la lutte contre la cybercriminalité (SDLC) ; Valérie Maldonado, ancienne « taulière » de l'OCLCTIC, puis sous-directrice de la SDLC ; la magistrate Myriam Quéméner, avocate générale près la cour d'appel de Paris, autrice d'une thèse consacrée à la criminalité économique et financière sur Internet en 2014. « Pour qu'on me prenne au sérieux », glisse la volubile sexagénaire, désormais experte auprès du conseil de l'Europe, qui a publié une dizaine d'ouvrages sur son sujet favori.



Ces précurseures ont eu raison. Au Far-West numérique, où les armes s'appellent virus informatiques, logiciels malveillants ou algorithmes trafiqués, les dangers pullulent, invisibles, protéiformes, mouvants. Car les technologies de l'information ont offert un terrain de jeu tout neuf aux malfrats de tout poil, petits délinquants et criminels chevronnés, hackers et mercenaires à la solde d'États-voyous, rivalisant d'imagination pour dérober de précieuses données, diffuser de fausses informations, prendre des données en otage ou, tout simplement, voler, escroquer, harceler.

Pour combattre ces malfaiteurs 2.0, police, gendarmerie, douane et Direction générale de la sécurité intérieure (DGSI) alignent leurs bataillons de cyber-enquêteurs, épaulés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Deux de ces services de pointe sont dirigés par des femmes : la commissaire divisionnaire Cécile Augeraud, 44 ans, à l'OCLCTIC ; la colonelle de gendarmerie Fabienne Lopez, au Centre de lutte contre les criminalités numériques (C3N). Le 14 juillet, c'est cette militaire de 53 ans qui menait, sabre au clair, l'escouade des cyber-gendarmes sur les Champs Élysées. À l'ex-Befti, rebaptisée BL2C, pour Brigade de lutte contre la cybercriminalité, le poste de numéro 2 est occupé par la commandante divisionnaire Véronique Bouchaux, 53 ans.

Pourtant, leurs consœurs se comptent sur les doigts de la main parmi les limiers du numérique. À l'exception de Cyberdouane, où la parité règne dans l'open-space partagé par la quinzaine d'agents qui chassent les trafics illicites de marchandises sur la Toile. « Beaucoup de filles souffrent du syndrome de l'imposteur, déplore Cécile Augeraud. Elles pensent que le cyber est trop technique, trop compliqué pour elles. » Sur une cinquantaine de policiers, elles ne sont que quatre à la BL2C, bientôt cinq. À la division opérationnelle de l'OCLCTIC, le brigadier-chef Sonia se sent moins seule depuis que deux autres femmes l'ont rejointe le 1er juillet dernier. Cette experte des escroqueries perpétrées grâce aux outils numériques, en poste depuis huit ans, leur promet un boulot passionnant.. « Impossible de s'ennuyer, on apprend des choses tous les jours », assure-t-elle.

Pas « geek » pour deux sous, Sonia, 41 ans, ne connaissait pas grand-chose à la planète cyber avant de quitter son commissariat pour rejoindre l'Office, attirée par « les belles affaires nécessitant beaucoup de professionnalisme et de rigueur ». Elle y a découvert les adresses IP, les cryptomonnaies, le dark web, les réseaux cryptés et les « ransomwares », ces logiciels qui chiffrent les fichiers d'un ordinateur dont l'utilisateur est sommé de payer une rançon pour les récupérer. « J'ai acquis une technicité, observe-t-elle, mais mon travail consiste aussi à faire des filatures, des perquisitions et des interpellations, puis à mettre les éléments recueillis en procédure. » Elle reste « policière avant tout ». « Nous ne sommes pas de purs techniciens, renchérit Véronique Bouchaux, de la BL2C. Le flair policier demeure essentiel. Et les classiques investigations sur la téléphonie et les flux financiers sont bien utiles pour débusquer les délinquants cachés derrière les écrans. »

À la DGSI, Karine*, major de police de 44 ans, a travaillé sur le versant sunnite du terrorisme islamique, puis à la coopération internationale, avant de côtoyer les petits génies de son nouveau service, 100% masculin. Imbattables pour extraire les données chiffrées planquées dans les entrailles des téléphones, ordinateurs et serveurs des criminels. Mais pas très doués pour communiquer avec les douaniers, gendarmes et policiers auxquels ils prêtent leurs talents. À Karine incombe le rôle d'aider les uns et les autres à se comprendre. « Je joue le rôle d'interface, je vulgarise », résume-t-elle. Sa collègue Justine, 32 ans, en fait autant. L'équipe de cette contractuelle diplômée en relations internationales anime le réseau d'agents chargés d'alerter les entreprises sur les risques cyber. Les deux ou trois premiers mois, elle a souffert. « Dans les réunions, j'avais parfois du mal à comprendre les échanges entre les ingénieurs et les industriels, se souvient-elle. Comme une langue étrangère qu'on connaît mal. » Aujourd'hui, elle la parle couramment.

Chloé, 38 ans, n'est ni policière, ni ingénieure, elle non plus. Mais cette spécialiste de l'intelligence économique et de la gestion de crise se trouve au cœur du réacteur de l'ANSSI, l'autorité chargée de la sécurité des administrations et des entreprises essentielles au bon fonctionnement de l'État. Elle coordonne les équipes du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. « La cybersécurité nécessite des compétences techniques, bien sûr, mais aussi des connaissances géopolitiques et la maîtrise de la communication, explique-t-elle. Mon métier, c'est la coopération avec les autres centres d'alerte, gouvernementaux, institutionnels ou privés pour prendre de vitesse les attaquants. » Sa collègue Sara, elle, accompagne l'écosystème de la défense dans la prise en compte des menaces numériques. « Parmi les coordinateurs sectoriels de l'ANSSI, les femmes sont proportionnellement bien représentées », note cette ingénieure de 39 ans venue de la Direction générale de l'armement.

Dans le monde cyber en manque de cerveaux, on lorgne du côté des filles. « Pour les recruter et les fidéliser, il faut dédramatiser notre domaine d'activité », juge Cécile Augeraud, qui porte la bonne parole auprès des futurs officiers et commissaires de l'École nationale supérieure de la police. « Il faut casser les stéréotypes pour donner aux femmes l'envie de s'engager dans cette voie, renchérit son homologue côté gendarmerie, la colonelle Lopez. Le cyber, ce n'est pas qu'un monde de post ados collés à leur ordinateur jusqu'à 3 heures du matin avec un sandwich avarié ! »

Le brigadier-chef Michèle* fait mentir ce cliché. Cette brindille brune de 43 ans, mordue de développement informatique, ne porte pas de sweat à capuche, mais elle offre un précieux soutien technique aux enquêteurs de la BL2C. « Je les aide à exploiter les données qu'ils recueillent pour qu'ils puissent faire rapidement le tri et dégager des pistes d'investigation », précise-t-elle.

Chez les trentenaires, de plus en plus de jeunes femmes biberonnées au numérique n'ont aucun complexe sur le sujet. Léa*, cyberdouanière de 32 ans, avoue dans un éclat de rire que, oui, elle est geek. Passionnée par la matière, elle ne se lasse pas des opérations d'infiltration sur le Dark Web, le côté obscur de la Toile, ni des « coups d'achat » qui permettent parfois de démasquer des marchands d'armes ou de stupéfiants en ligne. Sara, de l'ANSSI, est une adepte des compétitions de hacking. « C'est indispensable pour comprendre comment les attaquants fonctionnent, quels outils ils utilisent », estime-t-elle.

