FINANCES PUBLIQUES

J. 20 1372

CONCOURS EXTERNE POUR L'ACCÈS AU GRADE D'INSPECTEUR DES FINANCES PUBLIQUES AFFECTÉ AU TRAITEMENT DE L'INFORMATION EN QUALITÉ DE PROGRAMMEUR DE SYSTÈME D'EXPLOITATION

ANNÉE 2021

_____

ÉPREUVE ÉCRITE D'ADMISSIBILITÉ N° 1

Durée : 4 heures – Coefficient : 4

_____

Rédaction d'une note de synthèse à partir d'un dossier relatif aux questions économiques et financières

_____

Toute note inférieure à 5/20 est éliminatoire.

_____

Recommandations importantes

Le candidat trouvera au verso la manière de servir la copie dédiée.

Sous peine d'annulation, en dehors du volet rabattable d'en-tête, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tels que nom, prénom, signature, paraphe, localisation, initiale, numéro ou toute autre indication, même fictive, étrangère au traitement du sujet.

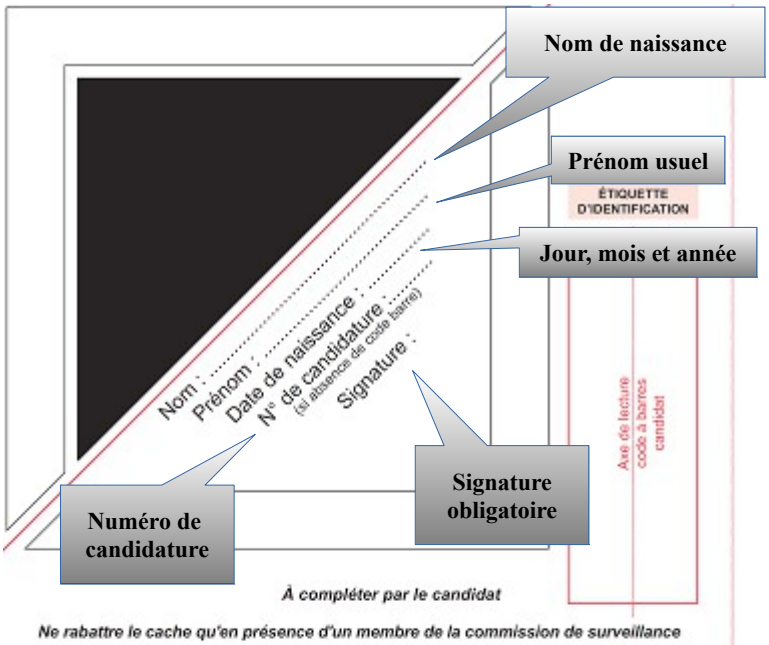
Sur les copies, les candidats devront écrire et souligner si nécessaire au stylo bille, plume ou feutre de couleur noire ou bleue uniquement. De même, l'utilisation de crayon surligneur est interdite.

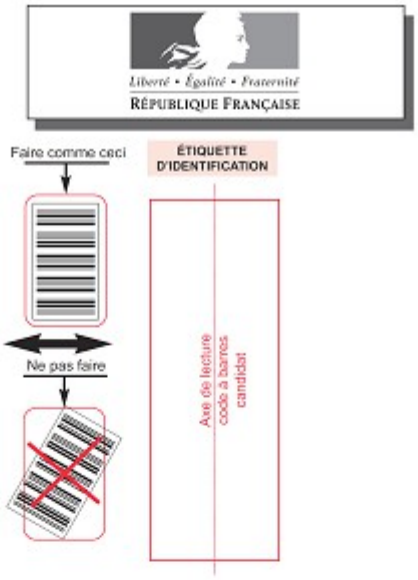
Il devra obligatoirement se conformer aux directives données.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Tournez la page S.V.P.

Le candidat complétera l'intérieur du volet rabattable des informations demandées et se conformera aux instructions données





Concours externe - interne - professionnel - ou examen professionnel (1)
(1) Rayer les mentions inutiles

Externe

Pour l'emploi de : **Inspecteur des Finances Publiques affecté au traitement de l'information en qualité de programmeur de système d'exploitation**

Épreuve n° : **1**

Matière : **006 – Rédaction d'une note de synthèse**

Date : **19 11 20 20**

Nombre d'intercalaires supplémentaires :

Préciser éventuellement le nombre d'intercalaires supplémentaires

À L'ATTENTION DU CANDIDAT

En dehors de la zone d'identification rabattable, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tel que nom, prénom, signature, paraphe, localisation, initiale, numéro, ou toute autre indication même fictive étrangère au traitement du sujet.

Il est demandé aux candidats d'écrire et de souligner si nécessaire au stylo bille, plume ou feutre, de couleur noire ou bleue uniquement. Une autre couleur pourrait être considérée comme un signe distinctif par le jury, auquel cas la note de zéro serait attribuée. De même, l'utilisation de crayon surligneur est interdite.

Les étiquettes d'identification codes à barres, destinées à permettre à l'administration d'identifier votre copie, ne doivent être détachées et collées dans les deux cadres prévus à cet effet qu'en présence d'un membre de la commission de surveillance.

Suivre les instructions données pour les étiquettes d'identification

NOTE / 20 ,

RÉSERVÉ À L'ADMINISTRATION

À L'ATTENTION DU CORRECTEUR

Pour remplir ce document :
Utilisez un stylo ou une pointe feutre de couleur NOIRE ou BLEUE.

EXEMPLE DE MARQUAGE : Faire comme ceci — Ne pas faire

Pour porter votre note, cochez les gélules correspondantes.

Reportez la note dans les zones NOTE / 20 et dans le cadre A

En cas d'erreur de codification dans le report des notes cochez la case erreur et reportez la note dans le cadre B.

Cadre A réservé à la notation		
20	19	18
17	16	15
14	13	12
11	10	09
08	07	06
05	04	03
02	01	00
Décimales		
,00	,25	,50 ,75

Cadre B réservé à la notation rectificative		
20	19	18
17	16	15
14	13	12
11	10	09
08	07	06
05	04	03
02	01	00
Décimales		
,00	,25	,50 ,75
Erreur		

NOTE / 20 ,

EN AUCUN CAS, LE CANDIDAT NE FERMERA LE VOLET RABATTABLE AVANT D'Y AVOIR ÉTÉ AUTORISÉ PAR LA COMMISSION DE SURVEILLANCE

FINANCES PUBLIQUES

SUJET

RÉDACTION D'UNE NOTE DE SYNTHÈSE À PARTIR D'UN DOSSIER RELATIF AUX QUESTIONS ÉCONOMIQUES ET FINANCIÈRES

Code matière : 006

Les candidates et les candidats peuvent avoir à leur disposition sur la table de concours le matériel d'écriture, une règle, un correcteur, des surligneurs.

À l'aide des seuls documents joints, vous rédigerez une note de synthèse relative à la cybersécurité et à ses enjeux notamment économiques.

Vous rédigerez ensuite, à l'aide de vos connaissances personnelles, une note de propositions de deux pages au maximum visant à renforcer la protection des entreprises les plus vulnérables face aux risques accrus de cybercriminalité.

Tournez la page S.V.P.

Liste des documents

Document n° 1	Déclaration de M. Laurent Nunez, secrétaire d'État auprès du Ministre de l'Intérieur, sur la cybersécurité à Lille – Extraits Source : Site www.vie-publique.fr – 22 janvier 2019	(3 pages)
Document n° 2	RISQUES : Prévention des risques majeurs – Extraits Source : Site www.gouvernement.fr – article non daté	(3 pages)
Document n° 3	Communiqué de presse, Précautions élémentaires, Guide des bonnes pratiques de l'informatique et Glossaire – Extraits Source : Site de l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI)	(4 pages)
Document n° 4	Plus de 7 entreprises sur 10 ont subi au moins une tentative de fraude en 2019 Source : Site www.forbes.fr – Maurice Midena – 13 mai 2020	(3 pages)
Document n° 5	Demain : les enjeux de la cybersécurité pour les PME et ETI – Extrait Source : Site www.bpifrance.fr – 01 juillet 2019	(1 page)
Document n° 6	Les gestes barrières numériques, meilleurs remparts face à l'explosion de la cybercriminalité Source : Site www.usinenouvelle.com – Hassan Meddah – 05 mai 2020	(2 pages)
Document n° 7	Cybersécurité : risques et enjeux économiques – Extraits du Rapport moral sur l'argent dans le monde Source : Site de l'Association d'Économie Financière – Nicolas Arpagian – 2015-2016	(3 pages)
Document n° 8	La cybersécurité : quelles réponses aux menaces nouvelles ? – Extrait Source : Site www.vie-publique.fr – 28 janvier 2019	(3 pages)
Document n° 9	Cyberdéfense : la France se dote d'une nouvelle doctrine militaire Source : Site Europe 1 – 18 janvier 2019	(1 page)
Document n° 10	Rapport d'information déposé par la Commission des Affaires Européennes sur l'avenir de la cybersécurité européenne – Extrait Source : Site de l'Assemblée nationale – Eric Bothorel – 14 novembre 2019	(2 pages)

Le fonds documentaire comporte 25 pages.

Déclaration de M. Laurent Nunez, secrétaire d'État auprès du Ministre de l'Intérieur, sur la cybersécurité à Lille – Extraits

Source : Site www.vie-publique.fr – 22 janvier 2019

(...)

Mesdames Messieurs,

C'est un plaisir pour moi d'ouvrir pour la première fois, en tant que membre du gouvernement, ce Forum International de la Cybersécurité, cette 11ème édition du FIC. Lille est à l'intersection de nombreuses voies européennes, physiques et numériques. Ce matin plus encore avec ce rendez-vous devenu incontournable pour les acteurs mondiaux de la cybersécurité. (...)

Si nous sommes rassemblés ce matin, c'est que nous partageons la conviction que la cybersécurité constitue un enjeu majeur pour nos sociétés.

Cet enjeu n'est d'ailleurs pas nouveau. Je suis certain que dès le 1er FIC en 2007, nous parlions déjà des escroqueries en ligne. Elles se sont malheureusement bien améliorées depuis, et les mails en mauvais français facilement détectables sont plus rares. En revanche, les techniques de *phishing* sont plus sophistiquées, elles permettent aussi de toucher davantage de personnes, augmentant ainsi l'espérance de gain. Elles restent d'actualité pour nous tous.

De même, pour les attaques de système d'information. Le premier FIC fêtait quasiment les 10 ans de la loi Godfrain qui les réprimait. Et pour autant, cet enjeu est toujours bien présent et se renouvelle en raison d'une plus grande connectivité des systèmes, de la multiplication des terminaux de tous types, d'une limite usage privé / usage professionnel plus ténue, du développement des services en ligne. Cette interdépendance est une force mais aussi une vulnérabilité.

D'autres défis sont plus récents.

2018 s'est ainsi achevée comme 2017 avec un haut niveau de cyberattaques, entraînant des fuites importantes de données professionnelles et personnelles. Ces fuites ont concerné une personne sur 12, oui je dis bien une personne sur 12, ce qui a fait de 2018 une année terrible.

La semaine dernière, nous apprenions l'existence d'une base de données comprenant jusqu'à 772 millions d'adresses mail piratées et plus de 20 millions de passeports. Cela interroge chacun d'entre nous sur sa propre sécurité et la protection de ses données.

La mise en œuvre du RGPD (Règlement Général sur la Protection des Données) et de la directive européenne NIS (*Security of Network and Information System*) devrait aider tous acteurs à mieux se protéger. On désigne des secteurs et des opérateurs de services essentiels qui doivent renforcer leur sécurité et alerter l'ANSSI, laquelle doit veiller à diffuser ces éléments auprès des services spécialisés de répression comme de renseignement.

Le développement du *darkweb* constitue également un défi, en ce qu'il permet le développement de marchés criminels en ligne. Ces nouveaux espaces proposent à la vente des stupéfiants, des armes, des médicaments, des codes de cartes bancaires, mais aussi des outils informatiques malveillants. Réservés aux initiés dans un premier temps, ils sont désormais plus facilement accessibles pour une génération « *digital native* ». Ils permettent en outre une navigation anonyme.

Mais, ce ne peut rester un espace sans droit. Les enquêtes doivent pouvoir s'y déployer et je salue à cet égard le recours grandissant aux enquêtes sous pseudonyme par la police et la gendarmerie. Des enquêtes judiciaires récentes ont montré l'intérêt de ces investigations.

Aux confins de la problématique cyber et dans son articulation avec les réseaux sociaux et son rôle de véhicule d'information, le cyber devient également une arme de manipulation des opinions. Je pense à la diffusion virale de *fake news*. La proximité d'échéances électorales est à ce titre un sujet de préoccupation.

Pour remédier à cette propagation, le Gouvernement a fait adopter une nouvelle législation le 20 novembre 2018 avec une loi ordinaire sur la manipulation de l'information et une loi organique applicable à l'élection présidentielle. C'est une réponse à la fois mesurée mais ferme par rapport à ceux qui voudraient fragiliser notre société et intervenir dans notre système électoral.

Une autre forme de défi nouveau : l'internet des objets et la 5G. Prenons l'exemple de la voiture connectée – voiture autonome. C'est, du point de vue de la cybersécurité, un challenge en termes de sécurité de la conduite, de protection des données personnelles, de risque de piratage des nombreux objets qui s'y connectent à commencer par nos propres smartphones. La multiplication de ces objets dans notre vie quotidienne, dans notre vie professionnelle exige une vraie sécurité. Par construction, mais encore plus à cause de failles de sécurité.

La sécurité doit être intégrée dès la conception des produits et des applications, c'est la *Security by design* comme s'est imposée la *Privacy by design*. Tel est le double thème que vous avez choisi pour ce forum international, qui reflète ainsi deux impératifs forts du ministère de l'Intérieur, garantir la sécurité et protéger les libertés. (...)

Nos dispositifs de lutte contre les arnaques et les escroqueries en ligne, tout d'abord, évoluent. Au-delà de la traditionnelle plainte au commissariat de police ou à la brigade de gendarmerie – qui reste possible –, nous proposons désormais aux victimes d'usage frauduleux d'une carte bancaire une plateforme de signalement : la plateforme PERCEVAL, opérée par la gendarmerie nationale.

Facile d'accès, rapide, elle simplifie les démarches des victimes. Parce qu'elle permet de recueillir un grand nombre de signalements, elle apporte une vue plus complète des phénomènes de fraude et permet d'améliorer la détection des fraudes massives.

En 6 mois, elle a recueilli 69 000 signalements, pour un préjudice total de 33 M€. Autant de victimes qui ont pu faire valoir leurs droits.

Mais aussi, des rapprochements qui se sont traduit par l'ouverture de 55 enquêtes judiciaires et l'identification à ce stade d'une trentaine d'auteurs. (...)

Ainsi, la police nationale a créé un réseau de référents cyber zonaux à titre expérimental sur trois régions pilotes, Grand-Est, Bretagne et Nouvelle Aquitaine, pour sensibiliser le tissu économique local au risque cyber ainsi qu'à la délinquance financière par l'animation d'un réseau partenarial zonal et local entre les services de police judiciaire et le secteur privé. En effet, je le rappelle 63 % des cyberattaques ciblent des entreprises.

Mais ces agents, ce sont aussi des enquêteurs sur le volet répressif.

Et ces enquêteurs cyber ont besoin d'être formés. Des efforts importants sont réalisés pour cela. J'ai ainsi remis, il y a quelques instants, les diplômes délivrés par l'université de Troyes à 6 enquêteurs NTECH (lire « N » « Tech ») de la gendarmerie nationale, issu de la dernière promotion. Formés à haut niveau, ils sont directement employables pour réaliser des enquêtes cyber ou des actes de criminalistique numérique. Je salue à cet égard l'action résolue du centre de lutte contre les criminalités numériques de la gendarmerie – le C3N – et du réseau Cybergend qui fédère à ce jour plus de 4 500 enquêteurs numériques à travers tout le territoire, effectif que nous souhaitons doubler d'ici 2022.

Sur la méthode, nous évoluons également, en privilégiant les partenariats, à l'instar du Centre de réponse à incident créé au sein de la police judiciaire pour anticiper les menaces cyber et soutenir

les actions judiciaires contre la cybercriminalité. Il est devenu un vecteur de coopération technique en matière de cybersécurité et a rejoint la communauté européenne des centres de réponse à incident animé par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Il a noué des partenariats forts avec plusieurs acteurs du secteur privé français spécialisés notamment dans le conseil, les antivirus, l'analyse de données, ou la lutte contre le *phishing*.

(…)

Tournez la page S.V.P.

RISQUES : Prévention des risques majeurs – Extraits

Source : Site www.gouvernement.fr – article non daté

RISQUES CYBER

Une cyber-attaque est une atteinte à des systèmes informatiques réalisée dans un but malveillant. Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des appareils communicants comme les téléphones mobiles, les smartphones ou les tablettes. Il existe 4 types de risques cyber aux conséquences diverses, affectant directement ou indirectement les particuliers, les administrations et les entreprises : la cybercriminalité, l'atteinte à l'image, l'espionnage, le sabotage.

CYBERCRIMINALITÉ

En pleine recrudescence, de nombreuses attaques ciblent les particuliers mais aussi les entreprises et les administrations. Elles visent à obtenir des informations personnelles afin de les exploiter ou de les revendre (données bancaires, identifiants de connexion à des sites marchands, etc.). Hameçonnage (*phishing*) et « Rançongiciel » (*ransomware*) sont des exemples connus d'actes malveillants portant préjudices aux internautes. Pour s'en prémunir, des réflexes simples existent.

Quels sont les différents types d'attaques ?

Attaque par hameçonnage (phishing)

L'hameçonnage, *phishing* ou filoutage est une technique malveillante très courante sur Internet. L'objectif : opérer une usurpation d'identité afin d'obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel.

1. Le cybercriminel se « déguise » en un tiers de confiance (banques, administrations, fournisseurs d'accès à Internet…) et diffuse un mail frauduleux, ou contenant une pièce jointe piégée, à une large liste de contacts. Le mail invite les destinataires à mettre à jour leurs informations personnelles (et souvent bancaires) sur un site internet falsifié vers lequel ils sont redirigés.
2. La liste comprend un nombre si important de contacts et augmente les chances que l'un des destinataires se sente concerné par le message diffusé.
3. En un clic, il est redirigé vers le site falsifié qui va recueillir l'ensemble des informations qu'il renseigne.
4. Ces informations sont alors mises à disposition du cybercriminel qui n'a plus qu'à faire usage des identifiants, mots de passe ou données bancaires récupérées.

(…)

Attaque par « rançongiciel » (ransomware)

Les rançongiciels sont des programmes informatiques malveillants de plus en plus répandus (ex : Locky, TeslaCrypt, Cryptolocker, etc.). L'objectif : chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

1. Le cybercriminel diffuse un mail qui contient des pièces jointes et / ou des liens piégés. Le corps du message contient un message correctement rédigé, parfois en français, qui demande de payer rapidement une facture par exemple.