Le maréchal des logis-chef Mélissa, 30 ans, préfère le « bidouillage ». Petite déjà, elle adorait démonter des ordinateurs et écrire des lignes de code. En 2014, elle a été l'un des premiers « C-Ntech » de la gendarmerie, ces « Correspondants en technologies numériques » habilités à exploiter les données des téléphones et des ordinateurs. Comme dans ce récent dossier de pédopornographie où les investigations de Mélissa ont permis d'identifier douze mineures de moins de 15 ans victimes du même homme, à La Réunion.

Sa collègue du C3N, l'adjudante Céline, a participé à l'une des plus incroyables enquêtes cyber : l'infiltration en 2020 de la messagerie cryptée EncroChat, très prisée des réseaux européens de criminalité organisée. Grâce aux 120 millions de messages et d'images interceptés, des milliers de malfrats ont été envoyés derrière les barreaux, d'énormes quantités de drogue et d'armes saisies, des centaines de projets d'assassinat déjoués. Cette prouesse a valu à la jeune militaire le prix « Coup de cœur » décerné par le Cercle des femmes de la cybersécurité en octobre 2021. Et à sa cheffe, la colonelle Fabienne Lopez, le Trophée européen de la femme cyber militaire.

*Prénom d'emprunt

L'explosion de la cybercriminalité

35 millions d'euros dérobés par un cyber-escroc à un promoteur immobilier en décembre 2022. Un hôpital d'Ajaccio paralysé en mars dernier par un rançongiciel – un logiciel malveillant qui prend en otage les fichiers ou bloque l'accès aux données. L'opérateur téléphonique La Poste mobile visé par une attaque informatique en juillet. La cybercriminalité est déjà l'un des fléaux du troisième millénaire. Et ces infractions pénales commises « à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet » n'épargnent personne, entreprises, administrations, collectivités ou individus.

En 2021, une société sur deux a été visée. Quand la tentative aboutit, la proie perd en moyenne 27% de son chiffre d'affaires annuel. Au point que 60% des PME victimes déposent le bilan dans les dix-huit mois. Et ces dégâts sont sous-évalués, en réalité, car un patron sur deux seulement porte plainte.

Selon une étude récente de l'Insee, les deux-tiers des Français déclarent qu'eux-mêmes, des membres de leur famille ou des amis ont été exposés à une forme de cybercrime au cours des trois années précédentes. Arrivent en tête, pour la moitié d'entre eux, le hameçonnage ou « phishing » (un message incitant à se connecter à un site frauduleux), suivi des virus et autre logiciels frauduleux (41,7%) et du piratage de leur boîte mail ou de

leur compte sur un réseau social (19,1%). La magistrate Myriam Quéméner est formelle : « On assiste globalement à un glissement de la délinquance et de la criminalité vers le numérique. »

Cybersécurité : le "filtre anti-arnaques" lancé en version bêta pour l'été 2023, selon Jean-Noël Barrot

aefinfo, 28/10/22
Le "filtre anti-arnaques", promesse de campagne d'Emmanuel Macron, "sera proposé en version bêta à l'été 2023 "avant d'être généralisé d'ici à l'été 2024", annonce Jean-Noël Barrot, ministre délégué chargé de la Transition numérique et des Télécommunications, au Campus cyber, jeudi 27 octobre 2022. Cet outil, qui filtrera "les adresses internet correspondant à des sites malveillants", s'inscrit dans la volonté du gouvernement de "garantir la cybersécurité du quotidien". Dans sa feuille de route, Jean-Noël Barrot entend aussi "conforter" la filière de la cybersécurité à travers "France 2030".
Face à la "forte augmentation incivilités et délinquance en ligne", qui "plonge nos concitoyens dans une forme d'insécurité numérique", Jean-Noël Barrot se fixe "deux objectifs" : "garantir la cybersécurité du quotidien" et "conforter la filière souveraine de la cybersécurité". En présentant sa "feuille de route" au Campus cyber, jeudi 27 octobre 2022, comme il l'avait annoncé aux "universités d'été" d'Hexatrust (lire sur AEF info), le ministre délégué chargé de la Transition numérique et des Télécommunications a dévoilé plusieurs mesures "en complément" de la Lopmi, qui "apportera des réponses régaliennes nouvelles et puissantes au sujet qui nous préoccupe" (lire sur AEF info).

Des outils de protection "simples, gratuits, facultatifs"
Outre la sensibilisation aux "gestes barrières à adopter en ligne", l'exécutif veut mettre à disposition de la population des "outils de protection simples, gratuits, facultatifs". Jean-Noël Barrot a chargé une "task force" d'élaborer le "filtre anti-arnaques" promis par Emmanuel Macron pendant la dernière campagne présidentielle (lire sur AEF info). Cet outil, qui devrait être disponible sur poste fixe et sur mobile, "avertira en temps réel les internautes" qu'ils consultent un site malveillant.
"Dans un premier temps nous nous attaquerons aux faux sites ayant pour objectif de dérober des données personnelles et bancaires, […] car il s'agit d'arnaques particulièrement graves et fréquentes."
"Dès la fin novembre, nous lancerons 'mon service sécurisé', fruit du travail d'une start-up d'État incubée par l'Anssi", indique également le ministre. Annoncé par Guillaume Poupard aux Assises de la cybersécurité de Monaco (lire sur AEF info), ce service "permettra aux agents publics de sécuriser et d'homologuer facilement et gratuitement les services publics en ligne, qu'il s'agisse de sites web, d'applications mobiles ou d'API". Par ailleurs, le gouvernement prépare la mise en œuvre
du "cyberscore" pour l'automne 2023. Issu de travaux parlementaires, cet outil "permettra aux internautes de connaître le niveau de sécurité de leurs données sur les sites et réseaux sociaux qu'ils utilisent, à l'image du nutriscore pour les produits alimentaires" (lire sur AEF info).

"Provoquer la désirabilité"
Concernant la consolidation de la filière, Jean-Noël Barrot entend "veiller à la bonne exécution" du plan "France 2030", dans lequel s'inscrit désormais la stratégie d'accélération cyber annoncée début
2021 (lire sur AEF info). Florent Kirchner, chef de division au CEA, deviendra coordinateur national de cette stratégie au 1er décembre, en remplacement de William Lecat (lire sur AEF info).Le ministre annonce également le financement de 17 nouveaux projets à hauteur