2. En un clic, le logiciel est téléchargé sur l'ordinateur et commence à chiffrer les données personnelles : les documents bureautiques (.doc, .xls, .odf…etc), les photos, la musique, les vidéos…etc.
3. Les fichiers devenus inaccessibles, un message s'affiche pour réclamer le versement d'une rançon, payable en bitcoin ou via une carte prépayée, en échange de la clé de déchiffrement. Attention, rien n'indique que le déchiffreur en question soit efficace !

Pour s'en prémunir :

– N'ayez pas une confiance aveugle dans le nom de l'expéditeur de l'e-mail. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.

– Méfiez-vous des pièces jointes, elles pourraient être contaminées. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.

– Ne répondez jamais à une demande d'informations confidentielles par mail.

– Passez votre souris au-dessus des liens, faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français ou de la langue pratiquée par votre interlocuteur (ex : orthographe).

– Effectuez des sauvegardes régulièrement sur des périphériques externes.
– Mettez à jour régulièrement tous vos principaux logiciels en privilégiant leur mise à jour automatique.

(...)

ATTEINTE À L'IMAGE

Lancées à des fins de déstabilisation contre des administrations et des entreprises et régulièrement relayées par les réseaux sociaux, les attaques de déstabilisation sont aujourd'hui fréquentes et généralement peu sophistiquées, faisant appel à des outils et des services disponibles en ligne. De l'exfiltration de données personnelles à l'exploitation de vulnérabilité, elles portent atteinte à l'image de la victime en remplaçant le contenu par des revendications politiques, religieuses, etc.

(...)

ESPIONNAGE

Très ciblées et sophistiquées, les attaques utilisées pour l'espionnage à des fins économiques ou scientifiques sont souvent le fait de groupes structurés et peuvent avoir de lourdes conséquences pour les intérêts nationaux. De fait, il faut parfois des années à une organisation pour s'apercevoir qu'elle a été victime d'espionnage, l'objectif de l'attaquant étant de maintenir discrètement son accès le plus longtemps possible afin de capter l'information stratégique en temps voulu.

Quels sont les différents types d'attaques ?

Les modes opératoires de ces attaques rappellent ceux que les analystes américains ont baptisé APT (*Advanced Persistent Threat*) et qui touchent régulièrement des institutions et des industriels œuvrant dans des secteurs sensibles. Nombre de ces attaques sont très similaires, tant par leurs modes opératoires que par les techniques d'infiltration et d'exfiltration employées.

Attaque par point d'eau (watering hole)

La technique du « point d'eau » consiste à piéger un site Internet légitime afin d'infecter les équipements des visiteurs du secteur d'activité visé par l'attaquant. Objectif : infiltrer discrètement les ordinateurs de personnels œuvrant dans un secteur d'activité ou une organisation ciblée pour

récupérer des données.

1. Le cybercriminel exploite une vulnérabilité d'un site web et y dépose un virus (*malware*). Le site qui sert d' « appât » est choisi spécifiquement pour attirer la victime ciblée par l'attaque in fine.
2. La victime ciblée est incitée à se rendre ou est redirigée automatiquement sur le site contaminé. Son navigateur exécute alors le malware et l'installe à son insu sur ces appareils (ordinateur, téléphone). Le cybercriminel dispose alors d'un accès total ou partiel à l'appareil infecté.
3. Le cybercriminel demeure discret afin de capter le plus longtemps possible des données.

Pour s'en prémunir :

– Mettez à jour régulièrement tous vos principaux logiciels, notamment ceux en charge du filtrage du web.

– Effectuez des sauvegardes régulières sur des périphériques externes (ex : disque dur).

(…)

SABOTAGE

Le sabotage informatique est le fait de rendre inopérant tout ou partie d'un système d'information d'une organisation via une attaque informatique.

Quels sont les différents types d'attaques ?

Le sabotage s'apparente à une « panne organisée », frappant tout ou partie des systèmes, selon le type d'atteinte recherchée – désorganisation durable ou non, médiatisée ou non, plus ou moins coûteuse à réparer. Pour y parvenir, les moyens d'attaques sont d'autant plus nombreux que les organisations ne sont pas toujours préparées à faire face à des actes de malveillance. Le sabotage et la destruction de systèmes informatiques peuvent avoir des conséquences dramatiques sur l'économie d'une organisation, sur la vie des personnes, voire sur le bon fonctionnement de la Nation s'ils touchent des secteurs d'activité clés. Afin d'éviter ce type de menace, l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information, met l'accent sur la prévention.

À ce titre, elle :

- publie des recommandations de sécurité ;
- labellise des produits et des prestataires de confiance ;
- définit une réglementation permettant à l'administration et aux entreprises de sécuriser efficacement leurs systèmes d'information (Loi de programmation militaire).

Vous êtes victime ?

Suite à une escroquerie ou une cyberattaque, déposez plainte auprès d'un service de Police nationale ou de Gendarmerie nationale ou bien adressez un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

Consultez le site CYBERMALVEILLANCE.GOUV.FR du dispositif national d'assistance aux victimes de cybermalveillance, qui met à disposition des fiches conseil pour se prémunir et réagir face aux attaques informatiques les plus courantes et qui peut vous mettre en relation avec des prestataires de services informatiques de proximité susceptibles de vous aider à remettre votre système en état de fonctionnement suite à une attaque.

Communiqué de presse, Précautions élémentaires, Guide des bonnes pratiques de l'informatique et Glossaire – Extraits

Source : Site de l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI)

L'ANSSI célèbre ses dix ans et affirme ses nouvelles ambitions – Communiqué de presse – Paris – 04 juin 2019

Le 4 juin 2019, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) rassemble l'ensemble de l'écosystème du numérique au Ground Control, à Paris, pour célébrer ses 10 ans d'existence. L'occasion pour l'agence d'esquisser les contours de l'ANSSI de demain, vouée à davantage s'ouvrir et s'orienter vers l'innovation. Une transformation tournée vers la formation, le partage de la donnée technique et la co-construction avec les écosystèmes régaliens, de la recherche et du numérique.

10 ANS D'ACTION DE L'ANSSI

Créée en 2009, l'ANSSI a vu ses missions, son périmètre d'action et la liste de ses bénéficiaires s'élargir, au point de devenir la référence en matière de cybersécurité en France. Ces dix années ont connu des cyberattaques retentissantes, celle de TV5 Monde en 2015, mais également les attaques Wannacry et NotPetya en 2017. Au fur et à mesure, la menace a profondément évolué, pour devenir de plus en plus sophistiquée, mieux élaborée et plus destructrice. C'est face à cette menace que s'est construite l'ANSSI, en renforçant ses capacités opérationnelles au bénéfice des victimes, mais également en approfondissant son analyse et sa compréhension de la menace.

Ces dix dernières années, l'ANSSI a également déployé une série de chantiers de plus en plus ambitieux. En 2013, la France est devenue le premier pays à imposer des exigences de cybersécurité sur ses infrastructures critiques. Puis en 2016, la directive Network and Information Security (NIS) a positionné l'Union européenne en pointe en matière de cybersécurité. L'ANSSI a ainsi développé des relations fortes et de confiance avec les opérateurs d'importance vitale (OIV), puis avec les opérateurs de services essentiels (OSE). Sur le plan international, en 2017, la France a organisé la première conférence visant à promouvoir la stabilité du cyberespace et a présenté la stratégie française de cyberdéfense. En dix ans, l'agence a prouvé la pertinence du modèle français, séparant les activités défensives qui lui ont été confiées, des activités cyber offensives.

En tant que prescripteur, l'ANSSI a produit depuis 2009 de nombreux documents techniques, d'organisation et de recommandations pour accompagner et sensibiliser aux bonnes pratiques de sécurité numérique un large panel de publics, experts ou non. Enfin, en lançant ses Visas de sécurité en 2018, l'ANSSI a contribué au rayonnement de l'excellence française en matière d'évaluation de sécurité, basée sur une expérience acquise au fil des années. Pendant dix ans, l'agence n'a cessé de travailler pour faire émerger un écosystème français de cybersécurité de confiance.

L'année 2019 connaît des menaces et usages nouveaux. Face aux enjeux qui se dessinent, **l'ANSSI de demain sera encore davantage ouverte et orientée vers l'innovation.**

« L'ANSSI des dix prochaines années s'inscrira au cœur du paysage du numérique et de l'innovation. Plus que jamais, les acteurs publics doivent susciter l'adhésion, fédérer, accompagner les acteurs privés, académiques et citoyens impliqués sur ces enjeux » affirme Guillaume Poupard, directeur général de l'ANSSI.

Tous connectés, tous impliqués, tous responsables : c'est bien l'ensemble des acteurs régaliens, privés, académiques et citoyens qui construiront ensemble la confiance numérique de demain. *« L'ANSSI accompagne, anime, prescrit, certifie et régule, mais en définitive l'effort de protection doit être fait par tous »* avance Claire Landais, Secrétaire générale de la défense et de la sécurité nationale.

L'ANSSI DE DEMAIN

Miser sur la formation pour relever les défis de la cybersécurité

Le constat est largement partagé : le développement de la sécurité numérique en France, véritable filière d'avenir, est freiné par le déficit de personnes formées. C'est pourquoi la formation sera un axe de travail majeur pour l'ANSSI pour les 10 années à venir. L'agence labellise des formations initiales avec SecNumedu et depuis 2018, les formations continues avec SecNumedu-FC. En complément, l'ANSSI collabore depuis quelques mois avec le ministère de l'Éducation et de la Jeunesse et le ministère des Armées pour intégrer la sécurité numérique à la fois dans les programmes scolaires et dans le futur Service national universel (SNU).

Mieux connaître la menace grâce aux données techniques

Depuis 2019, l'accès et le traitement des données techniques permet à l'ANSSI de renforcer son efficacité en matière de détection. Le défi des prochaines années sera d'inventer les nouveaux moyens et outils pour continuer à être en pointe en matière d'analyse de la menace afin d'anticiper toujours plus les attaques de demain. En complément, l'ANSSI plaide aujourd'hui pour l'ouverture, le partage et la mutualisation responsables de certaines données techniques. Une démarche qui vise à stimuler l'innovation publique et privée et augmenter la connaissance collective de la menace.

Co-construire pour renforcer l'efficacité collective

L'ANSSI, et l'écosystème cyber en général, ont beaucoup à gagner à renforcer les synergies entre les acteurs régaliens, le monde de la recherche et celui du numérique. Cette démarche d'ouverture et d'innovation est ancrée dans l'ADN de l'ANSSI. Ainsi, l'agence souhaite partager son expertise et certains de ses outils avec des startups, des entreprises, petites comme grandes, innovantes en cybersécurité.

Publié à l'occasion du Cyber festival, le guide de Bonnes pratiques à l'usage des professionnels en déplacement, élaboré par l'ANSSI et le ministère de l'Europe et des affaires étrangères illustre cette démarche de co-construction.

En matière de recherche, la création du conseil scientifique, mais également le partenariat renforcé avec Inria, qui verra bientôt le jour, s'inscrivent dans cette logique d'ouverture et de partage. Ces initiatives rapprochent concrètement acteurs régaliens et académiques.

L'ÉCOSYSTÈME FRANÇAIS DE CYBERSÉCURITÉ S'ORGANISE

Pour Cédric O, Secrétaire d'État chargé du Numérique, *« la transformation numérique de notre société et de notre économie se fera en confiance ou ne se fera pas. C'est pourquoi les acteurs français de la cybersécurité (grands groupes, startups, monde de la recherche, administrations…) doivent s'organiser et rassembler leurs forces pour répondre à ce défi essentiel. En particulier, nous allons réfléchir au projet de création d'un grand campus de la cybersécurité qui réunirait l'ensemble de l'écosystème ».*

Cette initiative dédiée à la recherche de synergies doit permettre de renforcer nos capacités d'innovation en matière de cybersécurité. Elle résonne tout particulièrement avec les ambitions d'ouverture de l'ANSSI, qui y apportera tout son soutien.

(…)

Précautions élémentaires – Source ANSSI non datée

La sécurité du numérique est l'affaire de tous. Elle repose avant tout sur des mesures simples et des bonnes pratiques à adopter sans modération dans la sphère privée et professionnelle. Fondées sur le bon sens, ces précautions élémentaires ne peuvent être négligées sans s'exposer à des risques, qui exploitent souvent des vulnérabilités connues.

Se protéger sur Internet n'est plus une option pour les administrations, les entreprises et les particuliers. Pour les accompagner dans leurs usages du numérique, l'ANSSI publie régulièrement des guides de recommandations ainsi que des documents de prévention et de sensibilisation à destination de tous.

Identifier un mail frauduleux, élaborer des mots de passe robustes, mettre à jour vos logiciels, contrôler la diffusion de vos informations personnelles… mais aussi mieux comprendre les techniques utilisées par les cybercriminels et leurs objectifs, c'est agir pour être mieux protégé sur Internet… Pour accompagner la diversité d'utilisateurs et de besoins, l'ANSSI vous propose de nombreux supports d'information ainsi que des campagnes de sensibilisation.

(…)

Guide des bonnes pratiques de l'informatique – Source ANSSI non datée

L'ANSSI et la CPME présentent douze règles essentielles pour la sécurité des systèmes d'information des petites et moyennes entreprises.

Les problématiques rencontrées par les petites et moyennes entreprises pour la sécurité de leurs systèmes d'information sont nombreuses : protection des fichiers clientèle, des données personnelles et du savoir-faire technologique, sécurité des systèmes de production… Or, les TPE/PME sont confrontées, chaque jour, à de nouveaux risques menaçant leur intégrité, leur image et leur compétitivité : vol de données, escroqueries financières, sabotage de sites d'e-commerce.

Pour mieux appréhender les problématiques des petites structures, l'Agence travaille en partenariat avec la CPME (Confédération des Petites et des Moyennes Entreprises) qui apporte son expertise de terrain : ce Guide est le fruit d'une réflexion et d'échanges menés en commun.

La prévention des incidents et attaques informatiques relève souvent de réflexes simples, qui concourent à une protection globale de l'entreprise. Le « Guide des bonnes pratiques de l'informatique » présente douze recommandations à destination des non-spécialistes, issues de l'analyse d'attaques réussies et de leurs causes.

(...)

Extraits du glossaire de l'Agence Nationale de la sécurité des systèmes d'information– Source ANSSI non datée

Cybersécurité

État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des

données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense

Certification de sécurité

Délivrée par l'ANSSI. Elle porte sur des produits de sécurité (matériels ou logiciels). Elle atteste de la conformité d'un produit de sécurité à un niveau de sécurité donné. Il s'agit d'une évaluation à l'état de l'art réalisée en fonction d'une cible de sécurité et d'un niveau de sécurité visé. Elle est matérialisée par un rapport de certification et un certificat tous deux signés par le Directeur Général de l'Agence. Le catalogue des produits de sécurité certifiés, accompagnés de leur cible de sécurité et de leur rapport de certification est publié sur le site Web de l'Agence. On parle de certification « premier niveau » (CSPN) ou de certification « Critères Communs ». Cette certification est délivrée par l'ANSSI sur la base des travaux dévaluation menés par un CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information). Les CESTI sont des laboratoires accrédités par le COFRAC (Comité Français d'Accréditation) et agréés par l'ANSSI. Le catalogue des CESTI est publié sur le site Web de l'Agence. Au sein de l'ANSSI, c'est le Centre National de Certification de la Sous-direction Expertise qui remplit ces missions.

Homologation de sécurité

L'homologation est délivrée par une autorité d'homologation pour un système d'information avant sa mise en service opérationnel. L'homologation permet d'identifier, d'atteindre puis de maintenir un niveau de risque de sécurité acceptable pour le système d'information considéré. Elle est imposée pour les systèmes d'information traitant des informations classifiées (IGI 1300) ou pour les télé-services dans le cadre du Référentiel Général de Sécurité (RGS). Dans le cadre des systèmes traitant des informations classifiées (IGI 1300), la décision d'homologation doit être communiquée à l'ANSSI. Dans le cadre des télé-services (RGS), la décision d'homologation doit être communiquée aux utilisateurs des télé-services. L'ANSSI peut, dans certains cas, être autorité d'homologation ou participer aux commissions d'homologation. La liste des homologations délivrées par l'ANSSI ou auxquelles elle a participé n'est pas publiée.

Opérateur d'importance vitale

L'article R. 1332-1 du code de la défense précise que les opérateurs d'importance vitale sont désignés parmi les opérateurs publics ou privés mentionnés à l'article L. 1332-1 du même code, ou parmi les gestionnaires d'établissements mentionnés à l'article L. 1332-2. Un opérateur d'importance vitale : exerce des activités mentionnées à l'article R. 1332-2 et comprises dans un secteur d'activités d'importance vitale ; gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population.

Plus de 7 entreprises sur 10 ont subi au moins une tentative de fraude en 2019

Source : Site www.forbes.fr – Maurice Midena – 13 mai 2020

Le risque de fraude et de cybercriminalité ne faiblit pas pour les entreprises. Les fraudeurs multiplient les attaques sur une même cible pour augmenter leurs chances de réussite : près d'une entreprise sur 3 a subi plus de 5 tentatives de fraude en 2019 (1/4 en 2018). L'usurpation d'identité reste la technique privilégiée par les fraudeurs, suivie par la cyberfraude et la fraude interne selon le baromètre annuel d'Euler Hermès.

Le télétravail a exacerbé la vulnérabilité des entreprises en matière de cybersécurité. Et pour cause : le risque n'a jamais été aussi élevé, et loin de leur lieu de travail, jamais les collaborateurs n'ont été plus exposés. En 2019, plus de 7 entreprises sur 10 ont subi au moins une tentative de fraude. Si ce chiffre est stable par rapport à 2018, on remarque une multiplication des attaques de la part des fraudeurs sur une même cible pour augmenter leurs chances de réussite : près d'une entreprise sur 3 a subi plus de 5 tentatives de fraude en 2019 (1/4 en 2018), selon le baromètre annuel d'Euler Hermès. Pour la 6ème année consécutive, le leader européen de l'assurance fraude, et l'Association nationale des Directeurs Financiers et de Contrôle de Gestion (DFCG), ont interrogé plus de 200 entreprises implantées en France sur leur exposition, leur ressenti et leurs mesures de prévention face aux risques de fraude et cybercriminalité. Décryptage des résultats de ce baromètre annuel.