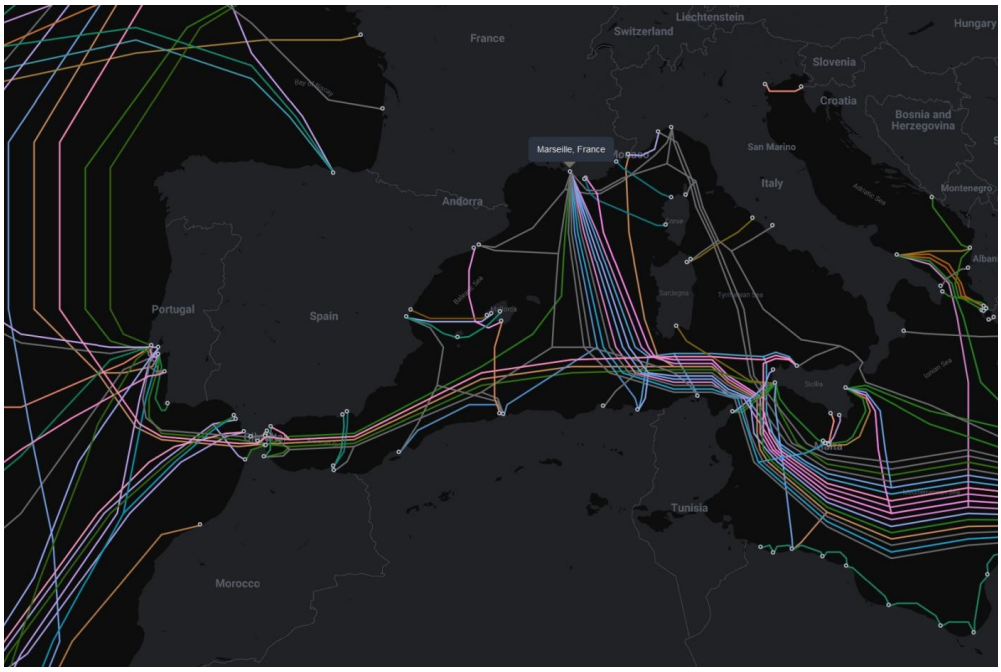
de 39 millions d'euros dans le cadre de "France 2030", dont des outils "d'analyse de la menace cyber" ou une plateforme "permettant de mettre en lien IA d'un côté et cybersécurité de l'autre", qui sera gérée par le Campus cyber et devra proposer huit cas d'usage d'ici fin 2023.
Rappelant qu'il n'existe pas de code NAF propre aux entreprises de cybersécurité, Jean-Noël Barrot "appelle de [s]es vœux" la création d'un "répertoire unique des entreprises", qui facilitera "la mise en réseau des acteurs du secteur". Le ministre note par ailleurs que la filière cyber est confrontée "plus que les autres" à des tensions sur le recrutement, puisque 15 000 postes sont vacants, selon le président du Campus cyber, Michel Van Den Berghe. Si l'État va "consacrer 140 millions d'euros à la formation aux métiers de la cybersécurité avec l'objectif de créer 30 000 emplois supplémentaires" (lire sur AEF info), Jean-Noël Barrot invite son auditoire à provoquer "ensemble la désirabilité de cette filière", grâce à l'alternance et la valorisation, notamment au travers des "Olympiades des métiers", "dont la finale se tiendra à Lyon en 2024".
"Attirer et former les 'talents de demain'" fait partie des axes de travail du Campus cyber, rappelle Michel Van Den Berghe, selon lequel "seulement 3 % des jeunes qui suivent une formation dans le numérique se sentent attirés par les métiers de la cybersécurité". Pour "faire connaître" ces métiers aux plus jeunes, le Campus cyber a formé plus de 500 enseignants en partenariat avec la Dgesco en octobre et s'apprête à lancer des campagnes de communication. "Il faut également qu'on change l'image de la cybersécurité auprès du grand public et des parents qui sont souvent déterminants dans les choix de leurs enfants", estime le président du Campus cyber. Outre des discussions avec les producteurs de la série du "Bureau des légendes", il annonce la création d'un festival, le "Cyberfest", pour accueillir "le maximum de jeunes et de familles".

Un "bilan objectivé" du plan de relance
Jean-Noël Barrot a demandé à l'Anssi "un bilan objectivé" des 950 "parcours de sécurisation" mis en place par l'agence à destination des administrations publiques, collectivités territoriales et hôpitaux pour un budget de 176 millions d'euros dans le cadre du plan de relance puis de France 2030 (lire sur AEF info). Lors des Assises de Monaco, plusieurs dirigeants d'entreprises de cybersécurité française s'étaient plaint de la faiblesse des retombées. Les sociétés de conseil françaises qui participent à ces parcours "vendent des produits étrangers", regrettait Elena Poincet, CEO de Tehtris, assimilant ce volet du plan de relance à "un échec". Sans entrer dans ce débat, le ministre indique que l'Anssi sera également chargée de proposer "une feuille de route opérationnelle pour envisager la suite à donner à ce dispositif". "En cette fin de période du 'quoi qu'il en coûte', l'État peut amorcer la démarche mais se sont bien aux acteurs de prévoir également les investissements nécessaires de manière récurrente et pérenne", prévient-il, jugeant les "parcours de sécurisation" "vertueux" puisque basés sur une logique de cofinancement. "Ainsi les collectivités territoriales pouvaient bénéficier d'un financement de l'État de 50 000 euros, à condition qu'elles investissent en parallèle 70 000 euros."

Pièce 12

Le sabotage de câbles de fibre optique en France a perturbé le web mondial

Un avant-goût des conséquences terribles que pourrait avoir un sabotage massif des câbles sous-marins.



©submarinecablemap.com

Le journal du Geek

Le 22 octobre 2022, par Antoine Gautherie

Dans la nuit du 17 au 18 octobre, un câble de fibre optique majeur a été sectionné dans les Bouches-du-Rhône. Il s'agit indiscutablement d'un acte de vandalisme selon Zscaler, une entreprise de cybersécurité qui exploite cette infrastructure de SFR ; et ce sabotage a eu des conséquences sur la connectivité web un peu partout dans le monde.

En effet, comme on peut le voir sur la carte ci-dessus, ces câbles sont positionnés en amont d'une autre structure de transit vers le réseau de câbles sous-marins. Ce dernier constitue la colonne vertébrale du réseau Internet mondial ; un positionnement stratégique qui explique les conséquences ressenties par certains utilisateurs à l'autre bout de la planète.

Dans un rapport d'incident repéré par Netcost Security, l'entreprise a expliqué que « *la coupure d'un câble majeur dans le Sud de la France a impacté la connectivité* **en Asie, en Europe, aux États-Unis,** *et potentiellement dans d'autres régions du monde* ». En pratique, cela s'est traduit par des **pertes de paquets** ou une **latence accrue** sur les réseaux concernés.

Au bout du compte, il est apparu que trois câbles distincts ont été sectionnés dans un délai relativement court — une information qui donne encore plus de crédit à la piste du sabotage pour et simple, selon le directeur de Zscaler Jay Chaudhry cité par CRN. Le

premier a déjà été réparé, et les travaux sont apparemment en cours sur les deux autres lignes. **L'identité des auteurs, en revanche, reste inconnue à ce jour** ; il faudra attendre la conclusion des enquêtes en cours en France, mais aussi dans d'autres pays concernés selon Netcost.

L'infrastructure sous-marine, nerf de la guerre en Urkaine ?

Certains y ont vu un lien avec deux autres incidents qui se sont déroulés au Royaume-Uni. La semaine dernière, des câbles sous-marins ont été endommagés dans le nord du pays ; les résidents des îles Féroé, puis Shetland se sont ainsi retrouvés privés de téléphone et d'Internet pendant une durée prolongée.

Mais d'après le gouvernement britannique cité par le Guardian, il s'agissait tout simplement d'accidents. Les câbles en question auraient été **endommagés par des chalutiers** — le type d'incident le plus fréquent sur ces installations. Les enquêtes sont toujours en cours, mais pour l'instant, aucun élément rendu public ne permet d'établir un lien entre ces incidents.

Cela n'a pas empêché certains observateurs de spéculer, notamment en pointant du doigt la Russie. Il s'agit probablement d'une conséquence de la **paranoïa caractérisée** qui entoure les installations sous-marines depuis le **sabotage du Nord Stream.**

Ce pipeline gazier est au cœur d'un immense marasme diplomatique. Plusieurs états ont **accusé à demi-mots le gouvernement russe d'avoir endommagé délibérément l'installation** dans le cadre du bras de fer qui l'oppose au reste de l'Europe. Le Kremlin a **nié toute implication**, accusant au passage les États-Unis et leurs alliés d'avoir endommagé le pipeline eux-mêmes afin de nuire aux intérêts russes.