Le risque de fraude et de cybercriminalité reste toujours aussi intense

En 2019, plus de 7 entreprises sur 10 ont été victimes d'au moins une tentative de fraude. Un chiffre similaire à celui constaté en 2018 et en 2017, preuve de la résilience des fraudeurs. Ces derniers maintiennent une pression intense sur les entreprises françaises. Plus inquiétant encore, la récurrence de ces attaques sur une même cible. En effet, en 2019, 29 % des répondants à l'enquête Euler Hermès – DFCG ont été visés par plus de 5 tentatives (24 % en 2018). Les fraudeurs n'hésitent pas à revenir à la charge constamment, jusqu'à ce que le système de défense de leur cible cède. Malheureusement, cette persévérance porte ses fruits : 27 % des entreprises interrogées ont subi au moins une fraude avérée en 2019, soit une légère progression (26 % en 2018). Comment expliquer cette efficacité croissante ? Le moment de l'attaque est un premier élément : 43 % des entreprises ont remarqué une recrudescence des attaques en période de congés, week-end ou veille de week-end (35 % en 2018). Les fraudeurs concentrent leurs efforts sur les périodes où les entreprises sont les moins armées pour se protéger (moins de personnel, moins d'attention, etc).

Mais subir une fraude, combien cela coûte-t-il concrètement ? La facture se révèle généralement assez salée : pour près d'une entreprise sur 3, le préjudice subi est supérieur à 10 K€ (comme en 2018). De quoi fragiliser fortement la trésorerie des entreprises et dans certains cas compromettre leur activité, plus encore dans le contexte actuel où les chaînes d'approvisionnement sont perturbées et la demande à l'arrêt.

L'usurpation d'identité reste la technique préférée des pirates devant les outils cyber

L'usurpation d'identité est la technique plébiscitée par les fraudeurs, citée 4 fois parmi le top 5 du baromètre Euler Hermes – DFCG. La fraude au faux fournisseur est toujours la plus utilisée par les pirates, citée par 48 % des répondants. Elle est suivie par la fraude au faux président, qui a sensiblement progressé (38 %), les autres usurpations d'identité (banques, avocats, commissaires au compte – 31 %) et la fraude au faux client (24 %).

« L'usurpation d'identité est un grand classique de la fraude, et elle est de loin la technique favorite

des fraudeurs. Son usage a toutefois évolué : là où auparavant le mail était le facteur déclencheur, de nouvelles techniques plus pointues sont apparues et permettent aux fraudeurs de gagner en efficacité. On peut notamment penser à l'intelligence artificielle et aux logiciels d'imitation de voix grâce auxquels les fraudeurs ont plus de crédibilité dans leurs tentatives, et qui permettent de constituer des scénarios d'usurpation d'identité extrêmement convaincants », explique Armelle Raillard, experte assurance- fraude chez Euler Hermes France.

Par ailleurs, l'intrusion dans les systèmes d'information (29 %) apparaît également dans le top 5. Elle est utilisée à la fois en tant qu'attaque directe, avec les rançongiciels (cités par 15 % répondants), mais aussi comme un moyen de préparer une fraude. Enfin, la fraude interne a été plus utilisée en 2019 qu'en 2018, citée par 14 % des répondants (12 % en 2018).

Les entreprises ont de plus en plus peur de subir une fraude ou une cyberfraude

Les entreprises semblent de plus en plus conscientes de la menace qui plane. En effet, 84 % des répondants craignent une accentuation du phénomène sur l'année à venir (+ 6 points par rapport à notre dernière enquête).

Christian Laveau, président du Groupe de Travail Cyberfraude de la DFCG, indique : « Les entreprises et leurs directions financières doivent veiller à la robustesse de leurs dispositifs de contrôle interne et de lutte contre la cyberfraude. Le risque est que la crise que nous traversons conduise à une moindre vigilance ou à la « dégradation temporaire » des dispositifs de contrôle en raison de la priorité, légitime, donnée à la continuité d'exploitation. Les cyberfraudeurs peuvent en profiter pour exploiter toute faille du dispositif de prévention et de contrôle et accentuer leurs attaques. »

Des mesures concrètes de défense ont été prises, mais sont-elles suffisantes ?

La prise de conscience des entreprises est rassurante, d'autant qu'elle semble aller plus loin que la simple crainte. En effet, 60 % des entreprises interrogées ont mis en place une cartographie des risques. Mieux encore : 93 % d'entre elles ont identifié sur cette cartographie le risque de fraude, et 78 % ont répertorié le risque de cybercriminalité. La preuve que ces menaces sont bien considérées comme un fléau par les entreprises. Certaines entreprises ont, de ce fait, décidé de créer ou transférer un budget dédié à la lutte contre la fraude. Elles sont près de 40 % selon l'enquête Euler Hermes – DFCG.

Philippe Guillaumie, président du Comité Scientifique de la DFCG précise : « La mise en place du télétravail à grande échelle dans le cadre de la crise sanitaire a ouvert de nouvelles brèches du fait du développement des solutions numériques et illustre de nouveau la grande vulnérabilité des entreprises à la cyberfraude. Dans ce contexte, les dispositifs de contrôle interne doivent être maintenus ou renforcés, y compris dans ces circonstances exceptionnelles vis-à-vis du risque accentué de fraude interne, mais un investissement significatif doit être aussi consenti pour tester régulièrement la résistance des Systèmes d'Information face à la cyberfraude et identifier/réparer les failles possibles. Le recours à l'assurance est également un dispositif de protection efficace, mais il ne dispense pas d'une politique de prévention. »

Autre motif d'optimisme, 60 % des entreprises disposent désormais d'un plan d'urgence à activer en cas d'attaque, alors qu'elles n'étaient que 50 % lors de la précédente édition de notre baromètre. Une amélioration notable, qui prouve que la lutte contre la fraude est un sujet pris en compte par les entreprises. Mais l'est-il assez ?

« Il y a du mieux, et les entreprises s'en félicitent : elles sont 74 % à juger leur dispositif défense satisfaisant, contre 69 % l'an passé. Mais il y a encore du chemin à parcourir pour que les systèmes

de défenses soient optimisés : plus de 6 répondants sur 10 n'ont toujours pas alloué de budget spécifique à la lutte contre fraude et la cybercriminalité pour cette année. Nous sommes sur la bonne voie, mais les entreprises doivent aller plus loin dans leur démarche pour se mettre à l'abri des attaques. Des dispositifs comme l'assurance-fraude existent, et permettent aux entreprises de transférer ce risque majeur sur une tierce partie pour ne pas avoir à l'assumer entièrement », conclut Armelle Raillard.

Tournez la page S.V.P.

Demain : les enjeux de la cybersécurité pour les PME et ETI – Extrait
Source : Site www.bpifrance.fr – 01 juillet 2019

Les PME (Petites et Moyennes Entreprises) et ETI (Entreprises de Taille Intermédiaire) sont devenues les cibles privilégiées de la cybercriminalité de « masse ». Pourtant leurs dirigeants n'en font pas encore une priorité. Pourquoi un tel paradoxe ? Comment y remédier ?

« *En matière de cybersécurité, la question pour un chef d'entreprise n'est pas de savoir s'il va être attaqué, mais quand* ». C'est en tout cas ce qu'affirment Vivien Pertusot, directeur adjoint de Bpifrance Le Lab, et Francois Picarle, directeur investissement, Bpifrance. Selon une étude PWC, en 2017, près de 75 % des ETI déclaraient au moins un incident cyber. **Il est donc temps pour les dirigeants de PME-ETI de s'emparer du sujet.**

Tous concernés par la cybersécurité

À l'ère de la révolution digitale, le risque cyber est un **défi majeur pour toutes les entreprises**. « *Généralement peu protégées* », les PME-ETI sont des cibles faciles pour les cybercriminels. « *Elles sont peu nombreuses à avoir une politique de confidentialité, d'accès à la donnée, etc. Et elles sensibilisent peu leurs collaborateurs à la cybersécurité* » explique Vivien Pertusot. Alors face à des réseaux mafieux toujours plus organisés et des tutoriels d'attaques accessibles à tous, elles sont extrêmement vulnérables.

De plus, la **filière de la cyber est inadaptée aux besoins des PME/ETI**. Les offres existantes sont souvent trop chères ou trop spécifiques. C'est pourquoi, selon François Picarle « *les chefs d'entreprise doivent mener eux-mêmes et avec leurs équipes, leur propre analyse de risque. Et donc bien comprendre où sont les richesses, les actifs sensibles de l'entreprise qui pourraient être attaqués ou mis à mal par des cyberattaques* ».

Si les dirigeants sont souvent conscients de ce risque, ils sont peu décidés à agir. Or, les solutions les plus efficaces sont à portée de tous. « *La première, et peut-être la plus fondamentale, c'est la formation. Les collaborateurs sont les premières sources de vulnérabilité dans une entreprise* » explique le directeur adjoint de Bpifrance Le Lab.

Toujours selon notre expert, la 2e solution est « *pour le dirigeant d'entreprise d'avoir une politique de données. Donc de savoir ce qui peut être protégé, ce qui doit être protégé et ce qui peut, dans certains cas de figure, se retrouver volé par un cybercriminel.* »

(...)

Les gestes barrières numériques, meilleurs remparts face à l'explosion de la cybercriminalité
Source : Site www.usinenouvelle.com – Hassan Meddah – 05 mai 2020

Sauvegarde de leurs données, mise à jour des correctifs de sécurité, durcissement des mots de passe… Les entreprises sont incitées à respecter les gestes élémentaires de cybersécurité pour se prémunir des rançongiciels et protéger leurs données.

Les pirates ne sont pas au chômage partiel. Le groupe français Tarkett, spécialiste de revêtement de sols avec un chiffre d'affaires de 3 milliards d'euros, l'a appris à ses dépens. Par un communiqué de presse diffusé le 4 mai 2020, il a révélé être victime d'une cyberattaque. « *Les suspicions de la cyberattaque remontent au 29 avril. Des systèmes informatiques ont été éteints par mesure préventive »*, explique à l'Usine Nouvelle un porte-parole pour le groupe.

Si Tarkett reconnaît que les activités commerciales et de production sont perturbées depuis, il communique peu de détails sur l'ampleur des dégâts et les sites touchés parmi ses 33 usines réparties dans le monde entier. On suppose tout de même que l'attaque doit être sévère puisque la victime a avisé son assureur en cybersécurité et sollicité des experts informatiques et d'investigation « *mondialement reconnus »* pour permettre un retour à la normale des opérations le plus rapidement possible.

En pleine recrudescence des cyberattaques dues aux usages numériques en période de confinement (recours massif au télétravail, utilisation des solutions de réunion virtuelle…), Tarkett est-il aussi une victime indirecte du Covid-19 ? Le groupe ne dit rien sur l'origine de l'attaque malveillante.

USURPER L'IDENTITÉ D'UN FOURNISSEUR

Y a-t-il des entreprises spécifiquement visées, des secteurs plus ciblés en cette période pandémie ? Clairement, le secteur hospitalier reste une cible privilégiée. À la crise sanitaire, certains acteurs malveillants veulent ajouter une crise cyber. « *Depuis le début de la crise sanitaire, des attaques par déni de service ont eu lieu contre l'AP-HP (Paris) le 22 mars dernier et contre l'AP-HM (Marseille) et une attaque par rançongiciel contre l'établissement public de santé de Lomagne (Gers) »*, ont rappelé les sénateurs lors de publication d'une étude publiée mi-avril intitulée « Désinformation, cyberattaque et cybermalveillance : l'autre guerre du Covid-19 ». Ils jugent que les systèmes d'information des acteurs de la santé sont vulnérables, rappelant que l'ANSSI (Agence nationale pour la sécurité des systèmes d'information) avait dénombré 18 attaques par rançongiciels en 2019.

Mais aucun acteur économique n'est à l'abri. Le 20 avril dernier, le MEDEF (Le Mouvement des entreprises de France) a sensibilisé ses 173 000 entreprises adhérentes aux cyberattaques possibles. « *L'accroissement de l'usage du télétravail et de la dématérialisation des procédures qui en découlent, associé aux difficultés économiques inhérentes à la situation de crise du Covid-19 présentent un risque accru d'escroqueries à la fausse commande ou aux modifications de coordonnées de virement bancaire (FOVI/BEC) en usurpant l'identité d'un employé pour récupérer son salaire ou d'un fournisseur pour régler les factures ou encore émanant d'un dirigeant sous le sceau du secret »*.

L'ANSSI relativise toutefois la recrudescence des cyberattaques ou plutôt précise leur nature. Chargée de cyber-défendre en priorité les services de l'État et les acteurs stratégiques du pays, elle estime qu'il n'y a pas plus de cyberattaques majeures qu'auparavant sur ce type de cibles. Cela n'a même rien à voir avec les dégâts réalisés par un virus comme NotPetya en 2017 à l'origine d'une cyberattaque mondiale. Selon l'agence de cybersécurité, « *ce qui explose c'est la*

cybercriminalité », à base d'attaques moins sophistiquées mais qui peuvent tout de même causer des dégâts auprès des entreprises mal préparées, mal protégées.

DES ATTAQUES MOINS REPÉRABLES

Le développement du télétravail généralisé et des connexions à distance facilite le travail des pirates. « *Avec le télétravail, les attaquants n'attaquent pas forcément plus. Ils changent surtout leur mode opératoire. Ils ciblent les bonnes personnes dans les organisations par mail, par phishing (hameçonnage, ndlr) et autre arnaque de plus haut niveau »*, estime Loïc Guézo, expert en cybersécurité et secrétaire général du Clusif, le club de la sécurité de l'information français.

Les pirates profitent également du développement du cloud. « *Ils peuvent par exemple se créer un compte chez Microsoft juste en achetant une licence Office 365. Disposant alors d'une adresse mail standard de type Microsoft, ils peuvent lancer des attaques moins repérables qu'auparavant. Malheureusement Microsoft et Google peinent à empêcher des attaques à partir de comptes hébergés dans leur Cloud vers d'autres comptes d'entreprises hébergés chez eux »*, détaille Loïc Guézo.

Face à un virus cyber comme face à un virus de type Covid-19, il faut adopter des gestes barrières… numériques. À travers une communication massive, le MEDEF ne manque de rappeler les conseils élémentaires à ses adhérents : sauvegarde des données avec une copie déconnectée, applications des mises à jour de sécurité sur les équipements connectés dès qu'elles sont disponibles, utilisation de mots de passe solides et robustes… L'organisation patronale a aussi organisé le 9 avril dernier un Webinaire avec le service de cybersécurité de la gendarmerie et la société Wavestone, entreprise spécialisée en cybersécurité. *« Environ 170 entreprises y ont participé. Beaucoup d'interrogations ont tourné autour des outils d'échange et de partage qui n'avaient peu ou pas été utilisés jusqu'à présent. Les entreprises voulaient savoir quelles plates-formes elles pouvaient utiliser et comment… Cela démontre qu'elles sont particulièrement sensibles à la protection de leurs données »* explique-t-on au MEDEF. La crise aura eu au moins cette vertu.

Cybersécurité : risques et enjeux économiques – Extraits du Rapport moral sur l'argent dans le monde
Source : Site de l'Association d'Économie Financière – Nicolas Arpagian – 2015-2016

(…)

UNE EXPOSITION CROISSANTE AU RISQUE NUMÉRIQUE

La numérisation de nos existences est en marche. Qu'il s'agisse de nos vies personnelles où les smartphones sont devenus nos béquilles mentales, à qui nous confions les coordonnées de nos relations, les multiples mots de passe de nos réseaux sociaux et comptes bancaires ainsi que les photos et les messages qui jalonnent notre quotidien. Avec une situation paradoxale : ces téléphones intelligents rassemblent de plus en plus de données personnelles, voire intimes, mais leur sécurisation laisse encore largement à désirer. Alors que les antivirus et autres pare-feu équipent désormais les ordinateurs même domestiques, ces smartphones sont largement utilisés sans protection particulière. On demande donc à l'utilisateur/trice quels que soient son âge, sa formation ou son intérêt pour le sujet de prendre en charge la sécurisation de son équipement et de sa connexion. Chaque titulaire d'un accès à Internet a ainsi une « obligation de surveillance » dudit accès (article L-336-3 du Code de la propriété intellectuelle). Et l'article L-335-7-1 du Code de la propriété intellectuelle prévoit qu'un titulaire d'un abonnement à Internet peut voir sa responsabilité pénale engagée au titre de la contravention de négligence caractérisée. Cette exigence de sécurisation rompt avec la règle ancienne qui voulait que les services de l'État, qu'il s'agisse de l'autorisation de circuler d'un véhicule ou de la mise sur le marché d'un médicament, évaluent seuls les aspects de sécurité. Ne mettant à la disposition des consommateurs que des biens ou des services dont la dangerosité à l'usage avait été évaluée et encadrée. Dans le domaine du numérique, le consommateur final se trouve chargé de cette tâche. Quitte à voir par la suite sa responsabilité juridique et financière mise en cause.

Le canal numérique devient le moyen naturel de commercer, de se renseigner, de consommer et parfois de convoler. Autant d'occasions démultipliées de susciter la créativité des pirates. Tout ce que les délinquants et les criminels faisaient de mal dans le monde physique depuis des lustres trouve des déclinaisons par voie informatique : usurpation d'identité, détournement de fonds, chantage/extorsion, vol d'informations, vol de ressources, escroquerie, etc. La capacité de démarcher rapidement un grand nombre de futures victimes et le fait de pouvoir rapatrier sans délai et à coût réduit le fruit de son vol, le tout dans une relative impunité judiciaire, expliquent l'essor de la cybercriminalité. Celle-ci est encore recensée de manière très partielle par les services officiels, comme l'Observatoire national de la délinquance et des réponses pénales (ONDRP).

Soucieuses de leur productivité, les entreprises incitent leurs collaborateurs à travailler lors de leurs déplacements et, le cas échéant, à leur domicile. Cette mobilité démultiplie les modes de connexion au système d'information central. Wifi publics, recours à des ordinateurs en libre-service ou à des équipements personnels pour se brancher sur l'informatique de la société… On est loin de la gestion d'un parc de machines entièrement maîtrisé par une Direction des systèmes d'information omnisciente. Le phénomène touche les entreprises de toutes tailles et de tous secteurs, et gagne de plus en plus les administrations.

Si des solutions techniques protègent l'accès aux systèmes d'information et assurent une réelle confidentialité des échanges, les pirates optent désormais pour une tactique plus sournoise. En effet, faute de pouvoir/savoir casser la serrure, ils se renseignent pour savoir où vous cachez vos clés. C'est toute l'utilité de l'ingénierie sociale : l'élaboration d'un scénario fondé sur une approche très personnalisée de celui/celle qui détient l'information ciblée. Une consultation assidue des réseaux sociaux fournit à peu de frais tous les éléments de contexte permettant d'aborder de manière crédible un cadre dirigeant. En ayant identifié ses *hobbies*, ses expériences professionnelles passées ainsi que ses relations en affaires, le pirate dispose d'une matière éditoriale complète et à jour pour

finaliser un discours d'approche très efficace. La cible croira à une sollicitation fortuite tandis qu'il s'agira d'un moyen d'entrer dans son cercle de connaissances. Une telle cartographie permet si besoin de préparer une rencontre dans la vie bien réelle. Le piratage en 2012 de l'intranet de la présidence de la République française a débuté par un message opportunément envoyé sur Facebook à un collaborateur du chef de l'État. En cliquant sur un lien contenu dans ledit message, il a infecté l'ordinateur qui lui servait à accéder à son compte de messagerie professionnelle. Ce travail préalable de *social engineering* a donc été pertinent pour mener à bien cette mission d'espionnage.