À l'heure actuelle, l'enquête n'a toujours pas produit de résultats probants — ou du moins, ils n'ont pas été rendus publics. Mais l'incident a déclenché un véritable branle-bas de combat sur tout le continent. Plusieurs pays, à commencer par la France, ont annoncé un renforcement considérable de la surveillance autour de toutes les installations sous-marines — en particulier celles qui sous-tendent l'Internet mondial. Et cette affaire de sabotage en France prouve que cette décision est justifiée et nécessaire; elle nous donne un petit avant-goût des conséquences terribles que pourrait avoir un sabotage massif des câbles sous-marins.

«Maîtriser notre cybersécurité passe par une industrie souveraine»

Le Figaro Tech, par Ingrid Vergara
Publié le 27/10/2022 à 20:20

Jean-Noël Barrot, ministre délégué chargé de la Transition numérique.

DÉCRYPTAGE - Face au risque cyber, Jean-Noël Barrot, le ministre délégué au Numérique, détaille sa feuille de route. Hôpital de Corbeil-Essonnes, mairies de Caen et de Chaville, conseil départemental de Seine- Maritime, pour ne citer qu'eux… Le rythme des cyberattaques ne faiblit pas en 2022. Une collectivité locale sur trois en France a déjà été victime d'une intrusion informatique et pratiquement une entreprise française sur deux. «Nous assistons à une forte augmentation et une transformation de la délinquance dans le cyberespace, constate Jean-Noël Barrot, ministre délégué chargé de la Transition numérique. Or cette situation plonge nos concitoyens dans une forme d'insécurité numérique, et sape la confiance envers des technologies pourtant porteuses de promesses et de progrès.» Lancée il y a un an et demi pour faire monter le niveau général de protection du pays, la stratégie nationale de cybersécurité, coordonnée par le chercheur Florent Kirchner, commence à porter ses premiers fruits. Les diagnostics de sécurité menés auprès d'hôpitaux et de collectivités territoriales sous l'égide de l'agence nationale de cybersécurité (Anssi), dont les effectifs ont été renforcés pour 2023, ont ainsi permis à la ville de Caen d'éviter la catastrophe en bloquant la propagation de l'attaque au bout de quelques minutes grâce à une protection numérique mise en place à la suite d'un de ces programmes de sécurisation. Financés à hauteur de 120 millions d'euros, ces audits doivent aider quelque 950 acteurs, dont 150 hôpitaux, à mieux se protéger.

Passer un nouveau cap de sécurité nécessite absolument un effort collectif. «Cela passe par une prise de conscience collective des gestes barrières à adopter en ligne, face aux attaques ou de tentatives d'escroquerie. Que ce soient les collaborateurs dans les entreprises, les agents publics, mais également tout un chacun dans sa vie privée. Il faut avoir conscience que la menace est là, qu'elle progresse et qu'il faut s'en prémunir. En adoptant une forme d'"hygiène numérique", on peut parer une grande partie de ces attaques qui viennent jouer bien souvent sur notre négligence ou sur nos mauvaises habitudes», souligne-t-il.

Pour aider les internautes au quotidien, le gouvernement proposera dans les prochains mois un outil qui filtrera préventivement les adresses correspondant à des sites malveillants. Basé sur le Domain Name System (DNS), qui traduit les noms de domaine internet en adresse IP, il ressemblera à ce quiest déjà utilisé au Royaume-Uni ou en Belgique. «Mon objectif est que ce filtre soit prêt en version bêta à l'été 2023, avant la Coupe du monde de rugby, pour qu'il puisse être enrichi et déployé à l'horizon des Jeux olympiques de 2024», précise Jean-Noël Barrot.
En attendant, l'État veut déjà s'assurer que les services publics répondent aux meilleurs standards de sécurité et de protections des données des citoyens. «Dès fin novembre, nous lançons la plateforme Monservicesécurisé, qui permettra de sécuriser facilement et gratuitement les services publics en ligne, et de protéger les données des internautes. Ces services pourront être testés et homologués grâce au support de l'Anssi», précise-t-il. Pour l'ensemble des sites et applications, un «Cyber-score» sera aussi lancé fin 2023. «Ce Cyber-score permettra aux internautes de connaître le niveau de sécurité de leurs données sur les sites, les réseaux sociaux ou les applications qu'ils utilisent, un peu à l'image du Nutri-

score pour les produits alimentaires.» Le cahier des charges et les critères sont en cours d'élaboration.

39 millions pour 17 projets

«La maîtrise de notre cybersécurité passe par le développement d'une industrie souveraine», insiste le ministre. Dans ce cadre, il annonce le financement de 17 nouveaux projets innovants à hauteur de 39 millions d'euros, dans le cadre de France 2030. Parmi eux, un outil d'évaluation du risque cyber développé par la société CybelAngel, un projet porté par la société Snowpack qui s'appuie sur des technologies du CEA, l'appui financier au «start-up studio» du Campus Cyber ou encore le développement d'une plateforme mettant en lien intelligence artificielle et cybersécurité pour augmenter les capacités de détection et de réponse à des incidents. Bien conscient que le plus grand défi du secteur reste la pénurie de compétences, le gouvernement veut y mettre les moyens.

«Nous allons contribuer à former des milliers d'experts en cybersécurité, notamment grâce à une enveloppe de 140 millions d'euros inscrite dans le plan France 2030. L'objectif est d'avoir 75.000 experts à l'échelle nationale en 2025, contre 45.000 actuellement. Il faut aussi que nous puissions féminiser ces métiers. Seuls 11 % des experts dans le cyber sont des femmes. Attirer de futurs talents passe aussi par une meilleure valorisation des métiers. Il faut faire évoluer les mentalités et donner envie pour que ces métiers et les formations qui permettent d'y accéder soient plus attractifs pour les jeunes. Sensible au sujet, le coproducteur du Bureau des Légendes, Alex Berger, travaille, de son côté, sur une nouvelle série télévisée pour démystifier le monde de la cybersécurité.

Pièce 14

Jeux olympiques : comment Paris 2024 se prépare à la menace des cyberattaques
18h08 , le 21 octobre 2022 Par Marius Bocquet
Le Journal du Dimanche

À moins de deux ans des Jeux olympiques, l'équipe cybersécurité de Paris 2024 s'entraîne face à la menace des cyberattaques. Lors des derniers JO, en 2021, pas moins de 4,4 milliards événements de sécurité informatique ont été dénombrés.

Le 4 août 2024, vers 21 heures, les coureurs du 100 mètres hommes seront dans les starting-blocks pour la finale des Jeux olympiques 2024, au Stade de France. Pour le monde entier, qui aura les yeux rivés sur les athlètes, ce sera une grande fête. « *Mais moi, ce n'est pas ce que je verrai »*, déclare au JDD Franz Regul, responsable de la sécurité des systèmes d'information pour Paris 2024. « *Ce que je verrai, c'est un ordinateur entouré de périphériques avec à peu près de 80 000 spectateurs à l'intérieur et quelques centaines d'athlètes. C'est un système technologique qui va nous permettre de gérer l'accueil des participants, des spectateurs, des journalistes, la captation et la retransmission des compétitions, la sécurité des participants et tout un tas de fonctions liées aux opérations de ce site* », énumère-t-il.