La généralisation de la numérisation de nos activités (dossiers de santé, impôts, comptes bancaires, correspondances professionnelles et personnelles, réseaux sociaux, smartphones géolocalisés, objets connectés, etc.) ouvre autant de brèches possibles pour atteindre le but poursuivi : vol d'identités, d'argent ou d'informations confidentielles. Sans oublier des opérations spécifiquement numériques comme le déni de service (paralysie d'un site internet sous le coup d'un très grand nombre de connexions frauduleuses simultanées) ou le chantage au chiffrement (les données chiffrées par les pirates sont rendues de nouveau accessibles en échange d'une rançon). De telles pratiques peuvent atteindre indifféremment des personnes ou des institutions soigneusement identifiées au préalable comme n'importe quelle entité dès lors qu'elle est connectée au réseau. Ce qui fait de tout utilisateur du Net une victime potentielle d'une cyberattaque.

(...)

QUAND LES ENTREPRISES DE RENOM OPTENT POUR L'ARME NUMÉRIQUE

La concurrence économique porte largement sur la capacité de l'un des compétiteurs à acquérir de l'information avant les autres. Cette aptitude à connaître ce que prévoit le rival, à identifier ses spécificités cachées et à réduire ainsi la part d'incertitude intéresse tous les dirigeants d'entreprise. Surtout si on les persuade qu'ils pourront acquérir cette information stratégique à un coût raisonnable, dans un délai rapide et sans risque réel d'être identifiés. C'est la raison pour laquelle il ne faut pas considérer les cyberattaques ou les recours offensifs aux technologies de l'information dans le monde de l'entreprise comme relevant des seules organisations mafieuses. On constate au contraire que de très grandes sociétés, en principe honorablement connues et signataires de nombre de chartes humanistes (pour le respect des droits des enfants, de la parité homme/femme, du recyclage des déchets et autres promesses de contribuer à un monde meilleur), sont prêtes à financer des campagnes d'attaques sur la Toile.

Qu'il s'agisse de voler de l'information ou d'organiser une campagne de dénigrement contre un concurrent. En octobre 2013, Samsung, le n° 1 mondial des téléphones portables, a été condamné par un tribunal de Taïwan pour avoir payé des blogueurs et des étudiants afin de dénigrer les produits de son concurrent HTC. En juin 2014, Microsoft a été pris la main dans le sac à rémunérer des blogueurs influents pour publier des articles favorables à la nouvelle version de son navigateur Internet Explorer.

En septembre 2013, dans une enquête publiée en deux volets dans le *Journal du Net*, j'ai expliqué comment une dizaine de grandes entreprises ou associations professionnelles avaient bénéficié de la publication de textes en leur faveur dans les colonnes de grands médias français : *Les Échos*, *L'Obs*, *Mediapart*, *Le Figaro*, le *Journal du Net*, etc. En usurpant des identités, en volant les photos de vraies personnes, en invoquant des noms d'employeurs prestigieux, de faux analystes ou experts ont pris la plume pour vanter les mérites ou critiquer vertement des sociétés commerciales ou des personnalités. Misant sur le crédit des supports de presse utilisés pour donner de la consistance et du poids à leurs prises de positions, tant vis-à-vis des internautes que des moteurs de recherche. Pour que ces articles soient le mieux référencés possibles et donc participent à la mise en avant de leurs intérêts. Et quelquefois, ce procédé est utilisé pour des opérations financières. Ainsi, le 5 janvier 2015, j'ai démontré dans le *Journal du Net* comment l'offre publique d'achat (OPA) sur la société Club Méditerranée d'un montant de 1 MdA comportait un volet d'influence visant à dévaloriser l'un des deux candidats au rachat, l'italien Bonomi. En totale violation du Règlement général de

l'Autorité des marchés financiers (AMF) et du Code pénal, des articles publiés dans les pages de *Mediapart*, du quotidien *Les Échos* ou du *Journal du Net* tentaient de saper l'image de l'investisseur italien afin de décrédibiliser son offre. L'investigation technique a permis de remonter jusqu'à un cabinet de conseil. Les explications et les détails fournis par des personnes travaillant ou ayant travaillé au sein de cette officine ont complété la description de leur mode opératoire. C'est l'objet d'une enquête détaillée publiée le 12 janvier 2015 dans le *Journal du Net* où l'on apprend que ces professionnels ne se contentent pas d'alimenter les médias en articles sans aucune fiabilité, mais qu'ils sont également des contributeurs très actifs de l'encyclopédie en ligne Wikipédia. Ce qui leur a permis d'accéder à un statut élevé dans la hiérarchie des rédacteurs/correcteurs de ce site très fréquenté. Ils monnaient à leurs clients leur aptitude à embellir les notices les concernant, voire à biaiser celles de leurs concurrents. Un réel pouvoir d'influence alors que nombre d'internautes considèrent Wikipédia comme leur première source d'information.

(...)

Tournez la page S.V.P.

La cybersécurité : quelles réponses aux menaces nouvelles ? – Extrait

Source : Site www.vie-publique.fr – 28 janvier 2019

(...)

Quelles réponses contre la cybermenace ?

La surveillance d'Internet

Pour surveiller les cybercommunications et lutter contre la cybercriminalité, les États se sont dotés de dispositifs de surveillance dédiés à Internet. Des organes inter-étatiques de surveillance existent, comme le réseau Échelon. Géré conjointement par les États-Unis, le Canada, l'Australie, le Royaume-Uni et la Nouvelle-Zélande, Échelon est le plus gros réseau de surveillance des télécommunications et cybercommunications au monde. Toutefois, de tels outils sont à double tranchant puisqu'ils peuvent servir à des fins d'espionnage (économique, militaire) ou de contrôle des populations.

La collaboration avec les géants du Net

Pour exercer leur autorité sur le cyberespace, les États doivent compter sur la coopération des géants du Net. En plus d'avoir des moyens techniques et financiers supérieurs à de nombreux États, ces derniers ont le pouvoir de dissimuler ou au contraire de rendre publiques les informations qui circulent via leurs services.

Une difficile réponse internationale

Face au caractère international de la cybermenace, les États ont tôt pressenti la nécessité d'une réponse internationale commune. Mais celle-ci se heurte à la lenteur des procédures de coopération nationale, ainsi qu'à la réticence des États à partager certaines informations. Les carences de la coopération internationale en matière de cybersécurité sont ainsi apparues au grand jour à l'occasion des attentats terroristes qui ont frappé l'Europe ces dernières années. En réponse à ces attaques, les différents gouvernements se sont engagés à plus de coopération.

Vers un droit international de la cybersécurité ?

Malgré les appels répétés de nombreux responsables politiques, il n'existe toujours pas de droit international contraignant en matière de cybersécurité. En effet, il existe des divergences de fond quant à la manière dont les États envisagent leur cybersécurité.

L'exception européenne

En 2001, le Conseil de l'Europe est à l'origine du premier traité de coopération internationale sur la cybersécurité. Connu sous le nom de Convention de Budapest, ce traité a été signé par les 45 États membres du Conseil de l'Europe, même si tous ne l'ont pas ratifié par la suite.

Au sein d'Europol, l'Union européenne (UE) a inauguré, en 2013, le Centre européen de lutte contre la cybercriminalité, visant à faciliter la coopération entre États européens dans la lutte contre le cybercrime.

La Commission européenne a proposé, en septembre 2017, le « paquet cybersécurité » qui comprend un ensemble de mesures dont l'introduction d'une certification de cybersécurité à

l'échelle de l'UE et la consolidation de l'Agence permanente de l'UE pour la citoyenneté.

Le cas français

La France fait de la cybersécurité sa priorité depuis les années 2000. Le retour de la menace terroriste en 2015 l'a poussée à intensifier ses efforts en la matière. La Stratégie nationale pour la sécurité du numérique a fixé cinq objectifs :

- garantir la souveraineté nationale ;
- répondre aux actes de cybermalveillance ;
- informer le grand public ;
- faire de la sécurité numérique un avantage concurrentiel pour les entreprises ;
- renforcer la voix de la France à l'international.

La surveillance d'Internet

La lutte contre la cybercriminalité passe d'abord par la surveillance d'Internet. Le décret n°2015-125 permet le blocage administratif des sites pédopornographiques et faisant l'apologie du terrorisme. En 2015 est votée la loi « Renseignement », qui renforce les moyens d'action des services de renseignement dans la sphère numérique. À la suite des attentats de Paris en 2015, le gouvernement a également lancé l'opération « Stop Djihadisme » afin de contrecarrer les campagnes de propagande jihadiste sur les réseaux sociaux.

La cybersécurité dans le droit français

En France, la cybercriminalité est prise en compte dans le droit depuis la loi informatique et libertés (1978) qui réglemente la liberté de ficher les personnes humaines. Aujourd'hui, les pratiques numériques sont encadrées par un 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 cyberattaques visant directement l'État.

Traquer les cybercriminels

La police et la gendarmerie disposent de divers organes dédiés à la répression de la cybercriminalité. Parmi eux :

- l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) au sein de la Police judiciaire ;
- le Centre de lutte contre les criminalités numériques (C3N) au sein de la Gendarmerie nationale ;
- la Brigade d'enquête sur les fraudes liées aux technologies de l'information (BEFTI) au sein de la préfecture de police de Paris.

Défendre les usagers

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée en 2009 pour défendre et protéger les systèmes d'information et les usagers du numérique contre les cyberattaques. Ses missions sont les suivantes :

- surveiller les réseaux afin de détecter les attaques et permettre de réagir au plus vite ;

Tournez la page S.V.P.

- développer des produits et services de cybersécurité à destination des usagers ;
- apporter son expertise et son assistance aux administrations et aux entreprises ;
- sensibiliser le public sur les cybermenaces.

Le gouvernement a lancé en 2017 un dispositif national d'assistance aux victimes d'actes de cybermalveillance. 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 cyberattaques – particuliers, entreprises ou collectivités territoriales – et des prestataires de services susceptibles de les aider dans leurs démarches.

La cyberdéfense

Créé en 2017 et dépendant du ministère des armées, le Commandement de la cyberdéfense (COMCYBER) a la responsabilité de la cyberdéfense militaire qui recouvre l'ensemble des actions défensives et offensives conduites dans le cyberespace. Le COMCYBER est constitué de 3 400 cybercombattants, auxquels viendront s'ajouter 1 000 combattants supplémentaires d'ici 2025.

Le 18 janvier 2018, la ministre des armées a présenté la doctrine de lutte informatique offensive (LIO) qui complète la lutte informatique défensive (LID). La ministre a ainsi officialisé le volet offensif de la doctrine cybermilitaire française. La LIO et la LID renforcent la posture permanente de cyberdéfense (PPC) créée par la loi de programmation militaire 2019-2025. La PCC permet de protéger en permanence tous les réseaux militaires et de réagir à toute attaque contre les intérêts de la défense de la France.

Livre blanc de la cyberdéfense, la Revue stratégique de cyberdéfense a été publiée en février 2018 par le Secrétariat général de la défense nationale (SGDN).

Cyberdéfense : la France se dote d'une nouvelle doctrine militaire
Source : Site Europe 1 – 18 janvier 2019

La ministre des Armées, Florence Parly, lève le voile vendredi sur la mise en place d'une stratégie militaire propre au cyberespace, et qui doit notamment venir appuyer les forces sur le terrain.

Jean-Yves Le Drian l'avait déjà esquissée en 2015. Quatre ans plus tard, Florence Parly franchit une nouvelle étape. Vendredi, la France se dote officiellement d'une doctrine militaire cyberoffensive. L'État français entend désormais, en complément des armes conventionnelles et en appui des opérations militaires, utiliser un arsenal d'attaques cyber et de ripostes graduées dans un espace de confrontation dématérialisé.

Appuyer les forces sur le terrain. Après l'Armée de Terre, la Marine et l'aviation, la « lutte informatique offensive » (LIO) forme une quatrième force armée. Elle investit totalement ce qui est devenu un champ de bataille à part entière, en préparation et en appui, par exemple, d'opérations militaires. La France ne s'interdit plus de riposter, en attaquant via le cyberespace pour répondre à une agression armée, pour isoler un poste de commandement ennemi, pour mettre la pagaille dans la propagande hostile, ou bien encore pour saboter les communications sur le terrain, par exemple, entre un char et un avion adverses.

Différents types d'attaque. Le détail de cette stratégie doit être précisé par la ministre des Armées vendredi, en fin de matinée, à l'occasion d'une visite à Balard du centre des opérations du commandement de la cyberdéfense. Il s'agit d'acter de manière officielle la mise en place de toute une palette d'attaques cyber, graduées, discrètes ou non, et plus ou moins réversibles, avec l'idée toutefois de rester dans les clous du droit de la guerre.

4 400 « cybercombattants ». Les différentes missions relatives à la cyberdéfense seront menées par des spécialistes qui devront être formés dès les écoles militaires. La Défense française entend ainsi recruter 1 000 nouveaux postes d'ici 2025, date à laquelle elle devrait compter 4 400 « cybercombattants ». Le budget, lui, reste le même : 1,6 milliard d'euros pour la période 2019-2025.

Tournez la page S.V.P.

Rapport d'information déposé par la Commission des Affaires Européennes sur l'avenir de la cybersécurité européenne – Extrait

Source : Site de l'Assemblée nationale – Eric Bothorel – 14 novembre 2019

(...)

II. L'ENISA, UNE AGENCE EUROPÉENNE RENFORCÉE AU SERVICE D'UNE CYBERSÉCURITÉ PLUS INTÉGRÉE

A. LE PAYSAGE TRÈS ÉCLATÉ DE LA CYBERSÉCURITÉ EUROPÉENNE

De nombreux pays membres de la Convention de Budapest qui l'ont signée dès 2001 appartiennent à l'Union européenne, mais les initiatives au sein de celle-ci sont longtemps restées rares, ou cantonnées au niveau national. Néanmoins, au cours des années 2000 commencent à s'agréger des éléments disparates qui conduiront à l'établissement d'une véritable stratégie de cybersécurité européenne à partir de 2013.

1. Premières esquisses stratégiques de l'Union européenne

En 2001, la Commission européenne publiait une communication sur la sécurité des communications et des réseaux appelant à l'élaboration d'une politique européenne commune. Cette communication prenait appui sur les progrès réalisés en matière de sécurité des signatures électroniques avec la directive adoptée le 13 décembre 1999. Cet objectif plusieurs fois affirmé de sécurité des réseaux (on ne parle pas encore de cybersécurité) s'est poursuivi avec la « stratégie pour une société de l'information sûre » de 2006 et le plan d'action et la communication sur la protection des infrastructures d'information critiques de 2009.

Il faut souligner que si les cybermenaces n'entrent pas dans les menaces prioritaires identifiées dans la première stratégie de sécurité de l'Union européenne parue en 2003, le rapport du Secrétaire général et Haut représentant sur la mise en œuvre de cette stratégie, qui date lui de 2008, place le défaut de cybersécurité au nombre des cinq menaces majeures listées.

Ces enjeux commencent donc à faire l'objet d'une certaine doctrine encore disparate et abordant les enjeux par plusieurs angles, économique ou sécuritaire, au sein de l'Union européenne dans le courant des années 2000.

2. Une action de cybersécurité dispersée

a. Sécurité des réseaux et de l'information

i. La création de l'ENISA

La création de l'ENISA (l'Agence européenne chargée de la sécurité des réseaux et de l'information, toujours appelée par l'acronyme anglais de « *European Network and Information Security Agency* ») en 2004, concrétise la montée en puissance de ces problématiques sur la scène européenne. En 2005, l'agence est établie à Héraklion, en Crète, et dispose d'un budget et d'un nombre d'agents assez modestes. À titre d'exemple, pour 2012, elle est dotée de 8,5 millions d'euros et d'une soixantaine d'agents.

Toutefois, les moyens et la durée du mandat de l'ENISA sont d'emblée limités et apparaissent insuffisants au regard de l'étendue des missions qui lui sont dévolues. Plusieurs règlements ont prolongé successivement la durée du mandat de l'ENISA jusqu'au règlement de 2013, le dernier

avant que l'Acte de Cybersécurité n'établisse la permanence de l'Agence et n'en assure la refondation. Avec ces prolongations se sont également progressivement affirmées des missions toujours plus riches pour l'Agence, notamment pour accompagner la stratégie numérique pour l'Europe qui se mettait en place à partir de 2010. Le mandat de son directeur exécutif a également pu être prolongé et ses moyens accrus durant le cadre financier pluriannuel suivant.

ii. La création d'un centre d'intervention d'urgence

Dans la continuité de cette stratégie pour l'agenda numérique et pour la sécurité des réseaux et de l'information, une décision de la Commission européenne du 11 septembre 2012 a instauré une équipe d'intervention d'urgence dans le domaine de la sécurité informatique ayant pour mission de protéger les institutions européennes contre les cyberattaques.

Le CERT-UE compte 30 membres issus de la Commission européenne, du Secrétariat général du Conseil, du Parlement européen, du Comité des régions et du Comité économique et social. Comme les autres CSIRT publics et privés, il a vocation à répondre de manière efficace à des incidents de sécurité informatique et aux cybermenaces, 24 heures sur 24 et 7 jours sur 7. Plus précisément, le CERT-UE doit centraliser les demandes d'assistance émanant des équipes de cybersécurité locales, traiter les alertes et réagir aux attaques informatiques, prévenir les incidents par la diffusion d'informations et de bonnes pratiques, et établir et maintenir à jour une base de données des vulnérabilités. Ses missions recouvrent donc la prévention, la détection, la réponse et la réparation des incidents informatiques.

Au-delà de ces missions traditionnelles qui incombent à tout CSIRT, le CERT-UE vise à construire et compléter les capacités existantes des institutions, organes et agences de l'Union et à encourager l'émergence d'une culture de la confiance au sein de cet environnement protégé.

b. Sécurité intérieure : Centre européen de lutte contre la cybercriminalité

Dans le cadre de la stratégie de sécurité intérieure de l'Union adoptée en 2010, un Centre européen de lutte contre la cybercriminalité (EC3), composante d'Europol, a été créé en 2013 afin d'apporter une réponse institutionnelle à la forte progression de la cybermenace. Sa mission consiste à renforcer la répression de la cybercriminalité dans l'Union, et à protéger les citoyens, les entreprises et les gouvernements. Pour ce faire, EC3 rassemble auprès des pays l'information et l'expertise, soutient les enquêtes pénales menées par les États membres, promeut des solutions et sensibilise aux enjeux de cybersécurité à l'échelle de l'Union.

Votre rapporteur tient à souligner que les représentants de l'ENISA lui ont expliqué le temps qu'avait mis à se développer la coopération pénale à l'échelle européenne sur les sujets de cybersécurité et l'importance des progrès réalisés en ce domaine grâce à des enceintes telles que le groupe de coopération instauré par la directive SRI.

(...)