La cybersécurité est un sport d'équipe

À moins de deux ans de l'événement sportif le plus regardé au monde, l'organisation des JO de Paris 2024 se prépare plus que jamais à la menace cyber. Il faut dire que, dans un monde qui se numérise de plus en plus, les cyberattaques n'épargnent pas un grand événement tel que les Jeux olympiques. Lors des derniers JO de Tokyo, en 2021, 4,4 milliards événements de sécurité informatique ont été dénombrés, contre 510 millions lors des précédents Jeux de Rio en 2016. « *Évidemment on ne sous-estime la menace cyber. On s'y prépare attentivement avec mon équipe et c'est un sujet qui est pris très au sérieux par la direction générale des Jeux olympiques* », assure Franz Regul. Pour faire face à cette menace, la stratégie de Paris 2024 s'articule en quatre piliers.

Une tour de contrôle cybersécurité

Le premier repose sur la formation et la sensibilisation, alors que près de 90 % des actes de cybercriminalité sont liés à des facteurs humains. « *Concrètement, on met en place des formations auprès des participants à l'organisation, on diffusera le moment venu des guides de sensibilisation et on a mis en place des animations pour sensibiliser nos collaborateurs, notamment un escape game* », détaille le responsable cybersécurité.

Par ailleurs, son équipe accompagne et intervient dans la centaine d'applications et de projets qui gravitent autour des JO. Autre dispositif : une « *tour de contrôle cybersécurité*

», dans laquelle des analystes et experts vont utiliser des outils basés sur l'intelligence artificielle pour détecter tous les signes d'activités suspectes ou malveillantes.

« *L'idée est de se protéger de menaces très concrètes comme les ransomware qui ont pu frapper les JO d'hiver de PyeongChang en 2018 ou des vols de mots de passe* », explique Franz Regul. Enfin, l'équipe cybersécurité de Paris 2024 mise sur l'entraînement, avec notamment des « *cyber wargames* ». « *On va se tourner vers des fournisseurs pour nous attaquer en vrai, simuler le comportement des hackers et évaluer notre niveau de préparation* », explique Franz Regul. Le Comité d'organisation des JO de Paris 2024 a choisi comme partenaires la société américaine Cisco et l'entreprise française Atos. Une partie de leur travail sera par ailleurs d'être présents sur les forums du darkweb et de surveiller ce qui s'y passe.

Une prime aux bugs

Paris 2024 devrait enfin lancer dans quelques jours son programme de « *bug bounty* » (« prime aux bugs »). Il s'agit de s'adresser à la communauté des chercheurs en cybersécurité et de récompenser ceux qui trouveront des failles dans le système. L'organisation travaille aussi en lien avec le Comité international olympique (CIO), l'Agence nationale de la sécurité informatique (Ansi) et le ministère de l'Intérieur.

« *La cybersécurité est un sport d'équipe* », résume Franz Regul. Au total, plusieurs centaines de personnes travailleront à la cybersécurité des JO 2024. Pour l'instant, l'organisation n'a pas repéré d'attaque notable. « *On voit surtout des activités opportunistes, des tentatives d'usurpation, des réservations de noms de domaine, mais, à date, pas d'activité sérieuse* », confie Franz Regul.

Meta admet que son métavers est un « monde vide » et « triste »

Le métavers de Meta peine à séduire les internautes. Malgré les investissements massifs du groupe de Mark Zuckerberg, Horizon Worlds reste désespérément désert.

Le 17 octobre 2022 Par Florian Bayard / 01Net

Un an près s'être rebaptisé Meta, le groupe de Mark Zuckerberg dresse un bilan mitigé d'Horizon Worlds, son métavers. Dans un document interne obtenu par nos confrères du *Wall Street Journal*, Meta révèle que le métavers n'a pas séduit autant d'utilisateurs qu'espéré.

Lancé à la fin 2021, Horizon Worlds compte moins de **200 000 utilisateurs actifs mensuels**, révèle la note interne. Initialement, Meta espérait atteindre le seuil des 500 000 usagers avant fin 2022. L'objectif a été finalement revu à la baisse. Meta ambitionnait malgré tout de passer le cap des 280 000 utilisateurs avant 2023.

Pour rappel, le monde numérique de Meta est actuellement disponible au Canada, aux États-Unis, en France, en Espagne et au Royaume-Uni, par le biais d'un casque de réalité virtuelle.

Le métavers, un désert numérique

Apparemment, la plupart des internautes **abandonnent le métavers** après un mois. Après quelques passages, ils cessent de se connecter à Horizon. Le nombre d'usagers s'est d'ailleurs fortement contracté depuis le printemps. En début d'année, Meta revendiquait encore 300 000 utilisateurs.

> *« Un monde vide est un monde triste »*, résume Meta dans sa note interne.

Les mondes numériques mis au point par Meta, comme *Hot Girl Summer Rooftop Pool Party* et *Questy's*, sont complètement désertés. De plus, les mondes conçus par des utilisateurs d'Horizon sont trop peu visités par les autres. Meta estime que seulement **9 % des univers développés par des joueurs** attirent au moins 50 personnes. La plupart des espaces ne sont jamais visités. Notez qu'il y a moins de 1 % des usagers qui conçoivent leurs propres univers.

Même son de cloche du côté des employés de Meta. D'après un autre document interne, les salariés du groupe ne se connectent presque jamais à Horizon Worlds. Ils estiment qu'une visite dans le métavers est une expérience « *déroutante et frustrante ».* Malgré ces vives critiques, Meta demande à ses employés de s'y rendre au moins une fois par semaine.

Pour mieux comprendre les griefs des usagers, Meta a mené une enquête auprès des utilisateurs actifs. Apparemment, les internautes regrettent de ne pas trouver facilement *« d'autres personnes avec lesquelles passer du temps »*. C'est **un cercle vicieux**. Moins il y a d'utilisateurs sur Horizon, plus les joueurs actifs risquent de décrocher et de déserter le métavers. Les utilisateurs ont également regretté l'absence de jambes, ce qui rend les

avatars peu réalistes. Meta a répondu à la critique en promettant l'ajout de jambes virtuelles dans le courant de l'année prochaine.

15 milliards de dollars d'investissement

Pour mettre au point son métavers, Meta a pourtant **dépensé 15 milliards de dollars**, rapporte *Business Insider*. Cet investissement massif a contribué à plomber les résultats financiers du groupe. Reality Labs, la division consacrée à la conception du métavers, perd en effet plus de deux milliards de dollars tous les trimestres.

Face à ce bilan peu enthousiasmant, l'entreprise s'est montrée **plus mesurée lors de la conférence Meta Connect** de 2022. L'an dernier, Meta n'hésitait pas à présenter son métavers comme une véritable révolution. Cette année, la firme laisse entendre que la révolution annoncée prendra encore du temps. Mark Zuckerberg a notamment clamé que *« l'avenir n'est pas si loin »*, ce qui tranche avec le ton enthousiaste de fin 2021.

« *Le ton était beaucoup plus mesuré qu'il y a un an, comme un retour sur Terre. Ils se sont rendus compte à quel point c'était compliqué de créer ce monde, et aussi peut-être que les gens ne veulent pas y vivre 24 heures sur 24* », explique Carolina Milanesi, analyste chez Creative Strategies.

Les solutions de Meta

Malgré le succès limité de son métavers, Meta n'abandonne pas. Bien décidé à attirer les internautes, le géant de la Silicon Valley a annoncé l'arrivée d'une version Web d'Horizon Worlds. Il n'y aura plus besoin d'acheter un casque de réalité virtuelle. L'arrivée d'**Horizon sur PC**, smartphone et tablette devrait permettre de séduire de nouveaux usagers. On ignore cependant quand la version Web sera disponible.

Dans le document interne, on apprend aussi que **Meta a suspendu le développement de nouvelles fonctionnalités**. Jusqu'à nouvel ordre, les équipes du groupe vont se concentrer sur l'amélioration de l'expérience et la correction des bugs de l'interface.

Enfin, Meta envisage de faciliter la manière dont les utilisateurs peuvent **gagner de l'argent dans le métavers**. En miroir des influenceurs sur TikTok ou YouTube, les créateurs de mondes numériques pourraient à terme être rémunérés par les marques. Meta estime qu'une rémunération pourrait séduire davantage d'internautes.

> *« Certains créateurs ont le désir de travailler à temps plein dans le métavers. S'il y avait des rôles à temps plein avec une bonne rémunération, certains créateurs feraient de la construction du métavers leur travail quotidien à temps plein »*, avance Meta dans son rapport interne.

Piratage : combien coûte un compte TikTok, LinkedIn ou Facebook sur le Dark Web ?

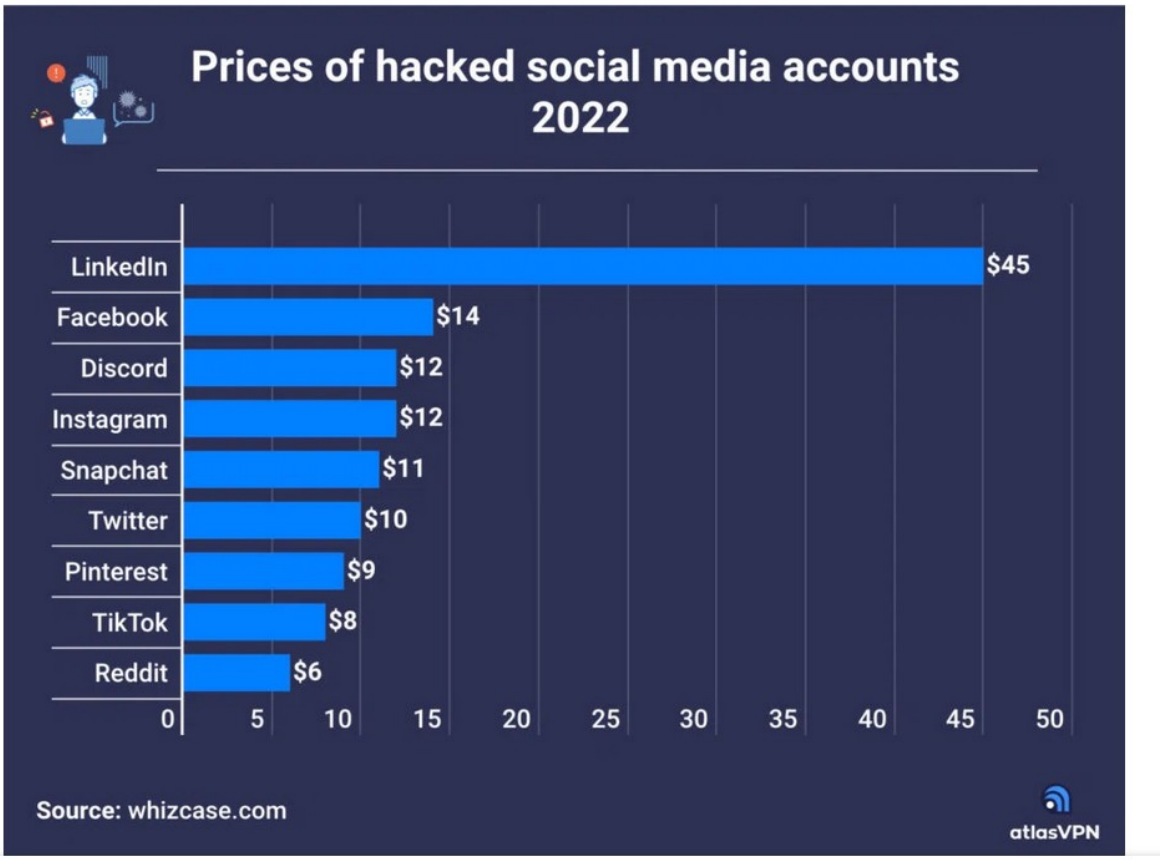
Une nouvelle étude révèle le prix des comptes piratés de réseaux sociaux que l'on peut acheter aujourd'hui sur le Dark Web. Des tarifs dérisoires pour avoir accès à des données aussi sensibles.

Gabriel Manceau 19/10/2022 – 01Net

Les cartes bancaires sont loin d'être les seuls produits vendus en ligne par les cybercriminels. En effet, pour moins de 15 dollars, il est possible d'acheter sur le Dark Web le compte d'un réseau social populaire. Instagram, Facebook, TikTok, Twitter, etc. aucun n'échappe au piratage.

Des prix dérisoires pour les comptes de réseaux sociaux piratés

L'inflation ne semble pas trop avoir touché le prix des comptes de réseaux sociaux piratés sur le Dark Web. Une nouvelle étude de *Whizcase*, partagée par *atlasVPN*, fait la liste des comptes sociaux ayant le plus de valeur sur les réseaux parallèles entre janvier et septembre 2022. Comme vous pouvez le voir sur le graphique ci-dessous, le moins coûteux est un compte Reddit dont le prix est estimé à 6 dollars environ.



© Whizcase et atlasVPN

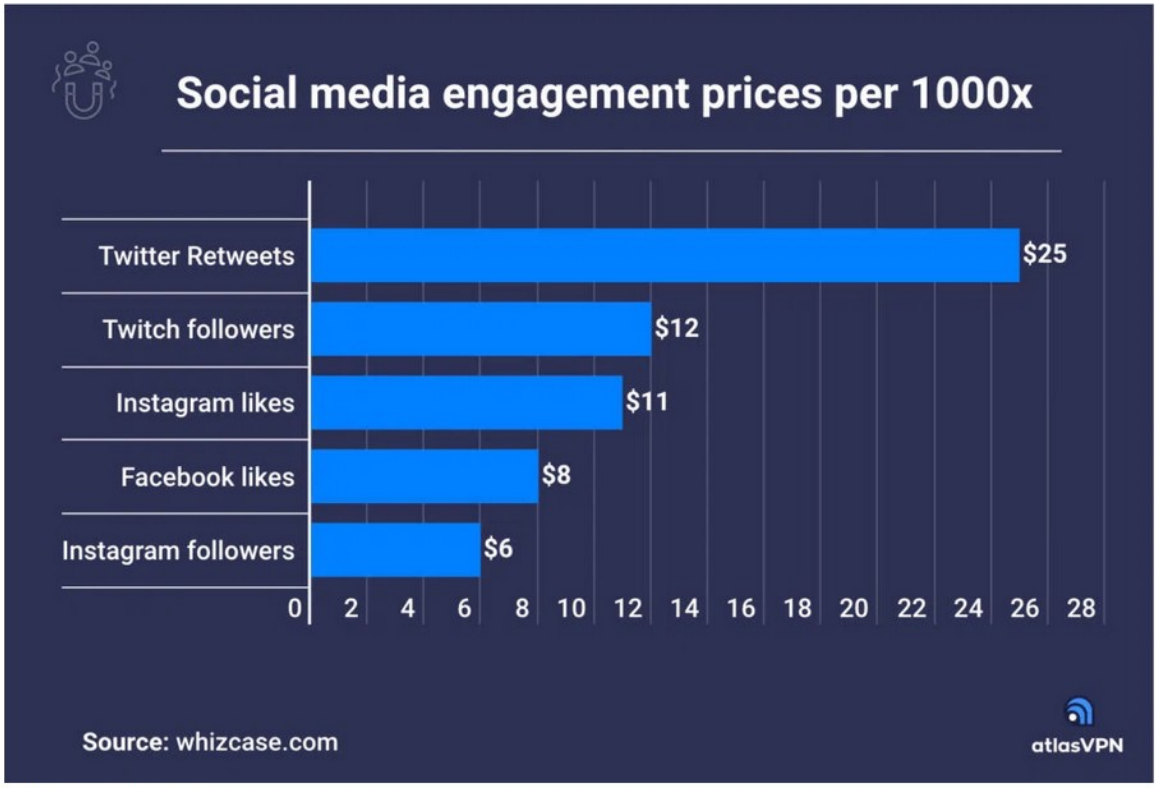
On remonte la liste avec TikTok, Pinterest et Twitter qui sont vendus pour 10 dollars ou moins. Les comptes Snapchat, Instagram, Discord et Facebook ont un peu plus de valeur, sans dépasser les 14 dollars. En revanche, **il faudra débourser approximativement 45 dollars pour acquérir un compte LinkedIn**. Cela n'a rien de surprenant dans la mesure où il touche une clientèle professionnelle, ce qui pour les personnes mal intentionnées ouvre la porte à des gains potentiels plus importants.

Des prix très accessibles qui permettent de vendre des dizaines, voire des centaines de milliers de comptes, pour un coût relativement faible. Ces comptes vendus illégalement se trouvent sur les réseaux cryptés du Dark Web qui nécessitent un logiciel spécial pour y accéder. Les cybercriminels se protègent également en exigeant une invitation pour rentrer sur la plupart de ces places de marché.

Que font les pirates avec les comptes sociaux piratés ?

Les données d'utilisateurs sont régulièrement volées et mises en vente sur le Dark Web. Parmi elles, des comptes sociaux piratés sont utilisés pour créer des « fermes de robots » qui ont pour objectif de manipuler l'engagement sur les réseaux sociaux. Une activité bien plus lucrative que de vendre en direct les comptes.

Ainsi, **1 000 retweets d'un post Twitter coûteraient environ 25 dollars**. Obtenir des followers sur Twitch serait actuellement le deuxième type d'engagement le plus coûteux : 12 dollars pour mille, toujours. Suivent les likes et followers sur Instagram et Facebook. Quelques dollars supplémentaires permettent de choisir le pays d'origine de ces engagements.



© Whizcase et atlasVPN

Ces « vrais » comptes sociaux ont beaucoup plus de valeur que les nouveaux dans la mesure où ils appartiennent à des individus avec un historique d'utilisation. Ainsi, il est beaucoup plus difficile pour les réseaux sociaux d'identifier ce genre de manipulation.

Prudence donc avec l'intérêt que vous accordez aux contenus les plus populaires sur les réseaux sociaux, ils pourraient avoir été créés de toute pièce pour quelques centaines de dollars. Les dégâts causés par le piratage de comptes sociaux peuvent malheureusement aller beaucoup plus loin. Si un compte est associé à une méthode de paiement, les pirates peuvent effectuer des achats en ligne.

On pense également à la demande d'argent à des amis qui sont plus enclins à vous faire confiance. Pour les professionnels qui font de la publicité payante sur les réseaux sociaux, les conséquences peuvent aussi être désastreuses. La prudence reste donc de mise.

Il faut vraiment que vous arrêtiez d'aller sur les réseaux sociaux avec votre ordi pro

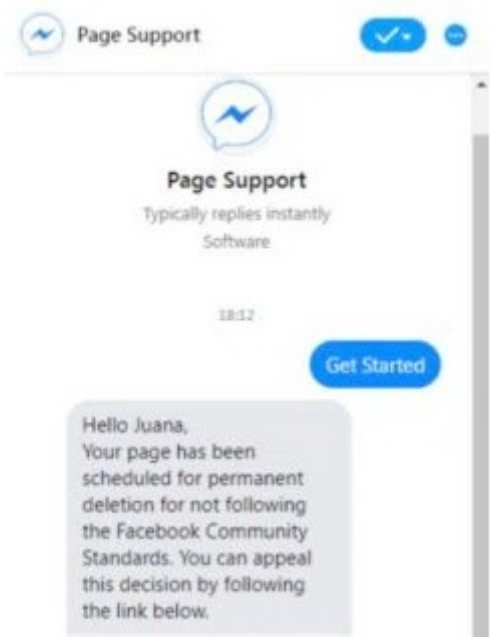
On sait que vous le faites

Bogdan Bodnar, NUMERAMA
Publié le 23 octobre 2022 à 20h05

Si les cyberattaques contre les entreprises sont aussi fréquentes, c'est aussi parce que les employés ont multiplié les portes d'entrées pour les hackers. Ouvrir un fichier malveillant depuis un compte perso sur un ordi pro, c'est prendre le risque d'exposer toute sa société.

Votre ordinateur pro vous sert à travailler puis à traîner sur Instagram le soir ? Félicitations, vous facilitez la tâche des hackers. De nombreux groupes de pirates cherchent à approcher les employés depuis les réseaux sociaux pour voler ensuite tous les identifiants d'entreprises. Le 13 octobre 2022, une nouvelle opération de phishing destiné à dérober des comptes Facebook Business a été révélée. Ces hackers mènent une campagne – baptisée Ducktail par l'entreprise WithSecure – ciblant des employés imprudents depuis des mois à travers le monde entier.

Une fois le fichier malveillant ouvert, les malfaiteurs ont la possibilité de récupérer toutes les données enregistrées, y compris les identifiants, pour s'attaquer ensuite aux comptes professionnels.



Une capture d'écran d'un chatbot frauduleux. Ce dernier invite l'utilisateur à taper ses identifiants et son numéro de téléphone. // Source : Trustwave

Difficile de se montrer sévère avec les employés, avec le télétravail qui a effacé toutes séparations entre usage privé et professionnel. Les pauses se font au salon, il n'y a personne pour surveiller si l'on traine sur les réseaux sociaux. Et, pourquoi changer

d'ordinateur si l'on a déjà Netflix sur le très performant MacBook prêté par la boîte ? L'entreprise Yubico, spécialiste dans la sécurité des objets informatiques, révèle dans un sondage que 57 % des personnes interrogées utilisent un appareil fourni par leur entreprise pour leurs loisirs.

Les sites les plus consultés pendant les heures de travail ? Twitter à près de 50%, suivi de Spotify et Facebook, selon un rapport de WithSecure. Au même moment, les attaques par ransomware explosent : les signalements ont augmenté de 255 % en 2020, indique l'ANSSI.

Les hackers criminels ont immédiatement compris l'aubaine que représentent des centaines de millions d'employés affalés sur leur canapé avec, entre les mains, une porte d'entrée vers tous les dossiers sensibles d'une entreprise.

Diversifier les mots de passe, une première étape essentielle

Maintenant que l'on a exposé le pire scénario envisageable, que faut-il faire ? Se déconnecter de tous les réseaux sociaux ? Fermer son ordinateur une fois la journée terminée ? Ce serait un bon moyen d'éviter les cyberattaques, mais la réalité n'est pas aussi simple.

LinkedIn est, par exemple, une plateforme essentielle pour de nombreux employés, tout en étant un terrain de chasse pour de nombreux malfaiteurs qui cherchent à tromper leurs victimes en se faisant passer pour des recruteurs. La prudence reste la principale recommandation. Évitez d'ouvrir des fichiers douteux et pour réduire les chances de tomber dessus, il vaut mieux réduire la fréquentation des réseaux sociaux ou de sa boite mail personnelle.

Diversifier ses mots de passe est tout aussi essentiel. Si un pirate parvient à dérober l'un de vos codes, il tentera sur le champ d'utiliser cette même combinaison pour d'autres applications. À ce sujet, il est assez ironique de constater que c'est la génération Z qui est moins sensible à la sécurité du mot de passe : 15 % des baby boomers maintiennent le même code secret pour tous les comptes contre 30 % des plus jeunes. C'est une chose d'utiliser les nouveaux outils numériques, encore faut-il en comprendre tous les enjeux.

TÉMOIGNAGE. « Tout est parti d'un SMS » Kelly, victime d'une arnaque téléphonique qui explose

SMS frauduleux, appels abusifs… Les cybercriminels ne manquent pas de techniques ni de créativité pour s'en prendre à votre argent. Les signalements d'arnaques téléphoniques sont en pleine recrudescence. Kelly Boujnah, 34 ans, en a fait les frais. Elle raconte comment en moins d'une heure, elle a perdu 1 500 euros.

Ouest France

Camille Da Silva – 23 octobre 2022

Vous en avez sûrement reçu quelques-uns, voire des dizaines : ces SMS vous indiquant qu'il est urgent de mettre à jour votre carte Vitale, que votre colis doit être affranchi ou que les impôts souhaitent vous rembourser.

Toujours accompagnés d'un lien sur lequel il est tentant de cliquer, et suivis d'appels téléphoniques : des interlocuteurs charmants, qui se disent agents de la Sécurité sociale ou encore conseillers bancaires. Derrière ces démarchages crédibles, se cachent des arnaques bien huilées, très juteuses, qui ne comptent plus leurs victimes.

« Je ne me suis doutée de rien »

Kelly Boujnah, 34 ans, en a fait les frais. En janvier, cette mère de famille, créatrice de joaillerie, s'est fait soutirer la coquette somme de 1 500 €. Et tout a commencé « **bêtement** », avec un simple SMS : « **On me proposait de renouveler ma carte Vitale,** raconte cette Lyonnaise, la voix encore empreinte de colère. **Je clique sur le lien et j'arrive sur un site qui ressemble trait pour trait à celui de la Sécurité sociale.** »

Elle n'y voit que du feu, et entre ses identifiants. « **Ils me proposent de me faire livrer ma carte Vitale pour quelques euros et je donne mes coordonnées bancaires. Avec du recul, je trouve ça complètement débile. Mais c'est un enchaînement d'inattentions : j'étais fatiguée, je voulais que ça aille vite… Je ne me suis doutée de rien.** »

Le lendemain soir, son téléphone sonne : « **Au bout du fil, la personne se présente comme une agente de ma banque faisant partie d'un service dédié aux arnaques.** » L'agente, à la voix angélique, l'informe qu'elle a remarqué un mouvement anormal sur son compte : un achat de 600 €.

Le cœur de Kelly s'emballe, elle ne comprend pas. « **Elle me demande si j'ai récemment cliqué sur un SMS de la Sécurité sociale, que c'est une arnaque courante, qu'ils ont piraté ma carte. À ce moment-là, je lui fais confiance parce qu'elle connaît tout de moi et de mes comptes. Mais en fait, c'est elle l'arnaqueuse.** »

1 500 € dérobés en moins d'une heure

La prétendue banquière l'informe que les voleurs tentent de faire plusieurs paiements. Des sommes toujours plus importantes. Elle lui dit qu'il faut agir vite et lui demande d'ouvrir son application pour valider des opérations, afin de bloquer ces transactions. Mais en réalité, Kelly est en train d'accepter les débits et ouvre la porte de ses comptes à l'arnaqueuse.

Au bout d'une heure d'échange, la trentenaire raccroche. Mais dans les jours qui suivent, elle ressasse l'appel et un virement anormal lui met la puce à l'oreille. Dans le bureau de sa véritable conseillère, elle comprend qu'un piège s'est refermé sur elle. Elle fait opposition, mais c'est trop tard : 1 500 € se sont envolés. « **Je suis cheffe d'entreprise, je travaille sur le numérique, je ne suis pas née de la dernière pluie, mais là… C'est tellement bien fait et ça va tellement vite, qu'on tombe dedans. Ça peut arriver à tout le monde.** »

Kelly a porté plainte et est entrée en bras de fer avec sa banque, qui refuse de la rembourser. Elle n'y est légalement pas tenue, la Lyonnaise ayant accepté de son propre chef l'accès à ses comptes. « **Ils disent que c'est ma faute. Je suis très en colère, il n'y a personne pour m'aider.** »

Sécurité, assurance-chômage, retraite… Pensez-vous qu'Emmanuel Macron pourra mener à bien ses réformes ?

Un principe de « pêche au filet »

Le cas de Kelly est loin d'être isolé. Elle a été victime d'une arnaque « **en explosion** », comme l'explique Jean-Jacques Latour, directeur expertise cybersécurité pour *cybermalveillance.gouv.fr.* « **Plus ce type d'arnaque se répand, plus c'est un signe qu'elle est rentable.** »

Les cybercriminels utilisent chaque fois le même mode opératoire : tout commence par un SMS accompagné d'un lien. Ce principe d'arnaque pour soutirer des informations existe depuis des années, et s'appuie sur le principe de pêche au filet : viser un très grand nombre de victimes, au hasard, en espérant en toucher au moins une partie.

Mais depuis l'an dernier, alors que ces vagues d'attaques étaient habituellement épisodiques, elles sont devenues « **incessantes** », observe l'expert. La raison ? **« La mise en application de la directive européenne DSP2, qui veut que toute une quantité**

d'opérations réalisées en ligne soit confirmée par un code secret ou une validation sur l'application de sa banque. Les cybercriminels sont donc bloqués. »

Alors, nouveauté : une fois vos informations hameçonnées par SMS, les pirates du Net vous appellent et se font passer pour des conseillers car ils ont besoin de vous pour agir sur vos comptes. Parfois, ils vont jusqu'à vous appeler en utilisant le numéro officiel de votre banque. Chose que **« n'importe qui peut faire avec un petit logiciel sur son ordinateur. Des gens plongent tous les jours et ça ne fait qu'augmenter. Les sommes soutirées se comptent souvent en milliers d'euros. »**

« Ce n'est pas le petit arnaqueur du coin »

Difficile de dire qui se cache derrière ces cyberattaques. D'après les quelques arrestations, il s'agit plutôt de Français, âgés de 20 à 30 ans, qui opèrent depuis des pays francophones. Ils sont organisés, travaillent en équipe et vivent parfois dans le luxe. « **Ce n'est pas le petit arnaqueur du coin qui fait ça dans sa cave. Ce sont des gens qui industrialisent la fraude et en font un business.** »

Un beau pactole, avec au départ, un simple SMS. Mais comment ont-ils accès à nos données ? « Votre numéro de téléphone, vous l'avez donné sur des dizaines de sites, pointe Jean-Jacques Latour. Et ces sites ont pu être attaqués ou avoir revendu leurs données. Des fichiers avec des noms, des numéros et des adresses e-mails, il y en a une palanquée qui circule sur le *darknet*, l'Internet des cybercriminels. »